Memorias del XVI Congreso Latinoamericano de Control Automático, CLCA 2014
Octubre 14-17, 2014. Cancún, Quintana Roo, México

Encriptado caótico en una red determinista de mundo pequeño

Reyes-De la Cruz D. * **Cruz-Hernández C.** *
Posadas-Castillo C. ** **Martínez-Clark R.** *

* *Centro de Investigación Científica y Educación Superior de Ensenada, Carretera Ensenada-Tijuana 3918, Zona Playitas, 22860 Ensenada. (e-mails: jreyes@cicese.edu.mx, ccruz@cicese.mx, rigomar@cicese.edu.mx).*
** *Facultad de Ingeniería Mecánica y Eléctrica Av. Universidad s/n. Ciudad Universitaria San Nicolás de los Garza, Nuevo León, C.P. 66451 (e-mail: cornelio.posadascs@uanl.edu.mx).*

Abstract: En este trabajo, se presenta el encriptamiento caótico de un mensaje a través de redes de mundo pequeño, se utiliza el oscilador de *Colpitts* como señal portadora. Se empleó la teoría de sistemas complejos para sincronizar la red de mundo pequeño de $N = 6$ nodos, se realizó un acoplamiento bidireccional para lograr la sinconización de la red.

Keywords: sistemas complejos, caos, redes de mundo pequeño determinista, comunicaciones seguras.

1. INTRODUCCIÓN

Muchos sistemas en la naturaleza y en la vida real están constituidos con un gran número de unidades dinámicas interconectadas, las cuales, en diversas ocasiones requiren tener un comportamiento colectivo para desarrollar una actividad en común, dicha actividad puede ser el trabajo en equipo, lo que a su vez, puede involucrar coordinación, formación, cooperación, sincronización, etc. Por ejemplo, los sistemas biológicos, sistemas neuronales, sistemas químicos, dentro de su estructura interna, albergan muchos organismos llamados nodos que interactúan entre sí; también se puede observar que estos sistemas en la mayoría de los casos muestran, alta conexión entre nodos vecinos (coeficiente de agrupamiento), otra característica, es la manera en que fluye la información de un nodo a otro, frecuentemente se encuentra una distancia de camino medio relativamente baja, tomando estas características en consideración, las redes de la vida real se pueden representar con modelos de mundo pequeño, ver *Comellas et al.* (2000).

Generalmente, las redes de *mundo pequeño* pueden identificarse por tres propiedades principales. Primera, la distancia de camino promedio no se incrementa logarítmicamente con el tamaño de la red, pero crece o disminuye conforme el número de nodos varía. Segunda, el grado de nodo promedio de la red es pequeño. Tercera, la red tiene un alto coeficiente de agrupamiento.

El primer intento satisfactorio para crear redes con coeficiente de agrupamiento grande y una distancia de camino promedio pequeña fue reportado por *Watts y Strogatz* (1998). Este trabajo fue pionero y a razón de esto, se produjo una avalacha de trabajos de investigación sobre redes en mundo pequeño. Este modelo comienza con una topología de red en vecino cercano y posteriormente basado en una probabilidad $0 < p \leq 1$, de esta manera, se remueve y se agregan conexiones a la red original. Posteriormente se produjo una variante del modelo de *Watts y Strogatz,* propuesto por *Newman y Watts* (1999), en este modelo de mundo pequeño se comienza igual que el modelo propuesto por *Watts y Strogatz*, pero en este caso, se agregan conexiones aleatoriamente entre pares de nodos, pero no se remueven conexiones de la red original. Los modelos de redes anteriormente mencionados son aleatorios. Lo que significa, que nuevos nodos se conectan a los nodos ya presentes en la red.

En el año 2000, utilizando la teoría de grafos *Comellas et al.* (2000) presentaron una red de comunicación utilizando un modelo determinista de mundo pequeño. Dos años después *Comellas y Samples* (2002) presentaron otras dos técnicas deterministas para crear redes de mundo pequeño con una distribución de grado constante y variable, respectivamente.

Como se mencionó existen modelos de mundo pequeño estocásticos, todos ellos son probablemente, ilustraciones razonables de cómo se forman algunas redes de la vida real. Sin embargo, con el fin de estar en consonancia con las características de la vida real, muchos de ellos son generados por la estocasticidad que hace que sea más difícil obtener una comprensión visual de cómo se forman las redes y cómo los diferentes nodos se relacionan entre sí. Por otra parte, muchos de ellos son de tamaño fijo (es decir, el tamaño de la red es fija), lo que no está de acuerdo con la propiedad de crecimiento de muchos sistemas de la vida real. Las redes deterministas proveen la posibilidad de calcular analíticamente sus propiedades, y

⋆ Al CONACYT por el apoyo económico brindado a través del proyecto de Grupos de investigación en Ciencia Básica, Ref. 166654.

los resultados pueden indirectamente verificar la exactitud de los modelos y métodos estocásticos.

En este trabajo, se utiliza un algoritmo para generar redes de mundo pequeño construidas de manera determinista, propuesto por *Zhang et al.* (2006). El algoritmo consiste en una técnica de construcción simple, que generará redes de mundo pequeño de manera determinista, que consiste en agregar conexiones y nodos conforme se incrementa el número de iteraciones, ver *Martínez et al.* (2013). El contenido de este trabajo está organizado de la siguiente manera: En la sección 1 se da una introducción general sobre sincronización de sistemas complejos. En la sección 2 se presentan los preliminares matemáticos. En la sección 3 se describe el algortimo empleado para generar redes deterministas de mundo pequeño. En las secciones 4 y 5 se muestran los resultados y simulaciones obtenidas. En la sección 6 se reportan las conclusiones.

2. SINCRONIZACIÓN DE REDES COMPLEJAS

Se considera una red dinámica compleja de N nodos idénticos, linealmente acoplados mediante la primer variable de estado de cada nodo, siendo cada nodo un subsistema dinámico *n-dimensional* descrito como sigue

$$\dot{\mathbf{x}}_i = f(\mathbf{x}_i) + \mathbf{u}_i, \qquad i = 1, 2, \ldots, N, \tag{1}$$

donde $\mathbf{x}_i = (x_{i1},\ x_{i2},\ ...,\ x_{in})^T \in \mathbb{R}^n$ son las variables de *estado* del nodo i, $\mathbf{u}_i = (u_{i1}, 0,\ ..., 0)^T \in \mathbb{R}$ es la señal de *control* del nodo i y es definida por

$$u_{i1} = c\sum_{j=1}^{N} a_{ij}\Gamma\mathbf{x}_j, \qquad i = 1, 2, \ldots, N, \tag{2}$$

la constante $c > 0$ representa la *fuerza de acoplamiento* de la red compleja y $\Gamma \in R^{n\times n}$ es una matriz constante de conexiones que indica que variables de estado están acopladas. Por simplicidad, se asume que $\Gamma = diag\,(r_1,\ r_2, \ldots, r_n)$ es una matriz diagonal con $r_i = 1$ para una i particular y $r_j = 0$ para $j \neq i$. Esto implica que dos nodos acoplados están conectados por su $i-$*ésima* variable de estado. Mientras que, $\mathbf{A} = (a_{ij}) \in \mathbb{R}^{N\times N}$ es la *matriz de acoplamiento*, la cual representa la topología de acoplamiento de la red compleja. Si existe una conexión entre el nodo i y el nodo j, entonces $a_{ij} = 1$; de otra forma $a_{ij} = 0$ para $i \neq j$. Los elementos de la diagonal de la matriz de acoplamiento $\mathbf{A}$ se definen como sigue

$$a_{ii} = -\sum_{j=1,\ j\neq i}^{N} a_{ij} = -\sum_{j=1,\ j\neq i}^{N} a_{ji}, \qquad i = 1, 2, \ldots, N, \tag{3}$$

sí el *grado* del nodo i es d_i, entonces $a_{ii} = -d_i$, $i = 1, 2, \ldots, N$.

Ahora, supongamos que la red compleja (1)-(2) está conectada sin tener nodos aislados. Entonces, $\mathbf{A}$ es una matriz de acoplamiento simétrica e irreducible. En este caso, se puede ver que un valor propio de la matriz de acoplamiento $\mathbf{A}$ es cero con multiplicidad 1 y todos los demás valores propios son estrictamente negativos, ver *Wang y Chen* (2002), *Wang* (2002).

El estado de sincronización de los nodos en sistemas complejos, puede caracterizarse por los valores propios diferentes de cero de la matriz de acoplamiento $\mathbf{A}$. En la red dinámica compleja definida por (1)-(2) habrá sincronización (asintótica) si, ver *Wang* (2002):

$$\mathbf{x}_1(t) = \mathbf{x}_2(t) = \ ... \ = \mathbf{x}_N(t), \text{ a medida que } t \to \infty. \tag{4}$$

La condición de acoplamiento (3) garantiza que el estado de sincronización es una solución $\mathbf{s}(t) \in \mathbb{R}^n$, de un nodo aislado, es decir, satisface

$$\dot{\mathbf{s}}(t) = f\left(\mathbf{s}(t)\right), \tag{5}$$

donde $\mathbf{s}(t)$ puede ser un *punto de equilibrio*, una *órbita periódica* ó un *atractor caótico*. En consecuencia el estado de sincronización,

$$\mathbf{x}_1(t) = \mathbf{x}_2(t) = \ ... \ = \mathbf{x}_N(t) = \mathbf{s}(t), \tag{6}$$

de la red dinámica compleja (1)-(2) es determinado por las dinámicas de un nodo aislado, la fuerza de acoplamiento c, la matriz de conexión Γ y la matriz de acoplamiento $\mathbf{A}$.

La dinámica de un nodo aislado se determina por $\bar{d}$, la cual, es una constante positiva, tal que cero es un punto exponencialmente estable, el sistema n-dimensional aislado está determinado por

$$\begin{cases} \dot{z}_1 = f_1(z) - \bar{d}z_1, \\ \dot{z}_2 = f_2(z), \\ \quad \vdots \\ \dot{z}_n = f_n(z). \end{cases} \tag{7}$$

Hay que notar que el sistema (7) corresponde al modelo matemático de un nodo aislado con una retroalimentación de estado $-\bar{d}z_1$.

2.1 Sincronización de redes complejas

El siguiente teorema establece las condiciones para lograr sincronización de la red dinámica compleja (1)-(2) en el sentido de la condición (4).

Teorema *Wang y Chen (2002); Wang (2002) Considere la red dinámica compleja (1)-(2). Sean*

$$0 = \lambda_1 > \lambda_2 \geq \lambda_3 \geq \cdots \geq \lambda_N \tag{8}$$

los valores propios de su matriz de acoplamiento $\mathbf{A}$*. Suponga que existe una matriz diagonal de orden* $n \times n$*,* $D > 0$ *y dos constantes* $\bar{d} < 0$ *y* $\tau > 0$*, tal que*

$$\left[Df(\mathbf{s}(t)) + d\Gamma\right]^T \mathbf{D} + \mathbf{D}\left[Df(\mathbf{s}(t)) + d\Gamma\right] \leq -\tau\mathbf{I}_n \tag{9}$$

para toda $d \leq \bar{d}$*, donde* $I_n \in \mathbb{R}^{n\times n}$ *es una matriz identidad. Si además,*

$$c\lambda_2 \leq \bar{d}, \tag{10}$$

entonces, el estado de sincronización (6) de la red dinámica compleja (1)-(2) es exponencialmente estable.

Dado que $\lambda_2 < 0$ y $\bar{d} < 0$, la desigualdad (10) es equivalente a

$$c \geq \left|\frac{\bar{d}}{\lambda_2}\right|. \tag{11}$$

Por tanto, la sincronía de la red dinámica compleja (1)-(2) con respecto a una topología específica puede ser caracterizada por el segundo valor propio mayor de la matriz de acoplamiento $\mathbf{A}$.

3. ALGORITMO GENERADOR DE REDES DE MUNDO PEQUEÑO DETERMINISTAS

Algoritmo generador de redes de mundo pequeño deterministas, ver *Zhang et al.* (2006)
Denotaremos nuestra red después de la evolución de l iteraciones como $N(l)$. Mediante este algoritmo, la red se crea por un procedimiento iterativo. El algoritmo de construcción es el siguiente: para $l = 0$ la red inicial, $N(0)$ es un triángulo que contiene tres nodos conectados en topología de vecino cercano, ver figura 1. Para $l \geq 1$, la red $N(l)$ se obtiene de $N(l-1)$ agregando por cada conexión creada en el paso $l-1$ un nuevo nodo y adjuntándolo a los nodos más cercanos. El algoritmo se puede resumir como sigue: En cada paso de iteración, para cada arista que exista en la red creada con la iteración anterior, se agrega un nuevo nodo, el cual, se conecta a sus vecinos más cercanos por medio de dos aristas.

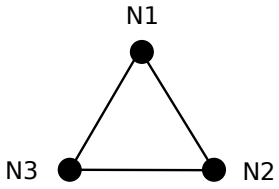

Fig. 1. Red determinista para $l = 0$.

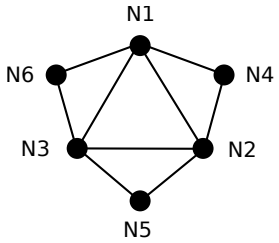

Fig. 2. Red determinista para $l = 1$.

4. SINCRONIZACIÓN DE RED EN MUNDO PEQUEÑO

4.1 Oscilador caótico de Colpitts como nodo

El oscilador de *Colpitts* en un sistema dinámico no lineal que presenta dinámica caótica, cuya evolución temporal obedece las siguientes ecuaciones diferenciales, ver *Bazili-auskas et al.* (2006):

$$\begin{cases} \dot{x}_1 = x_2 - f(x_3), \\ \dot{x}_2 = q - x_1 - bx_2 - x_3, \\ \dot{x}_3 = x_2 - d, \end{cases} \tag{12}$$

la función $f(x_3)$ está definida por

$$f(x_3) = \begin{cases} -a(x_3 + 1) & x_3 > 1, \\ 0 & x_3 \leq 1. \end{cases} \tag{13}$$

Los parámetros para obtener oscilaciones caóticas son los siguientes: $a = 81.41$, $b = 0.82$, $q = 7.14$, $d = 0.73$. Las condiciones iniciales del oscilador son: $x_1(0) = 0.5$, $x_2(0) = 0.2$, $x_3(0) = 0.8$. El atractor caótico generado por el oscilador de Colpitts (12) se muestra en la figura 3.

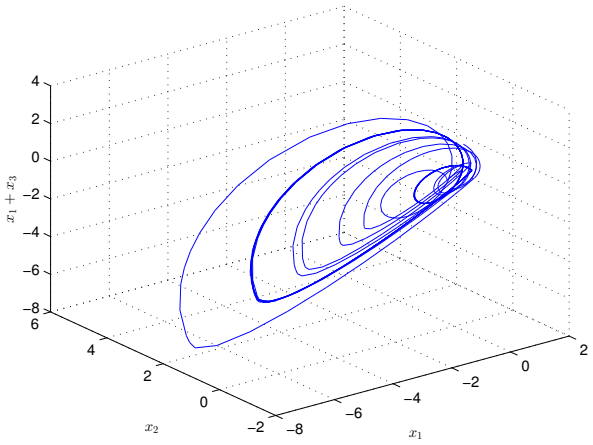

Fig. 3. Atractor caótico del oscilador de Colpitts (12).

Las ecuaciones de estado para N osciladores de Colpitts como nodos de una red dinámica compleja de acuerdo a (1) y (2), puede expresarse como se muestra a continuación:

$$\begin{aligned} \dot{x}_{i1} &= x_{i2} - f(x_{i3}) + c\sum_{j=1}^{N}(a_{ij}x_{j1}), \qquad i = 1, 2, \ldots, N, \\ \dot{x}_{i2} &= q - x_{i1} - bx_{i2} - x_{i3}, \\ \dot{x}_{i3} &= x_{i2} - d, \end{aligned} \tag{14}$$

la función $f(x_{i3})$ está definida por

$$f(x_{i3}) = \begin{cases} -a(x_{i3} + 1) & x_{i3} > 1, \\ 0 & x_{i3} \leq 1. \end{cases} \tag{15}$$

Para $\bar{d} = 0.7$, el nodo aislado del oscilador de *Colpitts* (14) se estabiliza.

4.2 Sincronización de osciladores de Colpitts de $N = 6$ nodos en una red determinista con topología de mundo pequeño

En esta sección se sincronizarán $N = 6$ nodos, que corresponden a la iteración $l = 1$ ver figura 2, por tanto obtenemos la matriz de acoplamiento A_{6n}, como se muestra a continuación,

$$A_{6n} = \begin{pmatrix} -4 & 1 & 1 & 1 & 0 & 1 \\ 1 & -4 & 1 & 1 & 1 & 0 \\ 1 & 1 & -4 & 0 & 1 & 1 \\ 1 & 1 & 0 & -2 & 0 & 0 \\ 0 & 1 & 1 & 0 & -2 & 0 \\ 1 & 0 & 1 & 0 & 0 & -2 \end{pmatrix}$$

Los valores propios de la matriz de acoplamiento A_{6n}: $\lambda_1 = 0$, $\lambda_2 = \lambda_3 = -1.6972$, $\lambda_4 = -4.0$, $\lambda_5 = -5.3028$. De acuerdo a la ecuación (11) se toma el valor propio más grande distinto de cero (λ_2), y se calcula la fuerza de acoplamiento c requerida para que la red en topología mundo pequeño (figura 2) sincronice asintóticamente,

$$c \geq \frac{|0.7|}{|1.6972|} \tag{16}$$

4.3 Simulaciones numéricas de la red con $N = 6$ nodos del oscilador de Colpitts

Tomando en cuenta los resultados obtenidos en la sección anterior, se realizaron simulaciones numéricas para una red de $N = 6$ nodos, las condiciones iniciales son: $x_{11}(0) = 0.5$, $x_{12}(0) = -0.5$, $x_{13}(0) = 0$, $x_{14}(0) = 0$, $x_{15}(0) = 0.4$, $x_{16}(0) = -0.2$, $x_{17}(0) = 1$, $x_{18}(0) = -1$, $x_{19}(0) = 0.3$, $x_{1,10}(0) = 1$, $x_{1,11}(0) = -0.75$, $x_{1,12}(0) = -0.8$, $x_{1,13}(0) = 0.4$, $x_{1,14}(0) = 0.8$, $x_{1,15}(0) = 0.2$, $x_{1,16}(0) = -1$, $x_{1,17}(0) = 1.3$, $x_{1,18}(0) = 1.3$, y se propuso $c = 0.5$ para cumplir con la condición de soncronización (16).

La figura 4 muestra las dinámicas del error del estado $\mathbf{x}_{i1}$ de los osciladores de Colpitts, nótese que aproximadamente en $t = 25$ *seg* se sincronizan los estados $\mathbf{x}_{i1}$, $\mathbf{x}_{i2}$ y $\mathbf{x}_{i3}$ de los $N = 6$ nodos.

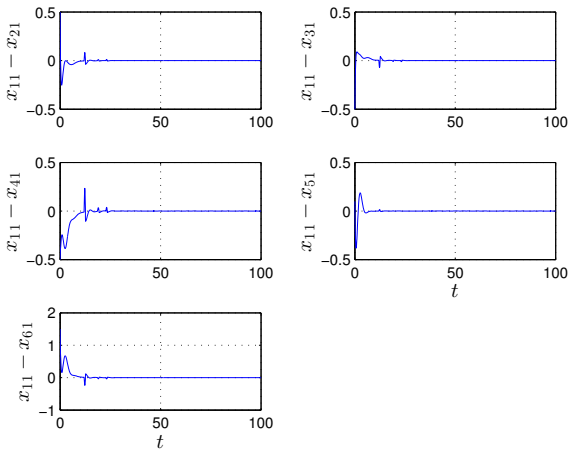

Fig. 4. Dinámicas del error del estado $\mathbf{x}_{i1}$ de los osciladores de Colpitts con $c = 0.5$, para $N = 6$ nodos.

La figura 5 muestra las dinámicas del error del estado $\mathbf{x}_{i2}$ de los osciladores de Colpitts, se puede observar que están sincronizados.

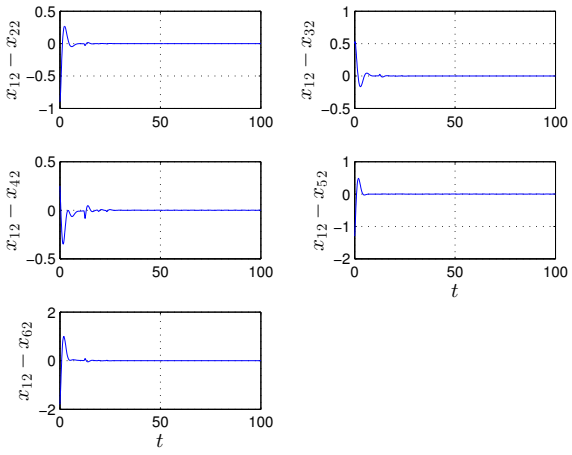

Fig. 5. Dinámicas del error del estado $\mathbf{x}_{i2}$ de los osciladores de Colpitts con $c = 0.5$, para $N = 6$ nodos.

La figura 6 muestra las dinámicas del error del estado $\mathbf{x}_{i3}$ de los osciladores de Colpitts, se puede observar que están sincronizados.

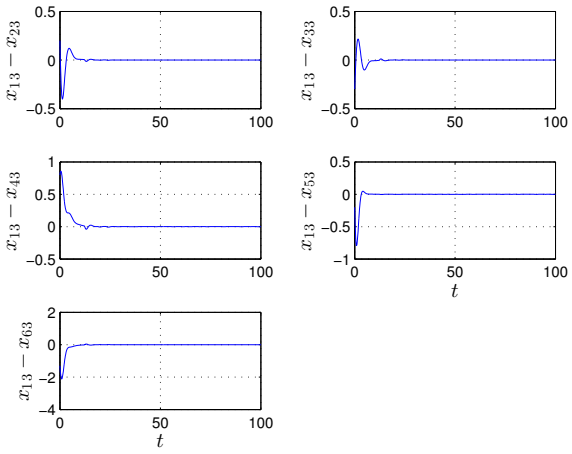

Fig. 6. Dinámicas del error del estado $\mathbf{x}_{i3}$ de los osciladores de Colpitts con $c = 0.5$, para $N = 6$ nodos.

5. ESQUEMA DE COMUNICACIÓN SEGURA EN RED DE MUNDO PEQUEÑO

A continuación se presenta el esquema de comunicación utilizado para enviar información confidencial encriptada atraves de la red de mundo pequeño (figura 2), cabe mencionar que previamente la red fue sincronizada.

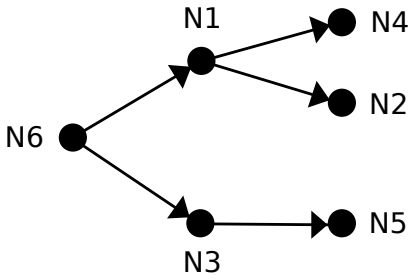

Fig. 7. Esquema de comunicación para red con $N = 6$ nodos.

La manera en que se envió el mensaje $m = sen(t)$ fue la siguiente: se tomó el nodo $N6$ como maestro y se envió el mensaje m a los nodos receptores $N1$ y $N3$, una vez recuperado el mensaje $\tilde{m}_1$ y $\tilde{m}_3$, respectivamente se retransmitió a los nodos $N4$, $N2$ y $N5$, recuperándose como $\tilde{m}_4$, $\tilde{m}_2$ y $\tilde{m}_5$ respectivamente ver figura 7. Se utilizó el remitente y destinatario arbitrariamente, pero es importante mencionar que el mensaje se puede enviar desde cualquier nodo en la red y puede ser recuperado en cualquier nodo, tampoco importa que ruta o intermediarios se tomen el mensaje siempre será recuperado, esto se debe a que previamente la red fue sincronizada y la comunicación empleada en este documento utiliza un canal para sincronizar y otro canal para enviar el mensaje encriptado. La figura 8 muestra el diagrama de bloques de la comunicación utilizada.

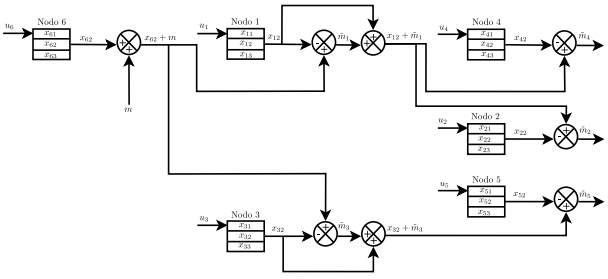

Fig. 8. Diagrama para red de comunicación de la figura 7.

En la figura 9 se observa el mensaje $m = 0.2sen(t)$ que se envía desde el nodo $N6$ y se recupera en el nodo $N4$, ver figura 7.

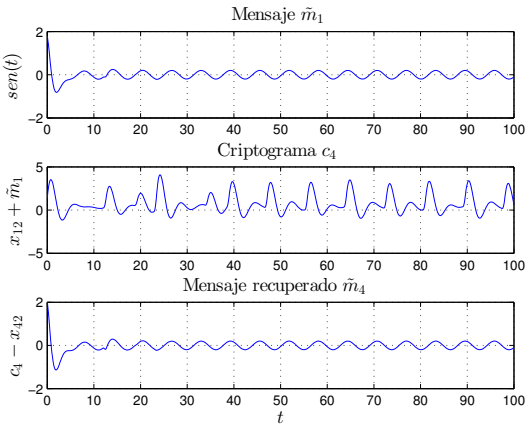

Fig. 9. Simulaciones numéricas de encriptamiento de información para red con $n = 6$ nodos, mensaje recuperado en el nodo $N4$.

En la figura 10 se observa el mensaje $m = 0.2sen(t)$ que se envía desde el nodo $N6$ y se recupera en el nodo $N2$, ver figura 7.

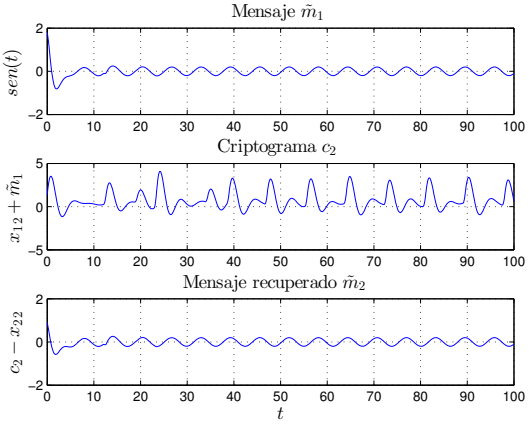

Fig. 10. Simulaciones numéricas de encriptamiento de información para red con $n = 6$ nodos, mensaje recuperado en el nodo $N2$.

En la figura 11 se observa el mensaje $m = 0.2sen(t)$ que se envía desde el nodo $N6$ y se recupera en el nodo $N5$, ver figura 7.

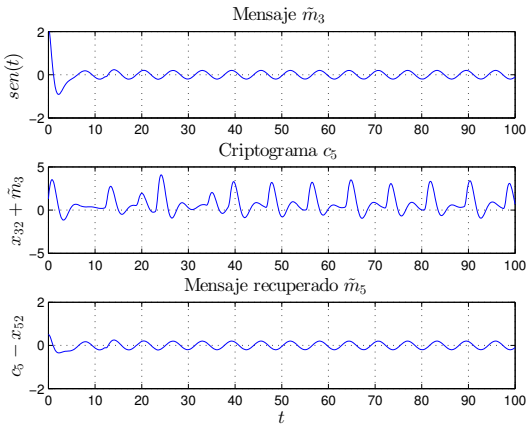

Fig. 11. Simulaciones numéricas de encriptamiento de información para red con $n = 6$ nodos, mensaje recuperado en el nodo $N5$.

6. CONCLUSIONES

En este documento se reportó la sincronización de una red determinista con topología mundo pequeño para $N = 6$ nodos utilizando la teoría de sincronización de sistemas complejos. Se utilizó el oscilador de Colpitts como modelo matemático para representar los nodos. Se realizó una comunicación segura utilizando el estado x_2 de los $N = 6$ nodos osciladores de Colpitts como portadora caótica, se concluye que un mensaje de tipo analógico puede ser enviado desde cualquier nodo de la red y recuperado en cualquier otro nodo, sin presentar errores en la recuperación del mensaje.

ACKNOWLEDGEMENTS

Al CONACYT por el apoyo económico brindado a través del proyecto de Grupos de investigación en Ciencia Básica, Ref. 166654.

REFERENCES

R. Martínez-Clark, D. Reyes-De la Cruz, C. Cruz-Hernández, R.M. López-Gutiérrez, L.F. Pinedo-Lomeli. Sincronización de robots móviles en redes complejas deterministas de mundo pequeño. COMPUMAT 2013, 27 al 29 de noviembre, La Habana, Cuba.

Francesc Comellas, Javier Ozón, Joseph G. Peters. Deterministic small-world communication networks. *Information Processing Letters*, 76:83–90, 2000.

Watts D.J. y Strogatz S.H. Collective dynamics of small-world networks. *Nature* 393:440–442, 1998.

Newman M. E. J. y Watts D. J. Renormalizationgroup analysis of the small-world network model. *Physical Lett. A* 263:341–346, 1999.

Francesc Comellas, Michael Sampels. Deterministic small-world networks. *Physica A* 309:231–235, 2002.

Zhongzhi Zhang, Lili Rong, Chonghui Guo. A deterministic small-world network created by edge iterations. *Physica A*, 363:567–572, 2006.

Xiao Fan Wang, Guanrong Chen. Synchronization in small-world dynamical networks. *Int. J. Bifurc. Chaos*, 12:187–192, 2002.

Xiao Fan Wang. Complex networks: topology, dynamics and synchronization. *International J. Bifurc. Chaos*, 12(5):885–916, 2002.

A. Baziliauskas, R. Krivickas, A. Tamasevicius. Coupled chaotic Colpitts oscillators: identical and mismatched cases. *Nonlinear Dynamics*, 44:151–158, 2006.