CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL INSTITUTO POLITÉCNICO NACIONAL

UNIDAD ZACATENCO

DEPARTAMENTO DE CONTROL AUTOMÁTICO

Comunicaciones Seguras en Sistemas de Liouville

Tesis que presenta

Juan Javier Montesinos García

Para Obtener el Grado de

Maestro en ciencias

En la Especialidad de

Control Automático

Director de la Tesis

Dr. Rafael Martínez Guerra

México, D.F. Julio 2015

Resumen

En este trabajo se expone la comunicación segura de datos por medio de sincronización de sistemas caóticos. La sincronización es vista desde la perspectiva del esquema maestro-esclavo, donde el maestro es el transmisor de datos y el esclavo el receptor. La seguridad de los datos es dada por encriptamiento atreves de enmascaramiento caótico, para esto se emplean osciladores electrónicos con dinámica caótica de tipo diferencialmente plano, diferencialmente no plano y Liouvilliano, el diseño de cada transmisor y receptor hace uso de las propiedades únicas de cada de sistema.

Abstract

In this work secure communication of data via chaotic system synchronization is presented. Synchronization is made as a master-slave scheme, where the master is the data transmitter and the slave the receiver. Data security is provided by encryption through chaotic masking using differentially flat, non-differentially flat and Liouvillian electronic oscillators with chaotic dynamic, The design of each transmitter and receiver makes extensive use of the unique properties of each system.

Agradecimientos

- Agradesco al Dr. Rafael Martínez Guarra por su consejos y dirección de este trabajo.
- Agradesco al Dr. Juan C. Cruz Victoria por su ayuda en la obtención de los resultados de esta tesis y por aceptar ser jurado en el examen de grado.
- Agradesco al Dr. Wen Yu Liu por aceptar ser jurado en el examen de grado.
- Agradesco a mis Padres y tíos por su apoyo.
- Agradesco mis compañeros Blas, Cesar, Jonny y Oscar.
- Agradesco al CONACYT y al CINVESTAV.

Dedicatoria

A mi familia por el cariño y apoyo brindado.

Índice general

Capítulo 1

Introducción

El estudio de la sincronización de sistemas no lineales comienza con los trabajos de Fujisaka y Yamada [17], Pikovsky [16], Afraimovich [15] y Pecora y Caroll [14]. A partir de estas publicaciones se ha descubierto un gran numero de aplicaciones a la sincronización de sistemas caóticos en biología, medicina, comunicaciones seguras, entre otros. En general la sincronización de sistemas se realiza, ya sea, mediante la aplicación de observadores de estados o bien, usando leyes de control que permiten la sincronización entre sistemas con dinámica completamente diferente [3, 22, 23, 25].

Las comunicaciones seguras vistas desde la perspectiva de de sincronización de sistemas [24, 29, 30] se basan en el esquema de maestro-esclavo, en el cual el sistema maestro es el transmisor de datos que enmascara el mensaje y emite la señal que transporta dicho mensaje, entonces, el sistema esclavo será el receptor que reconstruye el mensaje enmascarado y debe sincronizarse al maestro. En este tipo de encriptamiento de datos existen numerosos trabajos en los cuales el receptor es un observador de estados [3, 4, 5, 6, 7, 9, 10, 18] y otros en los que es una reconstrucción del sistema maestro [13], en todos estos el transmisor es un oscilador electrónico con dinámica caótica.

Los osciladores electrónicos con dinámica caótica son muy sensibles a variaciones en sus condiciones iniciales, un pequeño cambio en estas hará que los estados del oscilador sigan trayectorias completamente distintas esto añadido a su comportamiento similar a ruido son características deseables para encriptamiento de datos. El enmascaramiento caótico de datos es el método más efectivo y predominante para cifrar datos, sin embargo existen otros métodos de encriptamiento como son modulación y modulación por desplazamiento [3, 8, 11, 12].

Una clase de sistemas caóticos de particular interés son los denominados sistemas de Liouville [1, 2, 5, 6, 7], las propiedad principal de estos sistemas permite reconstruir estados sin recurrir a observadores, es por esto que pueden ser sincronizados con gran facilidad [1, 2], ademas, existen muchos osciladores electrónicos con dinámica caótica que son sistemas de Liouville por lo tanto su aplicación a comunicaciones seguras es factible y permiten diseñar transmisores y receptores de diversos tipos (observadores y reconstrucciones del transmisor) al tomar ventaja de sus propiedades únicas.

1.1. Motivación del tema de tesis

Una de las aplicaciones con mayor relevancia de la sincronización de sistemas caóticos son las comunicaciones seguras, en los últimos años se han presentado numerosos trabajos sobre comunicaciones seguras desde la perspectiva de sincronización en los cuales se recurre a observadores de varios tipos [3] y reconstrucciones de la dinámica del transmisor [13], sin embargo en el material bibliográfico revisado para la elaboración de la tesis no se reportan resultados que impliquen el uso de las propiedades de los sistemas de Liouville para encriptamiento de datos, es por esto que se plantea utilizar las propiedades de estos sistemas para encriptamiento de datos y analizar las ventajas que presentan en comparación con los métodos de encriptamiento mas representativos encontrados en la bibliografía.

1.2. Objetivo de la tesis

El objetivo principal de esta tesis es construir transmisores y receptores de datos para su uso en comunicaciones seguras, se desea que los transmisores sean sistemas de Liouville para que los receptores puedan diseñarse a partir de las propiedades de dichos sistemas, posteriormente, se analizaran las ventajas y desventajas de los receptores diseñados en comparación con otros métodos de encriptamiento que no hacen uso de estas propiedades.

1.3. Organización de la tesis

Este trabajo de tesis esta organizado de la siguiente forma: en el capitulo 2 se presentan conceptos básicos sobre el álgebra diferencial y sistemas diferencialmente planos, sistemas diferencialmente no planos y sistemas de Liouville; En el capitulo 3 se expone el encriptamiento de datos mediante enmascaramiento caótico usando un sistema diferencialmente plano como transmisor, a partir de este transmisor se diseñan dos receptores basados en las propiedades de los sistemas diferencialmente planos; En el capitulo 4 se muestra un encriptamiento de datos mediante enmascaramiento caótico usando un sistema diferencialmente no plano como transmisor, a partir de este transmisor se diseñan dos receptores basados en las propiedades de los sistemas diferencialmente no planos; En el capitulo 5 se expone el encriptamiento de datos mediante enmascaramiento caótico usando un sistema de Liouville como transmisor, a partir de este transmisor se diseñan dos receptores basados en las propiedades de los sistemas de Liouville y para finalizar en el Capitulo 6 se dan conclusiones y un el análisis comparativo de los esquemas de comunicaciones seguras desarrollados en capítulos anteriores.

Capítulo 2

Notaciones y definiciones básicas

En este capítulo se introducen algunas definiciones básicas sobre el álgebra diferencial que serán útiles para el desarrollo de este trabajo y para entender algunos de los resultados obtenidos.

Definición 2.1 Sean K y L campos, se dice que un elemento $x \in L$ es algebraico sobre K si y solamente si x satisface un polinomio con coeficientes en K.

Definición 2.2 Sea K un campo y $\delta : K \to K$ un mapeo tal que $\forall x, y \in K$ se cumple:

$$\begin{aligned} \delta(x+y) &= \delta(x) + \delta(y) \\ \delta(xy) &= \delta(x)y + x\delta(y) \end{aligned}$$

Tal mapeo δ recibe el nombre de derivación sobre K.

Definición 2.3 El par (K, δ), donde K es n campo y δ una derivación sobre el campo K, recibe el nombre de campo diferencial. Si ademas el operador derivada es único se dice que es un campo diferencial ordinario.

Definición 2.4 Sea (K, δ) un campo diferencial, el subconjunto $C_K = \{c \in K : \delta(c) = 0\}$ de K se le da el nombre de campo de constantes de K.

Definición 2.5 Sean Ky k dos campos diferenciales tales que $k \subset K$ y la derivación sobre K a k coincide con la derivación definida sobre k, entonces se dice que Kes una extensión del campo diferencial k y se denota por K/k.

Definición 2.6 Sea K/k una extensión de campos diferenciales y S un subconjunto de K. Al sub campo diferencial mas pequeño de K que contiene a k y a S se le denota por $K\langle S\rangle$ y se dice que es el campo diferencial generado por los elementos de S y de las derivadas de sus elementos sobre K.

Definición 2.7 Sea K/k una extensión de campos diferenciales. Dado un elemento $x \in K$ se dice que es diferencialmente algebraico sobre K si x es raíz de un polinomio diferencial no cero con coeficientes en K.

Definición 2.8 Sea K/k una extensión de campos diferenciales, si todo elemento de K es diferencialmente algebraico sobre k, entonces se dice que K/k es una extensión diferencialmente algebraica sobre k.

Definición 2.9 Sea K/k una extensión de campos diferenciales, dado un elemento $x \in K$, si x no es diferencialmente algebraico sobre k, entonces se dice que x es trascendental sobre k.

Definición 2.10 Sea K/k una extensión de campos diferenciales, si al menos un elemento $x \in K$ es diferencialmente trascendental sobre k, entonces K es una extensión diferencial trascendental sobre k.

Definición 2.11 Sea K/k una extensión de campos diferenciales, entonces se dice que un conjunto $\{\zeta_i : i \in I,\ I\, es\, un\, conjunto\, indice\}$ de elementos de K es diferencialmente K-algebraico dependiente si y solo si el conjunto de derivadas de cualquier orden $\left\{\zeta^{(vi)} : i \in I, vi = 0, 1, 2, ...\right\}$ es k-algebraicamente dependiente.

Definición 2.12 Un conjunto no diferencialmente k-algebraico dependiente se le dice diferencialmente k-algebraico independiente.

Definición 2.13 Sea K/k una extensión diferencial de campos, a toda familia diferencialmente k-algebraico independiente que es maximal con respecto a la inclusión de conjuntos se dice una base de trascendencia diferencial de K/k.

Definición 2.14 La cardinalidad de la base de trascendencia diferencial de K/k es conocida como grado de trascendencia diferencial de K/k y se le denota por $trddif\,(K/k)$, y la extensión K/k es diferencialmente algebraica si y solo si $trddif\,(K/k) = 0$.

Definición 2.15 El grado de trascendencia no diferencial es el numero de condiciones iniciales necesarias para calcular las soluciones de las ecuaciones algebraicas.

Definición 2.16 Sea K/k una extensión de campos diferenciales, se dice que K/k es una extensión puramente trascendental diferencial si y solo si existe una base de trascendencia diferencial $\xi = \{\xi_i : i \in I,\ I\, es\, un\, conjunto\, de\, indices\}$ de K/k tal que $K = k\,\langle\xi\rangle$.

Definición 2.17 Se define un sistema H/k como una extension de campos diferenciales finitamente generada.

Definición 2.18 Sea K/k un sistema, se dice que K/k es un sistema diferencial puramente trascendental si la extension K/k lo es.

Definición 2.19 Dados dos sistemas K/k y $\bar{K}/k$, se dice que son sistemas equivalentes o equivalentes por una reglamentación endógena si y solamente si cualquier elemento de K es algebraico sobre $\bar{K}$.

Definición 2.20 Una dinámica es una extension diferencialmente algebraica y finitamente generada $H/k\,\langle u\rangle$, dado un elemento H que es solución de un polinomio diferencial no cero sobre $k\,\langle u\rangle$ en la componente u y un numero finito de derivadas de u.

Definición 2.21 Condición de observabilidad algebraica: Sean $\{u, y\}$ un subconjunto de un campo diferencial H y la dinámica dada por $H/k\langle u\rangle$, se dice que un elemento $x \in H$ es observable respecto de $\{u, y\}$ si este es diferencialmente algebraico sobre $k\langle u, y\rangle$, entonces se dice que un estado x es observable si y solo si es observable sobre $\{u, y\}$, en otras palabras, el elemento x satisface una ecuación polinomial en termino de $\{u, y\}$ y algunas de sus derivadas con respecto al tiempo:

$$P\left(x, u, \dot{u}, ..., y, \dot{y}, ...\right) = 0$$

Con coeficientes en $k\langle u, y\rangle$.

Definición 2.22 Sea $K/k\langle u\rangle$ una dinámica con salida y, se dice que la dinámica es observable si todos sus estados son observables.

Definición 2.23 Sea el sistema H/k con salida $y = \{y_1, y_2, ..., y_m\}$ que es un subconjunto de H tal que $y$es una base de trascendencia diferencial de H/k, al entero que hace mínimo el grado de trascendencia diferencial se le denomina defecto algebraico.

Definición 2.24 Si existe una base de trascendencia diferencial $y = \{y_1, y_2, ..., y_m\}$ de H/k tal que $H = k\langle y\rangle$, entonces a esta base de trascendencia diferencial $y$se le denomina salida linealizante o salida plana del sistema H/k.

Definición 2.25 Un sistema H/k es diferencialmente plano si y solamente si su defecto algebraico es cero, es decir, el sistema es diferencialmente plano si todas sus variables (estados y entradas) pueden ser escritos como funciones diferenciales en términos de la salida plana y un numero finito de sus derivadas en el tiempo.

Definición 2.26 Un sistema H/k es diferencialmente no plano si el defecto algebraico es distinto de cero, lo que implica, que no todos sus estados y entradas pueden ser escritos como

funciones diferenciales en términos de la salida plana y un numero finito de sus derivadas en el tiempo.

Definición 2.27 Sea el sistema H/k y el campo M tal que $k \subset M \subset H$ de modo que M/k es el sub sistema plano de H/k. Se dice que H/k es Liouvilliano si los elementos $H - M$ pueden ser obtenidos por una adjunción de integrales o exponenciales de integrales de elementos de M y algunas de sus derivadas en el tiempo.

Capítulo 3

Comunicaciones seguras en sistemas diferencialmente planos

3.1. Sistemas diferencialmente planos y comunicaciones seguras

El concepto de planitud diferencial fue introducido en [26], un sistema no lineal se denomina diferencialmente plano si existe una función diferencial del estado llamada salida plana, tal que todas las variables de estado del sistema, sus entradas y salidas pueden ser expresadas como funciones diferenciales de la salida plana [20]. Considerando que la salida disponible del sistema y la salida plana son las mismas, y ademas, si las funciones de la salida plana con las que se describen los estados son algebraicas, el sistema cumple con la condición de observabilidad algebraica, en consecuencia sus estados pueden ser reconstruidos con un observador [2], aunque, también es posible reconstruir los estados del sistema y sus entradas por medio de la función diferencial de la salida plana con la cual son expresados.

Las dos características de los sistemas diferencialmente planos mencionadas anteriormente pueden ser aprovechadas para comunicaciones seguras [5], en este capítulo se proponen dos métodos para recuperar mensajes basados en estas propiedades. En estos métodos el encriptamiento se hace por medio de enmascaramiento caótico al esconder el mensaje dentro de la dinámica de un sistema diferencialmente plano y caótico, el primer método de recuperación de datos es mediante un observador de estados por modos deslizantes y como segundo método de recuperación se hace uso de la propiedad principal de los sistemas diferencialmente planos, es decir, el mensaje se recupera aplicando las ecuaciones diferenciales que describen los estados del sistema.

El oscilador de Van der Pol que es un sistema diferencialmente plano, caótico y que cumple la condición de observabilidad algebraica, también su estructura facilitara el diseño de los

receptores por eso se escoge como transmisor de datos para este capítulo, no obstante existen muchos otros osciladores que son diferencialmente planos, caóticos y observables que pueden ser aplicados a comunicaciones seguras de la manera que se muestra a continuación.

3.2. Sistema diferencialmente plano como transmisor de datos

Un sistema no lineal y diferencialmente plano puede ser representado de la siguiente forma [26]:

$$\begin{aligned} \dot{x} &= f(x,u) \\ y &= h\left(x,u,\dot{u},...,u^{(\gamma)}\right) \end{aligned}$$

Los estados y entradas pueden ser descritos de la siguiente manera:

$$\begin{aligned} x &= \mathcal{A}\left(y,\dot{y},...,y^{(\alpha)}\right) \\ u &= \mathcal{B}\left(y,\dot{y},...,y^{(\beta)}\right) \end{aligned} \tag{3.1}$$

Si $\mathcal{A}$ es una ecuación diferencial algebraica, los estados x cumplen la condición de observabilidad algebraica. El oscilador de Van der Pol posee amortiguamiento lineal, por esto se requiere de una entrada para que se mantenga oscilando, además, esta entrada hace que el oscilador exhiba un comportamiento caótico, con lo que resulta ideal para enmascaramiento. Su dinámica es descrita por las siguientes ecuaciones diferenciales:

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= \mu\left(1-x_1^2\right)x_2 - x_1 + u \\ y &= x_1 \end{aligned} \tag{3.2}$$

Donde $\mu > 0$ es una constante positiva que pondera el amortiguamiento no lineal. Dada la

salida $y = x_1$ el sistema es diferencialmente plano, los estados y la entrada se pueden escribir como:

$$\begin{aligned} x_1 &= y \\ x_2 &= \dot{y} \\ u &= \ddot{y} - \mu\left(1 - y^2\right)\dot{y} + y \end{aligned} \tag{3.3}$$

Ya que los estados x_1 y x_2 se expresan como un polinomio en términos de la salida y algunas de sus derivadas, el sistema es algebraicamente observable. El mensaje s será la entrada del oscilador, de modo que la dinámica del transmisor es:

$$\begin{aligned} \dot{x} &= f(x, u) \\ y &= h\left(x, u, \dot{u}, ..., u^{(\gamma)}\right) \end{aligned}$$

Donde:

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= \mu\left(1 - x_1^2\right)x_2 - x_1 + s \\ y &= x_1 \end{aligned} \tag{3.4}$$

De este modo el mensaje se encuentra oculto dentro de la dinámica del estado x_2. Como el oscilador es un sistema diferencialmente plano, el mensaje puede ser recuperado por medio de la salida plana, que el mensaje y la entrada coincidan es una casualidad asignada por la estructura del oscilador, el método de enmascaramiento no requiere forzosamente que el mensaje sea la entrada, este puede sumarse a la dinámica de cualquier otro estado que no contenga la entrada.

3.3. Receptor-Observador por modos deslizantes basado en el modelo del transmisor

Como el transmisor cumple la condición de observabilidad algebraica, sus estados pueden reconstruirse con un observador, entonces, se propone tratar el mensaje como una dinámica no modelada dentro del estado x_2. Los observadores por modos deslizantes son robustos ante este tipo de incertidumbre [19], así que, al hacer uso de un observador de este tipo se pueden estimar los estados del transmisor a partir de la salida plana sin que la incertidumbre afecte la sincronización, una vez que se dispone de un estimado de los estados y la salida plana, el mensaje puede reconstruirse a partir de la ecuación dinámica del estado que contiene al mensaje. La dinámica del observador es la siguiente:

$$\begin{aligned} \dot{\hat{x}}_1 &= \hat{x}_2 + k\,\mathrm{sign}(Ce) \\ \dot{\hat{x}}_2 &= \mu\left(1-\hat{x}_1^2\right)\hat{x}_2 - \hat{x}_1 \\ \hat{s} &= \dot{\hat{x}}_2 - \mu\left(1-\hat{x}_1^2\right)\hat{x}_2 + \hat{x}_1 \end{aligned} \tag{3.5}$$

Donde el error de sincronización e se define como:

$$e = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} x_1 - \hat{x}_1 \\ x_2 - \hat{x}_2 \end{bmatrix}$$

El vector C proviene de la salida del transmisor que puede ser escrita como:

$$y = Cx = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

A continuación tenemos la dinámica del error:

$$\begin{aligned} \dot{e}_1 &= x_2 - \hat{x}_2 - k\,\mathrm{sign}(Ce) \\ \dot{e_2} &= \mu\left(1-x_1^2\right)x_2 - x_1 + s - \mu\left(1-\hat{x}_1^2\right)\hat{x}_2 + \hat{x}_1 \end{aligned}$$

Definiendo

$$\phi(e) = \begin{bmatrix} e_2 \\ \mu\left(1 - x_1^2\right) x_2 + s - \mu\left(1 - \hat{x}_1^2\right) \hat{x}_2 - e_1 \end{bmatrix}$$

La dinámica del error esta dada por la ecuación:

$$\dot{e} = \phi(e) - kC^T \operatorname{sign}(Ce)$$

El transmisor deberá cumplir las siguientes condiciones para que el receptor sea estable:

H3.1 La norma de la dinámica del transmisor incluyendo al mensaje es acotada por una constante real positiva $\delta > 0$:

$$\|f(x,u)\| \leq \delta$$

Y en consecuencia:

$$\begin{aligned} \phi(e) &= \begin{bmatrix} x_2 - \hat{x}_2 \\ \mu\left(1 - x_1^2\right) x_2 - x_1 + s - \mu\left(1 - \hat{x}_1^2\right) \hat{x}_2 + \hat{x}_1 \end{bmatrix} \\ \phi(e) &= f(x,u) - f\left(\hat{x},u\right) \\ \|\phi(e)\| &= \|f(x,u) - f\left(\hat{x},u\right)\| \\ \|\phi(e)\| &\leq \delta \end{aligned}$$

H3.2

3.3.1. Prueba de estabilidad

Para demostrar la estabilidad del observador se propone la siguiente función candidata de Lyapunov:

$$V = \frac{1}{2} e^T e$$

Derivando la función y teniendo en cuenta la condición **H3.1** :

$$\begin{aligned}\dot{V} &= e^T\dot{e} = e^T\phi(e) - ke^TC^T\,\text{sign}(Ce)\\ \dot{V} &\leq \delta\,|e| - k\,|e|\\ \dot{V} &\leq -(k-\delta)\,|e|\end{aligned}$$

Al elegir $k > \delta$:

$$\dot{V} \leq 0 \tag{3.6}$$

Así los estados estimados serán muy similares a los estados del transmisor. El error en la recuperación del mensaje se define como:

$$\begin{aligned}e_s &= s - \hat{s}\\ e_s &= s - \dot{x}_2 + \mu\left(1-\hat{x}_1^2\right)\hat{x}_2 - \hat{x}_1\end{aligned}$$

A partir de (3.3)

$$e_s = s - \left[\mu\left(1-x_1^2\right)x_2 - x_1 + s\right] + \mu\left(1-\hat{x}_1^2\right)\hat{x}_2 - \hat{x}_1 \tag{3.7}$$

(3.6) implica que el error de sincronización se mantiene acotado y en consecuencia (3.7) indica que el error de recuperación del mensaje también se mantiene acotado, si los estados estimados cumplen: $\hat{x}_1 \to x_1$ y $\hat{x}_2 \to x_2$ el error de estimación del mensaje también tiende a cero:

$$e_s \to 0$$

De este modo se prueba que este transmisor es capaz de recuperar mensajes ya que el error en la recuperación del mensaje se mantiene acotado.

3.3.2. Resultados numéricos

Para comprobar la eficacia de este receptor se hace una simulación numérica, el mensaje será dado por la función del tiempo:

$$s = \sin(50\pi t)$$

El elegir esta función como mensaje facilitara detectar visualmente errores en amplitud o fase. Los parámetros del transmisor y receptor son los siguientes:

Parámetro	Valor
μ	8.53
$x_1(0)$	0
$x_2(0)$	0
k	10
$\hat{x}_1(0)$	1
$\hat{x}_1(0)$	2

Con estos valores se obtienen los siguientes resultados:

Después de que el receptor se ha sincronizado al transmisor el mensaje estimado y el real son muy parecidos:

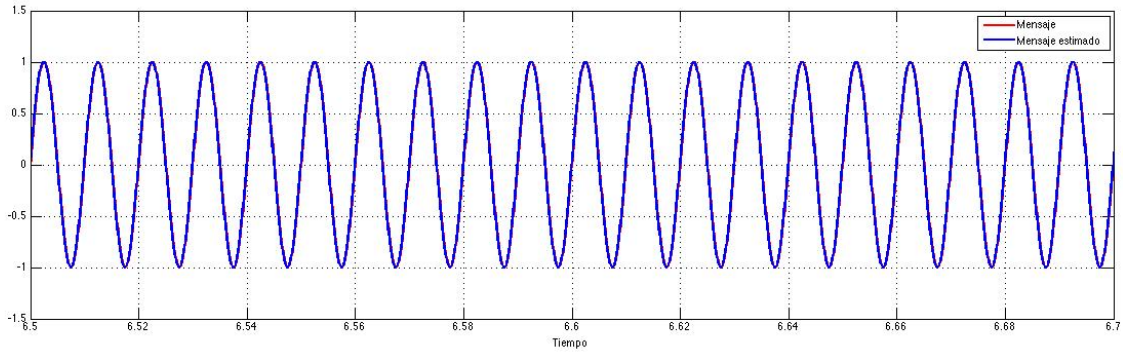

Figura 3.1. Mensaje y mensaje recuperado

Producir el mensaje recuperado toma menos de 2 segundos:

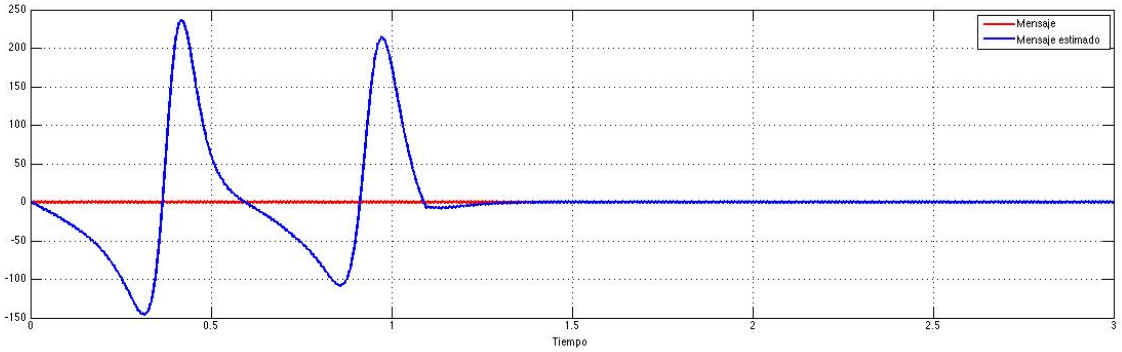

Figura 3.2. Convergencia del mensaje estimado al mensaje transmitido.

El error de recuperación del mensaje es el siguiente:

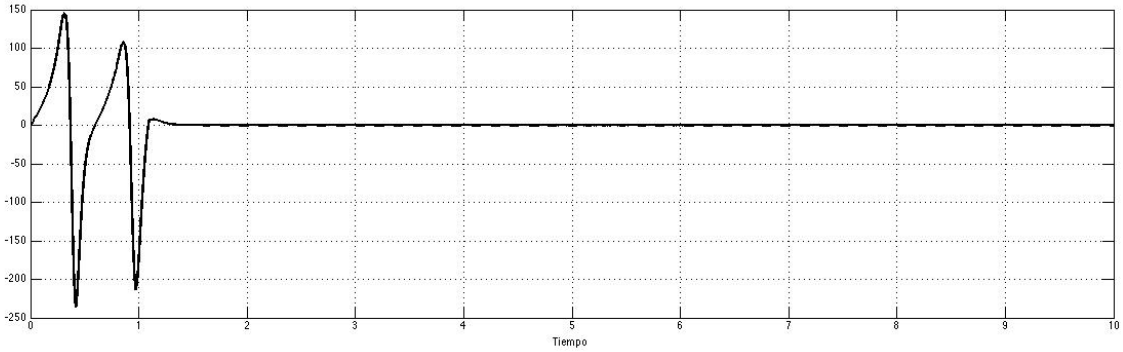

Figura 3.3. Error de recuperación del mensaje

Los estados del transmisor y receptor también convergen:

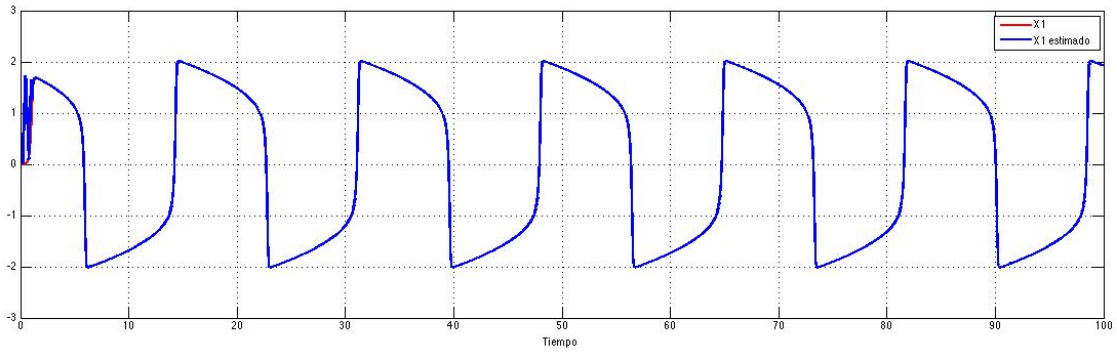

Figura 3.4. Estados x_1 y $\hat{x}_1$

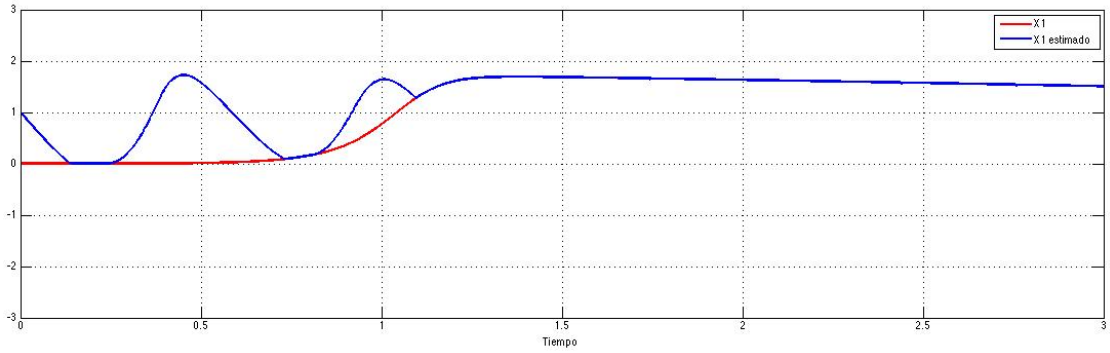

Figura 3.5. Convergencia de los estados x_1 y $\hat{x}_1$

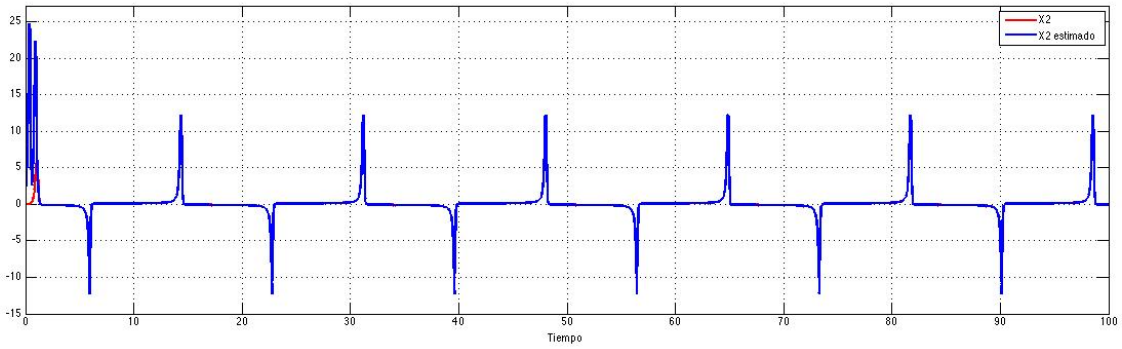

Figura 3.6. Estados x_2 y $\hat{x}_2$

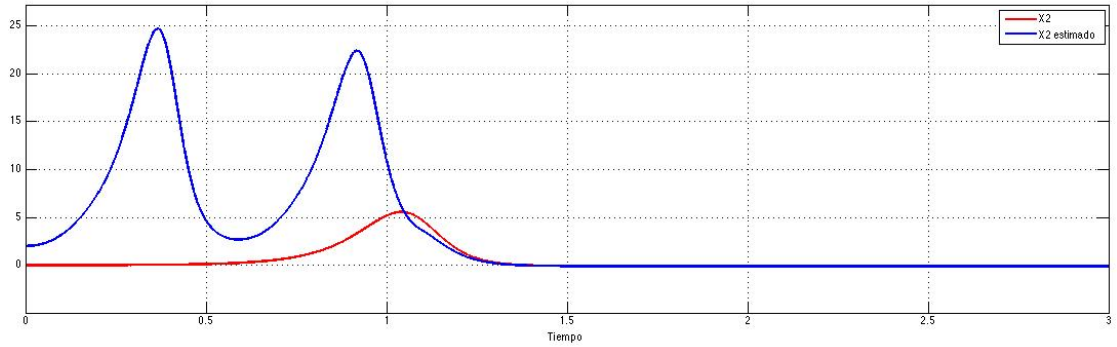

Figura 3.7. Convergencia de los estados x_2 y $\hat{x}_2$

El error de sincronización entre el transmisor y receptor es:

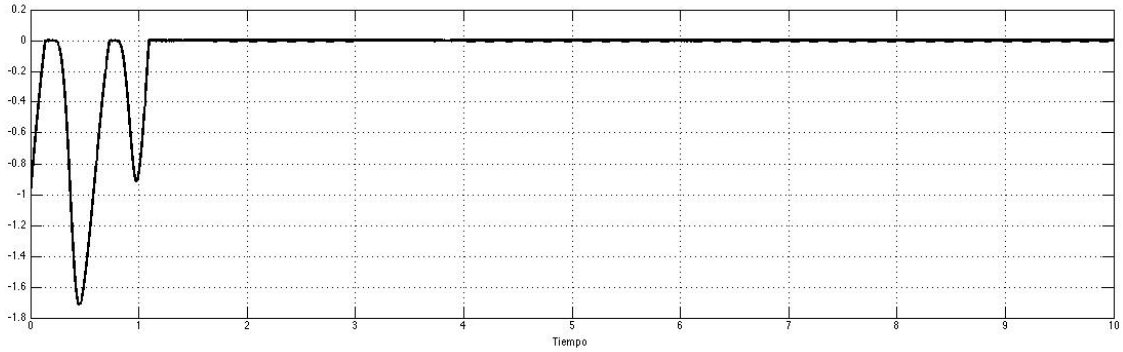

Figura 3.8. Diferencia entre los estados x_1 y $\hat{x}_1$

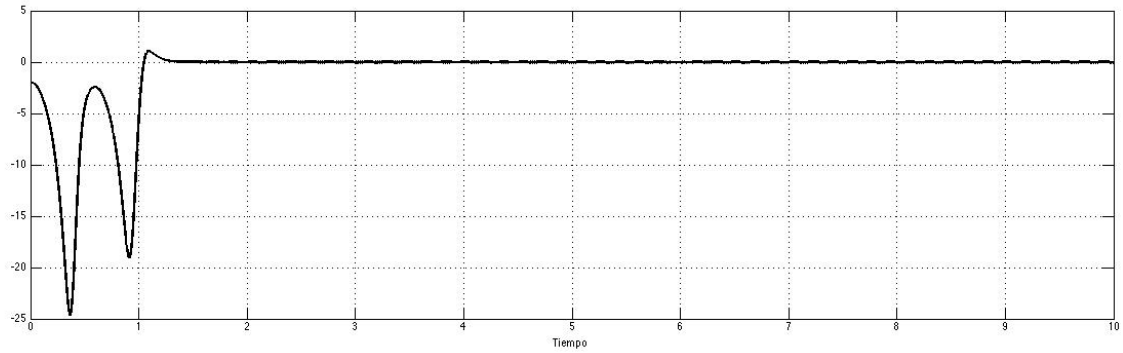

Figura 3.9. Diferencia entre los estados x_2 y $\hat{x}_2$

La salida que transporta el mensaje es:

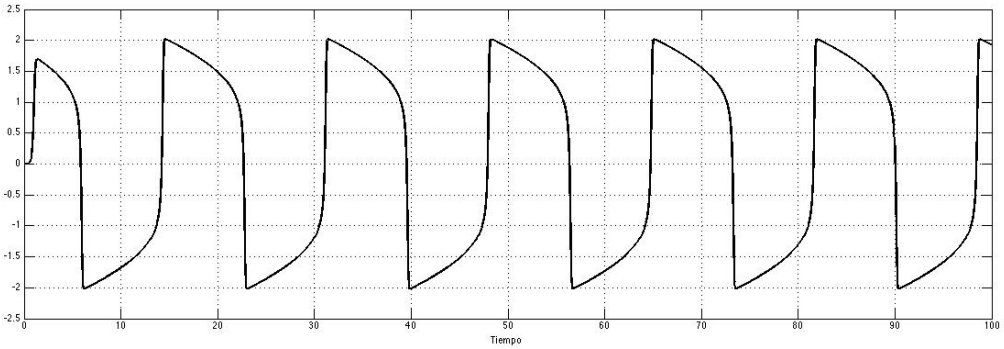

Figura 3.10. Salida y

El receptor puede recuperar exitosamente el mensaje, a pesar de que se deben esperar 2 segundos a que la sincronización ocurra, de lo contrario el mensaje estimado presentara errores en la reconstrucción de la parte inicial del mensaje.

3.4. Receptor basado en la propiedad de planitud diferencial

El mensaje oculto dentro de la dinámica del sistema puede ser reconstruido únicamente usando la propiedad de planitud, al incluir el mensaje en la derivada de alguno de los estados será necesario disponer de esta derivada, lo que implica derivar la salida plana para acceder a ella. En el caso especifico del oscilador de Van der Pol el mensaje coincide con la salida y puede ser reconstruido por (3.3), sin embargo, se tratara al mensaje como si fuera un termino desconocido de la dinámica del estado en el que se enmascara el mensaje, con la intención de que este método sea general para sistemas diferencialmente planos, aun si la entrada no coincide con el mensaje. El receptor requiere estimar los estados que forman la dinámica del estado en el cual esta inmerso el mensaje (x_2 en este ejemplo), después el mensaje se reconstruye despejándolo de la dinámica del estado que lo contiene, para el oscilador de Van der Pol el receptor es dado por las siguientes ecuaciones:

$$\begin{aligned} \hat{x}_1 &= y \\ \hat{x}_2 &= \dot{y} \\ \hat{s} &= \dot{\hat{x}}_2 - \mu\left(1-\hat{x}_1^2\right)\hat{x}_2 + \hat{x}_1 \end{aligned} \tag{3.8}$$

A diferencia del método anterior no hay tiempo de espera para que los estados del receptor converjan a los del transmisor, esto significa que el error de reconstrucción del mensaje siempre es cero y que los datos pueden transmitirse inmediatamente, el error de recuperación del mensaje es definido como:

$$e_s = s - \hat{s}$$

Y en vista de (3.3) y (3.8):

$$e_s = 0$$

Un inconveniente mayor de este método de reconstrucción del mensaje es que se requiere derivar la señal de la salida varias veces, Los canales de transmisión en general tienen ruido que no siempre es diferenciable, entonces, este ruido será amplificado tras cada derivada aumentando el error [21], también, la señal de salida debe ser continuamente diferenciable y suave, de lo contrario las partes no diferenciales causaran que el error sea diferente de cero.

3.4.1. Resultados numéricos

En las simulaciones numéricas se utiliza el siguiente mensaje:

$$s = \sin(0.5\pi t)$$

Los parámetros del transmisor y receptor son los siguientes:

Parámetro	Valor
μ	8.53
$x_1(0)$	0
$x_2(0)$	0

Con estos valores se obtienen los siguientes resultados:

A diferencia del receptor anterior, en este no hay tiempo de espera para que se sincronicen el receptor y el transmisor:

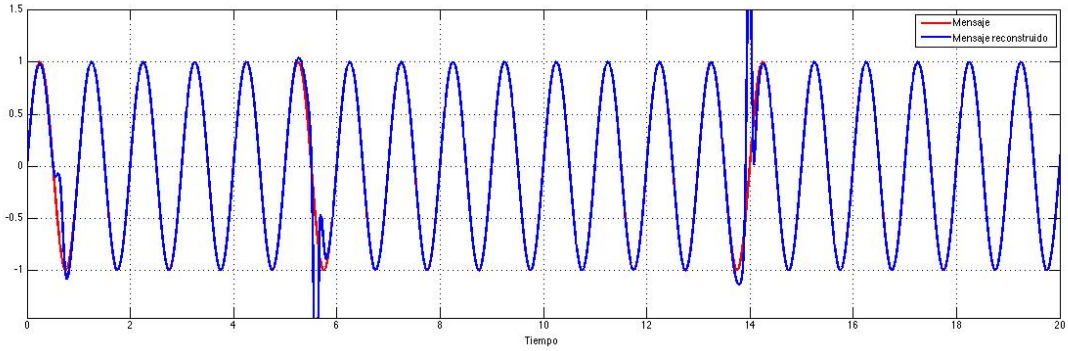

Figura 3.11. Mensaje y mensaje recuperado

El mensaje no es reconstruido correctamente en los puntos en los que los estados no son suaves, en este caso los cambios abruptos de amplitud en x_2 coinciden con estas inexactitudes. El error de recuperación del mensaje es el siguiente:

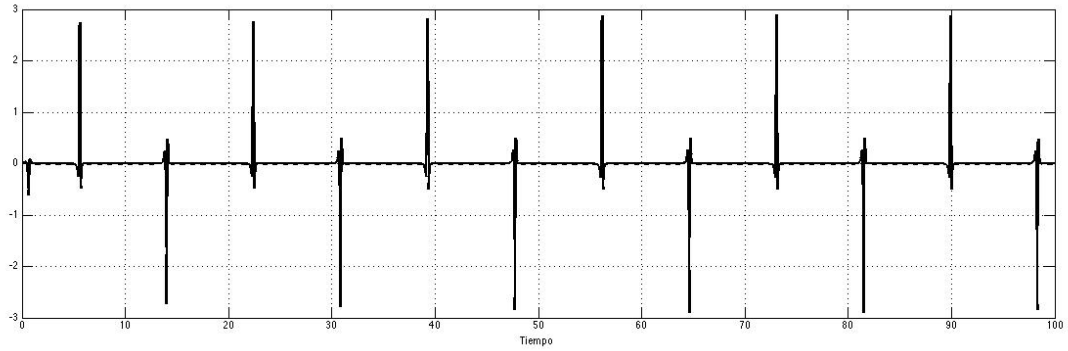

Figura 3.12. Error de recuperación del mensaje

Los estados del transmisor y receptor son:

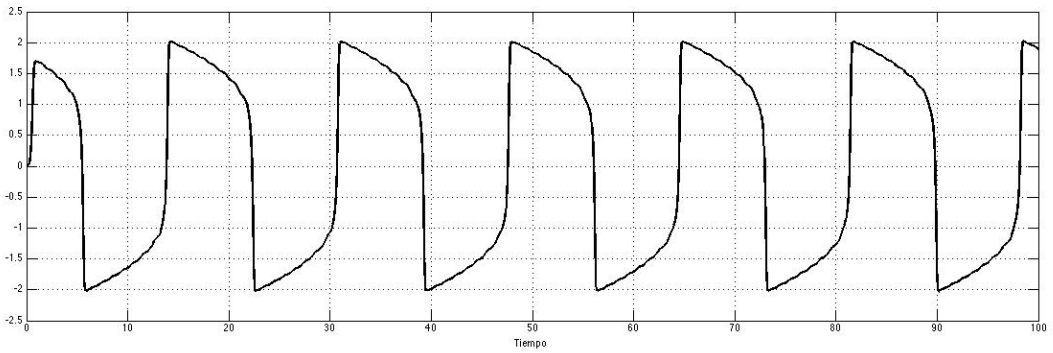

Figura 3.13. Estados x_1 y $\hat{x}_1$

La señal producida por el segundo estado no es lo suficientemente suave:

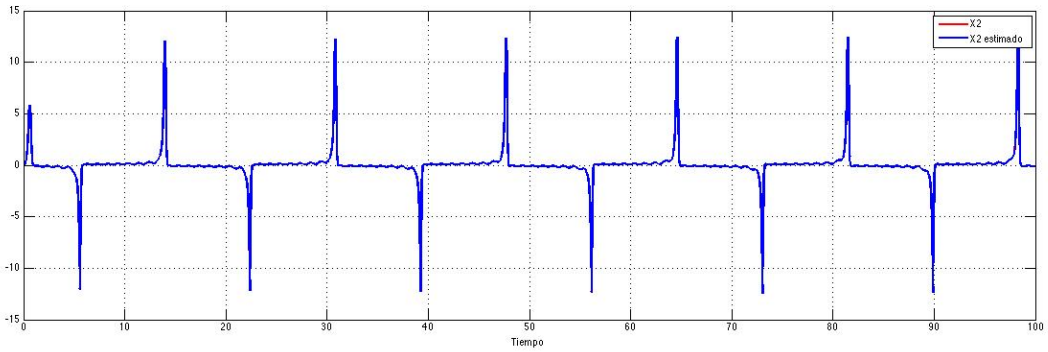

Figura 3.14. Estados x_2 y $\hat{x}_2$

El error de sincronización entre el transmisor y receptor es:

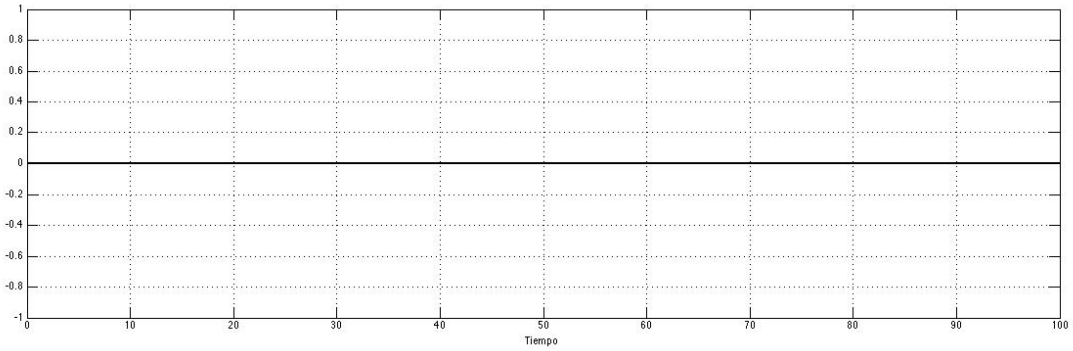

Figura 3.15. Diferencia entre los estados x_1 y $\hat{x}_1$

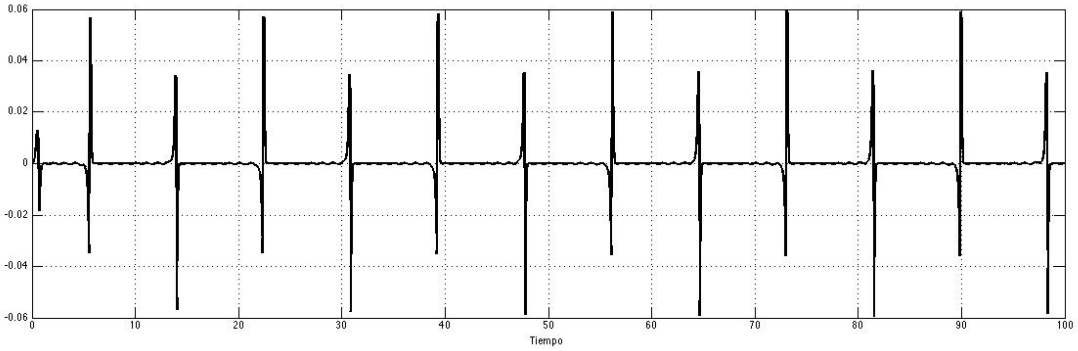

Figura 3.16. Diferencia entre los estados x_2 y $\hat{x}_2$

Los cambios abruptos en la amplitud del segundo estado generan inexactitudes en la reconstrucción del mensaje y del segundo estado. El mensaje no es visible en la salida que transporta lo transporta:

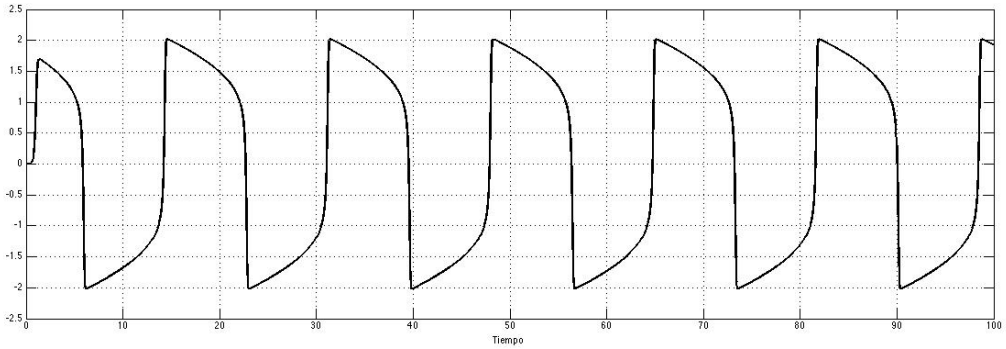

Figura 3.17. Salida y

El receptor recupera el mensaje sin tiempo de espera, a cambio de esto, el mensaje reconstruido presenta errores a causa de los cambios abruptos en el estado x_2, es por esto que los estados del transmisor deben ser suaves y continuamente diferenciables, la reconstrucción del estado x_1 es muy precisa causando que no pueda verse ninguna diferencia entre el estado estimado y el real.

3.5. Comentarios finales

Ambos receptores tienen características positivas y negativas, el observador produce un estimado aceptable después de que se sincroniza al transmisor, en cambio debe esperarse a que la sincronización ocurra para transmitir el mensaje. El segundo transmisor se sincroniza inmediatamente y no es necesario esperar para enviar el mensaje, pero el estimado del mensaje presentara diferencias con el mensaje real en ciertos puntos, ademas de que es necesario que los estados del transmisor sean una señal suave y continuamente diferenciable para reducir este fenómeno.

La mayor ventaja de este esquema de comunicación es que el mensaje no se encuentra presente en la salida, pues esta oculto dentro de la dinámica de otro estado del cual la salida es independiente. Un problema presente en ambos receptores es la dificultad para producir una llave de encriptamiento, en el observador aun si se varían las condiciones iniciales el mensaje convergerá y en el segundo receptor las condiciones iniciales no influyen. Otro inconveniente es que el operador del receptor posee una copia de la dinámica del transmisor, por lo tanto toda la información sobre el enmascaramiento se encuentra disponible al publico.

Capítulo 4

Comunicaciones seguras en sistemas diferencialmente no planos

4.1. Sistemas diferencialmente no planos y comunicaciones seguras

Numerosos sistemas no poseen la propiedad de planitud diferencial, se dice que un sistema es diferencialmente no plano, si existe al menos una variable del sistema, la cual no puede ser expresada en términos de una función de la salida y un número finito de sus derivadas en el tiempo. Por otra parte al número de variables del sistema, tales que no puedan ser representadas en términos de la salida plana y sus derivadas, se le define como el defecto del sistema [26], por lo tanto los sistemas diferencialmente no planos están algebraicamente caracterizados por un número entero positivo llamado el defecto del sistema, y se dice que un sistema es diferencialmente no plano si su defecto es diferente de cero. En un sistema los estados que no poseen la característica de planitud diferencial no pueden ser escritos como una función de la salida y sus derivadas, en consecuencia tampoco cumplen con la condición de observabilidad algebraica. Algunos osciladores caóticos diferencialmente no planos tienen características deseables para comunicaciones seguras por medio de enmascaramiento, pero, dado que no cumplen con la condición de observabilidad algebraica es difícil diseñar un receptor con los métodos mostrados en el capítulo anterior. En este capítulo también se presenta un enmascaramiento caótico de datos, pero a diferencia del capítulo anterior, el mensaje es ocultado dentro de la salida del sistema. La señal que transporta el mensaje se trata de manera similar a una perturbación acotada a la salida, debido a que algunos observadores basados en modos deslizantes son robustos ante este tipo de perturbaciones [3], se presentan dos diseños de receptor con este enfoque, el primero hace uso del algoritmo de

Super-Twisting mientras que el segundo usa la combinación de un filtro por modos deslizantes (similar a un Delta-modulador) y un observador polinomial exponencial.

4.2. Sistema diferencialmente no plano como transmisor de datos

El transmisor será un sistema no lineal y diferencialmente no plano descrito por las ecuaciones dinámicas:

$$\begin{aligned} \dot{x} &= f(x,u) \\ y &= Cx + s \end{aligned}$$

Donde $x \in \mathbb{R}^n$, y es la salida y s el mensaje, para el desarrollo primer receptor, el transmisor debe poder escribirse como una cadena de integradores mediante una transformación, de modo que sea equivalente al sistema:

$$\dot{n} = \gamma(n,u)$$

Con:

$$\begin{aligned} \dot{n}_1 &= n_2 \\ \dot{n}_2 &= n_3 \\ &\vdots \\ \dot{n}_n &= g(n,u) \\ y &= n_{n-1} + s \end{aligned}$$

Es necesario que el transmisor también sea un sistema caótico, para que el enmascaramiento de datos sea más efectivo por los cambios abruptos en su dinámica y su sensibilidad a condiciones iniciales dificultara la estimación del mensaje mediante criptoanalisis. El oscilador de Colpitts es un sistema que llena los requisitos mencionados y es útil como fuente de ondas

periódicas, ademas gracias a su comportamiento caótico a frecuencias fundamentales altas y bajas su uso en comunicaciones seguras es más práctico, su dinámica es dada por:

$$\begin{aligned} \dot{x}_1 &= x_2 - f(x_3) \\ \dot{x}_2 &= \gamma - x_1 - bx_2 - x_3 \\ \dot{x}_3 &= x_2 - d \\ y &= x_2 \end{aligned} \tag{4.1}$$

Con:

$$f(x_3) = \begin{cases} -a(x_3+1) & x_3 < -1 \\ 0 & x_3 \geq -1 \end{cases}$$

Al seleccionar $y = x_2$ como salida dos estados del oscilador serán diferencialmente no planos y tampoco cumplirán la condición de observabilidad algebraica:

$$\begin{aligned} x_1 &= \gamma - \dot{y} - by - x_3 \\ x_2 &= y \\ \dot{x}_3 &= y - d \end{aligned} \tag{4.2}$$

Para el desarrollo del primer receptor el transmisor debe estar en forma de cadena de integradores, o bien, debe ser escrito de esa manera mediante una transformación, el siguiente cambio de coordenadas hace que el sistema tome la forma deseada:

$$\begin{aligned} n_1 &= x_3 \\ n_2 &= x_2 - d \\ n_3 &= \gamma - x_1 - bx_2 - x_3 \end{aligned}$$

Al derivar, la dinámica del sistema transformado equivale a una cadena de integradores:

$$\begin{aligned} \dot{n}_1 &= n_2 \\ \dot{n}_2 &= n_3 \\ \dot{n}_3 &= -2n_2 + d + f(n_1) - bn_3 \end{aligned}$$

Donde la salida es $y = n_2$, el mensaje s es enmascarado añadiéndolo a la salida:

$$y = n_2 + s$$

Así el mensaje puede ser transmitido de manera segura para que el receptor tenga acceso a el y pueda recuperarlo.

4.3. Receptor-observador basado en el algoritmo de Super-Twisting

El primer receptor es un observador de estados por modos deslizantes basado en el algoritmo de Super-twisting que tiene las características de ser robusto ante perturbaciones a la salida e incertidumbre. Este observador resulta práctico para el tipo de encriptamiento de datos que se emplea en este trabajo, pues que el mensaje puede ser visto como una perturbación acotada a la salida. El usar el algoritmo de Super-Twisting produce un efecto de castañeo mucho menor al encontrado en modos deslizantes de primer orden, con esto se mejora el desempeño del receptor y permite el uso de mensajes de menor amplitud causando que el mensaje sea menos visible en la señal con la que es encriptado. Otro beneficio de tener un castañeo reducido es que el mensaje reconstruido es mucho más parecido al mensaje original, es decir se tiene una reconstrucción más precisa del mensaje. Ya que la dinámica del transmisor es una cadena de integradores solo es necesario sincronizar los últimos dos estados del receptor, pues, los demás estados pueden ser obtenidos al integrar el estado siguiente, por lo tanto la parte de la dinámica del transmisor a la que el receptor debe sincronizarse es:

$$\begin{aligned} \dot{n}_{n-1} &= \dot{n}_1 = n_2 \\ \dot{n}_n &= \dot{n}_2 = f(n,u) \\ y &= \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} n_1 \\ n_2 \end{bmatrix} + s \end{aligned}$$

Y la dinámica del receptor es:

$$\begin{aligned} \dot{\hat{n}}_1 &= \hat{n}_2 + k_a (y - \hat{y}) + m\tau^{-1} |y - \hat{y}|^{\frac{1}{2}} sign (y - \hat{y}) \\ \dot{\hat{n}}_2 &= k_b (y - \hat{y}) + m^2 \tau^{-2} sign (y - \hat{y}) \\ \hat{y} &= \hat{n}_1 \\ \hat{s} &= y - \hat{y} \end{aligned} \tag{4.3}$$

Donde $k_a > 0$, $k_b > 0$, $m > 0$ y $0 < \tau < 1$ son constantes positivas y $\hat{s}$ es el mensaje reconstruido. Teniendo en cuenta que la salida del transmisor es escrita como:

$$y = Cx = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

El mensaje reconstruido es:

$$\hat{s} = Cn + s - C\hat{n}$$

Conforme el estado estimado $\hat{n}$ converge al estado del transmisor n, el mensaje reconstruido $\hat{s}$ se aproxima al mensaje original s. El error de recuperación del mensaje es:

$$e_s = s - \hat{s} = s - (Cn + s - C\hat{n}) = -Cn + C\hat{n} \tag{4.4}$$

Si la diferencia entre el estado real y el estimado se acerca a cero también lo hace la diferencia entre el mensaje real y el estimado. Las siguientes hipótesis son necesarias para la demostración de estabilidad del receptor:

H4.1 Existe constantes no negativas L_{0f} y L_{1f} tales que la siguiente condición quasi-Lipschitz se mantiene:

$$\|\Delta_f\| \leq L_{0f} + \|e\| \left(L_{1f} + \|A_\mu\|\right)$$

H4.2 La señal de información esta acotada de la siguiente manera:

$$\|s\|_\Lambda^2 = s^T \Lambda s \leq \left(s^+\right)^2 < \infty, 0 < \Lambda = \Lambda^T.$$

H4.3 Existe una matriz definida positiva $0 < Q = Q^T$ tal que la ecuación de Riccati:

$$PA_\mu + A_\mu^T P + PRP + Q = 0 \tag{4.5}$$

Tiene solución $0 < P = P^T$ con:

$$\begin{aligned} R &= \Lambda_f^{-1} + 2\|\Lambda_f\| L_{1f} I, 0 < \Lambda_f = \Lambda_f^T \\ Q &= Q_0 + 2\left(L_{1f} + \|\Lambda_\mu\|\right)^2 I \end{aligned}$$

Y se elige:

$$\begin{gathered} \Lambda_f = \lambda_f I \quad L_{1f} = \mu \quad R = \left(\lambda_f^{-1} + 2\lambda_f \mu\right) I \\ Q_0 = q_0 I \quad Q = \left(q_0 + 8\mu^2\right) I \end{gathered} \tag{4.6}$$

H4.4 Existe $K = m\tau^{-1} \begin{pmatrix} |e+s|^{\frac{1}{2}} \\ m\tau^{-1} \end{pmatrix} P^{-1} C^T \geq 0$ en el que no todas las componentes de K son cero.

4.3.1. Prueba de estabilidad

Se define el error de sincronización como:

$$e = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} n_1 - \hat{n}_1 \\ \frac{1}{m}\left(n_2 - \hat{n}_2\right) \end{bmatrix}$$

Derivando el error de sincronización:

$$\begin{aligned}\dot{e}_1 &= \dot{n}_1 - \dot{\hat{n}}_1 \\ &= n_2 - \hat{n}_2 - k_a\left(y-\hat{y}\right) - m\tau^{-1}\left|y-\hat{y}\right|^{\frac{1}{2}} sign(y-\hat{y})\end{aligned}$$

La derivada de la componente e_2 es:

$$\begin{aligned}\dot{e}_2 &= \frac{1}{m}\left(\dot{n}_2 - \dot{\hat{n}}_2\right) \\ &= \frac{1}{m}\left[\Phi(n_1,n_2) - k_b\left(y-\hat{y}\right) - m^2\tau^{-2} sign(y-\hat{y})\right]\end{aligned}$$

Se agrega un parámetro de regularización $\mu > 0$:

$$\left[\begin{array}{c}\dot{e}_1 \\ \dot{e}_2\end{array}\right] = \left[\begin{array}{c} e_2 - k_a\left(e+s\right) - m\tau^{-1}\left|e+s\right|^{\frac{1}{2}} sign(e+s) + \mu e_1 - \mu e_1 \\ \frac{1}{m}\Phi(n_1,n_2) - \frac{k_b}{m}\left(e+s\right) - m^2\tau^{-2} sign\left(e+s\right) + \mu e_2 - \mu e_2\end{array}\right]$$

$$\begin{aligned}\dot{e} &= \left[\begin{array}{cc}-\mu & 1 \\ 0 & -\mu\end{array}\right]\left[\begin{array}{c}e_1 \\ e_2\end{array}\right] - \left(\begin{array}{c}k_a \\ k_b\end{array}\right)(e+s) \\ &\quad -m\tau^{-1}\left(\begin{array}{c}\left|e+s\right|^{\frac{1}{2}} \\ m\tau^{-1}\end{array}\right) sign\left(\left[\begin{array}{cc}1 & 0\end{array}\right]\left[\begin{array}{c}e_1 \\ e_2\end{array}\right] + s\right) + \left(\begin{array}{c}\mu e_1 \\ \frac{\Phi(n_1,n_2)}{m} + \mu e_2\end{array}\right)\end{aligned}$$

$$\begin{aligned}\dot{e} &= \left[\begin{array}{cc}-\mu & 1 \\ 0 & -\mu\end{array}\right]\left[\begin{array}{c}e_1 \\ e_2\end{array}\right] - \left(\begin{array}{c}k_a \\ k_b\end{array}\right)e \\ &\quad -m\tau^{-1}\left(\begin{array}{c}\left|e+s\right|^{\frac{1}{2}} \\ m\tau^{-1}\end{array}\right) sign\left(\left[\begin{array}{cc}1 & 0\end{array}\right]\left[\begin{array}{c}e_1 \\ e_2\end{array}\right] + s\right) + \left(\begin{array}{c}\mu e_1 - k_a s \\ \frac{\Phi(n_1,n_2)}{m} + \mu e_2 - k_b s\end{array}\right)\end{aligned}$$

la derivada del error es reescrita como:

$$\dot{e} = A_\mu e - k_2 e - k_1 sign(Ce+s) + \Delta f \tag{4.7}$$

Donde:

$$k_1 = m\tau^{-1}\begin{pmatrix} |e+s|^{\frac{1}{2}} \\ m\tau^{-1} \end{pmatrix}, k_2 = \begin{pmatrix} k_a \\ k_b \end{pmatrix}, \Delta f = \begin{pmatrix} \mu e_1 - k_a s \\ \frac{\Phi(n_1,n_2)}{m} + \mu e_2 - k_b s \end{pmatrix}$$

La ganancia $k_2 > 0$ puede escogerse de modo que reduzca los efectos del mensaje dentro de la incertidumbre. El receptor permite que el error de recuperación del mensaje $e_s = s - \hat{s}$ se mantenga acotado y converge al conjunto residual:

$$D_\varepsilon = \{e_s | \, \|e_s\|_P \leq \bar{\mu}(k)\}$$

Donde P es la solución de las ecuaciones de Riccati (4.5) y

$$\bar{\mu}(k) = \left(\frac{\rho(K)}{\sqrt{(K\alpha_p)^2 + \rho(K)\alpha_Q} + K\alpha_p} \right)$$

Con:

$$\begin{aligned} \rho(K) &= 2\|\Lambda_f\| L_{0f}^2 + 4k_2 s^+ \sqrt{n\Lambda_f^{-1}} \\ K\alpha_p &= K\left(\lambda_{min}\left(P^{-1/2}C^T C P^{-1/2}\right)\right) \\ \alpha_Q &= \lambda_{min}\left(P^{-1/2}Q^T Q P^{-1/2}\right) \end{aligned}$$

Para demostrar este resultado se usa la siguiente función candidata de Lyapunov:

$$V(e) = \|e\|_P^2 = e^T P e, 0 < P = P^T$$

Derivando:

$$\begin{aligned} \dot{V}(e) &= 2e^T P\dot{e} = 2e^T P\left(A_\mu e - k_2 e - k_1 sign(Ce+s) + \Delta f\right) \\ \dot{V}(e) &= 2e^T P A_\mu e - 2e^T P k_2 e - 2e^T P k_1 sign(Ce+s) + 2e^T P\Delta f \end{aligned}$$

Las ganancias se seleccionan de modo que $k_1 > 0$ y $k_2 > 0$ y usando **H4.4:**

$$\dot{V}(e) \leq 2e^T P A_\mu e - 2Ke^T C^T sign(Ce + s) + 2e^T P \Delta f$$

Usando la desigualdad $X^T Y + Y^T X \leq X^T \Lambda_f X + Y^T \Lambda_f^{-1} Y$ para $0 < \Lambda_f = \Lambda_f^T$:

$$\dot{V}(e) \leq e^T (P A_\mu + A_\mu^T P) e - 2Ke^T C^T sign(Ce + s) + e^T P \Lambda^{-1} P e + \Delta_f^T \Lambda_f \Delta_f$$

Considerando **H4.1**:

$$\begin{aligned}
\dot{V}(e) &\leq e^T (P A_\mu + A_\mu^T P + PRP + Q) e - e^T Q e + L_{0f}^2 \\
&\quad + 2 \|\Lambda_f\| \left[\|e\|^2 \left(L_{1f} + \|A_\mu\|^2 \right) \right] - 2e^T C^T K sign(Ce + s) \\
\dot{V}(e) &\leq e^T (P A_\mu + A_\mu^T P + PRP + Q) e - e^T Q e \\
&\quad + 2 \|\Lambda_f\| L_{0f}^2 - 2e^T C^T K sign(Ce + s)
\end{aligned}$$

Teniendo en cuenta que:

$$\begin{aligned}
x^T sign(x + z) &= (x + z)^T sign(x + z) - z^T sign(x + z) \\
&\geq \sum_{i=1}^{n} |(x + z)_i| - \sum_{i=1}^{n} |z_i| \geq \sum_{i=1}^{n} |x_i| - \sum_{i=1}^{n} |z_i| - \sum_{i=1}^{n} |z_i| \\
&\geq \sum_{i=1}^{n} |x_i| - 2 \sum_{i=1}^{n} |z_i| \geq \sum_{i=1}^{n} |x_i| - 2\sqrt{n} \|z_i\|
\end{aligned}$$

El error y el mensaje contenidos en la funciona signo son separados y por medio de **H4.3:**

$$\begin{aligned}
\dot{V}(e) &\leq -e^T Qe + 2\left\|\Lambda_f\right\| L_{0f}^2 - 2e^T C^T K sign(Ce+s) \\
\dot{V}(e) &\leq -e^T Qe + 2\left\|\Lambda_f\right\| L_{0f}^2 - 2K\left(\sum_{i=1}^{n}\left|(Ce)_i\right| - 2\left\|s\right\|\sqrt{n}\right) \\
\dot{V}(e) &\leq -e^T Qe - 2K\sum_{i=1}^{n}\left|(Ce)_i\right| + \rho(k) \qquad (4.8)
\end{aligned}$$

Con $\rho(k) = 2\left\|\Lambda_f\right\| L_{0f}^2 + 4k\bar{s}\sqrt{n\Lambda_f^{-1}}$, entonces:

$$\dot{V}(e) \leq -\left\|e\right\|_Q - 2K\alpha_P\left\|e\right\|_P + \rho(k)$$

Donde:

$$\left(\sum_{i=1}^{n}\left|(Ce)_i\right|\right)^2 \geq \sum_{i=1}^{n}\left|(Ce)_i\right|^2 = \left\|Ce\right\|^2 = \left\|CP^{-1/2}P^{-1/2}e\right\|^2 \geq \alpha_P e^T Qe$$

Con $\alpha_P = \lambda_{min}\left(P^{-1/2}C^T CP^{-1/2}\right)$, después:

$$\dot{V}(e) = \frac{d}{dt}\left\|e\right\|_p^2 \leq -\left\|e\right\|_Q^2 - 2K\alpha\left\|e\right\|_P + \rho(k)$$

A partir de (4.6):

$$\dot{V}(e) = -\alpha_Q V(e) - \vartheta\sqrt{V(e)} + \beta \qquad (4.9)$$

Donde $\alpha_Q = \lambda_{min}\left(P^{-1/2}Q^T QP^{-1/2}\right) > 0$, $\vartheta = 2K\alpha_p$ y $\beta = \rho(k)$. El punto de equilibrio V^* de esta ecuación cumple:

$$-\alpha_Q V - \vartheta\sqrt{V} + \beta = 0$$

Entonces:

$$V^* = \left(\sqrt{\left(\frac{\vartheta}{2\alpha}\right)^2 + \frac{\beta}{\alpha}} - \frac{\vartheta}{2\alpha}\right)^2 = \frac{\left(\frac{\beta}{\alpha}\right)^2}{\left(\sqrt{\left(\frac{\vartheta}{2\alpha}\right)^2 + \frac{\beta}{\alpha}} - \frac{\vartheta}{2\alpha}\right)^2} = \tilde{\mu} \geq 0$$

Definiendo $\Delta = (V - V^*)^2$ y derivando:

$$\begin{aligned}
\dot{\Delta} &= 2(V - V^*)\dot{V} \leq 2(V - V^*)\left(-\alpha_Q V - \vartheta\sqrt{V} + \beta\right) \\
&= 2(V - V^*)\left[-\alpha_Q V - \vartheta\sqrt{V} + \beta + \left(\alpha_Q V^* + \vartheta\sqrt{V^*} - \beta\right)\right] \\
&\quad \times 2(V - V^*)\left[-\alpha(V - V^*) - \vartheta\left(\sqrt{V} - \sqrt{V^*}\right)\right] \\
&= -2\alpha(V - V^*)^2 - 2\vartheta\left(\sqrt{V} + \sqrt{V^*}\right)\left(\sqrt{V} - \sqrt{V^*}\right)^2 \leq 0
\end{aligned}$$

$$\dot{\Delta} = 2(V - V^*)\dot{V} \leq 2(V - V^*)\left(-\alpha_Q V - \vartheta\sqrt{V} + \beta\right)$$

Esto implica que para cualquier $V \neq V^*$ $\lim_{t\to\infty} V \to V^*$. Para:

$$G_t = 2\left[V - \bar{\mu}\right]_+^2 = V^2\left[1 - \frac{\bar{\mu}}{V}\right]_+$$

La función $[\bullet]_+$se define como:

$$[z]_+ = \begin{cases} z & , z \geq 0 \\ 0 & , z < 0 \end{cases}$$

Derivando G:

$$\begin{aligned}\dot{G}_t &= 2\left[V-\tilde{\mu}\right]_+ \dot{V} = 2V\left[1-\frac{\tilde{\mu}}{V}\right]_+ \dot{V} \\ &\leq 2V\left[1-\frac{\tilde{\mu}}{V}\right]_+ \left(-\alpha_Q V - \vartheta\sqrt{V}+\beta\right) \\ &= -2V\left[1-\frac{\tilde{\mu}}{V}\right]_+ \left[\alpha\left(V-V^*\right)+\vartheta\left(\sqrt{V}-\sqrt{V^*}\right)\right] \leq 0\end{aligned}$$

La ultima desigualdad implica que G converge a su punto fijo:

$$G_t \to G^* < \infty$$

Integrando desde 0 a t:

$$G_t - G_0 \leq -2\int_0^t V\left[1-\frac{\tilde{\mu}}{V}\right]_+ \left[\alpha\left(V-V^*\right)+\vartheta\left(\sqrt{V}-\sqrt{V^*}\right)\right] d\tau$$

Los que lleva a la siguiente desigualdad:

$$2\int_0^t V\left[1-\frac{\tilde{\mu}}{V}\right]_+ \left[\alpha\left(V-V^*\right)+\vartheta\left(\sqrt{V}-\sqrt{V^*}\right)\right] d\tau \leq G_0 - G_t \leq G_0$$

Dividiendo entre t y tomando los limites superiores de ambos lados se tiene:

$$\lim_{t\to\infty}\frac{1}{t}\int_0^t V\left[1-\frac{\tilde{\mu}}{V}\right]_+ \left[\alpha\left(V-V^*\right)+\vartheta\left(\sqrt{V}-\sqrt{V^*}\right)\right] d\tau \leq 0$$

Existe una sub secuencia t_k tal que:

$$V_{t_k}\left[1-\frac{\tilde{\mu}}{V}\right]_+ \left[\alpha\left(V-V^*\right)+\vartheta\left(\sqrt{V}-\sqrt{V^*}\right)\right] \to 0$$

Cuando $k \to \infty$:

$$G_{t_k} \to 0$$

Teniendo en cuenta que $G^* = 0$:

$$\left[1 - \frac{\bar{\mu}\,(k)}{V(e)}\right]_+ \to 0$$

Esto implica que $V(e) \leq \bar{\mu}(k)$, entonces:

$$\begin{aligned} V(e) &= \|e\|_p = e^T P e \geq e_1^T P e_1 \\ e_1 &= Cn - C\hat{n} = -e_s \\ e_1^T P e_1 &= \left(-e_s^T\right) P\,(-e_s) = e_s^T P e_s = \|e_s\|_P \end{aligned}$$

El error de estimación del mensaje converge al subconjunto D_ε pues:

$$\|e_s\|_P = \|e_1\|_P \leq \bar{\mu}\,(k)$$

De esta manera se prueba que el error de recuperación del mensaje también converge a $\bar{\mu}\,(k)$:

$$\|e_s\|_P \leq \bar{\mu}\,(k)$$

A pesar de tener el mensaje añadido a la salida y la incertidumbre Δ_f el error de sincronización se mantiene acotado, de la misma forma lo hace el error de recuperación del mensaje mostrando así las características principales de este observador, en la sección de resultados numéricos se mostraran los beneficios al tener un castañeo de amplitud pequeña.

4.3.2. Resultados numéricos

El mensaje es dado por la siguiente función del tiempo:

$$s = \sin(50\pi t)$$

Los parámetros del transmisor y receptor son los siguientes:

Parámetro	Valor
γ	0
b	0.8
d	0.6
a	30
$x_1(0)$	0
$x_2(0)$	0
$x_3(0)$	0
k_1	$\begin{bmatrix} 10 & 25 \end{bmatrix}^T$
k_2	$\begin{bmatrix} 15 & 20 \end{bmatrix}^T$
$\hat{n}_1(0)$	0
$\hat{n}_2(0)$	3
$\hat{n}_3(0)$	0

Los valores anteriores producen los siguientes resultados:

Mensaje estimado y el mensaje real después de la sincronización:

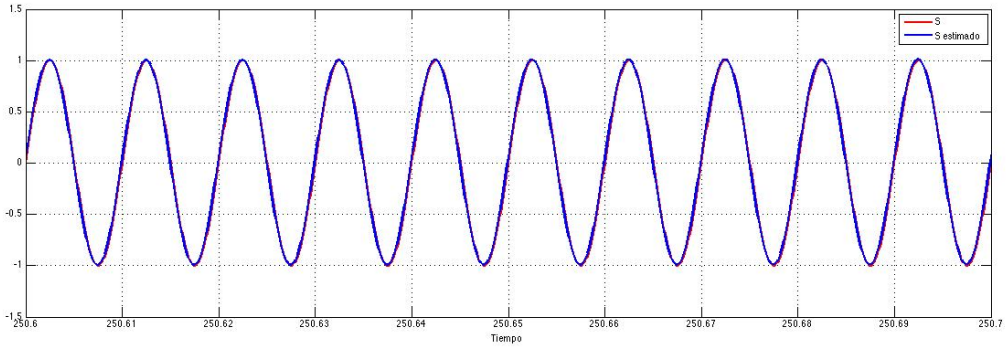

Figura 4.1. Mensaje y mensaje estimado

Convergencia del mensaje estimado al real:

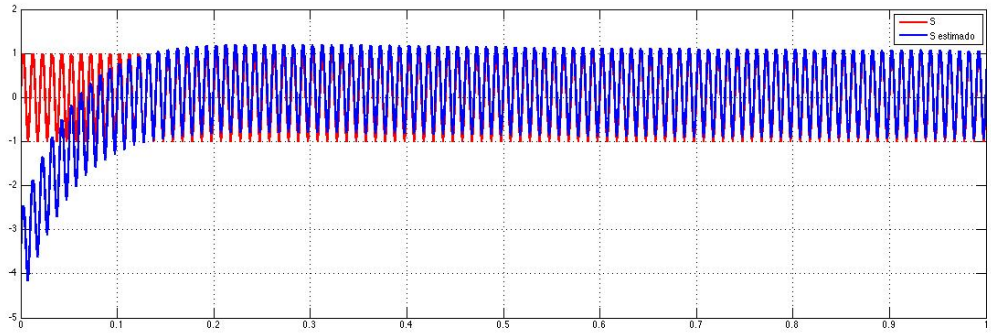

Figura 4.2. Convergencia del mensaje estimado al mensaje transmitido

El error de recuperación del mensaje:

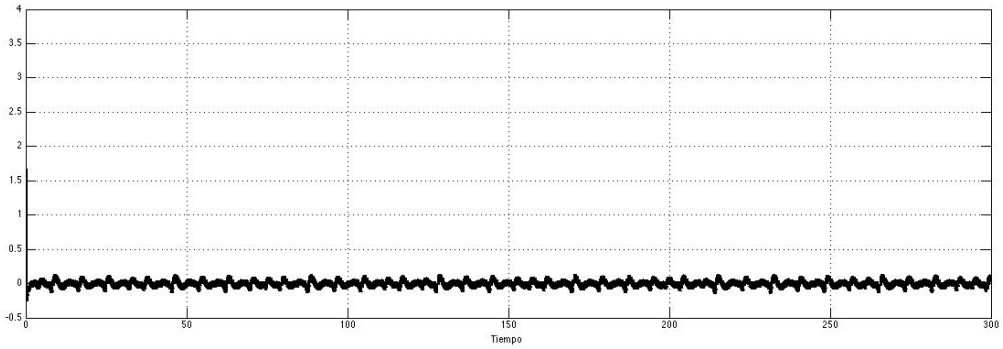

Figura 4.3. Error de recuperación del mensaje

Estados del transmisor y receptor:

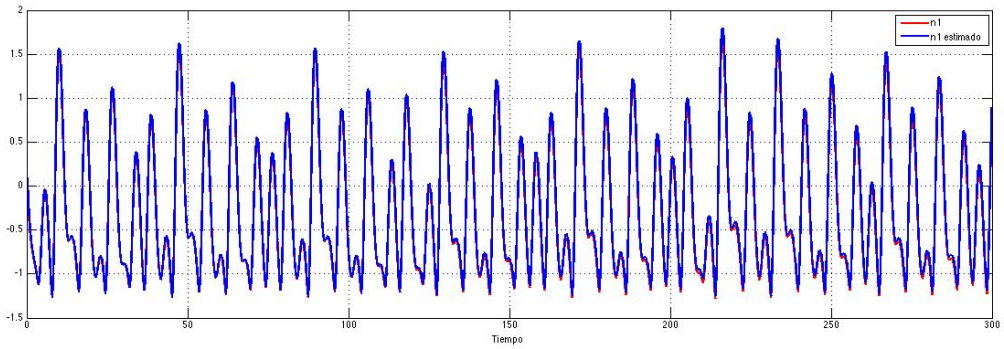

Figura 4.4. Estados n_1 y $\hat{n}_1$

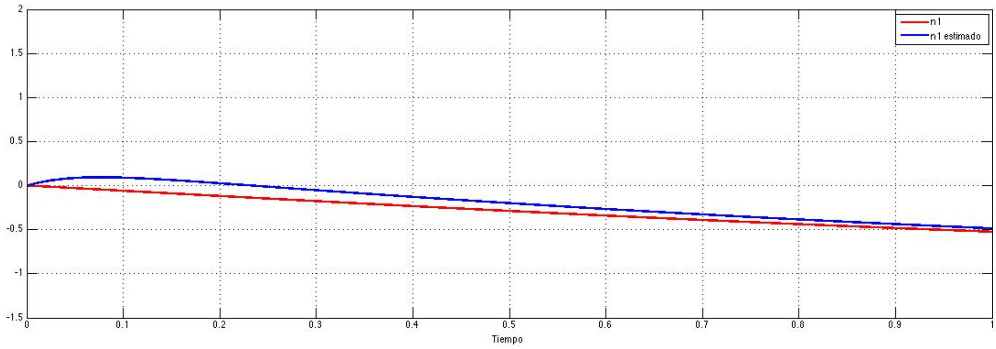

Figura 4.5. Convergencia de los estados n_1 y $\hat{n}_1$

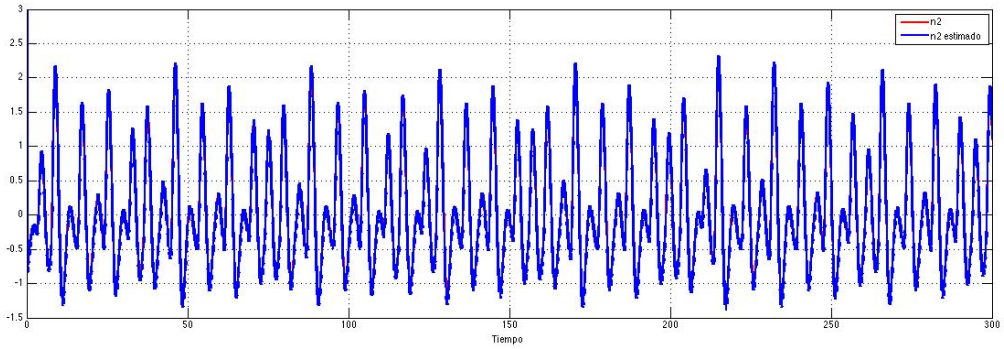

Figura 4.6. Estados n_2 y $\hat{n}_2$

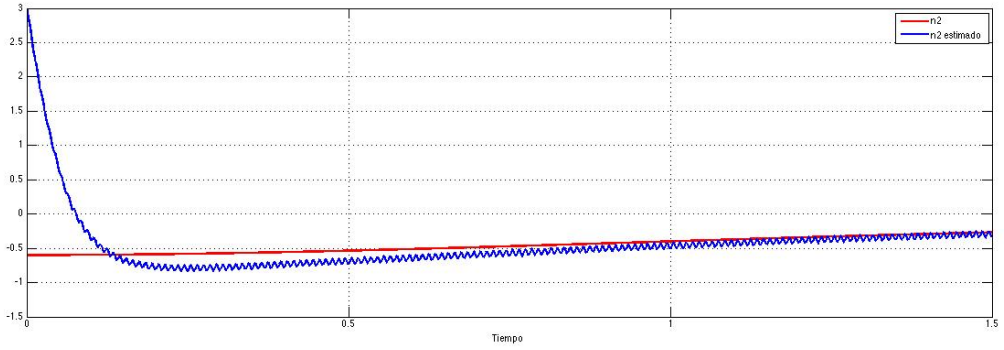

Figura 4.7. Convergencia de los estados n_2 y $\hat{n}_2$

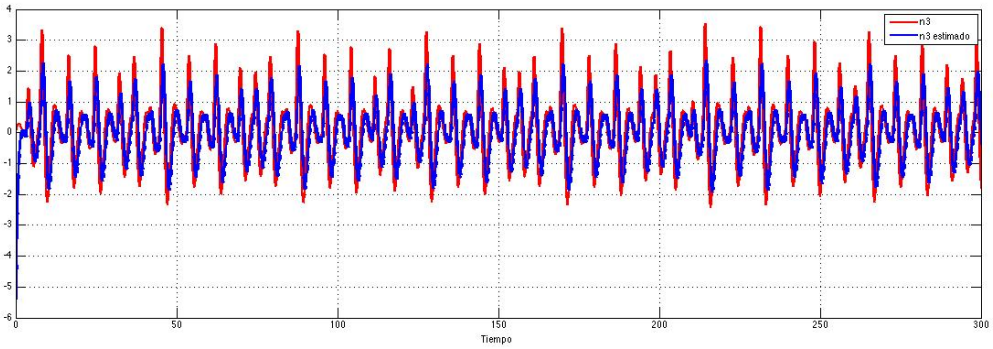

Figura 4.8. Estados n_3 y $\hat{n}_3$

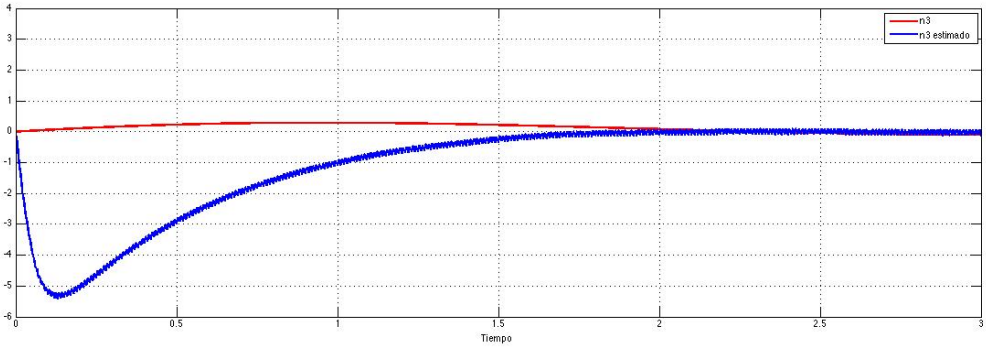

Figura 4.9. Convergencia de los estados n_3 y $\hat{n}_3$

Error de sincronización entre el transmisor y receptor:

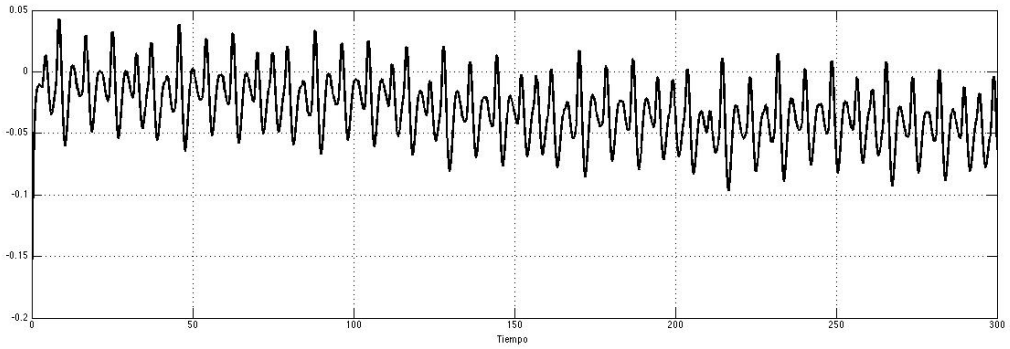

Figura 4.10. Diferencia entre los estados n_1 y $\hat{n}_1$

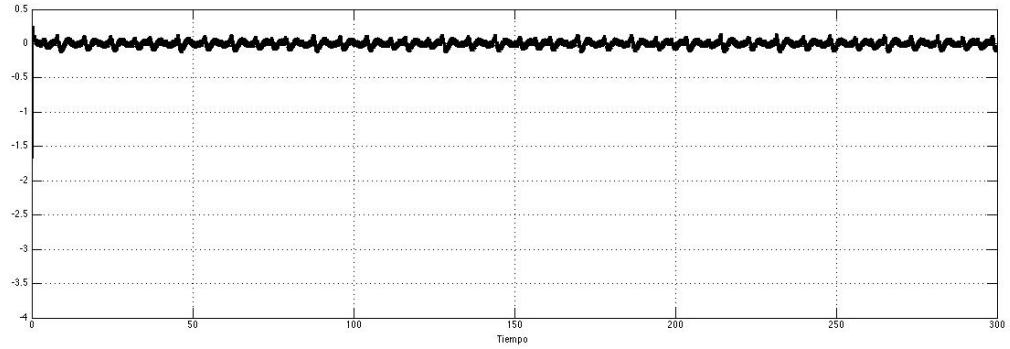

Figura 4.11. Diferencia entre los estados n_2 y $\hat{n}_2$

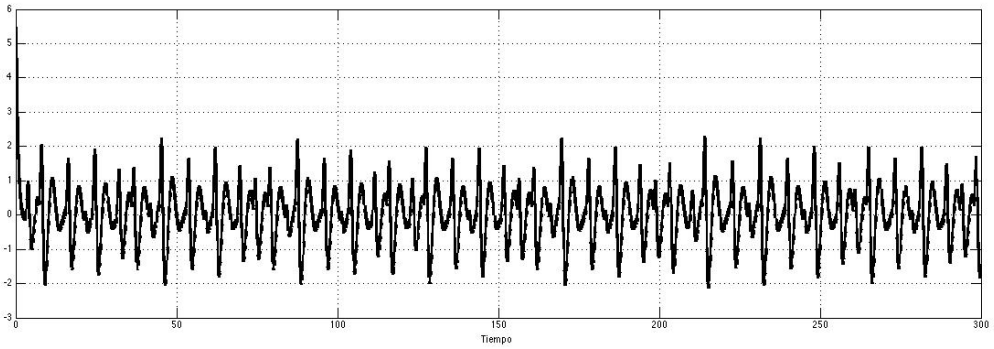

Figura 4.12. Diferencia entre los estados n_3 y $\hat{n}_3$

Salida que transporta el mensaje:

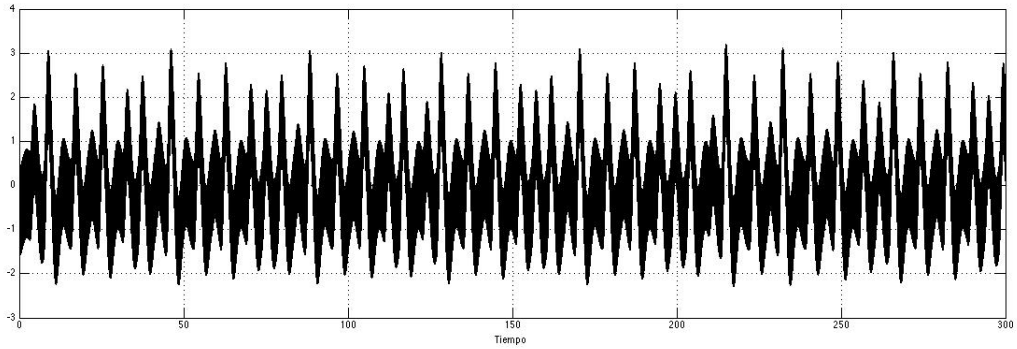

Figura 4.13. Salida y

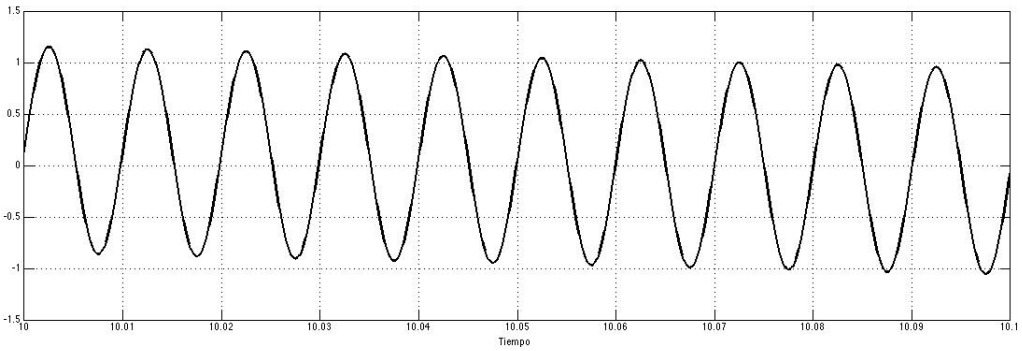

Figura 4.14. Acercamiento a la salida y

La sincronización entre el receptor y el transmisor toma menos de 1 segundo, es más rápido que el observador mostrado en el capítulo anterior y su error de recuperación del mensaje es menor.

4.4. Receptor-observador exponencial polinomial con filtro por modos deslizantes

El observador polinomial exponencial es un tipo de observador de Luenberger extendido, su característica principal es hacer que el error de sincronización decrezca más rápido que una cota exponencial, este observador no requiere que el transmisor este en alguna forma canónica, por eso será representado como un sistema no lineal en el que se puede separar la parte lineal y no lineal del sistema:

$$\begin{aligned} \dot{x} &= f(x,u) = Ax + \psi(x,u) \\ y &= Cx + s \end{aligned}$$

Donde $x \epsilon \mathbb{R}^n$ Son los estados del observador, A es la parte lineal del sistema, $\psi(x,u)$ la parte no lineal, y es la salida. Este observador por si solo no es robusto ante perturbaciones a la salida (como el mensaje que se utiliza en este capítulo). Una manera practica para

sobrevenir esta limitante es filtrar la señal que el observador recibe, la intención de aplicar un filtro previo es reducir los efectos del mensaje sobre la salida del transmisor, una vez que el filtro proporciona un estimado del estado que enmascara al mensaje, la salida filtrada es enviada al observador, el cual se encarga de reconstruir los estados del transmisor y finalmente reconstruir el mensaje. Las ecuaciones diferenciales que describen al observador y su filtro son:

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + \psi(\hat{x}, u) + \sum_{i=1}^{m} K_i (y_f - C\hat{x})^{2i-1} \\ \dot{y}_f &= k_f sign(y - y_f) \end{aligned}$$

Donde $\hat{x}\epsilon\mathbb{R}^n$ Son los estados del observador, y es la salida del transmisor, y_f es la salida del filtro por modos deslizantes, $\psi(\hat{x})$ es la parte no lineal del transmisor, $K_i\epsilon\mathbb{R}^n, 1 \leq i \leq m$ son los vectores de ganancias del receptor. Para demostrar la estabilidad del receptor las siguientes hipótesis son necesarias:

H4.5 La dinámica del transmisor es estable en el sentido de Lyapunov y es acotada de la siguiente forma:

$$\|\dot{x}\| < \delta, \delta > 0$$

H4.6 Para una $\varepsilon > 0$ y $A\epsilon\mathbb{R}^{nxn}$ existe una matriz $P = P^T > 0, P\epsilon\mathbb{R}^n$ que es solución de la ecuación:

$$A^T P + PA + L^2 P^2 + (1 + \varepsilon) I = 0$$

H4.7 La parte no lineal del transmisor $\psi(\hat{x}, u)$ satisface la condición:

$$2\hat{x}^T P\psi(\hat{x}, u) \leq L^2 \hat{x}^T P^2 \hat{x} + \hat{x}^T \hat{x}$$

H4.8 El mensaje es una señal acotada:

$$0 < |s| \leq \gamma < \infty$$

En la demostración de la estabilidad primero se prueba que el error entre la salida del transmisor sin mensaje $y = Cx$ y el estado estimado por el filtro x_f se mantiene acotada, después se demuestra la estabilidad del observador y que el error de recuperación del mensaje también se mantiene acotado y decrece más rápido que una cota exponencial.

4.4.1. Prueba de estabilidad

El filtro produce un aproximado del la salida del transmisor usada para enmascarar el mensaje, por facilidad se hace un cambio de variable a la salida del transmisor:

$$Cx = x_o$$

$$y_f = x_f$$

Se define el error de filtrado como:

$$e_f = x_o - x_f$$

Donde x_o es el estado usado para enmascarar la señal (en el oscilador de Colpitts x_2) y x_f es el estimado del estado. Se deriva el error:

$$\dot{e}_f = \dot{x}_o - \dot{x}_f = \dot{x}_o - k_f sign(e_f + s)$$

Considere un número real positivo α:

$$\begin{aligned} \dot{e}_f &= \dot{x}_o - k_f sign(e_f + s) + \alpha e_f - \alpha e_f \\ \dot{e}_f &= -\alpha e_f - k_f sign(e_f + s) + \dot{x}_o + \alpha e_f \end{aligned}$$

Definiendo el termino de incertidumbre $\Delta_f = \dot{x}_o + \alpha e_f$ y re escribiendo la derivada del error:

$$\dot{e}_f = -\alpha e_f - k_f sign(e_f + s) + \Delta_f$$

Se Usa la siguiente función de Lyapunov:

$$V_1 = \frac{1}{2} e_f^2$$

Derivando V_1:

$$\begin{aligned} \dot{V}_1 &= e_f \dot{e}_f = e_f \left(-\alpha e_f - k_f sign(e_f + s) + \Delta_f\right) \\ \dot{V}_1 &= -\alpha e_f^2 - k_f e_f sign(e_f + s) + e_f \Delta_f \end{aligned}$$

En vista de:

$$\begin{aligned} a sign(a+b) &= (a + b - b) sign(a+b) \\ &= (a+b) sign(a+b) - b sign(a+b) \\ &= |a+b| - b sign(a+b) \geq |a+b| - |b| \\ a sign(a+b) &\geq |a| - 2|b| \end{aligned}$$

Usando la desigualdad anterior: $e_f sign\left(e_f + s\right) \geq |e_o| - 2|s|$ y de **H4.5**:

$$\begin{aligned} \dot{V}_1 &\leq -\alpha e_f^2 - k_f \left(|e_f| - 2|s|\right) + e_f \Delta_f \\ \dot{V}_1 &\leq -\alpha e_f^2 - k_f |e_f| + 2k_f |s| + e_f \Delta_f \\ \dot{V}_1 &\leq -\alpha e_f^2 - k_f |e_f| + 2k_f |s| + e_f \left(\dot{x}_o + \alpha e_f\right) \\ \dot{V}_1 &\leq -\alpha e_f^2 - k_f |e_f| + 2k_f |s| + \delta e_f^2 + \alpha e_f^2 \\ \dot{V}_1 &\leq -\alpha e_f^2 - k_f |e_f| + 2k_f |s| + \delta |e_f| + \alpha |e_f| \\ \dot{V}_1 &\leq -\alpha e_f^2 - \left(k_f - \delta - \alpha\right) |e_f| + 2k_f |s| \end{aligned}$$

Con **H4.8** se define:

$$\begin{aligned} \rho(k) &= 2k_f |s| \geq 0 \\ \rho(k) &= 2k_f \gamma > 0 \end{aligned}$$

Dado que $|a|^2 = a^2$, teniendo en cuenta que $V_1 = \frac{1}{2}e^2$ y escogiendo $k_f > \delta + \alpha$:

$$\dot{V}_1 \leq -2\alpha V_1 - 2\left(k_f - \delta - \alpha\right)\sqrt{V_1} + \rho(k_f)$$

El resto de la demostración es similar a la del observador por Super-Twisting, la desigualdad anterior implica que:

$$\left[1 - \frac{\mu_f\left(k_f\right)}{V_1(e_f)}\right]_+ \to 0$$

Con:

$$\mu_f(k_f) = \left(\frac{\rho(k_f)}{\sqrt{k_f^2 + 2\rho(k_f)\alpha} + k_f}\right)$$

Por lo cual:

$$V_1(e_f) \leq \mu_f\left(k_f\right)$$

Implica que la norma del error de filtrado satisface la desigualdad:

$$\|e_f\|_P \leq \mu_f\left(k_f\right)$$

Esto significa que la diferencia entre el estado x_0 y el estimado x_f permanece acotada y tiende a $\mu_f\left(k_f\right)$, después de que el estado del filtro ha alcanzado a la salida del transmisor puede considerarse que $x_f = Cx$, así, es posible utilizar esta señal como entrada para el observador polinomial exponencial y que el observador no sea afectado por el mensaje sumado

a la salida. Ahora el observador puede reconstruir los demás estados del transmisor y de este modo recuperar el mensaje inmerso en la salida. Se define el error de sincronización:

$$e_o = x_f - C\hat{x} = Cx - C\hat{x}$$

Derivando el error de sincronización:

$$\dot{e}_o = \dot{x} - \dot{\hat{x}}$$

$$\dot{e}_o = Ax + \psi\left(x, u\right) - \left(A\hat{x} + \psi\left(\hat{x}, u\right) + \sum_{i=1}^{m} K_i \left(y - C\hat{x}\right)^{2i-1}\right)$$

Se agrupan términos:

$$\dot{e}_o = A\left(x - \hat{x}\right) + \left[\psi\left(x, u\right) - \psi\left(\hat{x}, u\right)\right] - \sum_{i=1}^{m} K_i C \left(x + s - \hat{x}\right)^{2i-1}$$

$$\dot{e}_o = A\left(e_o\right) + \phi(e_o) - \sum_{i=1}^{m} K_i C e_o^{2i-1}$$

Donde:

$$\phi(e_o) = \psi\left(x, u\right) - \psi\left(\hat{x}, u\right)$$

Teniendo en cuenta **H4.7** la parte no lineal $\phi(e_o)$ satisface:

$$2e_o^T P\phi(e_o) \leq L^2 e_o^T P^2 e_o + e_o^T e_o$$

Se usa la siguiente función candidata de Lyapunov:

$$V = e_o^T P e_o$$

Derivando:

$$
\begin{aligned}
\dot{V} &= \dot{e}_o^T P e_o + e_o^T P \dot{e}_o \\
\dot{V} &= \left[A(e_o) + \phi(e_o) - \sum_{i=1}^{m} K_i C e_o^{2i-1} \right]^T P e_o + e_o^T P \left[A(e_o) + \phi(e_o) - \sum_{i=1}^{m} K_i C e_o^{2i-1} \right] \\
\dot{V} &= e_o^T A^T P e_o + e_o^T P A e_o + 2 e_o^T P \phi(e_o) - 2 e_o^T P \sum_{i=1}^{m} K_i C e_o^{2i-1} \\
\dot{V} &\leq e_o^T A^T P e_o + e_o^T P A e_o + L^2 e_o^T P^2 e_o + e_o^T e_o - 2 e_o^T P \sum_{i=1}^{m} K_i C e_o^{2i-1} \\
\dot{V} &\leq e_o^T \left(A^T P + P A + L^2 P^2 + I \right) e_o - 2 e_o^T P \sum_{i=1}^{m} K_i C e_o^{2i-1}
\end{aligned}
$$

Considerando que se desea construir observadores de tercer orden o mayores ($m \geq 2$):

$$
\begin{aligned}
2 e_o^T P \sum_{i=1}^{m} K_i C e_o^{2i-1} &= 2 e_o^T P \left[K_1 C e_o + ... + K_m C e_o^{2m-1} \right] \\
2 e_o^T P \sum_{i=1}^{m} K_i C e_o^{2i-1} &= 2 e_o^T P K_1 C e_o + (C e_o)^2 \, 2 e_o^T P K_2 C e_o + (C e_o)^{2m-2} \, 2 e_o^T P K_m C e_o
\end{aligned}
$$

Se define $M_1 = P K_1 C$, $M_2 = P K_2 C$, ..., $M_m = P K_m C \geq 0$, como $e_o^T M_m e_o$ son números escalares $e_o^T M_m e_o = \left[e_o^T M_m e_o \right]^T$, entonces:

$$
\begin{aligned}
&(Ce)^0 \, e_o^T M_1 e_o + (C e_o)^0 \left(e_o^T M_1 e_o \right)^T + (C e_o)^2 \, e_o^T M_2 e_o + (C e_o)^2 \left(e_o^T M_1 e_o \right)^T + ... \\
&... + (C e_o)^{2m-2} \, e_o^T M_m e_o + (C e_o)^{2m-2} \left(e_o^T M_m e_o \right)^T = \sum_{i=1}^{m} (C e_o)^{2i-2} \, e_o^T \left(M_i + M_i^T \right) e_o
\end{aligned}
$$

Después:

$$\begin{aligned}\dot{V} &\leq e_o^T\left(A^TP+PA+L^2P^2+I\right)e_o-\sum_{i=1}^{m}(Ce)^{2i-2}\,e_o^T\left(M_i+M_i^T\right)e_o\\ \dot{V} &\leq e_o^T\left(A^TP+PA+L^2P^2+I\right)e_o\end{aligned}$$

A partir de **H4.6**:

$$A^TP+PA+L^2P^2+I\leq-\varepsilon I$$

$$\dot{V}\leq-\varepsilon\left\|e_o\right\|^2$$

Como $V=\|e_o\|^2$ a partir de la desigualdad de Rayleigh-Ritz : $\alpha\|e_o\|_P^2\leq V\leq\gamma\|e_o\|_P^2$, $\alpha=\lambda_{min}(P)$, $\gamma=\lambda_{max}(P)$, entonces:

$$\frac{d}{dt}\left\|e_o\right\|\leq-\frac{\varepsilon}{2\gamma}\left\|e_o\right\|$$

$$\left\|e_o(t)\right\|\leq\sqrt{\frac{\gamma}{\alpha}}\left\|e_o(0)\right\|exp\left(-\frac{\varepsilon}{2\gamma}t\right)$$

Haciendo $\xi=\sqrt{\frac{\gamma}{\alpha}}\|e_o(0)\|$ y $\lambda=\frac{\varepsilon}{2\gamma}t$:

$$\left\|e_o(t)\right\|\leq\xi exp\left(-\lambda t\right)$$

En vista de $\|e_o(t)\|=\|e_s(t)\|$ el error de recuperación del mensaje también decrece más rápido que la cota exponencial:

$$\left\|e_s(t)\right\|\leq\xi exp\left(-\lambda t\right)$$

De este modo el mensaje es recuperado y la norma del error de la estimación el mensaje se reduce conforme el tiempo pasa (la norma del error será tan pequeña como el castañeo inherente al filtro lo permita). Se ha demostrado que el filtro hace que el observador se

mantenga estable ante perturbaciones acotadas a la salida haciendo que puedan reconstruirse todos los estados y el mensaje.

4.4.2. Resultados numéricos

El mensaje es dado por la siguiente función del tiempo:

$$s = \sin(50\pi t)$$

Los parámetros del transmisor y receptor son los siguientes:

Parámetro	Valor
γ	2
b	0.8
d	0.6
a	30
$x_1(0)$	-2
$x_2(0)$	0.5
$x_3(0)$	0.5
k_f	10
k_1	$\begin{bmatrix} 0.16 & 16 & 0.8 \end{bmatrix}^T$
k_2	$\begin{bmatrix} 0.91 & 2.15 & 0 \end{bmatrix}^T$
$\hat{x}_1(0)$	0
$\hat{x}_2(0)$	-4
$\hat{x}_3(0)$	0.8

Los valores anteriores producen los siguientes resultados:

Mensaje estimado y el mensaje real después de la sincronización:

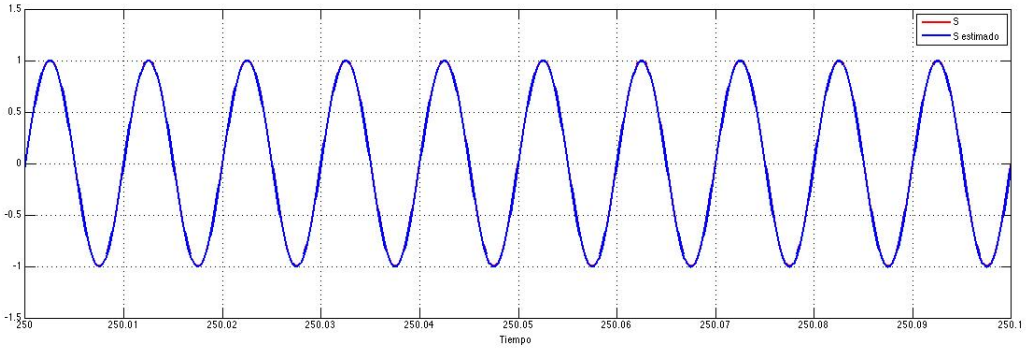

Figura 4.15. Mensaje y mensaje estimado

Convergencia del mensaje estimado al real:

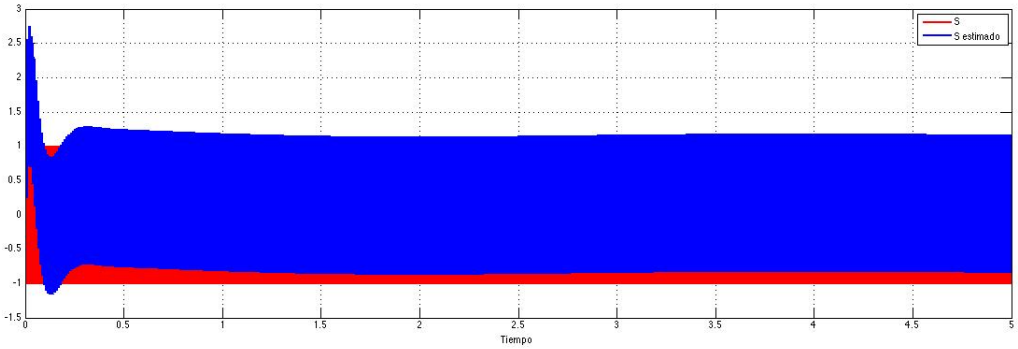

Figura 4.16. Convergencia del mensaje estimado al mensaje transmitido

El error de recuperación del mensaje es:

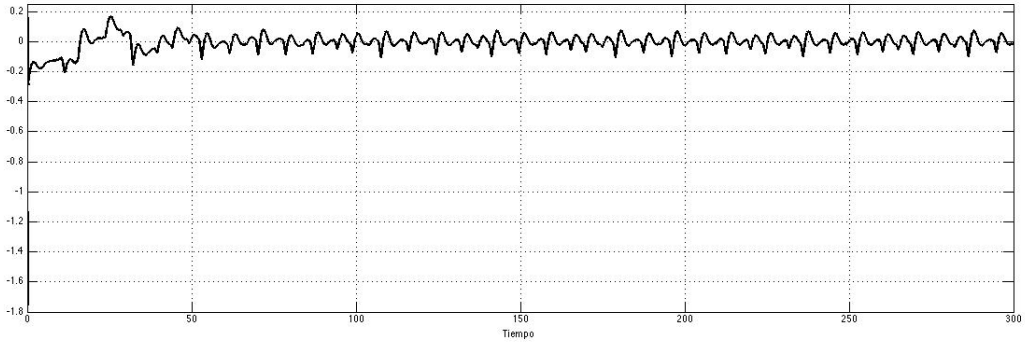

Figura 4.17. Error de recuperación del mensaje

Estados del transmisor y receptor:

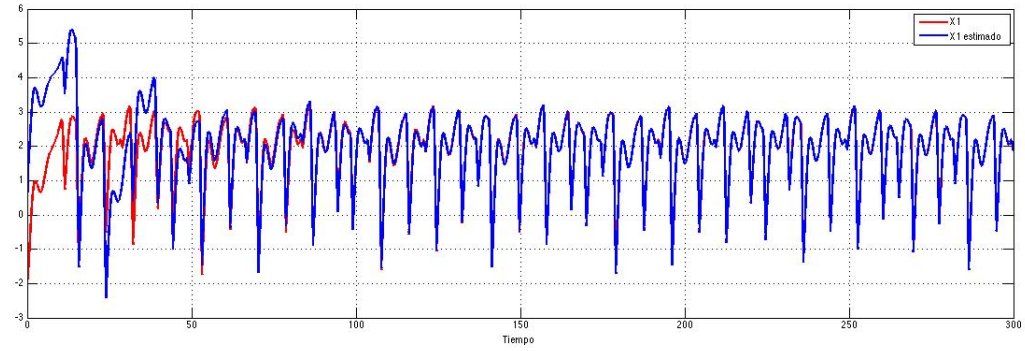

Figura 4.18. Estados x_1 y $\hat{x}_1$

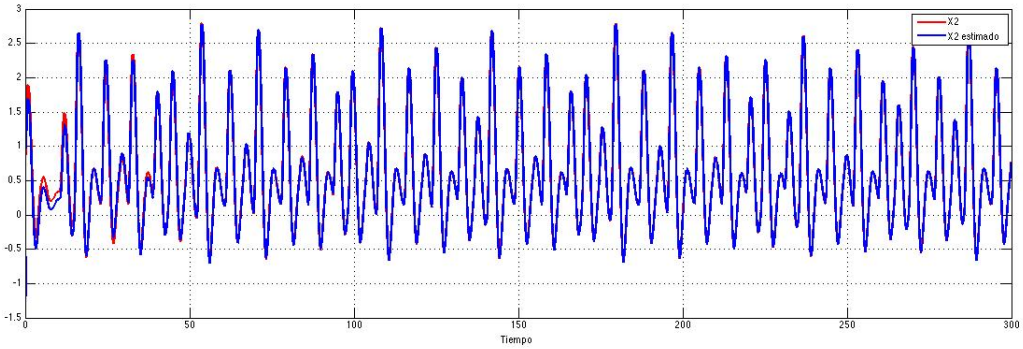

Figura 4.19. Estados x_2 y $\hat{x}_2$

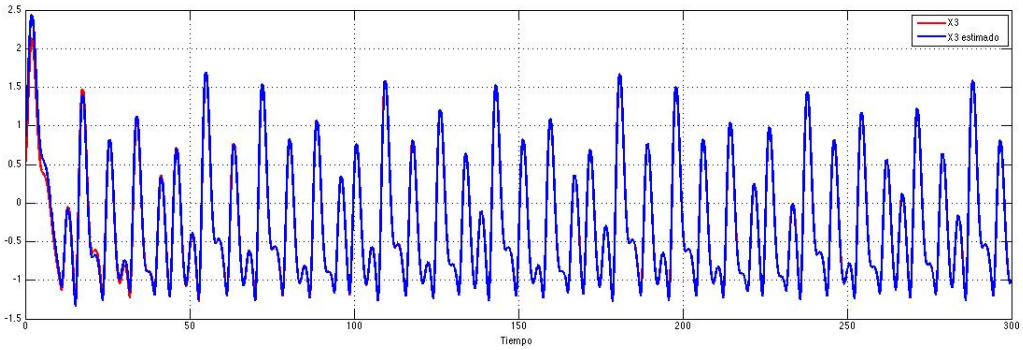

Figura 4.20. Estados x_3 y $\hat{x}_3$

Error de sincronización entre el transmisor y receptor:

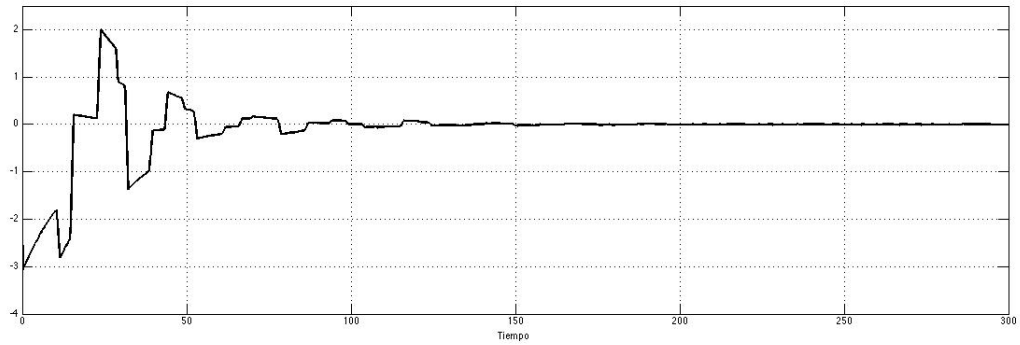

Figura 4.21. Diferencia entre los estados x_1 y $\hat{x}_1$

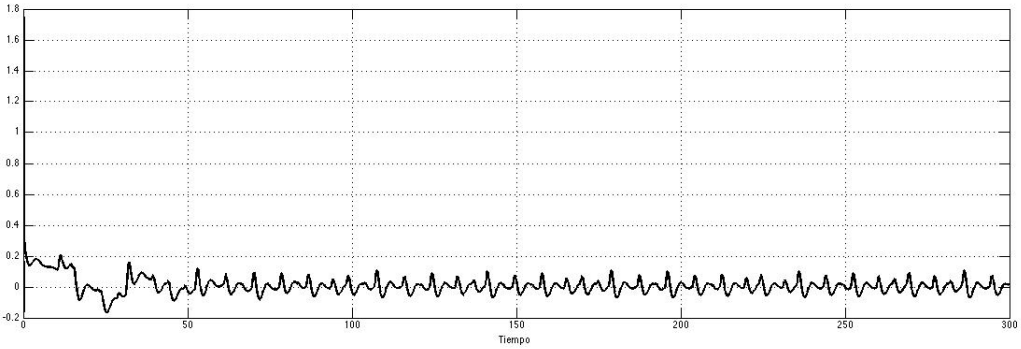

Figura 4.22. Diferencia entre los estados x_2 y $\hat{x}_2$

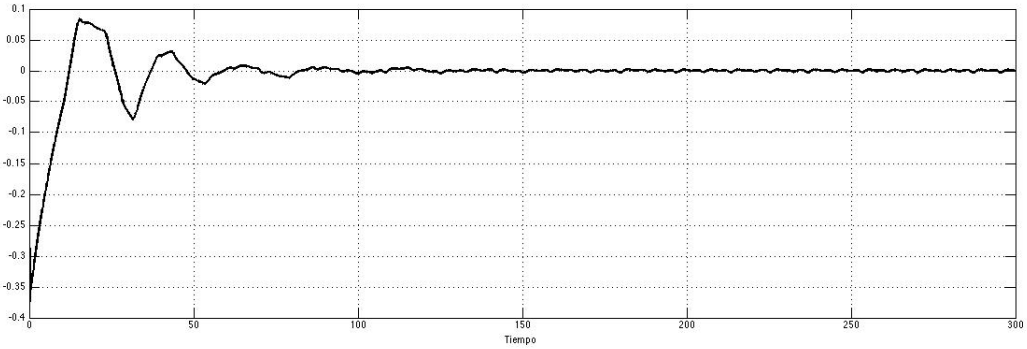

Figura 4.23. Diferencia entre los estados x_3 y $\hat{x}_3$

Salida que transporta el mensaje:

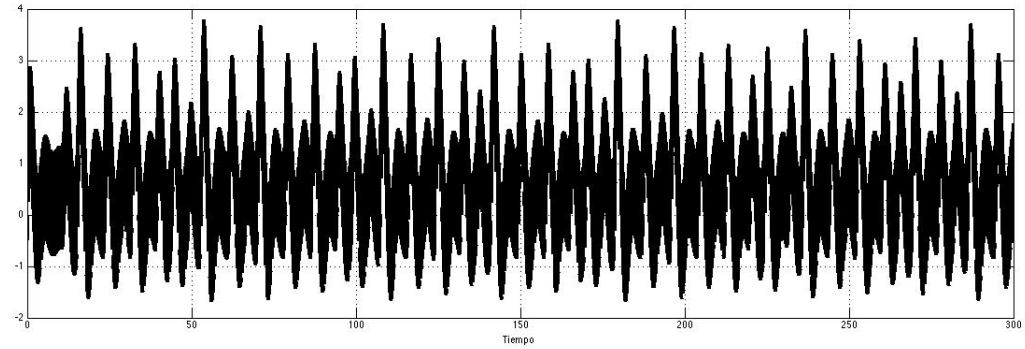

Figura 4.24. Salida y

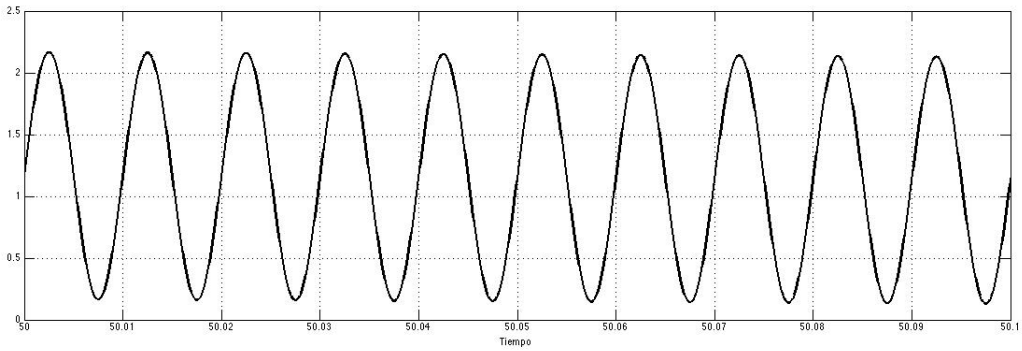

Figura 4.25. Acercamiento a la salida y

La sincronización entre el receptor y el transmisor tarda mas que los observadores anteriores (más de 50 segundos). Un efecto secundario del filtro por modos deslizantes es que el error de estimación del mensaje se mantiene oscilando alrededor de cero y es monotono y acotado, podría concluirse que al hacer que el observador sea robusto ante perturbaciones a la salida, se pierde la reducción constante del error que caracteriza a este observador.

4.5. Comentarios finales

Ambos observadores reconstruyeron exitosamente los estados del transmisor y el mensaje, aunque el transmisor no cumple la condición de observabilidad algebraica. El primer receptor se sincroniza mucho más rápido que el observador del capítulo tres e incluso más rápido que la combinación del observador polinomial exponencial y el filtro. Una ventaja más de este observador es que no necesita de una reconstrucción de la dinámica del transmisor, por lo tanto la estructura del transmisor permanece oculta de los usuarios. La desventaja del receptor basado en el algoritmo de Super-Twisting es que la reconstrucción del mensaje y los estados no es tan precisa a comparación de los otros observadores.

La combinación del observador polinomial exponencial y el filtro por modos deslizantes tiene un tiempo de sincronización mucho mayor a los demás observadores, pero las estimaciones de los estados y del mensaje son mucho más precisas, una contribución importante de este observador es el observador polinomial exponencial se mantiene estable ante perturbaciones

acotadas a la salida, si fuese utilizado por si solo no se mantendría estable y los estados estimados explotarían.

El mayor inconveniente de usar estos observadores como receptores es que el mensaje debe ser enmascarado con la salida, también la amplitud del mensaje debe ser mayor al castañeo propio de los modos deslizantes, pues de lo contrario no será posible separar el mensaje del castañeo y por ende no podrá ser recuperado, para comunicaciones seguras esto no es apropiado, pues al enmascarar un mensaje con amplitud similar a la de la señal usada para enmascararlo, hace que el mensaje sea visible dentro de esta señal, incluso a simple vista como es el caso de los resultados numéricos en este capítulo.

Capítulo 5

Comunicaciones seguras en sistemas Liouvillianos

5.1. Sistemas Liouvillianos

Los sistemas Liouvillianos son una clase de sistemas diferencialmente no planos que constituyen una extensión natural de los sistemas diferencialmente planos, un sistema diferencialmente no plano se dice Liouvilliano si los estados que no pueden ser escritos como una función en términos de la salida y sus derivadas en el tiempo, en cambio, pueden ser descritos como integrales de la salida o exponenciales de integrales de la salida y algunas de sus derivadas en el tiempo [1, 28].

Un sistema de Liouville es diferencialmente no plano y por lo tanto los estados que lo hacen ser Liouvilliano no cumplirán la condición de observabilidad algebraica [27], no obstante, estos estados pueden ser reconstruidos a través la ecuación formada por integrales de la salida y algunas derivadas en el tiempo, esta característica permite reconstruir estados sin la necesidad de un observador, incluso si no cumplen con la condición de observabilidad algebraica. Aplicar estos sistemas a comunicaciones seguras resulta ventajoso, ya que no es necesario implementar un observador de estados, también fortalece la seguridad del encriptamiento, pues en algunos casos no es necesario reconstruir la dinámica completa del transmisor haciendo que sea desconocida para los usuarios, por otra parte permiten reducir considerablemente los efectos del mensaje dentro de la señal que se usa para enmascararlos causando que sea difícil acceder al mensaje sin el receptor adecuado.

5.2. Sistemas Liouvillianos como transmisores de datos

En este capítulo se muestran dos métodos de encriptamiento y recuperación de mensajes totalmente distintos entre si, por lo mismo, también se presentan dos osciladores caóticos que cumplen las condiciones de ser Liouvillianos y cada uno corresponderá a un esquema de comunicaciones seguras. El primero es el oscilador de Colpitts del capítulo anterior, pero a diferencia del método de encriptamiento de ese capítulo, aquí el receptor necesita que el sistema tenga dos salidas; una con la que se sincroniza el receptor y otra que transporta el mensaje enmascarado. El segundo es el oscilador de Chua y su método de encriptamiento permite ocultar el mensaje dentro de la dinámica del oscilador, Ambos esquemas de comunicaciones hacen uso de las propiedades de los sistemas Liouvillianos para la reconstrucción del mensaje. para el primer método de enmascaramiento el transmisor es descrito por las siguientes ecuaciones dinámicas:

$$\begin{aligned} \dot{x} &= f(x,u) \\ y &= Cx \\ y_s &= x_L + As \end{aligned}$$

La salida y es usada para la sincronización del receptor y la salida y_s transporta y enmascara al mensaje s, x_L es un estado que hace al sistema ser de Liouville, $A > 0$ es una constante que reduce la amplitud del mensaje con la finalidad de que sea menos visible. El oscilador de Colpitts usado en el capítulo anterior puede ser usado para este método de encriptamiento ya que es un sistema Liouvilliano, si dinámica es la siguiente:

$$\begin{aligned} \dot{x}_1 &= x_2 - f(x_3) \\ \dot{x}_2 &= \gamma - x_1 - bx_2 - x_3 \\ \dot{x}_3 &= x_2 - d \\ y &= x_2 \end{aligned} \tag{5.1}$$

Donde:

$$f(x_3) = \begin{cases} -a(x_3+1) & x_3 < -1 \\ 0 & x_3 \geq -1 \end{cases}$$

El oscilador de Colpitts es un sistema de Liouville, las variables de estado que no cumplen con la condición de observabilidad algebraica pueden escribirse como una ecuación en términos de integrales de la salida, la entrada y algunas de sus derivadas:

$$\begin{aligned} x_1 &= \gamma - \dot{y} - by - \int (y-d)dt \\ x_2 &= y \\ x_3 &= \int (y-d)dt \end{aligned} \tag{5.2}$$

Para enmascarar el mensaje se elige el estado x_3, de modo que la salida que transporta el mensaje es:

$$y_s = x_3 + As$$

Las ecuaciones dinámicas que describen el transmisor son:

$$\begin{aligned} \dot{x}_1 &= x_2 - f(x_3) \\ \dot{x}_2 &= \gamma - x_1 - bx_2 - x_3 \\ \dot{x}_3 &= x_2 - d \\ y &= x_2 \\ y_s &= x_3 + As \\ f(x_3) &= \begin{cases} -a(x_3+1) & x_3 < -1 \\ 0 & x_3 \geq -1 \end{cases} \end{aligned} \tag{5.3}$$

Finalmente las señales y y y_s son transmitidas. El segundo método de encriptamiento es

similar al del capítulo 3, ya que. las propiedades de los sistemas de Liouville permiten ocultar mensajes dentro de la dinámica del sistema, pero a diferencia de los sistemas planos no será necesario derivar la señal de salida, otra ventaja, es que al igual que en el transmisor anterior la amplitud del mensaje puede ser reducida considerablemente haciendo que el mensaje sea menos visible dentro de la señal que lo transporta, el transmisor puede ser descrito por las siguientes ecuaciones dinámicas:

$$\begin{aligned} \dot{x} &= f(x,u) + CAs \\ y &= Cx \end{aligned}$$

A diferencia del capítulo 3 el transmisor debe enviar la derivada de la salida $\dot{y} = C\dot{x}$ para evitar la necesidad de derivar la señal. Para este esquema de comunicaciones propone que el transmisor sea un oscilador de Chua descrito por las siguientes ecuaciones diferenciales:

$$\begin{aligned} \dot{x}_1 &= C_1 \left[x_2 - x_1 - g\left(x_1\right) \right] \\ \dot{x}_2 &= C_2 \left(x_1 - x_2 + x_3 \right) \\ \dot{x}_3 &= -C_3 x_2 \\ y &= x_2 \end{aligned} \tag{5.4}$$

Con:

$$g(x) = M_1 x + \left(\frac{M_0 - M_1}{2} \right) \left(|x+1| - |x-1| \right)$$

Los estados x_1 y x_2 del oscilador pueden escribirse de la siguiente manera:

$$\begin{aligned} x_1 &= \frac{1}{C_2}\dot{y} + y - C_3 \int y dt \\ x_2 &= y \\ x_3 &= -C_3 \int y dt \end{aligned} \tag{5.5}$$

Por lo tanto el oscilador de Chua es Liouvilliano. El mensaje se enmascara añadiéndolo a la dinámica del transmisor:

$$\begin{aligned} \dot{x}_1 &= C_1 \left[x_2 - x_1 - g\left(x_1\right) \right] \\ \dot{x}_2 &= C_2 \left(x_1 - x_2 + x_3 \right) + As \\ \dot{x}_3 &= -C_3 x_2 \end{aligned}$$

Donde A es una ganancia que hace la amplitud del mensaje s muy pequeña, al escoger A mucho menor a la amplitud máxima de los estados del transmisor, la amplitud del mensaje es reducida, la seguridad del mensaje se beneficia de esto, pues discernir cambios tan pequeños dentro de la señal de salida es muy difícil. El transmisor emitirá la derivada de la salida:

$$\dot{y} = C_2 \left(x_1 - x_2 + x_3 \right) + As$$

Así el mensaje con amplitud reducida por A es enmascarado por los tres estados del transmisor.

5.3. Receptor usando la propiedad de los sistemas de Liouville

Este receptor se diseña para el primer transmisor (oscilador de Colpitts) y se basa en las propiedad que hace al sistema ser Liouvilliano, como el mensaje se encuentra inmerso en la salida y_s y el estado que enmascara el mensaje x_L hace que el sistema sea Liouvilliano, el estado x_L puede ser reconstruido y el mensaje recuperado mediante las siguientes ecuaciones dependientes de las salidas y y y_s del oscilador:

$$\begin{aligned} \hat{x}_3 &= \int (y - d) dt \\ \hat{s} &= \frac{1}{A} \left(y_s - \hat{x}_3 \right) \end{aligned}$$

El estado $\hat{x}_3$ es el estimado de $x_L = x_3$ y $\hat{s}$ es el estimado del mensaje s. Si el estado

estimado $\hat{x}_L$ es igual al estado del transmisor x_L el mensaje recuperado $\hat{s}$ es igual al mensaje transmitido s. teniendo en cuenta (5) el estado x_L puede ser expresado de la siguiente manera:

$$x_L = x_3 = \int (y - d)dt$$

El estado reconstruido $\hat{x}_L$ es:

$$\hat{x}_L = \hat{x}_3 = \int (y - d)dt$$

Considerando que el mensaje se encuentra inmerso en la salida y_s:

$$y_s = x_L + As = x_3 + As$$

Sustituyendo la salida y_s en el mensaje recuperado:

$$\begin{aligned} \hat{s} &= \frac{1}{A}\left[x_L + As - \int (y - d)dt\right] \\ \hat{s} &= \frac{1}{A}\left(x_L + As - x_L\right) \\ \hat{s} &= s \end{aligned}$$

El mensaje recuperado es igual al mensaje transmitido y el error en la recuperación del mensaje se define como:

$$e_s = s - \hat{s} = 0$$

Este receptor es muy sensible a las condiciones iniciales, estas deben ser iguales tanto en el transmisor como en el receptor, de otro modo el error en la recuperación del mensaje será distinto de cero. La sensibilidad a condiciones iniciales es una ventaja ya que la llave de encriptamiento se forma a partir de estas, los valores que puede tomar la llave comprenden todas las condiciones iniciales que generen comportamiento caótico en el oscilador.

5.3.1. Resultados numéricos

El mensaje es la siguiente función del tiempo:

$$s = \sin(50\pi t)$$

Los parámetros del transmisor y receptor son los siguientes:

Parámetro	Valor
γ	2
b	0.8
d	0.6
a	30
$x_1(0)$	-2
$x_2(0)$	0.5
$x_3(0)$	0.5
$\hat{x}_3(0)$	0.5
A	10^{-12}

Se obtienen los siguientes resultados:

El mensaje transmitido y el recuperado son idénticos en todo momento

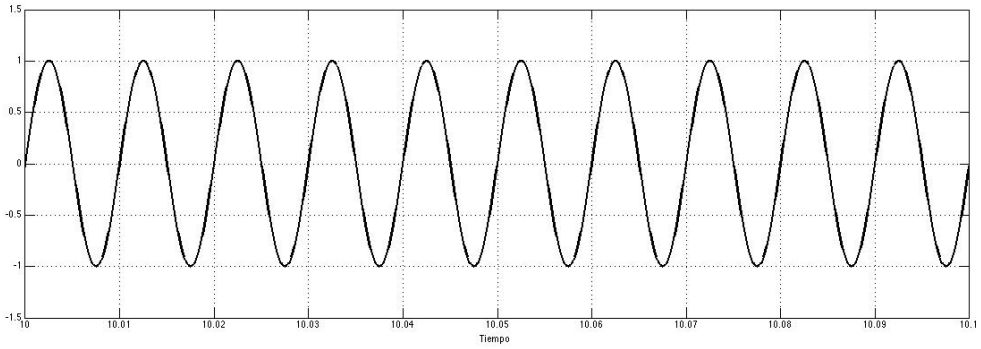

Figura 5.1. Mensaje y mensaje recuperado

El error de recuperación del mensaje es cero:

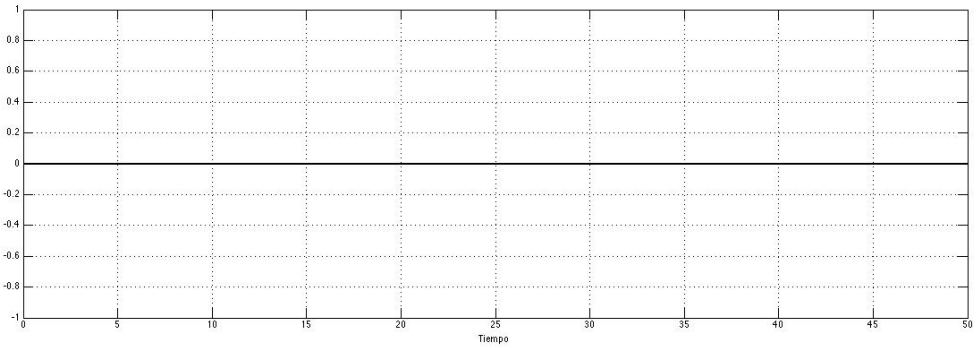

Figura 5.2. Error de recuperación del mensaje

Estado estimado:

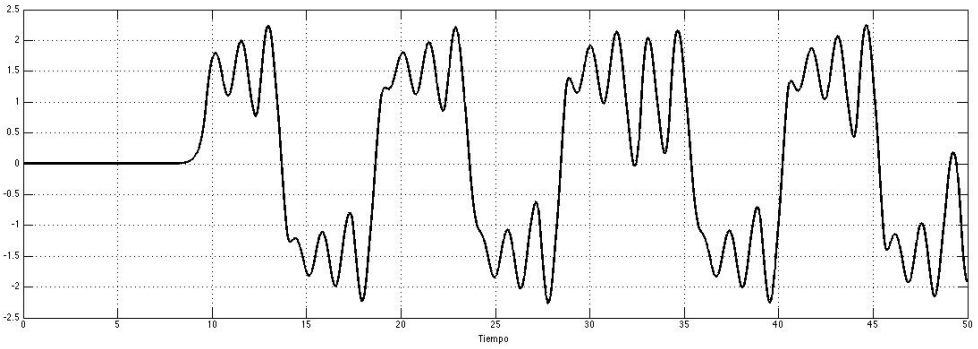

Figura 5.3. Estados x_1 y $\hat{x}_1$

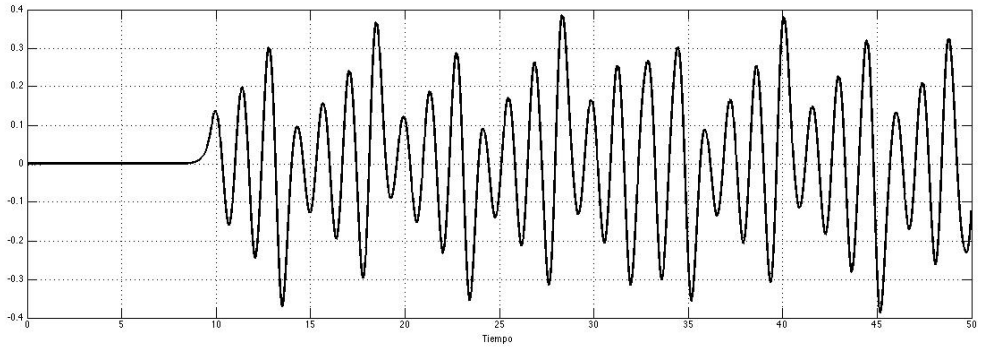

Figura 5.4. Estados x_2 y $\hat{x}_2$

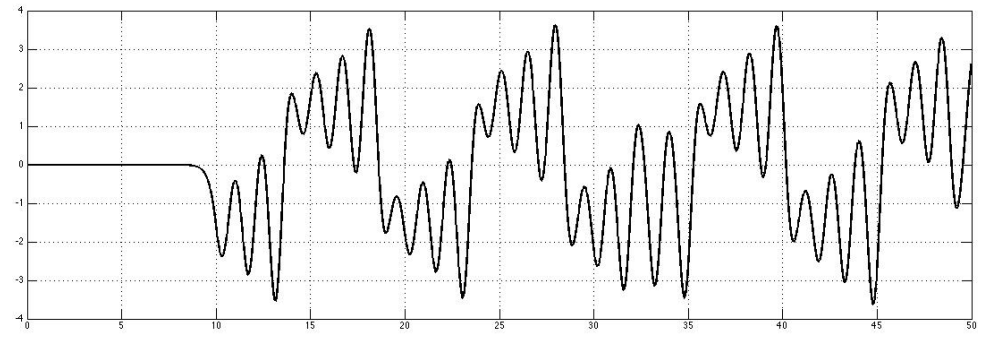

Figura 5.5. Estados x_3 y $\hat{x}_3$

El error de sincronización entre el transmisor y receptor es:

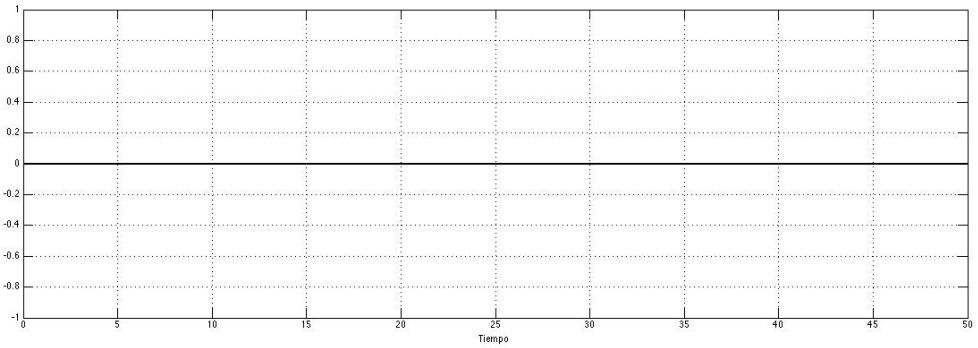

Figura 5.6. Diferencia entre los estados x_1 y $\hat{x}_1$

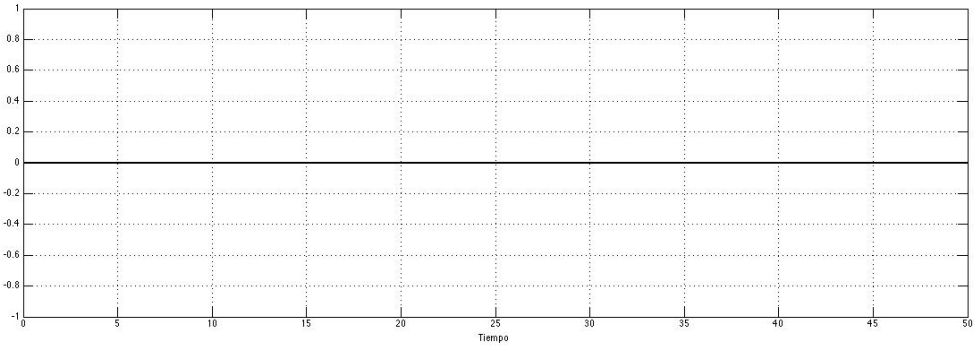

Figura 5.7. Diferencia entre los estados x_2 y $\hat{x}_2$

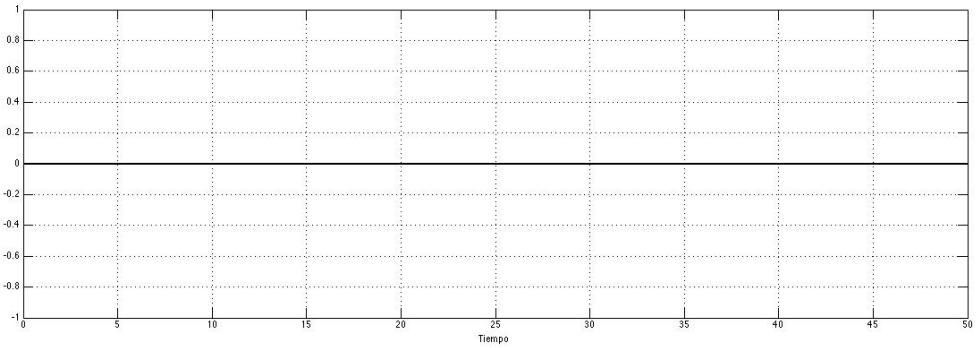

Figura 5.8. Diferencia entre los estados x_3 y $\hat{x}_3$

Salida que transporta el mensaje:

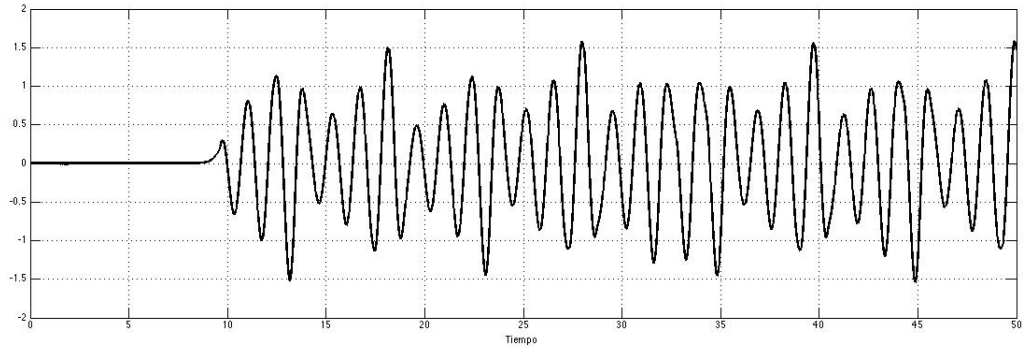

Figura 5.9. Salida y

El mensaje y el estado del transmisor x_L son reconstruidos sin error, dado que el valor A reduce la amplitud del mensaje, este permanece oculto dentro de la señal que lo transporta.

5.4. Receptor que usa la derivada de la salida

Este receptor corresponde al segundo transmisor (oscilador de Chua). La principal característica de los sistemas Liouvillianos permite que algunos de sus estados sean reconstruidos a partir de su salida y sin necesidad de usar observadores de estados, los receptores de datos

pueden diseñarse para tomar ventaja de esto para que las ecuaciones que los describen sean más pequeñas y simples que un observador. Teniendo en cuenta (5.5) es posible reconstruir los estados del transmisor sin recurrir a observadores de estados. El diseño del receptor toma ventaja de esta característica para simplificar su dinámica, basar el receptor únicamente (5.5) hace necesario conocer el mensaje pues:

$$\begin{aligned} \hat{x}_1 &= \frac{1}{C_2}\left(\dot{y} - As\right) + y - C_3 \int y dt \\ \hat{x}_2 &= y \\ \hat{x}_3 &= -C_3 \int y dt \end{aligned}$$

Para evitar la restricción mencionada el estado del receptor $\hat{x}_1$ se obtiene a partir de (5.4):

$$\begin{aligned} \dot{\hat{x}}_1 &= C_1\left[\hat{x}_2 - \hat{x}_1 - g\left(\hat{x}_1\right)\right] \\ \hat{x}_2 &= y \qquad (5.6) \\ \hat{x}_3 &= -C_3 \int y dt \\ \hat{s} &= \frac{\dot{y} - C_2\left(\hat{x}_1 - \hat{x}_2 + \hat{x}_3\right)}{K} \qquad (5.7) \end{aligned}$$

Donde $\hat{s}$ es el mensaje reconstruido. Una de las propiedades más importantes de este tipo de receptor es que no existe un periodo de espera para que el mensaje estimado converja al mensaje transmitido, es decir, el mensaje estimado siempre es igual al mensaje transmitido lo que implica que el error de recuperación del mensaje es cero en todo momento. El error en la recuperación del mensaje se define como:

$$e_s = s - \hat{s}$$

Sustituyendo (5.7)

$$e_s = s - \frac{\dot{y} - C_2\left(\hat{x}_1 - \hat{x}_2 + \hat{x}_3\right)}{A}$$

Y tendiendo en cuenta:

$$\dot{x}_2 = C_2 \left(x_1 - x_2 + x_3 \right) + As$$

Despejando la igualdad anterior:

$$s = \frac{\dot{x}_2 - C_2 \left(x_1 - x_2 + x_3 \right)}{A}$$

Sustituyendo en el error:

$$e_s = \frac{\dot{x}_2 - C_2 \left(x_1 - x_2 + x_3 \right)}{A} - \frac{\dot{y} - C_2 \left(\hat{x}_1 - \hat{x}_2 + \hat{x}_3 \right)}{A}$$

Ya que las condiciones iniciales del receptor y transmisor son las mismas

$$e_s = \frac{\dot{y} - C_2 \left(x_1 - y - C_3 \int y dt \right)}{A} - \frac{\dot{y} - C_2 \left(x_1 - y - C_3 \int y dt \right)}{A}$$

$$e_s = 0$$

El error de recuperación del mensaje es cero en todo momento. Al igual que el receptor anterior, este es muy sensible a las condiciones iniciales, un pequeño cambio en estas hace que el estimado del mensaje sea totalmente distinto al mensaje oculto en la dinámica del transmisor, la llave de encriptamiento puede construirse en base a estas condiciones iniciales mejorando la seguridad del encriptamiento.

5.4.1. Resultados numéricos

El mensaje es dado por la ecuación:

$$s = \sin(50\pi t)$$

Los parámetros del transmisor y receptor son los siguientes:

Parámetro	Valor
C_1	15.6
C_2	1
C_3	28
M_0	-1.143
M_1	-0.714
$x_1(0)$	0
$x_2(0)$	0
$x_3(0)$	0
$\hat{x}_1(0)$	0
$\hat{x}_2(0)$	0
$\hat{x}_3(0)$	0
A	10^{-12}

Con estos valores se consiguen los siguientes resultados:

El mensaje transmitido y el recuperado son muy parecidos:

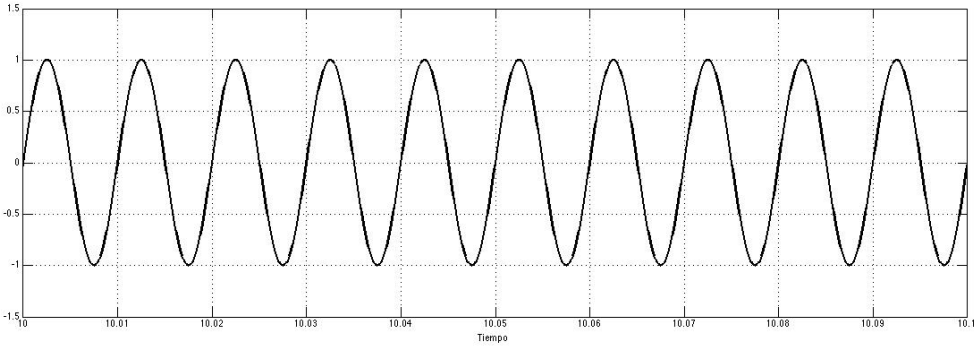

Figura 5.10. Mensaje y mensaje recuperado

El error de recuperación del mensaje es cero:

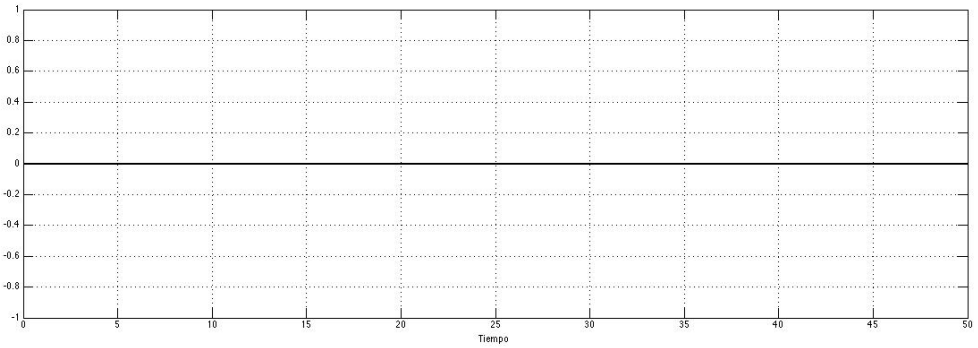

Figura 5.11. Error de recuperación del mensaje

Los estados estimados por el receptor y los estados del transmisor son:

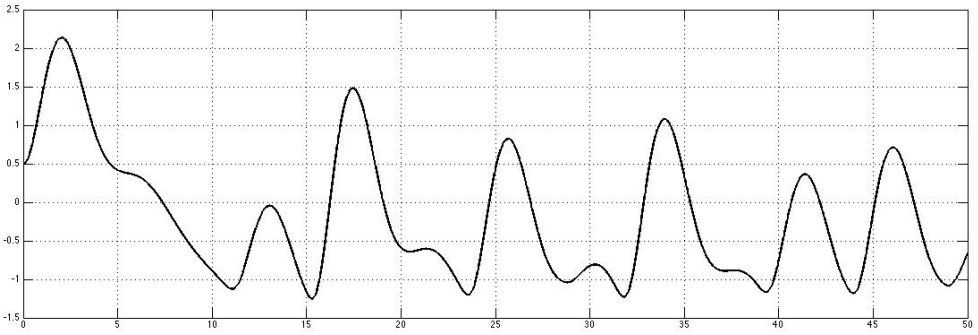

Figura 5.12. Estados x_1 y $\hat{x}_1$

El error de sincronización entre los estados del transmisor y los del receptor es:

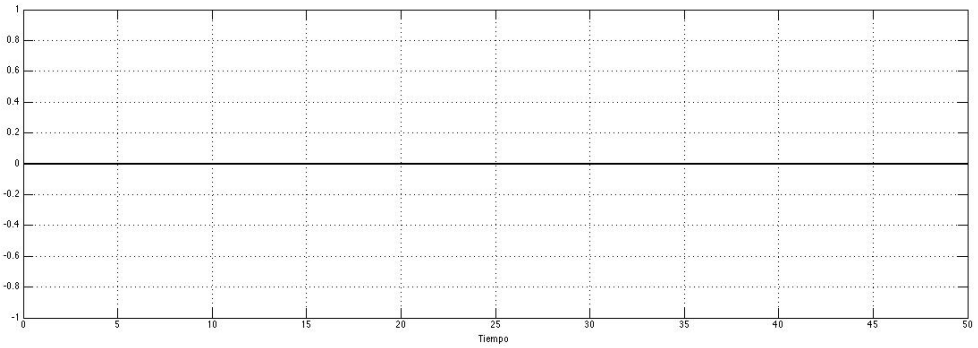

Figura 5.13. Diferencia entre los estados x_1 y $\hat{x}_1$

Salida que transporta el mensaje:

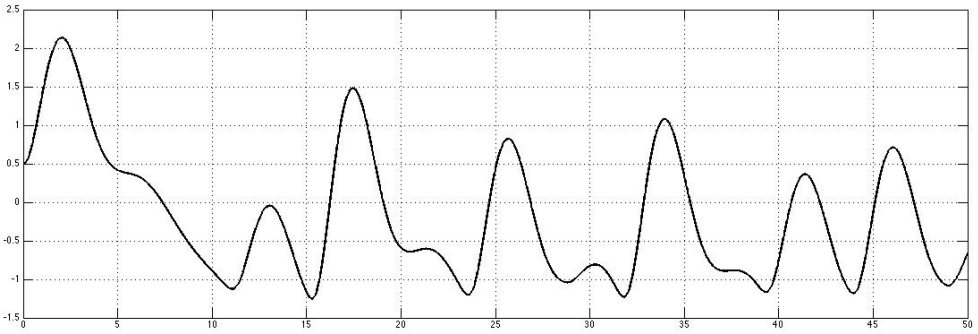

Figura 5.14. Salida y

5.5. Comentarios finales

Los métodos de encriptamiento presentados en este capítulo requieren que las condiciones iniciales del transmisor y receptor sean idénticas, de no serlo el error en la estimación del mensaje será distinto de cero y a causa del valor A la diferencia entre el mensaje estimado y el real será muy grande incluso si las condiciones iniciales son muy cercanas, sin embargo,

el estimado de los estados no es afectado de la misma forma, pues si las condiciones iniciales son cercanas, el error de sincronización entre los estados será pequeño por que no es afectado por A. Estas característica son de gran utilidad para aumentar la seguridad del mensaje al emplearlas como llave de encriptamiento en conjunto con el valor A.

Es importante mencionar que la sincronización entre el receptor y el transmisor ocurre inmediatamente, por lo tanto se puede transmitir el mensaje en el momento que se desee, también, el receptor no es una reconstrucción completa de la dinámica del transmisor, con lo cual, el usuario del receptor no necesita conocer la dinámica completa del transmisor para recuperar el mensaje, entonces, tanto la llave de encriptamiento como la dinámica del transmisor permanecen fuera del conocimiento del usuario. Los esquemas de comunicaciones seguras de este capítulo son un encriptamiento completo, debido a que poseen una llave de encriptamiento y a diferencia de los esquemas anteriores que solo eran enmascaramiento de datos, presentan ventaja en cuanto a la seguridad del mensaje, puesto que si el usuario desconoce la llave o no tiene el valor exacto de las condiciones iniciales la recuperación del mensaje no será exitosa.

Cabe remarcar que construir este tipo de receptores solo es posible si el transmisor es un sistema de Liouville y a diferencial de los observadores del capítulo cuatro, estos receptores pueden transmitir mensajes de amplitud muy pequeña, teoricamente el valor A puede ser tan pequeño como se desee, pero, en la realidad estará limitado por el ruido propio del canal de transmisión, es por esto que debe ser mayor al ruido para que el mensaje no se pierda.

Capítulo 6

Conclusiones y trabajo futuro

6.1. Conclusiones

En esta tesis se expusieron diversos esquemas de comunicación segura de datos utilizando sistemas diferencialmente planos, sistemas diferencialmente no planos y sistemas Liouvillianos como transmisores. En el capítulo tres se presentan los sistemas diferencialmente planos como transmisores de datos y se diseñan dos receptores a partir de sus características, el desempeño de ambos receptores es diferente ya que son totalmente distintos, el primero es un observador y el segundo una reconstrucción de la dinámica del transmisor, ambos produjeron reconstrucciones del mensaje, sin embargo la seguridad que estos esquemas de comunicación brindan a los datos no es la ideal, pues no es posible generar una llave de encriptamiento causando que la seguridad del mensaje dependa únicamente del enmascaramiento caótico.

En el capítulo cuatro se trabaja con sistemas diferencialmente no planos, estos sistemas representan un reto, ya que no cumplen con la condición de observabilidad algebraica y sus estados no pueden ser reconstruidos en base a derivadas o integrales de su salida (considerando que el sistema no sea de Liouville), estas restricciones impuestas por la naturaleza de los sistemas diferencialmente no planos nos obligan a ocultar el mensaje dentro de la salida del sistema y a tratarlo como una perturbación acotada a la salida, por lo mismo, los receptores son diseñados como observadores robustos ante este tipo de perturbación. Ambos receptores produjeron estimados del mensaje, pero, de manera similar al observador del capítulo tres la seguridad únicamente depende del enmascaramiento caótico, pues no es posible formar una llave de encriptamiento con las condiciones iniciales o ganancias. Cabe mencionar que una

aportación interesante en este capítulo es haber hecho al observador polinomial exponencial robusto ante perturbaciones acotadas a la salida (con el uso del filtro por modos deslizantes).

Finalmente en el capítulo cinco se presentan los sistemas de Liouville, que a pesar de ser diferencialmente no planos, permiten reconstruir algunos estados a partir de integrales de la salida, esta característica resulta útil y permite hacer un encriptamiento completo consistente de enmascaramiento caótico y llave de encriptamiento, ademas, el mensaje no es visible en la salida que lo transporta y el receptor no es una reconstrucción completa o igual del transmisor, todas estas propiedades resultan benéficas para la seguridad de los datos y se puede concluir que desde la perspectiva de comunicaciones seguras que los conjuntos de transmisor y receptor de este capítulo proporcionan mayor seguridad a los datos transmitidos que los mostrados en capítulos anteriores.

El utilizar observadores de estados para enmascaramiento caótico afecta la seguridad del mensaje, pues, los observadores están diseñados para que el error de sincronización al menos permanezca acotado y de preferencia tienda a cero sin importar la diferencia entre las condiciones iniciales del transmisor y receptor, usualmente la llave de encriptamiento se forma a partir de las condiciones iniciales del receptor y emplear un observador como receptor causa que una pequeña variación en la llave no tenga ningún efecto sobre la convergencia del mensaje estimado al mensaje real, incluso si la llave es incorrecta. Este inconveniente no se encuentra presente en los receptores desarrollados en el capítulo cinco, por esto proporcionan mucha mayor seguridad para los datos transmitidos a pesar de que su desarrollo es mucho mas sencillo.

6.2. Trabajo futuro

Durante la revisión bibliográfica para la elaboración de esta tesis se encontraron pocos artículos en los que se haga encriptamiento con sistemas en tiempo discreto [31, 32, 33], se encontró un menor numero de trabajos sobre sistemas de Liouville con salidas muestreadas [20] o sistemas de orden fraccional en tiempo discreto y no se encontró ninguna aplicación de estos a comunicaciones seguras, es por esto que se desea explorar las posibles aplicaciones de estos sistemas a las comunicaciones seguras.

Apéndice

Durante la elaboración de este trabajo se redactaron los siguientes artículos:

- Juan J. Montesinos-García, Rafael Martinez-Guerra, Sergio M. Delfín prieto, Sistemas caóticos Liouvillianos en comunicaciones seguras, Congreso nacional de control automático 2015 (Sometido).
- Juan J. Montesinos-García, Juan C. Cruz-Victoria, Rafael Martinez-Guerra, Sobre las ventajas de los sistemas de Liouville en las comunicaciones seguras, Congreso nacional de control automático 2015 (Sometido).
- Juan J. Montesinos-García, Juan C. Cruz-Victoria, Rafael Martinez-Guerra, Synchronization of Julia and Mandelbrot sets via geometric convergence feedback, International Journal of bifurcation and chaos (Sometido).

Bibliografía

[1] Martínez-Guerra, R., Gómez-Cortés, G. C., & Pérez-Pinacho, C. A. (2015). Synchronization of Integral and Fractional Order Chaotic Systems: A Differential Algebraic and Differential Geometric Approach With Selected Applications in Real-Time. Springer.

[2] Martinez-Guerra, R., & Mata-Machuca, J. L. (2013). Fault Detection and Diagnosis in Nonlinear Systems: A Differential and Algebraic Viewpoint. Springer.

[3] Martinez-Guerra, R., & Yu, W. (2008). Chaotic synchronization and secure communication via sliding-mode observer. International Journal of Bifurcation and Chaos, 18(01), 235-243.

[4] Martínez-Guerra, R., Cruz-Victoria, J. C., Gonzalez-Galan, R., & Aguilar-Lopez, R. (2006). A new reduced-order observer design for the synchronization of Lorenz systems. Chaos, Solitons & Fractals, 28(2), 511-517.

[5] Martinez-Guerra, R., & Mendoza-Camargo, J. (2004). Observers for a class of Liouvillian and, non-differentially flat systems. IMA Journal of Mathematical Control and Information, 21(4), 493-509.

[6] Martinez-Guerra, R.; Mata-Machuca, J.L., "An observer for the synchronization of chaotic Liouvillian systems: A real-time application to Chua's oscillator," 2012 IEEE 51st Annual Conference on Decision and Control (CDC), vol., no., pp.4071,4076, 10-13 Dec. 2012.

[7] Martínez-Guerra, R., Corona-Fortunio, D. M., & Mata-Machuca, J. L. (2013). Synchronization of chaotic Liouvillian systems: an application to Chua's oscillator. Applied Mathematics and Computation, 219(23), 10934-10944.

[8] Yang, T., & Chua, L. O. (1997). Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 44(10), 976-988.

[9] Liao, T. L., & Huang, N. S. (1999). An observer-based approach for chaotic synchronization

with applications to secure communications. IEEE Transactions on circuits and Systems I: Fundamental Theory and Applications, 46(9), 1144-1150.

[10] Mata-Machuca, J. L., Martínez-Guerra, R., Aguilar-López, R., & Aguilar-Ibañez, C. (2012). A chaotic system in synchronization and secure communications. Communications in Nonlinear Science and Numerical Simulation, 17(4), 1706-1713.

[11] Halle, K. S., Wu, C. W., Itoh, M., & Chua, L. O. (1993). Spread spectrum communication through modulation of chaos. International Journal of Bifurcation and Chaos, 3(02), 469-477.

[12] Dedieu, H., Kennedy, M. P., & Hasler, M. (1993). Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. Circuits and systems II: Analog and digital signal processing, IEEE Transactions on, 40(10), 634-642.

[13] Sobhy, M. I., & Shehata, A. E. (2001, May). Chaotic algorithms for data encryption. In icassp (pp. 997-1000). IEEE.

[14] Pecora, L. M., & Carroll, T. L. (1990). Synchronization in chaotic systems. Physical review letters, 64(8), 821.

[15] Afraimovich, V. S., Verichev, N. N., & Rabinovich, M. I. (1986). Stochastic synchronization of oscillation in dissipative systems. Radiophysics and Quantum Electronics, 29(9), 795-803.

[16] Pikovsky, A., Rosenblum, M., & Kurths, J. (2003). Synchronization: a universal concept in nonlinear sciences (Vol. 12). Cambridge university press.

[17] Fujisaka, H., & Yamada, T. (1983). Stability theory of synchronized motion in coupled-oscillator systems. Progress of Theoretical Physics, 69(1), 32-47.

[18] Lynnyk, V. (2006, December). Observer-based chaos synchronization in the generalized chaotic Lorenz systems and its application to secure encryption. 45th IEEE Conference on In Decision and Control, 2006 (pp. 3783-3788).

[19] Chen, M., Zhou, D., & Shang, Y. (2005). A sliding mode observer based secure communication scheme. Chaos, Solitons & Fractals, 25(3), 573-578.

[20] Aguilar-López, R., & Martínez-Guerra, R. (2006). Discrete algebraic estimator design for non-linear Liouvillian systems with sampled output: Application to a class of stirred bioreactor. Chemical Engineering Journal, 118(1), 23-28.

[21] Chartrand, R. (2011). Numerical differentiation of noisy, nonsmooth data. ISRN Applied Mathematics, 2011.

[22] Aguilar-López, R., & Martínez-Guerra, R. (2008). Synchronization of a class of chaotic signals via robust observer design. Chaos, Solitons & Fractals, 37(2), 581-587.

[23] Mata-Machuca, J. L., & Martínez-Guerra, R. (2012). Asymptotic synchronization of the Colpitts oscillator. Computers & Mathematics with Applications, 63(6), 1072-1078.

[24] Banerjee, S. (Ed.). (2010). Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption: Applications for Encryption. IGI Global.

[25] Aguilar-López, R., & Martinez-Guerra, R. (2007). Partial synchronization of different chaotic oscillators using robust PID feedback. Chaos, Solitons & Fractals, 33(2), 572-581.

[26] Fliess, M., Lévine, J., Martin, P., & Rouchon, P. (1992). On differentially flat nonlinearsystems. In Symposium on Nonlinear Control System Design, Bordeaux, France (pp. 159-163).

[27] Chelouah, A. (1997, December). Extensions of differential flat fields and Liouvillian systems. In IEEE conference on decision and control (Vol. 5, pp. 4268-4273). Institute of electrical engineers INC (IEE).

[28] Martínez-Guerra, R., González-Galan, R., Luviano-Juárez, A., & Cruz-Victoria, J. (2007). Diagnosis for a class of non-differentially flat and Liouvillian systems. IMA Journal of Mathematical Control and Information, 24(2), 177-195.

[29] Merkle, R. C. (1978). Secure communications over insecure channels. Communications of the ACM, 21(4), 294-299.

[30] Li, C., Liao, X., & Wong, K. W. (2005). Lag synchronization of hyperchaos with application to secure communications. Chaos, Solitons & Fractals, 23(1), 183-193.

[31] Lian, K. Y., Chiang, T. S., & Liu, P. (2000). Discrete-time chaotic systems: applications in secure communications. International Journal of Bifurcation and Chaos, 10(09), 2193-2206.

[32] Feki, M., Robert, B., Gelle, G., & Colas, M. (2003). Secure digital communication using discrete-time chaos synchronization. Chaos, Solitons & Fractals, 18(4), 881-890.

[33] Alvarez, G., Montoya, F., Romera, M., & Pastor, G. (2004). Cryptanalyzing a discrete-time chaos synchronization secure communication system. Chaos, Solitons & Fractals, 21(3), 689-694.