Optical Chaos Secure Communication

Abdelmalik Moujahid

Grupo de Inteligencia Artificial

Contenido

Idea principal

Diseñar un sistema de comunicación segura a nivel de hardware utilizando,

- láseres de semiconductor en régimen caótico,
- fibra óptica como canal de transmisión
- sincronización caótica como técnica de modulación,

con velocidades de transmisión del orden del Gbits por segundo.

Contexto sobre comunicaciones

Las portadoras de información de banda ancha son la clave de las técnicas de comunicación conocidas como espectro expandido, tales como el protocolo (CDMA) utilizado en los GPS y en los teléfonos 3G. La base de la tecnología de espectro expandido es expresada por Shannon atraves de la equación,

$$C = w \log_2(1 + s/n)$$

donde C es la capacidad del canal en bits por segundo, w es el ancho de banda en Hertzios, s y n son respectivamente las potencias de la señal y ruido.

Contexto sobre comunicaciones

En las comunicaciones basadas en caos,

- las señales de banda ancha son generadas a nivel físico (no hace falta un proceso de expansión/compresión),
- las señales caóticas ofrecen un cierto grado de privacidad intrínseca en la transmisión de datos.

Contexto sobre comunicaciones

- Inicialmente, los sistemas de comunicación segura basados en caos, se han implementado en circuitos eléctricos, los cuales se caracterizan por una dimensionalidad y ratios de transmisión muy bajos.
- La tendencia es trabajar en dominios ópticos, utilizando sistemas caóticos ópticos, en particular, láseres de semiconductor.

Sincronización del caos

Dado un sistema dinámico caótico autonomo:

$$\dot{x} = f(x)$$

el cual podemos reformular en un sistema no autónomo como:

$$\dot{x} = g(x, s(t))$$

donde $s(t) = h(x)$ es una cierta función del vector de estado que actuará como señal guiadora del sistema guiado. Para una función h conveniente, cualquier sistema,

$$\dot{y} = g(y, s(t))$$

sincroniza con el sistema original $lim_{t\to\infty}\|e(t)\| = 0$.

Sincronización del caos

La calidad y robustez de la sincronización depende de muchos factores:

- Configuración del sistema
- Parámetros adoptados
- Desajustes en los parámetros y condiciones operacionales entre emisor y receptor
- Suceptibilidad frente a perturbaciones (ruido, señal a codificar, etc)
- Tipo y fuerza de acoplamiento

Sincronización del caos

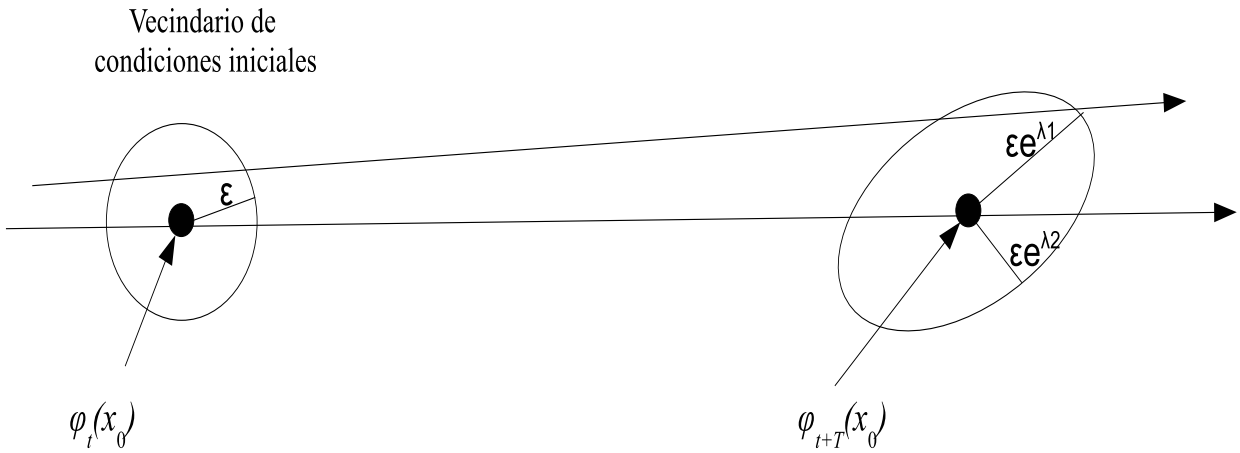
La robustez de la sincronización puede ser cuantificada mediante los exponentes de Lyapunov condicionales:

$$\lambda_i = lim_{t\to\infty}\frac{1}{t}log\|Df(\varphi_t(x_0))e_i\|$$

estos exponentes describen la expansión o contracción de desplazamientos pequeños a lo largo de la tracyectoria promediada sobre el atractor.

Una condición necesaria para la sincronización es que todos los λ_i sean negativos.

Sincronización del caos



Sensibilidad a las condiciones iniciales.

Sincronización del caos

La calidad de la sincronización puede ser cuantificada mediante el error de sincronización, ξ, y los coeficientes de correlación, ρ, entre las señales del emisor y receptor:

$$\xi = \frac{<|\ S^T(t) - S^R(t)\ |>}{<|\ S^T(t)\ |>}$$

$$\rho = \frac{< [S^T(t) - < S^T(t) >][S^R(t) - < S^R(t) >] >}{(<|\ S^T(t) - < S^T(t) >|^2><|\ S^R(t) - < S^R(t) >|^2>)^{1/2}}$$

Sincronización del caos

En un sistema de comunicación basado en caos, el error de sincronización es principalmente causado por:

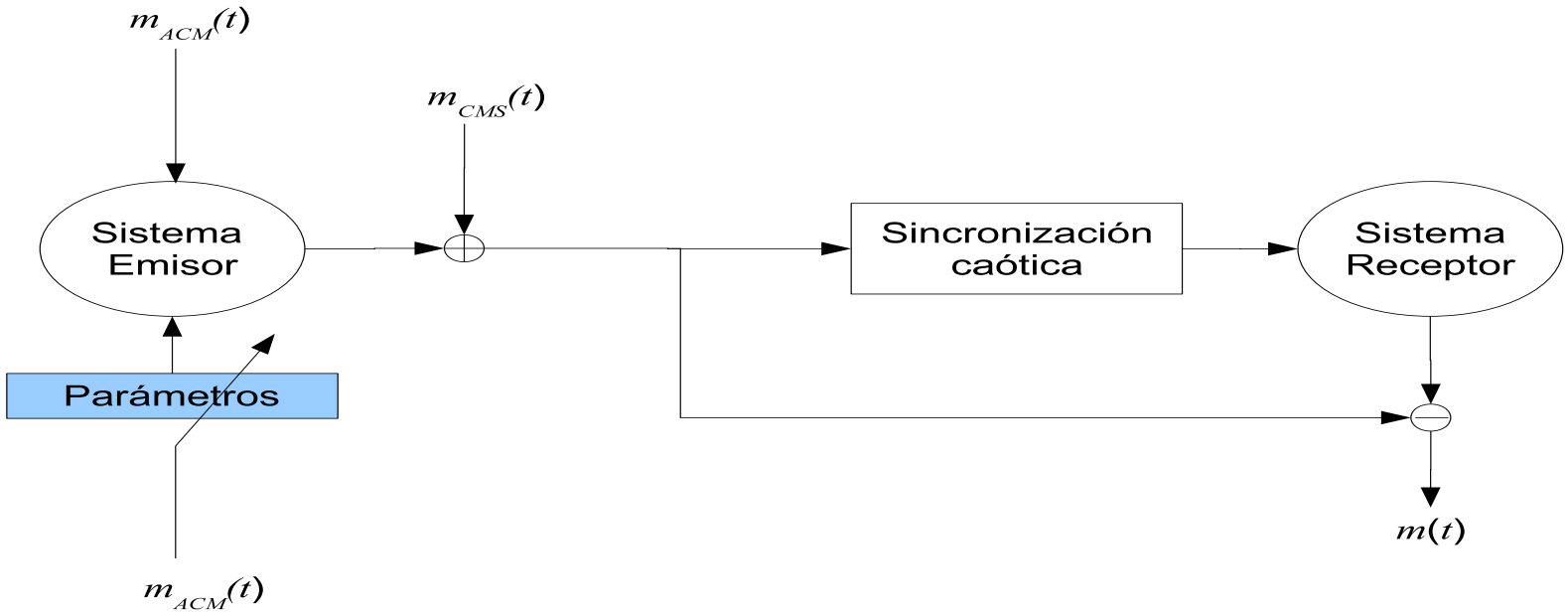
- Ruido (ruido del canal de transmisión y ruido entre emisor y receptor
- Proceso de codificación del mensaje

Esquemas de comunicación

Los esquemas de comunicación basados en la sincronización del caos pueden clasificarse en 3 tipos:

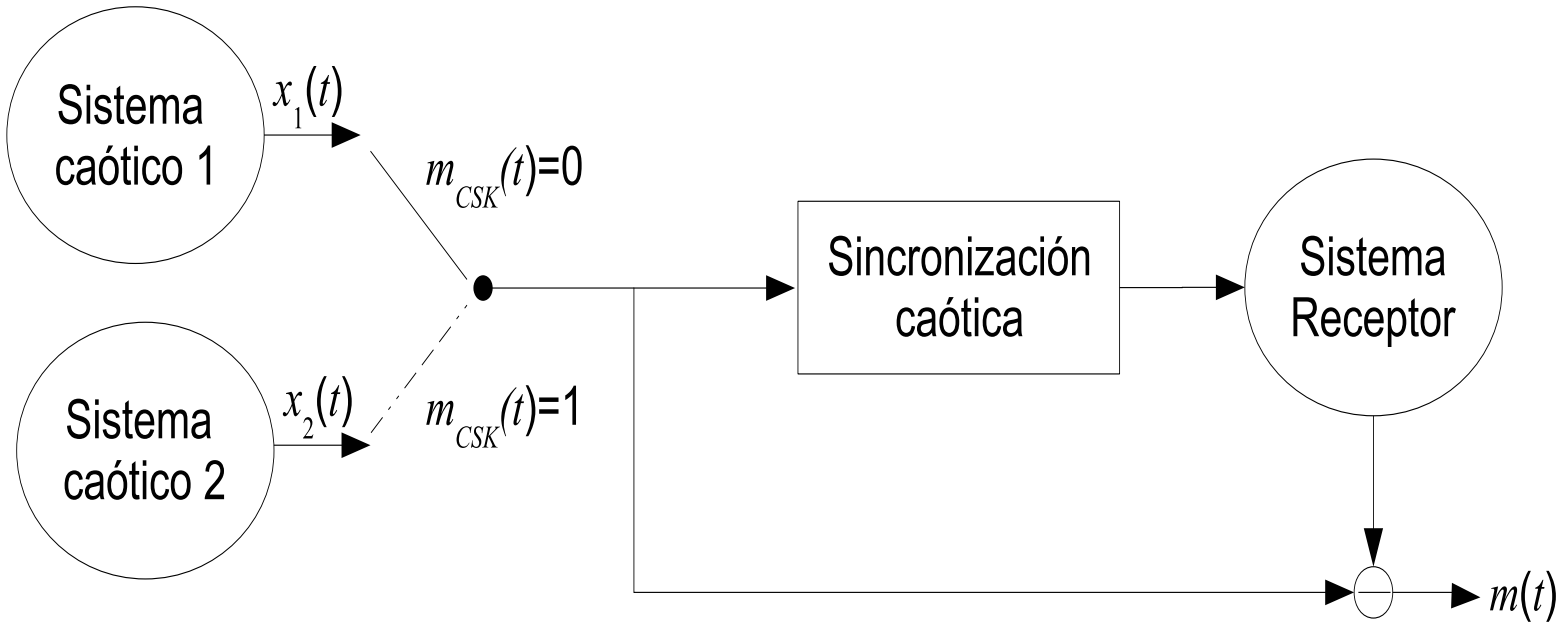
- Chaos masking (CMS)
- Additive chaos modulation (ACM)
- Chaos shift keying (CSK)

Esquemas de comunicación



Esquema básico de un sistema de comunicación basado en la sincronización. ACM: Additive chaos modulation. CMS: Chaos masking.

Esquemas de comunicación



Esquema básico de un sistema de comunicación basado en la sincronización. CSK: Chaos shift keying.

Láseres de semiconductor

Los láseres de semiconductor se caracterizan por:

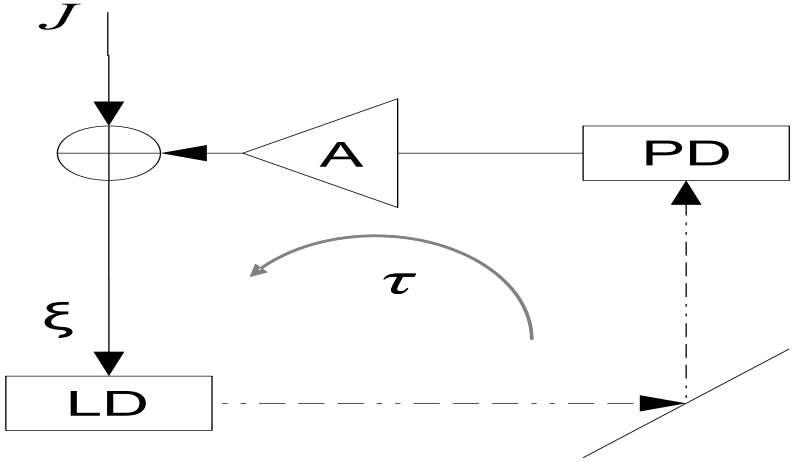
- tener respuestas no lineales muy complejas cuando están expuestos a inyección óptica, feedback óptico o feedback optoelectrónico,
- habilidad de sincronizarse unos con otros

Láseres de semiconductor

Trabajar en dominios ópticos usando láseres de semiconductor, permite:

- Alcanzar rangos de transmisión del orden del Gbit por segundo.
- Garantizar buenos niveles de seguridad
- Utilizar las redes de comunicación de alta velocidad ya existentes

Láseres de semiconductor



Esquema de un sistema de láser semiconductor con feedback optoelectrónico retardado.La linea discontinua indica el camino óptico.

Láseres de semiconductor

El láser genera pulsaciones con picos de intensidad caótica e intervalos entre picos también caóticos. Según S. Tang and J.M. Liu, la dinámica del láser puede ser descrita según el siguiente sistema de ecuaciones:

$$\dot{S} = -\gamma_c S + \Gamma g S$$

$$\dot{N} = \frac{J}{ed}[1 + \frac{\xi S(t-\tau)}{S_0}] - \gamma_s N - gS$$

S. Tang and J.M. Liu IEEE Journal of Quantum Electronics, Vol.37, No.3, March 2001 329-336.

Láseres de semiconductor

S intracavity photon density;

S_0 free-running intracavity photon density
when the laser is not subject to the feedback;

N carrier density

g optical gain coefficient

ξ dimensionless parameter
which correspond to the srength of the feedback;

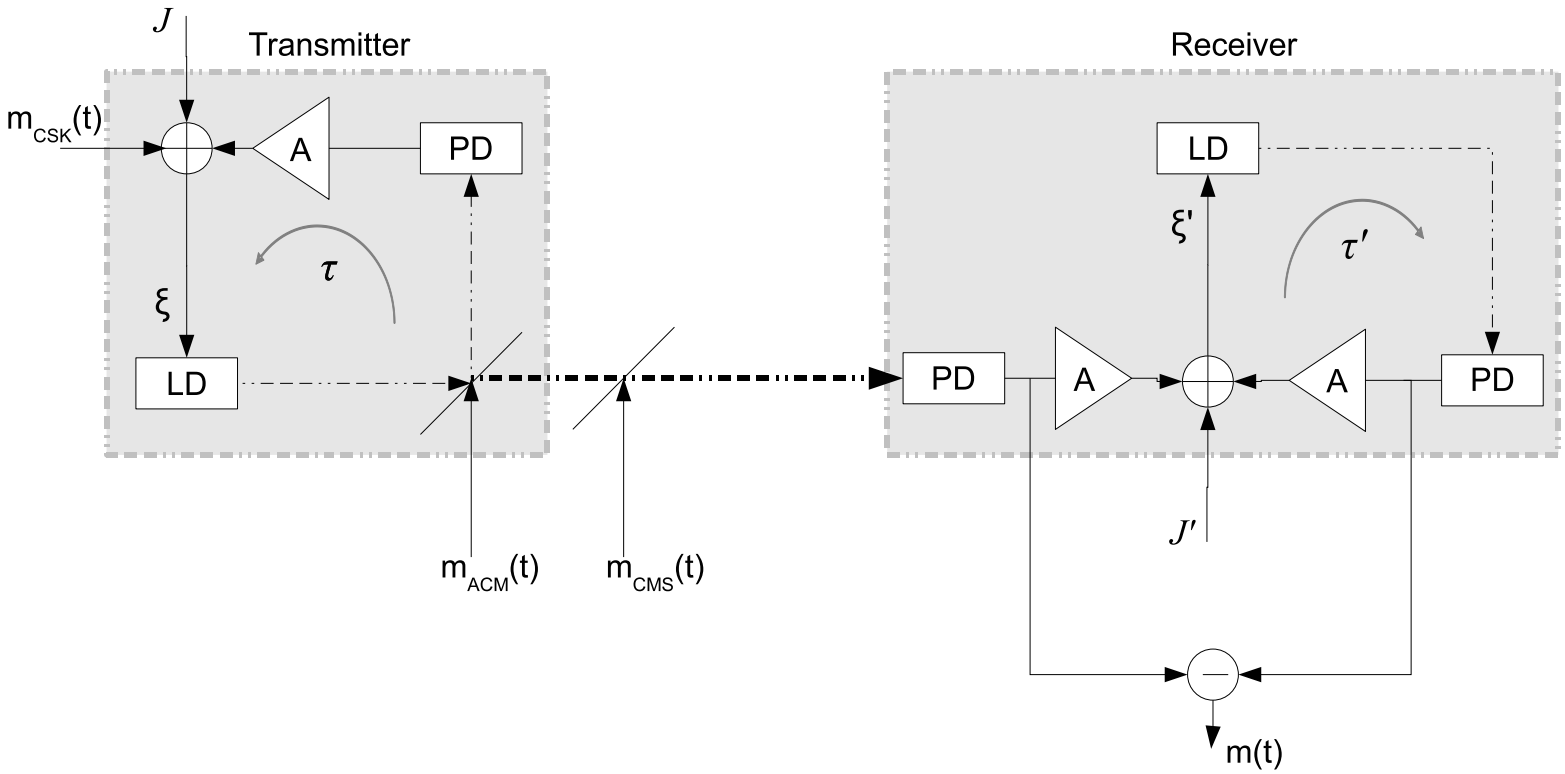
τ feedback delay time;

J bias current density;

γ_c cavity photon decay rate;

γ_s spontaneous carrier decay rate;

Láseres de semiconductor



Esquema unidireccional de comunicación usando láseres de semiconductor con feedback optoelectrónico retardado.

Objetivos

- Estudiar la estabilidad y robustez de la sincronización de los láseres de semiconductor
- Implementar un sistema de comunicación segura basado en caos ótpico
- Cuantificar su nivel de seguridad