Estimation d'état non linéaire : application à la synchronisation et aux cryptosystèmes chaotiques

Estelle Cherrier, José Ragot, Mohamed Boutayeb

CRAN UMR 7039, Institut National Polytechnique de Lorraine
LSIIT UMR 7005, Université Louis Pasteur, Strasbourg

Réunion du Groupe de Travail S3 Sûreté-Surveillance-Supervision
23 janvier 2007

Systèmes chaotiques

Propriétés

- Système déterministe
- Caractérisé par une extrême sensibilité aux conditions initiales
- Possède un comportement asymptotique apériodique

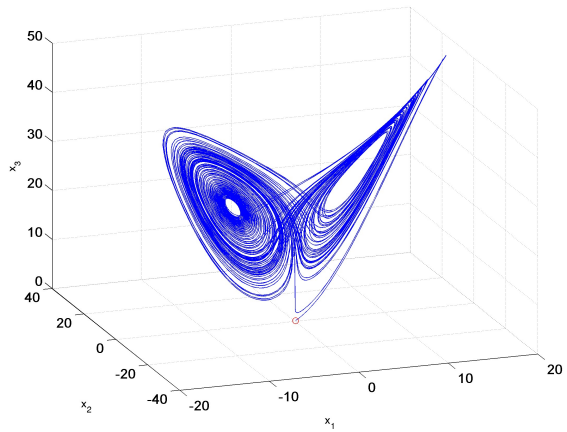
Systèmes chaotiques

Propriétés

- Système déterministe
- Caractérisé par une extrême sensibilité aux conditions initiales
- Possède un comportement asymptotique apériodique

Système de Lorenz (1963)

$$\dot{x}_1 = -\sigma x_1 + \sigma x_2$$
$$\dot{x}_2 = \gamma x_1 - x_2 - x_1 x_3$$
$$\dot{x}_3 = x_1 x_2 - \beta x_3$$



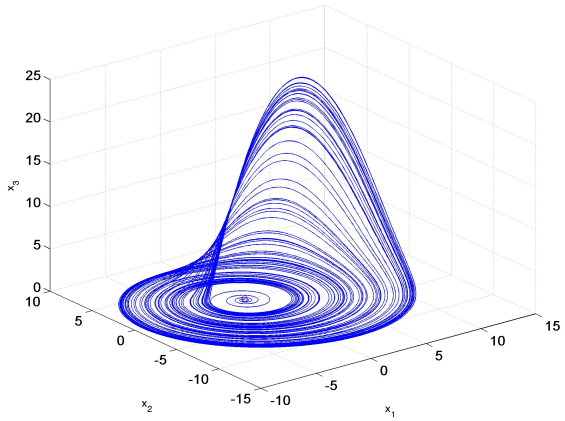
Systèmes chaotiques

Propriétés

- Système déterministe
- Caractérisé par une extrême sensibilité aux conditions initiales
- Possède un comportement asymptotique apériodique

Système de Rössler (1976)

$$\dot{x}_1 = -x_2 - x_3$$
$$\dot{x}_2 = x_1 + ax_2 + 0,01x_1 \ln(x_3)$$
$$\dot{x}_3 = c + x_3(x_1 - b)$$



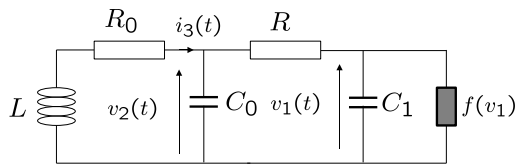
Systèmes chaotiques

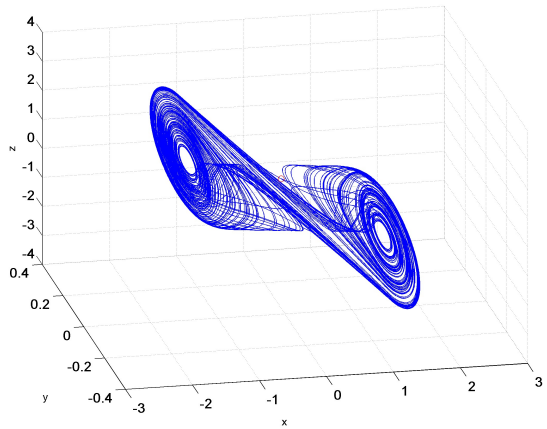
Propriétés

- Système déterministe
- Caractérisé par une extrême sensibilité aux conditions initiales
- Possède un comportement asymptotique apériodique

Circuit de Chua (1980)

$$\dot{x}_1 = \frac{1}{C_1}\left(G(x_2 - x_1) - f(x_1)\right)$$
$$\dot{x}_2 = \frac{1}{C_2}\left(G(x_1 - x_2) + x_3\right)$$
$$\dot{x}_3 = -\frac{1}{L}\left(x_2 + R_0 x_3\right)$$





Systèmes chaotiques

Propriétés

- Système déterministe
- Caractérisé par une extrême sensibilité aux conditions initiales
- Possède un comportement asymptotique apériodique

Signal chaotique

- semble aléatoire
- MAIS parfaitement déterministe

Systèmes chaotiques

Propriétés

- Système déterministe
- Caractérisé par une extrême sensibilité aux conditions initiales
- Possède un comportement asymptotique apériodique

Signal chaotique

- semble aléatoire
- MAIS parfaitement déterministe

Conséquence : il est possible de le reproduire (mêmes conditions initiales)

Systèmes chaotiques

Propriétés

- Système déterministe
- Caractérisé par une extrême sensibilité aux conditions initiales
- Possède un comportement asymptotique apériodique

Signal chaotique

- semble aléatoire
- MAIS parfaitement déterministe

Conséquence : il est possible de le reproduire (mêmes conditions initiales)
$\Rightarrow$ intérêt de la synchronisation : le récepteur n'a pas besoin de connaître les CI

Synchronisation

Du XVII$^{\text{ème}}$ siècle aux années 1980

- découverte par Christiaan Huygens (1629-1695)
- caractérise les systèmes périodiques
- notion de système forcé

$$\neq \text{ chaos} = \text{ phénomène incontrôlable}$$

Synchronisation

Du XVII^{ème} siècle aux années 1980

- découverte par Christiaan Huygens (1629-1695)
- caractérise les systèmes périodiques
- notion de système forcé

$$\neq \text{ chaos} = \text{ phénomène incontrôlable}$$

Synchronisation du chaos

Plusieurs étapes

- 1983 : Yamada et Fujisaka
- 1990 : Pecora et Carroll
- 1997 : approche utilisant les observateurs

Synchronisation

Du XVII^{ème} siècle aux années 1980

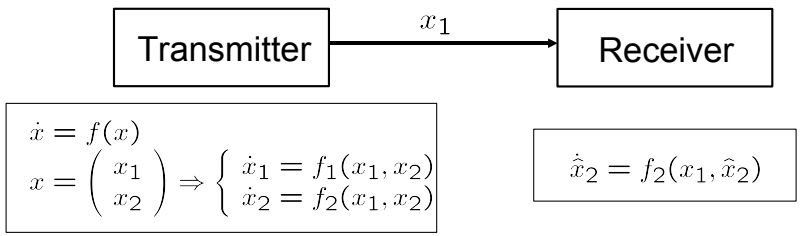
- découverte par Christiaan Huygens (1629-1695)
- caractérise les systèmes périodiques
- notion de système forcé

$$\neq \text{ chaos} = \text{ phénomène incontrôlable}$$

Synchronisation du chaos

Plusieurs étapes

- 1983 : Yamada et Fujisaka
- 1990 : Pecora et Carroll
- 1997 : approche utilisant les observateurs



Synchronisation

Du XVII^{ème} siècle aux années 1980

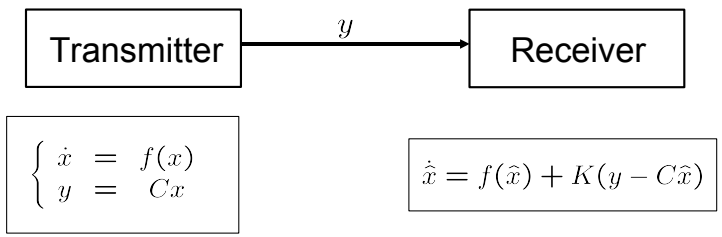
- découverte par Christiaan Huygens (1629-1695)
- caractérise les systèmes périodiques
- notion de système forcé

$$\neq \text{ chaos} = \text{ phénomène incontrôlable}$$

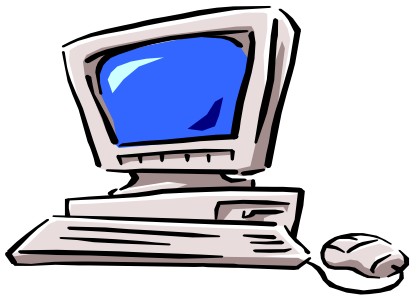
Synchronisation du chaos

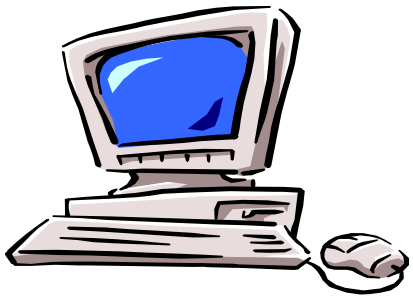
Plusieurs étapes

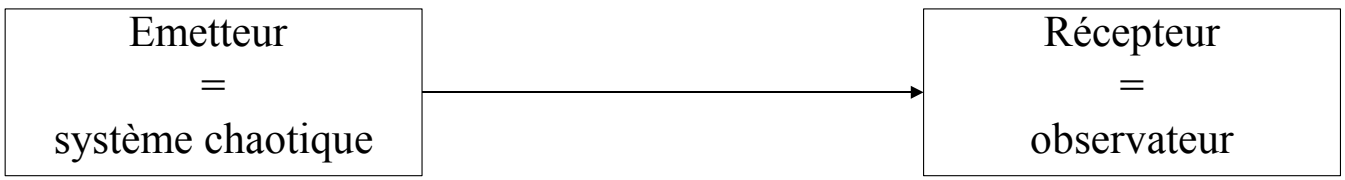
- 1983 : Yamada et Fujisaka
- 1990 : Pecora et Carroll
- 1997 : approche utilisant les observateurs



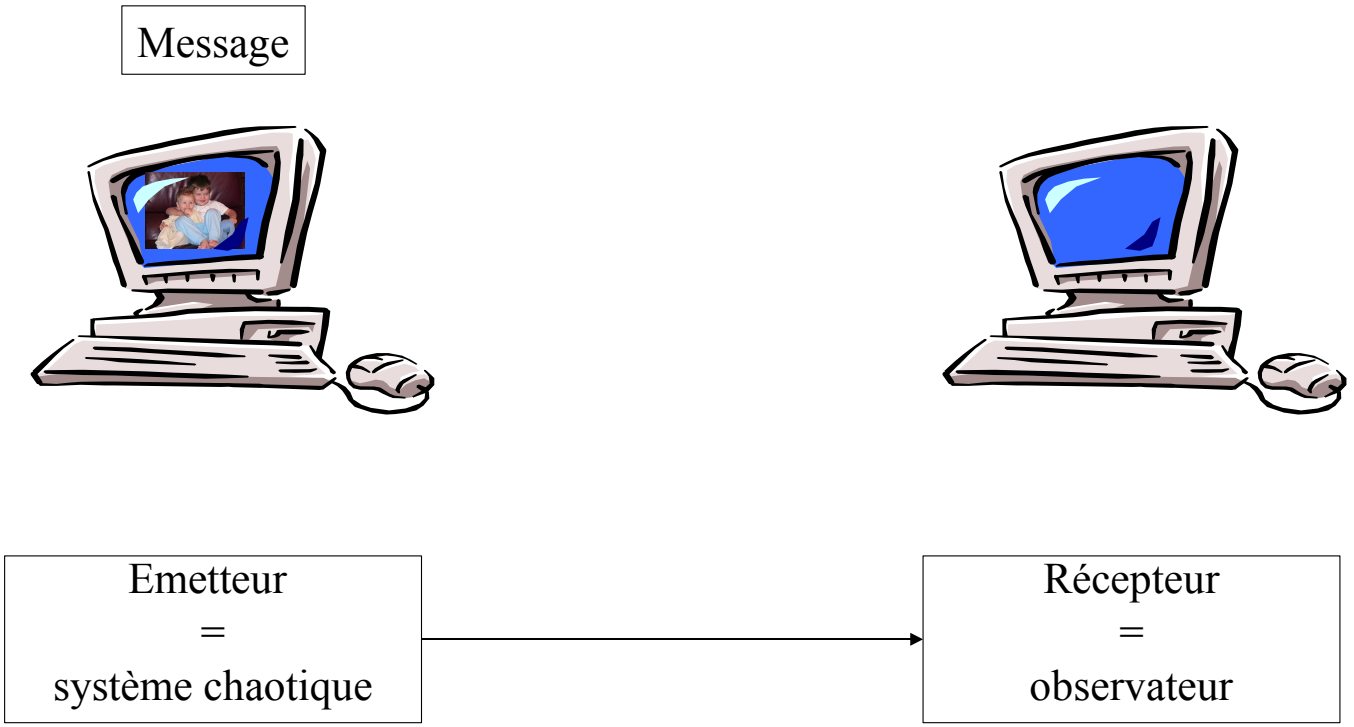
Application : conception d'un cryptosystème chaotique





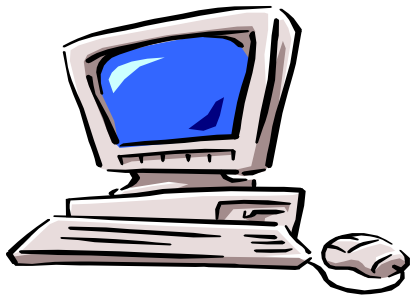


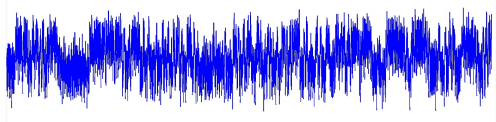
Application : conception d'un cryptosystème chaotique



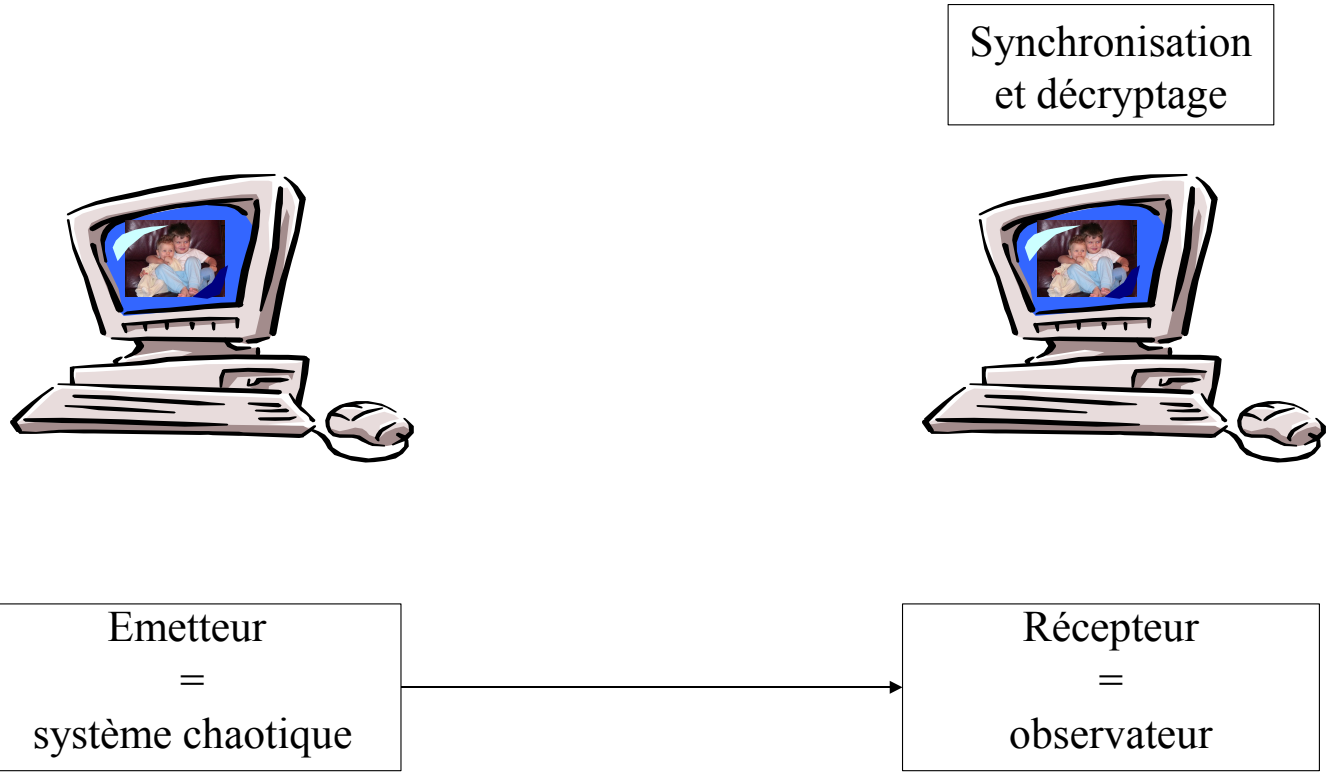
Application : conception d'un cryptosystème chaotique

Transmission du
message crypté



Emetteur = système chaotique		Récepteur = observateur

Application : conception d'un cryptosystème chaotique



Plan de la présentation

Plan de la présentation

Choix de l'émetteur chaotique

Objectifs

- l'émetteur doit générer un signal chaotique dans lequel l'information sera noyée
- le signal porteur chaotique doit être le plus *complexe* possible

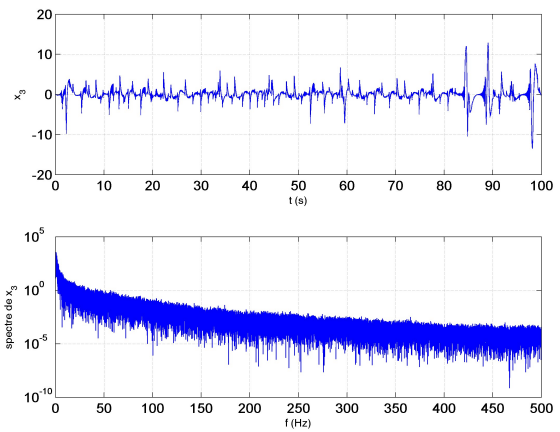
Choix de l'émetteur chaotique

Objectifs

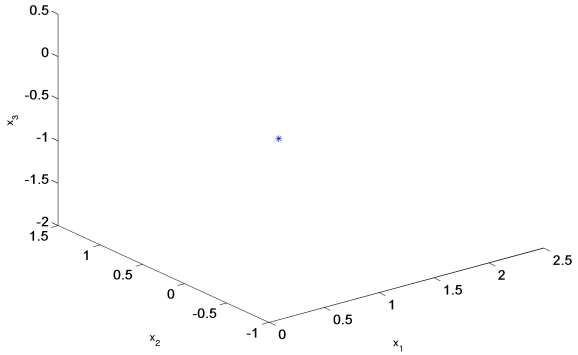
- l'émetteur doit générer un signal chaotique dans lequel l'information sera noyée
- le signal porteur chaotique doit être le plus *complexe* possible

Système chaotique à retard

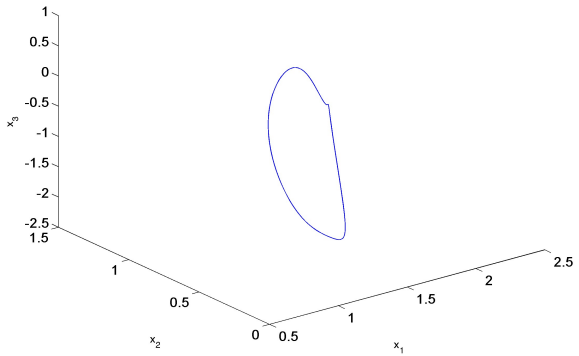
$$\begin{aligned} \dot{x}_1(t) &= -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta \tanh(x_1(t)) \\ \dot{x}_2(t) &= x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) &= -\beta x_2(t) - \gamma x_3(t) + \varepsilon \sin(\sigma x_1(t-\tau)) \end{aligned}$$



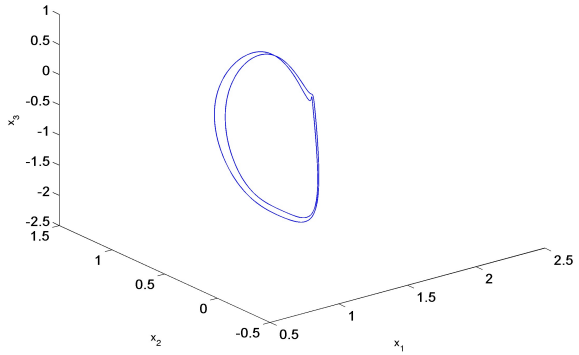
Route vers le chaos



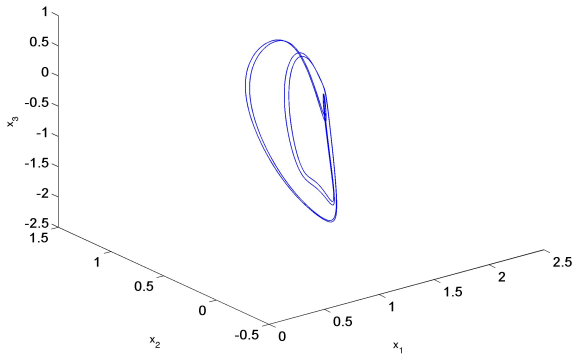
$\sigma = 0$



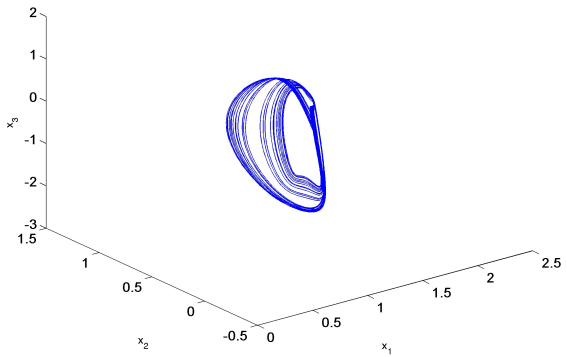
$\sigma = 1,76$



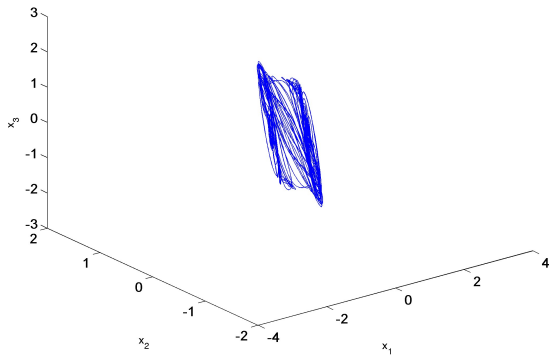
$\sigma = 1,77$



$\sigma = 1,80$

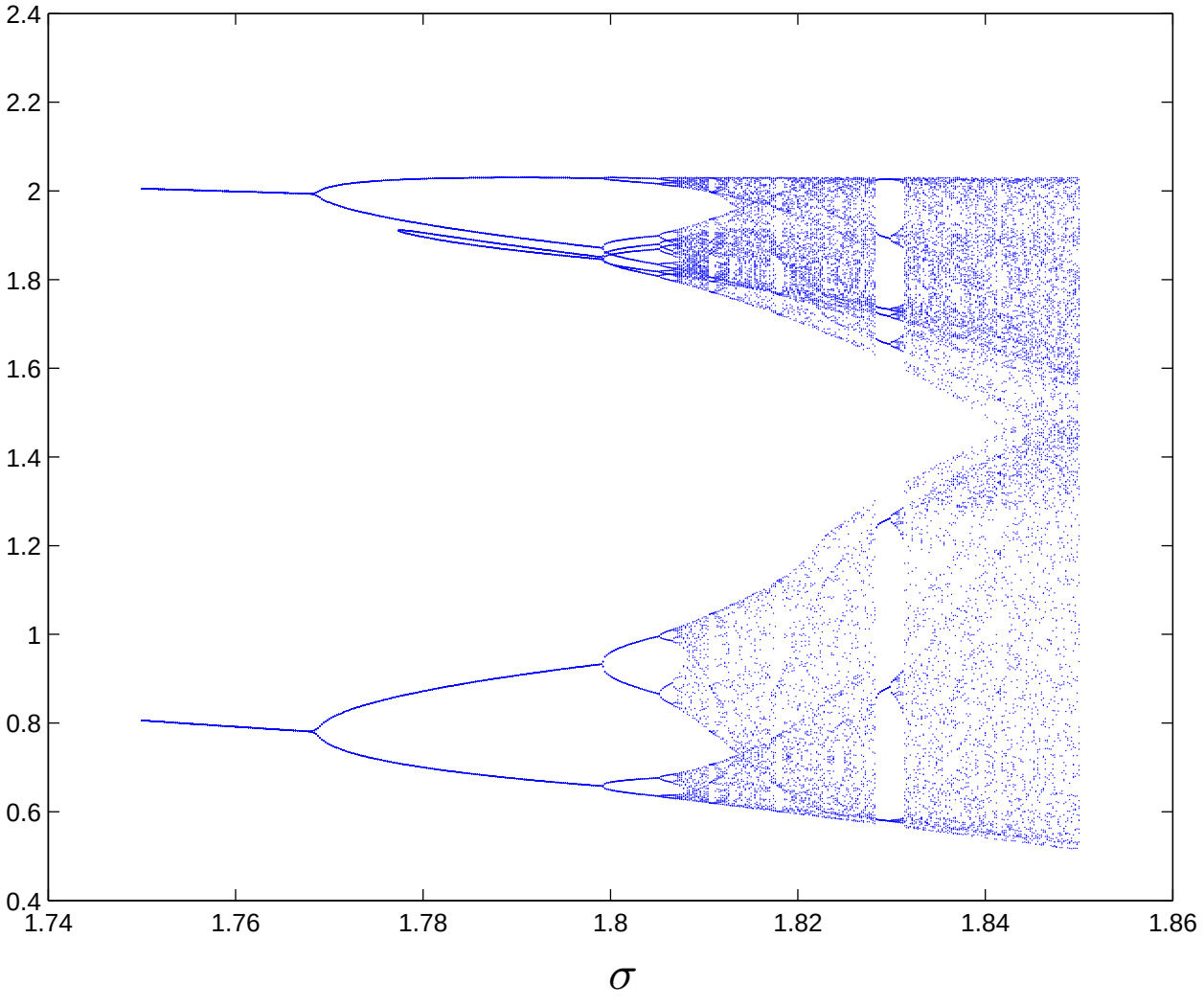


$\sigma = 1,81$



$\sigma = 2$

Diagramme de bifurcations



Structure de l'émetteur

Modèle dynamique du système étudié

$$\begin{cases} \dot{x}_1(t) = -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta \tanh(x_1(t)) \\ \dot{x}_2(t) = x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) = -\beta x_2(t) - \gamma x_3(t) + \varepsilon \sin(\sigma x_{1\tau}(t)(t)) \end{cases}$$

$$\downarrow$$

$$\begin{aligned} \dot{x}(t) &= Ax(t) + F\left(x(t)\right) + H\left(x_\tau(t)\right) \\ y(t) &= Cx(t) \end{aligned}$$

Structure de l'émetteur

Modèle dynamique du système étudié

$$\begin{cases} \dot{x}_1(t) = -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta \tanh(x_1(t)) \\ \dot{x}_2(t) = x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) = -\beta x_2(t) - \gamma x_3(t) + \varepsilon \sin(\sigma x_{1\tau}(t)(t)) \end{cases}$$

$$\downarrow$$

$$\begin{aligned} \dot{x}(t) &= Ax(t) + F\left(x(t)\right) + H\left(x_\tau(t)\right) \\ y(t) &= Cx(t) \end{aligned}$$

Notations

$$A = \begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix}$$

$$F(x(t)) = \begin{pmatrix} -\alpha\delta \tanh(x_1(t)) \\ 0 \\ 0 \end{pmatrix}$$

$$H(x_\tau(t)) = \begin{pmatrix} 0 \\ 0 \\ \varepsilon \sin(\sigma x_{1\tau}(t)) \end{pmatrix}$$

Structure de l'émetteur

Modèle dynamique du système étudié

$$\begin{cases} \dot{x}_1(t) = -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta \tanh(x_1(t)) \\ \dot{x}_2(t) = x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) = -\beta x_2(t) - \gamma x_3(t) + \varepsilon \sin(\sigma x_{1\tau}(t)(t)) \end{cases}$$

$$\downarrow$$

$$\begin{aligned} \dot{x}(t) &= Ax(t) + F\left(x(t)\right) + H\left(x_\tau(t)\right) \\ y(t) &= Cx(t) \end{aligned}$$

Notations

$$A = \begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix}$$

$$F(x(t)) = \begin{pmatrix} -\alpha\delta \tanh(x_1(t)) \\ 0 \\ 0 \end{pmatrix}$$

$$H(x_\tau(t)) = \begin{pmatrix} 0 \\ 0 \\ \varepsilon \sin(\sigma x_{1\tau}(t)) \end{pmatrix}$$

Condition de Lipschitz

F et H sont Lipschitziennes (de constantes k_F et k_H) :

$$\forall (x, x') \in (\mathbb{R}^3)^2, \quad \begin{aligned} \|F(x) - F(x')\| &\leqslant k_F \|x - x'\| \\ \|H(x) - H(x')\| &\leqslant k_H \|x - x'\| \end{aligned}$$

Transformation du système

Modèle équivalent

- on choisit la matrice $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix} \Rightarrow x_1(t) = y(t) - \zeta x_2(t)$

$$\begin{cases} \dot{x}(t) = \tilde{A}x(t) + \tilde{B}y(t) + \tilde{F}(x(t), y(t)) + \tilde{H}(x_\tau(t), y_\tau(t)) \\ y(t) = Cx(t) \end{cases}$$

Transformation du système

Modèle équivalent

- on choisit la matrice $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix} \Rightarrow x_1(t) = y(t) - \zeta x_2(t)$

$$\begin{cases} \dot{x}(t) = \tilde{A}x(t) + \tilde{B}y(t) + \tilde{F}(x(t), y(t)) + \tilde{H}(x_\tau(t), y_\tau(t)) \\ y(t) = Cx(t) \end{cases}$$

Notations

$$\tilde{A} = \begin{pmatrix} 0 & \alpha(1+\zeta) & 0 \\ 0 & -(1+\zeta) & 1 \\ 0 & -\beta & -\gamma \end{pmatrix}$$

$$\tilde{B} = \begin{pmatrix} -\alpha \\ 1 \\ 0 \end{pmatrix}$$

$$\tilde{F}(x(t), y(t)) = \tilde{F} = \begin{pmatrix} \alpha\delta \tanh(y(t) - \zeta x_2(t)) \\ 0 \\ 0 \end{pmatrix}$$

$$\tilde{H}(x_\tau(t), y_\tau(t)) = \tilde{H} = \begin{pmatrix} 0 \\ 0 \\ \varepsilon \sin(\sigma(y_\tau(t) - \zeta x_{2\tau}(t))) \end{pmatrix}$$

Transformation du système

Modèle équivalent

- on choisit la matrice $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix} \Rightarrow x_1(t) = y(t) - \zeta x_2(t)$

$$\begin{cases} \dot{x}(t) = \tilde{A}x(t) + \tilde{B}y(t) + \tilde{F}(x(t), y(t)) + \tilde{H}(x_\tau(t), y_\tau(t)) \\ y(t) = Cx(t) \end{cases}$$

Notations

$$\tilde{A} = \begin{pmatrix} 0 & \alpha(1+\zeta) & 0 \\ 0 & -(1+\zeta) & 1 \\ 0 & -\beta & -\gamma \end{pmatrix}$$

$$\tilde{B} = \begin{pmatrix} -\alpha \\ 1 \\ 0 \end{pmatrix}$$

$$\tilde{F}(x(t), y(t)) = \tilde{F} = \begin{pmatrix} \alpha\delta \tanh(y(t) - \zeta x_2(t)) \\ 0 \\ 0 \end{pmatrix}$$

$$\tilde{H}(x_\tau(t), y_\tau(t)) = \tilde{H} = \begin{pmatrix} 0 \\ 0 \\ \varepsilon \sin(\sigma(y_\tau(t) - \zeta x_{2\tau}(t))) \end{pmatrix}$$

Constantes de Lipschitz

- $k_{\tilde{F}} \leqslant k_F|\zeta|$
- $k_{\tilde{H}} \leqslant k_H|\zeta|$

Plan de la présentation

Conception du récepteur : observateur d'ordre plein

Observateur exponentiel :

$$\dot{\hat{x}} = \tilde{A}\hat{x} + \tilde{B}y + \hat{\tilde{F}} + \hat{\tilde{H}} + K(y - C\hat{x})$$

On note $e(t) = x(t) - \hat{x}(t)$.

Conception du récepteur : observateur d'ordre plein

Observateur exponentiel :

$$\dot{\hat{x}} = \tilde{A}\hat{x} + \tilde{B}y + \hat{\tilde{F}} + \hat{\tilde{H}} + K(y - C\hat{x})$$

On note $e(t) = x(t) - \hat{x}(t)$.

Théorème

S'il existe un gain K et deux matrices P, Q respectivement symétrique, définie positive et définie positive, et un réel strictement positif η tels que

$$\begin{pmatrix} (A-KC)^T P + P(A-KC) + \mu I_3 + Q + 2\eta P & 0 & P \\ 0 & \varphi Q + \rho I & 0 \\ P & 0 & -\frac{1}{\lambda} I_3 \end{pmatrix} < 0$$

avec $\lambda = \zeta k_F + \zeta k_H$, $\mu = \zeta k_F$, $\rho = \zeta k_H$, $\varphi = -e^{-2\eta\tau}$ alors l'erreur de synchronisation converge exponentiellement vers zéro, selon la formule :

$$\|e(t)\| \leqslant \sqrt{\frac{\alpha_1}{\alpha_2}} e^{-\eta t} \max_{\theta \in [-\tau, 0]} \|e(\theta)\|$$

avec $\alpha_1 = \lambda_M(P) + \tau\lambda_M(Q)$ et $\alpha_2 = \lambda_m(P)$.

Analyse de stabilité (1/3)

Démonstration :

- Fonctionnelle de Lyapunov-Krasovskii

$$V(e, e_\tau) = e^T P e + \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

- $e(t)$ converge exponentiellement vers 0 s'il existe $\phi > 0$ tel que
  - $V(e, e_\tau) > 0$
  - $\dot{V}(e, e_\tau) < e^{-\phi t} \max_{\theta \in [-\tau, 0]} V(e(0), e(\theta))$
- $\lambda_m(P)\|e\|^2 \leqslant V(e, e_\tau)$
- on dérive l'expression de V :

$$\dot{V} = \dot{e}^T P e + e^T P \dot{e} + e^T Q e - e^{-2\eta\tau} e_\tau^T Q e_\tau - 2\eta \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

Analyse de stabilité (1/3)

Démonstration :

- Fonctionnelle de Lyapunov-Krasovskii

$$V(e, e_\tau) = e^T P e + \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

- $e(t)$ converge exponentiellement vers 0 s'il existe $\phi > 0$ tel que
  - $V(e, e_\tau) > 0$
  - $\dot{V}(e, e_\tau) < e^{-\phi t} \max_{\theta \in [-\tau, 0]} V(e(0), e(\theta))$
- $\lambda_m(P)\|e\|^2 \leqslant V(e, e_\tau)$
- on dérive l'expression de V :

$$\dot{V} = \dot{e}^T P e + e^T P \dot{e} + e^T Q e - e^{-2\eta\tau} e_\tau^T Q e_\tau - 2\eta \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

Analyse de stabilité (1/3)

Démonstration :

- Fonctionnelle de Lyapunov-Krasovskii

$$V(e, e_\tau) = e^T P e + \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

- $e(t)$ converge exponentiellement vers 0 s'il existe $\phi > 0$ tel que
  - $V(e, e_\tau) > 0$
  - $\dot{V}(e, e_\tau) < e^{-\phi t} \max_{\theta \in [-\tau, 0]} V(e(0), e(\theta))$
- $\lambda_m(P)\|e\|^2 \leqslant V(e, e_\tau)$
- on dérive l'expression de V :

$$\dot{V} = \dot{e}^T P e + e^T P \dot{e} + e^T Q e - e^{-2\eta\tau} e_\tau^T Q e_\tau - 2\eta \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

Analyse de stabilité (1/3)

Démonstration :

- Fonctionnelle de Lyapunov-Krasovskii

$$V(e, e_\tau) = e^T P e + \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

- $e(t)$ converge exponentiellement vers 0 s'il existe $\phi > 0$ tel que
  - $V(e, e_\tau) > 0$
  - $\dot{V}(e, e_\tau) < e^{-\phi t} \max_{\theta \in [-\tau, 0]} V(e(0), e(\theta))$
- $\lambda_m(P)\|e\|^2 \leqslant V(e, e_\tau)$
- on dérive l'expression de V :

$$\dot{V} = \dot{e}^T P e + e^T P \dot{e} + e^T Q e - e^{-2\eta\tau} e_\tau^T Q e_\tau - 2\eta \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

Analyse de stabilité (2/3)

- majoration de $\dot{V}$:

$$\dot{V} \leqslant \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T \mathcal{M} \begin{pmatrix} e \\ e_\tau \end{pmatrix} - 2\eta \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

avec $\mathcal{M} = \begin{pmatrix} A_K^T P + P A_K + \lambda P^2 + \mu I + Q & 0 \\ 0 & -e^{-2\eta\tau} Q + \rho I \end{pmatrix}$

- expression de V :

$$V = \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T \mathcal{N} \begin{pmatrix} e \\ e_\tau \end{pmatrix} + \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

avec $\mathcal{N} = \begin{pmatrix} P & 0 \\ 0 & 0 \end{pmatrix}$

Analyse de stabilité (2/3)

- majoration de $\dot{V}$:

$$\dot{V} \leqslant \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T \mathcal{M} \begin{pmatrix} e \\ e_\tau \end{pmatrix} - 2\eta \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

avec $\mathcal{M} = \begin{pmatrix} A_K^T P + P A_K + \lambda P^2 + \mu I + Q & 0 \\ 0 & -e^{-2\eta\tau} Q + \rho I \end{pmatrix}$

- expression de V :

$$V = \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T \mathcal{N} \begin{pmatrix} e \\ e_\tau \end{pmatrix} + \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta$$

avec $\mathcal{N} = \begin{pmatrix} P & 0 \\ 0 & 0 \end{pmatrix}$

Analyse de stabilité (3/3)

- On en déduit :

$$\dot{V} + 2\eta V \leqslant \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T (\mathcal{M} + 2\eta\mathcal{N}) \begin{pmatrix} e \\ e_\tau \end{pmatrix}$$

- $\mathcal{M} + 2\eta\mathcal{N} < 0 \Rightarrow \dot{V} < -2\eta V \Rightarrow V(e, e_\tau) < e^{-2\eta t} \max_{\theta \in [-\tau, 0]} V(e(0), e(\theta))$
- or $\lambda_m(P)\|e\|^2 \leqslant V(e, e_\tau)$
- finalement $\|e(t)\| < \sqrt{\frac{\alpha_1}{\alpha_2}} e^{-\eta t} \max_{\theta \in [-\tau, 0]} \|e(\theta)\|$

Analyse de stabilité (3/3)

- On en déduit :

$$\dot{V} + 2\eta V \leqslant \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T (\mathcal{M} + 2\eta\mathcal{N}) \begin{pmatrix} e \\ e_\tau \end{pmatrix}$$

- $\mathcal{M} + 2\eta\mathcal{N} < 0 \Rightarrow \dot{V} < -2\eta V \Rightarrow V(e, e_\tau) < e^{-2\eta t} \max_{\theta \in [-\tau, 0]} V(e(0), e(\theta))$
- or $\lambda_m(P)\|e\|^2 \leqslant V(e, e_\tau)$
- finalement $\|e(t)\| < \sqrt{\frac{\alpha_1}{\alpha_2}} e^{-\eta t} \max_{\theta \in [-\tau, 0]} \|e(\theta)\|$

Analyse de stabilité (3/3)

- On en déduit :

$$\dot{V} + 2\eta V \leqslant \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T (\mathcal{M} + 2\eta\mathcal{N}) \begin{pmatrix} e \\ e_\tau \end{pmatrix}$$

- $\mathcal{M} + 2\eta\mathcal{N} < 0 \Rightarrow \dot{V} < -2\eta V \Rightarrow V(e, e_\tau) < e^{-2\eta t} \max_{\theta \in [-\tau, 0]} V(e(0), e(\theta))$
- or $\lambda_m(P)\|e\|^2 \leqslant V(e, e_\tau)$
- finalement $\|e(t)\| < \sqrt{\frac{\alpha_1}{\alpha_2}} e^{-\eta t} \max_{\theta \in [-\tau, 0]} \|e(\theta)\|$

Analyse de stabilité (3/3)

- On en déduit :

$$\dot{V} + 2\eta V \leqslant \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T (\mathcal{M} + 2\eta\mathcal{N}) \begin{pmatrix} e \\ e_\tau \end{pmatrix}$$

- $\mathcal{M} + 2\eta\mathcal{N} < 0 \Rightarrow \dot{V} < -2\eta V \Rightarrow V(e, e_\tau) < e^{-2\eta t} \max_{\theta \in [-\tau, 0]} V(e(0), e(\theta))$
- or $\lambda_m(P)\|e\|^2 \leqslant V(e, e_\tau)$
- finalement $\|e(t)\| < \sqrt{\frac{\alpha_1}{\alpha_2}} e^{-\eta t} \max_{\theta \in [-\tau, 0]} \|e(\theta)\|$

Synthèse du gain de l'observateur

On reprend l'expression :

$$\mathcal{M} + 2\eta\mathcal{N} = \begin{pmatrix} (A-KC)^T P + P(A-KC) + \lambda P^2 + \mu I + Q + 2\eta P & 0 \\ 0 & -e^{-2\eta\tau} Q + \rho I \end{pmatrix}$$

Synthèse du gain de l'observateur

On reprend l'expression :

$$\mathcal{M} + 2\eta\mathcal{N} = \begin{pmatrix} (A-KC)^T P + P(A-KC) + \lambda P^2 + \mu I + Q + 2\eta P & 0 \\ 0 & -e^{-2\eta\tau} Q + \rho I \end{pmatrix}$$

En appliquant le *complément de Schur*, $\mathcal{M} + 2\eta\mathcal{N} < 0$ *ssi* :

$$\begin{pmatrix} (A-KC)^T P + P(A-KC) + \mu I_3 + Q + 2\eta P & 0 & P \\ 0 & -e^{-2\eta\tau} Q + \rho I & 0 \\ P & 0 & -\frac{1}{\lambda} I_3 \end{pmatrix} < 0$$

Synthèse du gain de l'observateur

On reprend l'expression :

$$\mathcal{M} + 2\eta\mathcal{N} = \begin{pmatrix} (A-KC)^T P + P(A-KC) + \lambda P^2 + \mu I + Q + 2\eta P & 0 \\ 0 & -e^{-2\eta\tau} Q + \rho I \end{pmatrix}$$

En appliquant le *complément de Schur*, $\mathcal{M} + 2\eta\mathcal{N} < 0$ *ssi* :

$$\begin{pmatrix} (A-KC)^T P + P(A-KC) + \mu I_3 + Q + 2\eta P & 0 & P \\ 0 & -e^{-2\eta\tau} Q + \rho I & 0 \\ P & 0 & -\frac{1}{\lambda} I_3 \end{pmatrix} < 0$$

On effectue un changement de variable $L = PK$:

$$\begin{pmatrix} A^T P + PA - C^T L^T - LC + \mu I_3 + Q + 2\eta P & 0 & P \\ 0 & -e^{-2\eta\tau} Q + \rho I & 0 \\ P & 0 & -\frac{1}{\lambda} I_3 \end{pmatrix} < 0$$

Simulations

Paramètres

α	β	γ	δ	ε	σ	τ
9	14	5	0.5	10	10^4	1

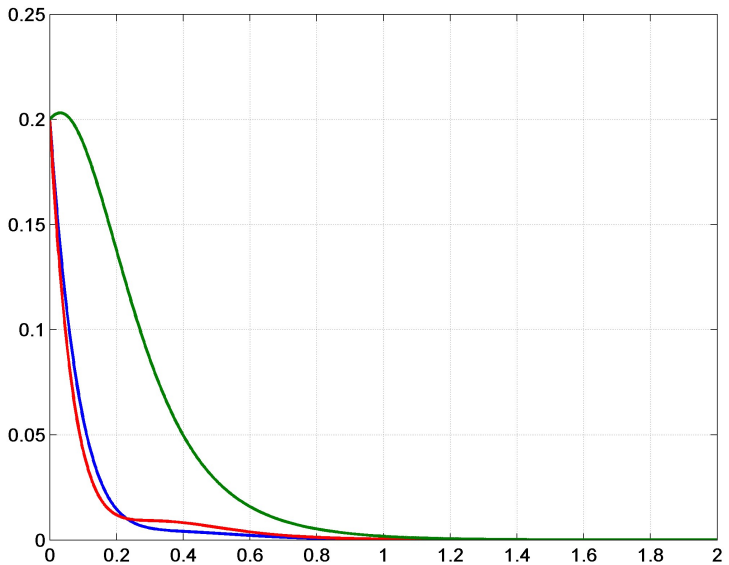
États initiaux

$$x_0 = \begin{pmatrix} 0,1 & 0,1 & 0,1 \end{pmatrix}^T$$
$$\hat{x}_0 = \begin{pmatrix} -0,1 & -0,1 & -0,1 \end{pmatrix}^T$$

Gain

$$K = \begin{pmatrix} 46,2 \\ 44,6 \\ -39,3 \end{pmatrix}$$

Erreurs d'estimation



Extension au cas général

- Modèle dynamique en dimension n : $\begin{array}{l} \dot{X} = AX + F(X) + H(X_\tau) \\ Y(t) = CX(t) \end{array}$

Extension au cas général

- Modèle dynamique en dimension n : $\begin{array}{l}\dot{X} = AX + F(X) + H(X_\tau) \\ Y(t) = CX(t)\end{array}$

Hypothèses

Il existe $p < n$ tel que

- $F(X(t)) = F\left(X_1(t), \ldots, X_p(t)\right)$, $H(X(t-\tau)) = H\left(X_1(t-\tau), \ldots, X_p(t-\tau)\right)$
- $C = \left(\begin{array}{c|c} I_p & \bar{C} \end{array}\right)$, $\bar{C} = (\zeta_i \delta_{ij(i)})_{(i,j)\in[1,n]\times[1,p]}$
  $\Rightarrow Y_i(t) = X_i(t) + \zeta_i X_{j(i)}(t), \quad p < j(i) \leqslant n$

Extension au cas général

- Modèle dynamique en dimension n : $\begin{array}{l}\dot{X} = AX + F(X) + H(X_\tau) \\ Y(t) = CX(t)\end{array}$

Hypothèses

Il existe $p < n$ tel que

- $F(X(t)) = F\left(X_1(t), \ldots, X_p(t)\right)$, $H(X(t-\tau)) = H\left(X_1(t-\tau), \ldots, X_p(t-\tau)\right)$
- $C = \left(\begin{array}{c|c} I_p & \bar{C} \end{array} \right)$, $\bar{C} = (\zeta_i \delta_{ij(i)})_{(i,j)\in[1,n]\times[1,p]}$
  $\Rightarrow Y_i(t) = X_i(t) + \zeta_i X_{j(i)}(t), \quad p < j(i) \leqslant n$

- Transformation du système : $\begin{array}{l}\dot{X} = \tilde{A}X + \tilde{B}Y + \tilde{F}(X,Y) + \tilde{H}(X_\tau, Y_\tau)) \\ Y = CX\end{array}$

Extension au cas général

- Modèle dynamique en dimension n : $\begin{array}{l}\dot{X} = AX + F(X) + H(X_\tau) \\ Y(t) = CX(t)\end{array}$

Hypothèses

Il existe $p < n$ tel que

- $F(X(t)) = F\left(X_1(t), \ldots, X_p(t)\right)$, $H(X(t-\tau)) = H\left(X_1(t-\tau), \ldots, X_p(t-\tau)\right)$
- $C = \left(\begin{array}{c|c} I_p & \bar{C} \end{array}\right)$, $\bar{C} = (\zeta_i \delta_{ij(i)})_{(i,j)\in[1,n]\times[1,p]}$
  $\Rightarrow Y_i(t) = X_i(t) + \zeta_i X_{j(i)}(t), \quad p < j(i) \leqslant n$

- Transformation du système : $\begin{array}{l}\dot{X} = \tilde{A}X + \tilde{B}Y + \tilde{F}(X,Y) + \tilde{H}(X_\tau, Y_\tau)) \\ Y = CX\end{array}$

Notations

$X = \left(\begin{array}{c} \bar{X} \\ \bar{\bar{X}} \end{array}\right)$, $\dim \bar{X} = (p \times n)$, $A = \left(\begin{array}{c|c} \bar{A} & \bar{\bar{A}} \end{array}\right)$

$$\Rightarrow AX = \left(\begin{array}{cc} \bar{A} & \bar{\bar{A}} \end{array}\right) \left(\begin{array}{c} Y - \bar{C}\bar{\bar{X}} \\ \bar{\bar{X}} \end{array}\right) = \bar{A}Y - \bar{A}\bar{C}\bar{\bar{X}} + \bar{\bar{A}}\bar{\bar{X}}$$

Identification : $\tilde{A} = \left(\begin{array}{c|c} 0_{n\times p} & \bar{A}\bar{C} + \bar{\bar{A}} \end{array}\right)$ et $\tilde{B} = \bar{A}$

Cas général (suite)

Constante de Lipschitz : fonction $\tilde{F}$

$$\tilde{F} = F\left(Y_1(t) - \zeta_1 X_{j(1)}(t), \ldots, Y_p(t) - \zeta_p X_{j(p)}(t)\right)$$

$$\begin{aligned} \|\tilde{F} - \hat{\tilde{F}}\| &= \|F\left(Y_1(t) - \zeta_1 X_{j(1)}(t), \ldots, Y_p(t) - \zeta_p X_{j(p)}(t)\right) \\ &\quad - F\left(Y_1(t) - \zeta_1 \hat{X}_{j(1)}(t), \ldots, Y_p(t) - \zeta_p \hat{X}_{j(p)}(t)\right)\| \\ \Rightarrow \quad &\leqslant k_F \zeta_{max} \| \left(X_{j(1)}(t) - \hat{X}_{j(1)}(t), \ldots, \; X_{j(p)}(t) - \hat{X}_{j(p)}(t)\right) \| \\ &\leqslant k_F \zeta_{max} \|\epsilon(t)\| \end{aligned}$$

avec $\zeta_{max} = \max_{i=1,p} |\zeta_i|$ et $\epsilon(t) = X(t) - \hat{X}(t)$

Constante de Lipschitz : fonction $\tilde{H}$

$$\tilde{H} = H\left(Y_1(t-\tau) - \zeta_1 X_{j(1)}(t-\tau), \ldots, Y_p(t-\tau) - \zeta_p X_{j(p)}(t-\tau)\right)$$

$$\Rightarrow \|\tilde{H} - \hat{\tilde{H}}\| \leqslant k_H \zeta_{max} \|\epsilon(t)\|$$

Observateur d'ordre réduit (1/2)

Modèle équivalent

- on choisit la matrice $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix} \Rightarrow x_1(t) = y(t) - \zeta x_2(t)$

$$\begin{cases} \dot{x}(t) = \tilde{A}x(t) + \tilde{B}y(t) + \tilde{F}(x(t), y(t)) + \tilde{H}(x_\tau(t), y_\tau(t)) \\ y(t) = Cx(t) \end{cases}$$

But = trouver une matrice E

- orthogonale au vecteur $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$
- telle que la matrice $\begin{pmatrix} E \\ C \end{pmatrix}$ soit de plein rang colonne

$$\Rightarrow \exists\ P, Q\ /\ \begin{pmatrix} P & Q \end{pmatrix} \begin{pmatrix} E \\ C \end{pmatrix} = I_3$$

Système singulier

$$\begin{cases} E\dot{x} = A_1 x + B_1 y + H_1(x_\tau) \\ y = Cx \end{cases} \quad \text{avec} \quad \begin{aligned} A_1 &= E\tilde{A} \\ B_1 &= E\tilde{B} \\ H_1 &= E\tilde{H} \end{aligned}$$

Observateur d'ordre réduit (2/2)

- État réduit : $z = Tx = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$
- Dynamique de l'observateur réduit : $\begin{array}{l} \dot{z} = Nz + Ky + r(z, y, z_\tau, y_\tau) \\ \hat{z} = z + TQy \end{array}$

Théorème

Si les conditions suivantes sont vérifiées :

- condition de détectabilité $\operatorname{rang} \begin{pmatrix} sE - A_1 \\ C \end{pmatrix} = \dim x, \ \forall s \geqslant 0$
- $\exists$ une matrice N telle que $NTPE - TP(A_1 + B_1 C) + KC = 0$
- la matrice $\begin{pmatrix} TPE \\ C \end{pmatrix}$ est inversible
- $\exists\, U = U^T > 0$ et $\Omega > 0$ telles que : $\begin{pmatrix} N^T U + UN + \Omega & UTP \\ (\star) & -\frac{1}{k_{H_1}} I_2 \end{pmatrix} < 0$, $k_{H_1} I_2 - \Omega < 0$

alors la fonction $r(z, y, z_\tau, y_\tau)$ peut être définie par : $r(z, y, z_\tau, y_\tau) = TPH_1(\hat{x}_\tau)$ où $\hat{x} = \begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} \begin{pmatrix} \hat{z} \\ y \end{pmatrix}$. Dans ce cas, $\hat{x} \to x$.

Démonstration

- Vecteur d'erreur de synchronisation réduit : $e = \hat{z} - z = z - TPEx$
- Dynamique de e :

$$\begin{aligned} \dot{e} &= Nz + Ky + r(z, y, z_\tau, y_\tau) - TP\left(A_1 x + B_1 y + H_1(x_\tau)\right) \\ &= Ne + TP\left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) \end{aligned}$$

- Fonctionnelle de Lyapunov-Krasovskii :

$$V = e^T U e + \int_{-\tau}^{0} e(t+\theta)^T \Omega e(t+\theta) d\theta$$

- On dérive l'expression de V :

$$\dot{V} = e^T \left(N^T U + UN + \Omega\right) e + 2e^T UTP\left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) - e_\tau^T \Omega e_\tau$$

- Majoration :

$$\dot{V} \leqslant e^T \left(N^T U + UN + k_{H_1}(UTP)(UTP)^T\right) e + e_\tau^T \left(k_{H_1} I_2 - \Omega\right) e_\tau$$

$\Rightarrow e \to 0$, puis $\hat{x} \to x$

Démonstration

- Vecteur d'erreur de synchronisation réduit : $e = \hat{z} - z = z - TPEx$
- Dynamique de e :

$$\begin{aligned} \dot{e} &= Nz + Ky + r(z, y, z_\tau, y_\tau) - TP\left(A_1 x + B_1 y + H_1(x_\tau)\right) \\ &= Ne + TP\left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) \end{aligned}$$

- Fonctionnelle de Lyapunov-Krasovskii :

$$V = e^T U e + \int_{-\tau}^{0} e(t+\theta)^T \Omega e(t+\theta) d\theta$$

- On dérive l'expression de V :

$$\dot{V} = e^T \left(N^T U + UN + \Omega\right) e + 2e^T UTP\left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) - e_\tau^T \Omega e_\tau$$

- Majoration :

$$\dot{V} \leqslant e^T \left(N^T U + UN + k_{H_1}(UTP)(UTP)^T\right) e + e_\tau^T \left(k_{H_1} I_2 - \Omega\right) e_\tau$$

$\Rightarrow e \to 0$, puis $\hat{x} \to x$

Démonstration

- Vecteur d'erreur de synchronisation réduit : $e = \hat{z} - z = z - TPEx$
- Dynamique de e :

$$\begin{aligned} \dot{e} &= Nz + Ky + r(z, y, z_\tau, y_\tau) - TP\left(A_1 x + B_1 y + H_1(x_\tau)\right) \\ &= Ne + TP\left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) \end{aligned}$$

- Fonctionnelle de Lyapunov-Krasovskii :

$$V = e^T U e + \int_{-\tau}^{0} e(t+\theta)^T \Omega e(t+\theta) d\theta$$

- On dérive l'expression de V :

$$\dot{V} = e^T \left(N^T U + UN + \Omega\right) e + 2e^T UTP\left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) - e_\tau^T \Omega e_\tau$$

- Majoration :

$$\dot{V} \leqslant e^T \left(N^T U + UN + k_{H_1}(UTP)(UTP)^T\right) e + e_\tau^T \left(k_{H_1} I_2 - \Omega\right) e_\tau$$

$\Rightarrow e \to 0$, puis $\hat{x} \to x$

Démonstration

- Vecteur d'erreur de synchronisation réduit : $e = \hat{z} - z = z - TPEx$
- Dynamique de e :

$$\begin{aligned} \dot{e} &= Nz + Ky + r(z, y, z_\tau, y_\tau) - TP\left(A_1 x + B_1 y + H_1(x_\tau)\right) \\ &= Ne + TP\left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) \end{aligned}$$

- Fonctionnelle de Lyapunov-Krasovskii :

$$V = e^T U e + \int_{-\tau}^{0} e(t+\theta)^T \Omega e(t+\theta) d\theta$$

- On dérive l'expression de V :

$$\dot{V} = e^T \left(N^T U + UN + \Omega\right) e + 2e^T UTP\left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) - e_\tau^T \Omega e_\tau$$

- Majoration :

$$\dot{V} \leqslant e^T \left(N^T U + UN + k_{H_1}(UTP)(UTP)^T\right) e + e_\tau^T \left(k_{H_1} I_2 - \Omega\right) e_\tau$$

$\Rightarrow e \to 0$, puis $\hat{x} \to x$

Synthèse des gains N et K

- $NTPE - TP(A_1 + B_1C) + KC = 0 \Leftrightarrow NT - TPA_2 = MC$
  avec $A_2 = A_1 + B_1C$ et $M = NTQ - K$
- $\exists\ L_1, L_2 : \begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} = \begin{pmatrix} L_1 & L_2 \end{pmatrix}$
- on multiplie (à droite) par $L_2 \Rightarrow NTL_2 - TPA_2L_2 = M$
- on multiplie (à droite) par $L_1 \Rightarrow N = TPA_2L_1$
- on définit une matrice R telle que $\begin{pmatrix} TPE \\ C \end{pmatrix} = \begin{pmatrix} I_2 & -F \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R \\ C \end{pmatrix}$
- D'où $\begin{cases} T(I_3 - QC) = R - FC \\ T = R + (TQ - F)C \\ T = R + SC \end{cases}$ avec $S = TQ - F$
- Finalement $N = RPA_2L_1 - SCPA_2L_1 \Rightarrow$ placement des pôles de S pour garantir la stabilité de N (si la paire (RPA_2L_1, CPA_2L_1) est détectable)

Synthèse des gains N et K

- $NTPE - TP(A_1 + B_1C) + KC = 0 \Leftrightarrow NT - TPA_2 = MC$
  avec $A_2 = A_1 + B_1C$ et $M = NTQ - K$
- $\exists\ L_1,\ L_2 : \begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} = \begin{pmatrix} L_1 & L_2 \end{pmatrix}$
- on multiplie (à droite) par $L_2 \Rightarrow NTL_2 - TPA_2L_2 = M$
- on multiplie (à droite) par $L_1 \Rightarrow N = TPA_2L_1$
- on définit une matrice R telle que $\begin{pmatrix} TPE \\ C \end{pmatrix} = \begin{pmatrix} I_2 & -F \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R \\ C \end{pmatrix}$
- D'où $\begin{cases} T(I_3 - QC) = R - FC \\ T = R + (TQ - F)C \\ T = R + SC \end{cases}$ avec $S = TQ - F$
- Finalement $N = RPA_2L_1 - SCPA_2L_1 \Rightarrow$ placement des pôles de S pour garantir la stabilité de N (si la paire (RPA_2L_1, CPA_2L_1) est détectable)

Synthèse des gains N et K

- $NTPE - TP(A_1 + B_1C) + KC = 0 \Leftrightarrow NT - TPA_2 = MC$
  avec $A_2 = A_1 + B_1C$ et $M = NTQ - K$
- $\exists\ L_1,\ L_2 : \begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} = \begin{pmatrix} L_1 & L_2 \end{pmatrix}$
- on multiplie (à droite) par $L_2 \Rightarrow NTL_2 - TPA_2L_2 = M$
- on multiplie (à droite) par $L_1 \Rightarrow N = TPA_2L_1$
- on définit une matrice R telle que $\begin{pmatrix} TPE \\ C \end{pmatrix} = \begin{pmatrix} I_2 & -F \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R \\ C \end{pmatrix}$
- D'où $\begin{cases} T(I_3 - QC) = R - FC \\ T = R + (TQ - F)C \\ T = R + SC \end{cases}$ avec $S = TQ - F$
- Finalement $N = RPA_2L_1 - SCPA_2L_1 \Rightarrow$ placement des pôles de S pour garantir la stabilité de N (si la paire (RPA_2L_1, CPA_2L_1) est détectable)

Synthèse des gains N et K

- $NTPE - TP(A_1 + B_1C) + KC = 0 \Leftrightarrow NT - TPA_2 = MC$
  avec $A_2 = A_1 + B_1C$ et $M = NTQ - K$
- $\exists\ L_1,\ L_2 : \begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} = \begin{pmatrix} L_1 & L_2 \end{pmatrix}$
- on multiplie (à droite) par $L_2 \Rightarrow NTL_2 - TPA_2L_2 = M$
- on multiplie (à droite) par $L_1 \Rightarrow N = TPA_2L_1$
- on définit une matrice R telle que $\begin{pmatrix} TPE \\ C \end{pmatrix} = \begin{pmatrix} I_2 & -F \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R \\ C \end{pmatrix}$
- D'où $\begin{cases} T(I_3 - QC) = R - FC \\ T = R + (TQ - F)C \\ T = R + SC \end{cases}$ avec $S = TQ - F$
- Finalement $N = RPA_2L_1 - SCPA_2L_1 \Rightarrow$ placement des pôles de S pour garantir la stabilité de N (si la paire (RPA_2L_1, CPA_2L_1) est détectable)

Synthèse des gains N et K

- $NTPE - TP(A_1 + B_1C) + KC = 0 \Leftrightarrow NT - TPA_2 = MC$
  avec $A_2 = A_1 + B_1C$ et $M = NTQ - K$
- $\exists\ L_1,\ L_2 : \begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} = \begin{pmatrix} L_1 & L_2 \end{pmatrix}$
- on multiplie (à droite) par $L_2 \Rightarrow NTL_2 - TPA_2L_2 = M$
- on multiplie (à droite) par $L_1 \Rightarrow N = TPA_2L_1$
- on définit une matrice R telle que $\begin{pmatrix} TPE \\ C \end{pmatrix} = \begin{pmatrix} I_2 & -F \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R \\ C \end{pmatrix}$
- D'où $\begin{cases} T(I_3 - QC) = R - FC \\ T = R + (TQ - F)C \\ T = R + SC \end{cases}$ avec $S = TQ - F$
- Finalement $N = RPA_2L_1 - SCPA_2L_1 \Rightarrow$ placement des pôles de S pour garantir la stabilité de N (si la paire (RPA_2L_1, CPA_2L_1) est détectable)

Synthèse des gains N et K

- $NTPE - TP(A_1 + B_1C) + KC = 0 \Leftrightarrow NT - TPA_2 = MC$
  avec $A_2 = A_1 + B_1C$ et $M = NTQ - K$
- $\exists\ L_1,\ L_2 : \begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} = \begin{pmatrix} L_1 & L_2 \end{pmatrix}$
- on multiplie (à droite) par $L_2 \Rightarrow NTL_2 - TPA_2L_2 = M$
- on multiplie (à droite) par $L_1 \Rightarrow N = TPA_2L_1$
- on définit une matrice R telle que $\begin{pmatrix} TPE \\ C \end{pmatrix} = \begin{pmatrix} I_2 & -F \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R \\ C \end{pmatrix}$
- D'où $\begin{cases} T(I_3 - QC) = R - FC \\ T = R + (TQ - F)C \\ T = R + SC \end{cases}$ avec $S = TQ - F$
- Finalement $N = RPA_2L_1 - SCPA_2L_1 \Rightarrow$ placement des pôles de S pour garantir la stabilité de N (si la paire (RPA_2L_1, CPA_2L_1) est détectable)

Synthèse des gains N et K

- $NTPE - TP(A_1 + B_1C) + KC = 0 \Leftrightarrow NT - TPA_2 = MC$
  avec $A_2 = A_1 + B_1C$ et $M = NTQ - K$
- $\exists\ L_1,\ L_2 : \begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} = \begin{pmatrix} L_1 & L_2 \end{pmatrix}$
- on multiplie (à droite) par $L_2 \Rightarrow NTL_2 - TPA_2L_2 = M$
- on multiplie (à droite) par $L_1 \Rightarrow N = TPA_2L_1$
- on définit une matrice R telle que $\begin{pmatrix} TPE \\ C \end{pmatrix} = \begin{pmatrix} I_2 & -F \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R \\ C \end{pmatrix}$
- D'où $\begin{cases} T(I_3 - QC) = R - FC \\ T = R + (TQ - F)C \\ T = R + SC \end{cases}$ avec $S = TQ - F$
- Finalement $N = RPA_2L_1 - SCPA_2L_1 \Rightarrow$ placement des pôles de S pour garantir la stabilité de N (si la paire (RPA_2L_1, CPA_2L_1) est détectable)

Simulations

Paramètres

α	β	γ	δ	ε	σ	τ
9	14	5	0.5	10	10^4	1

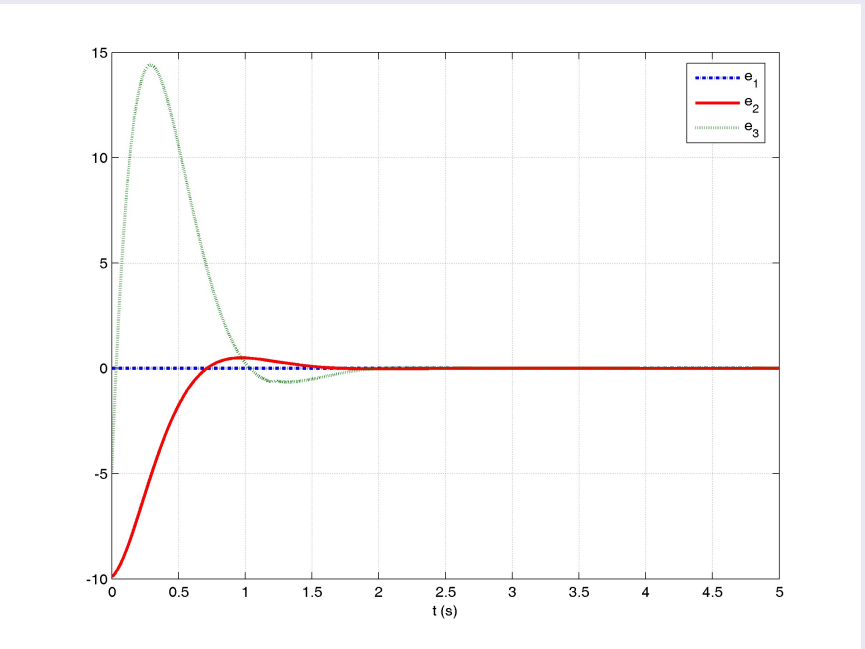
États initiaux

$$x_0 = \begin{pmatrix} 0,1 & 0 & 0,1 \end{pmatrix}^T$$
$$z_0 = \begin{pmatrix} 10 & 5 \end{pmatrix}^T$$

Gains

$$N = \begin{pmatrix} -1,00001 & 1 \\ -14 & -5 \end{pmatrix}$$
$$K = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

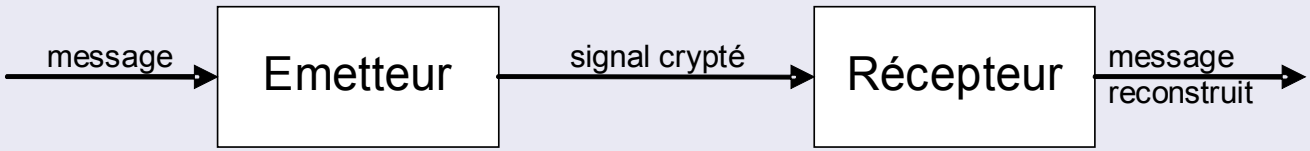
Erreurs d'estimation



Plan de la présentation

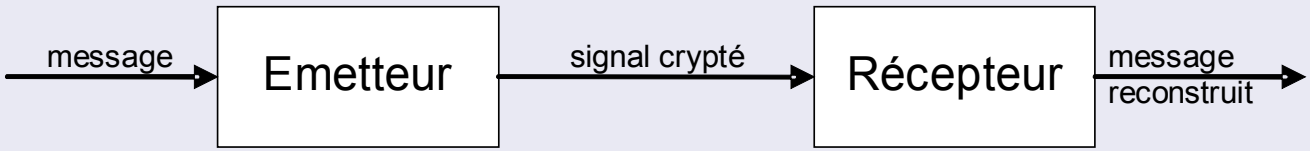
Cryptosystèmes chaotiques

Principe général : système de communications

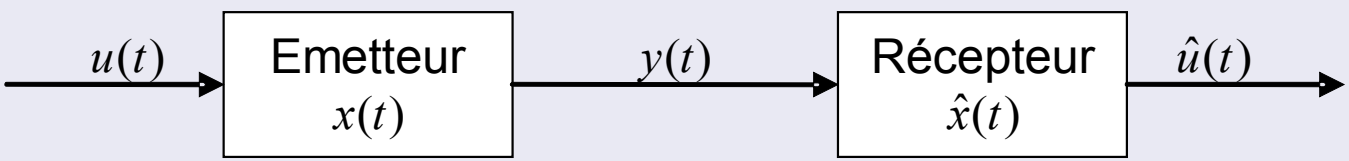


Cryptosystèmes chaotiques

Principe général : système de communications

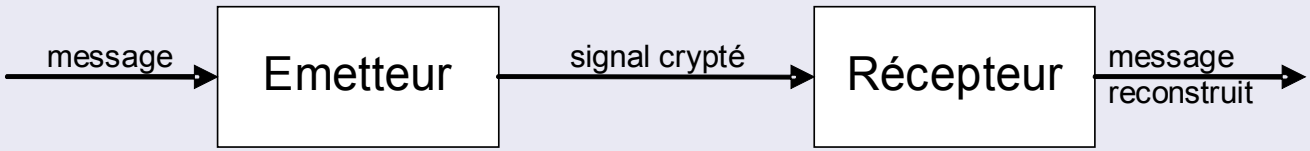


Observateur à entrées inconnues, ou cryptage par inclusion

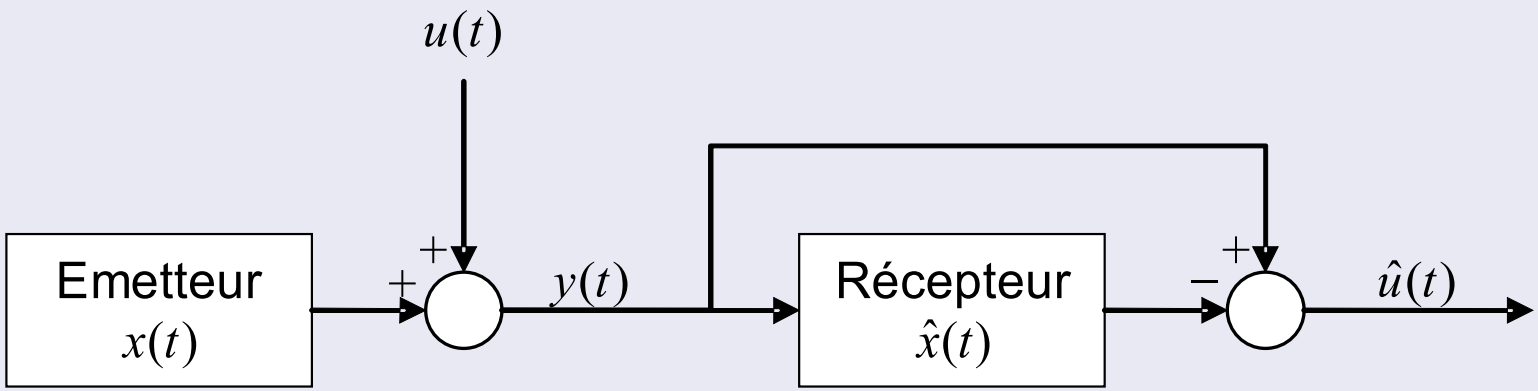


Cryptosystèmes chaotiques

Principe général : système de communications

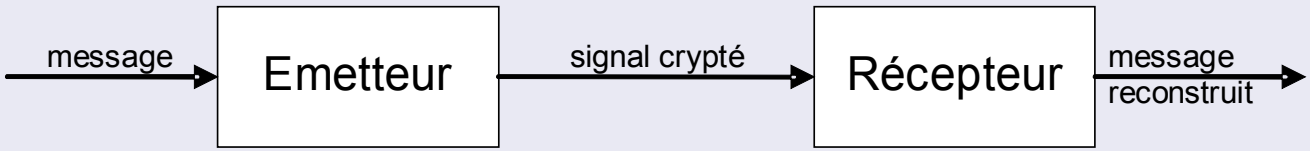


Cryptage par addition

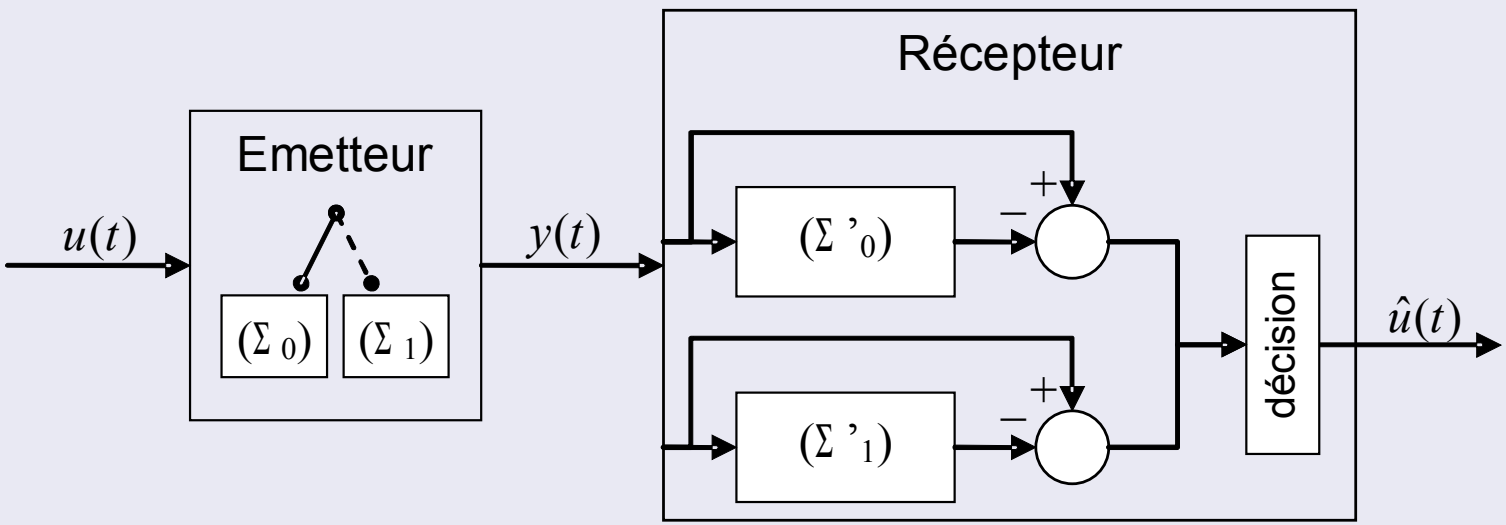


Cryptosystèmes chaotiques

Principe général : système de communications

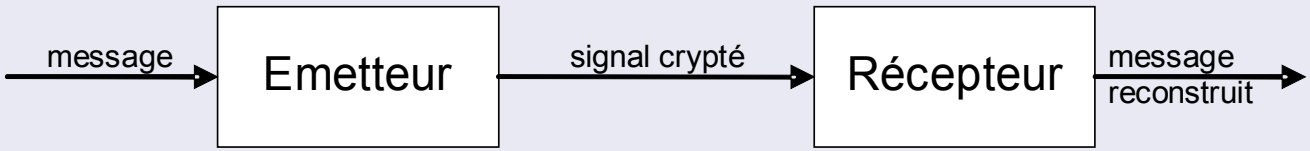


Cryptage par commutation

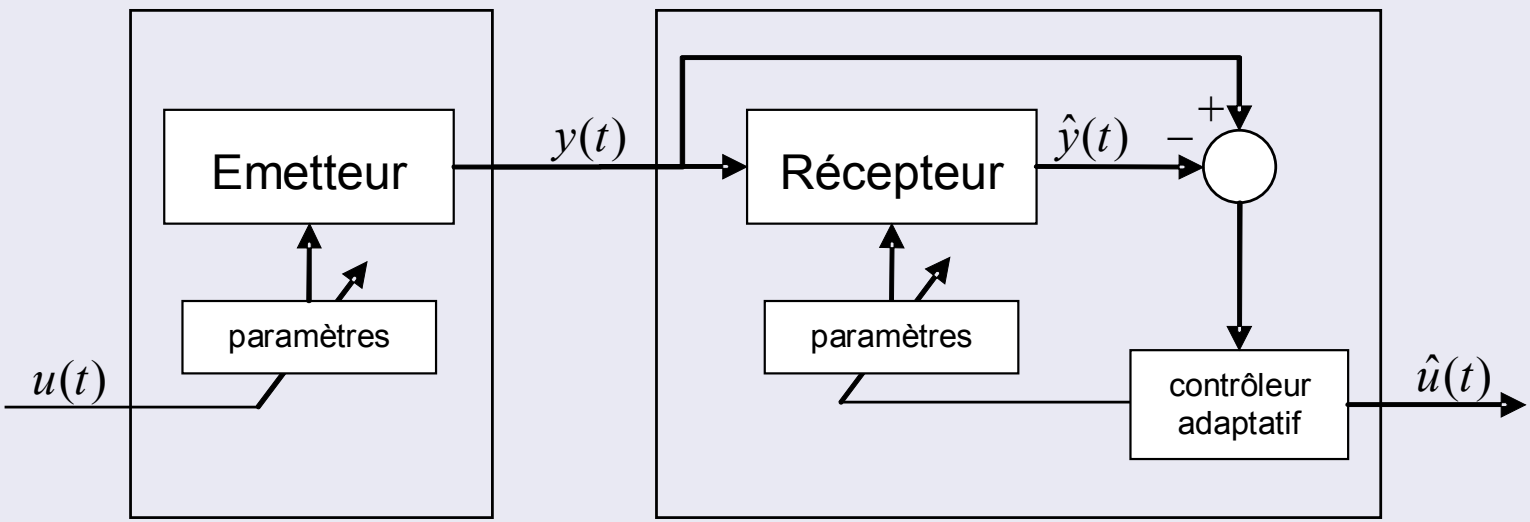


Cryptosystèmes chaotiques

Principe général : système de communications

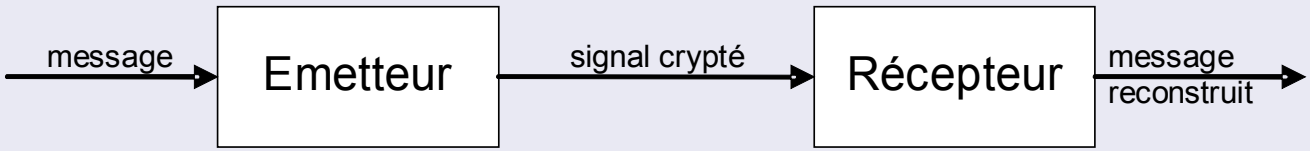


Cryptage par modulation de paramètre

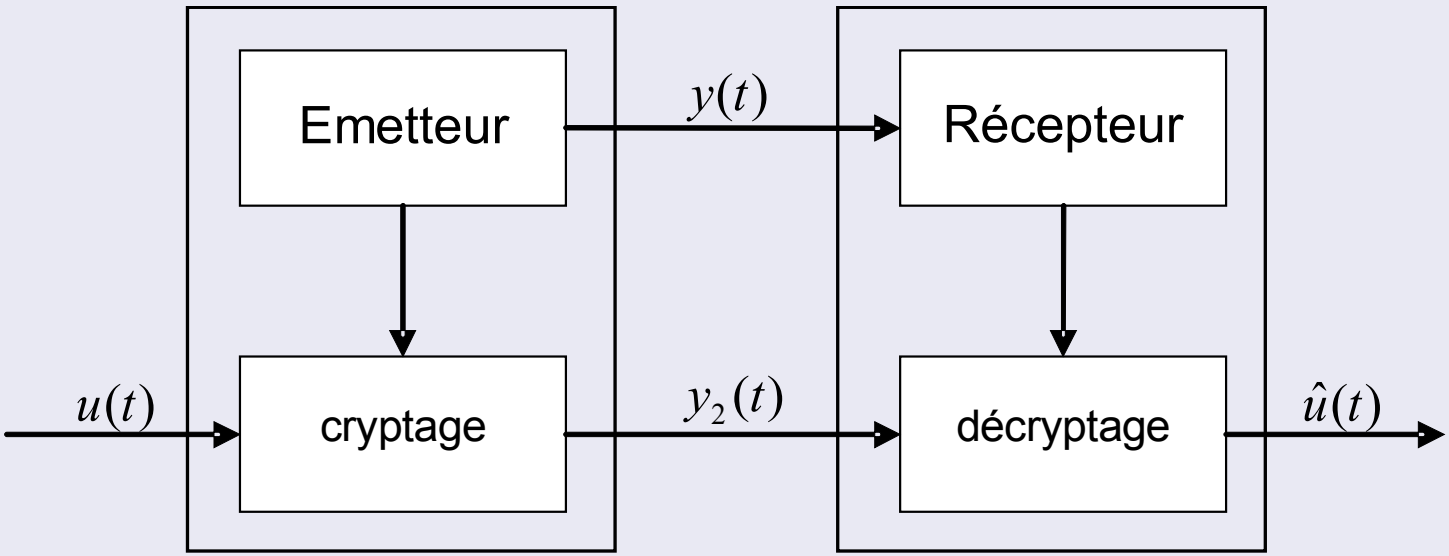


Cryptosystèmes chaotiques

Principe général : système de communications



Transmission à deux voies

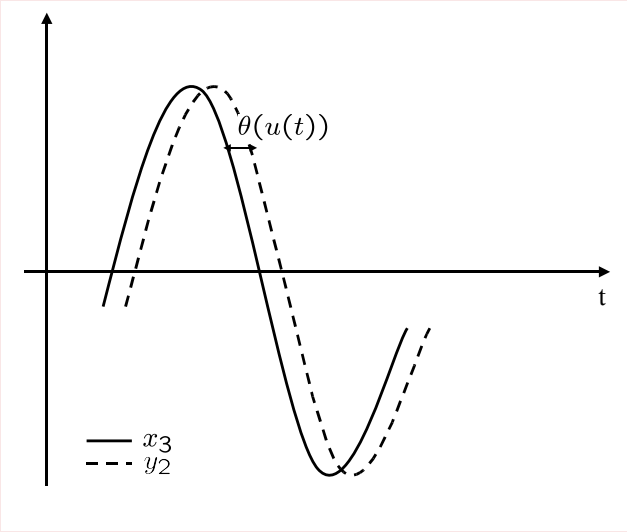


Modulation de phase

Méthode proposée

Modulation de la phase du second signal chaotique par une fonction du message
$\Rightarrow$ second signal transmis :

$$y_2(t) = x_3\left(t - \theta\left(u(t)\right)\right)$$



Choix de la fonction de modulation

$$\theta(u(t)) = T_u u(t)$$

Décryptage : approche analytique

Formule de Taylor-Lagrange :

$$\begin{aligned} y_2(t) - x_3(t) &= y_2(t) - x_3(t - T_u u(t)) \\ &= \sum_{k=1}^{n} \frac{(-T_u u(t))^k}{k!} x_3^{(k)}(t) - \int_{t-T_u u(t)}^{t} \frac{(t - T_u u(t) - s)^n}{n!} x_3^{(n+1)}(s) ds \end{aligned}$$

Décryptage : approche analytique

Formule de Taylor-Lagrange :

$$\begin{aligned} y_2(t) - x_3(t) &= y_2(t) - x_3(t - T_u u(t)) \\ &= \sum_{k=1}^{n} \frac{(-T_u u(t))^k}{k!} x_3^{(k)}(t) - \int_{t-T_u u(t)}^{t} \frac{(t - T_u u(t) - s)^n}{n!} x_3^{(n+1)}(s) ds \end{aligned}$$

Approximation à l'ordre un :

$$y_2(t) - x_3(t) = -T_u u(t) \dot{x}_3(t)$$

Décryptage : approche analytique

Formule de Taylor-Lagrange :

$$\begin{aligned} y_2(t) - x_3(t) &= y_2(t) - x_3(t - T_u u(t)) \\ &= \sum_{k=1}^{n} \frac{(-T_u u(t))^k}{k!} x_3^{(k)}(t) - \int_{t-T_u u(t)}^{t} \frac{(t - T_u u(t) - s)^n}{n!} x_3^{(n+1)}(s) ds \end{aligned}$$

Approximation à l'ordre un :

$$y_2(t) - x_3(t) = -T_u u(t) \dot{x}_3(t)$$

Formule de décryptage

$$\hat{u}(t) = \frac{\hat{x}_3(t) - y_2(t)}{T_u \dot{\hat{x}}_3(t)}$$

Simulations numériques

- Système émetteur :

$$\begin{cases} \dot{x}_1(t) = -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta \tanh(x_1(t)) \\ \dot{x}_2(t) = x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) = -\beta x_2(t) - \gamma x_3(t) + \varepsilon \sin(\sigma x_{1\tau}(t)) \end{cases}$$

- Paramètres :

α	β	γ	δ	ε	σ	τ
9	14	5	$0,5$	100	10^4	1

- Signaux transmis au récepteur :
  - $y(t) = Cx(t)$ avec $C = (\ 1 \quad \zeta \quad 0\ )$, $\zeta = 10^{-5}$
  - $y_2(t) = x_3(t - T_u u(t))$ avec $T_u = 0,01$ s

Transmission d'un texte

Texte original

message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide

Baudelaire "Harmonie du soir", extrait des Fleurs du mal
Voici venir les temps où vibrant sur sa tige
Chaque fleur s'évapore ainsi qu'un encensoir;
Les sons et les parfums tournent dans l'air du soir;
Valse mélancolique et langoureux vertige!

Chaque fleur s'évapore ainsi qu'un encensoir;
Le violon frémit comme un coeur qu'on afflige;
Valse mélancolique et langoureux vertige!
Le ciel est triste et beau comme un grand reposoir.

Le violon frémit comme un coeur qu'on afflige,
Un coeur tendre, qui hait le néant vaste et noir!
Le ciel est triste et beau comme un grand reposoir;
Le soleil s'est noyé dans son sang qui se fige.

Un coeur tendre, qui hait le néant vaste et noir,
Du passé lumineux recueille tout vestige!
Le soleil s'est noyé dans son sang qui se fige...
Ton souvenir en moi luit comme un ostensoir!

Texte crypté

ÍÔÓÒÐÏÎÍÌËÊÉÇÆÅÄÃÂÁ¿¾½¼»º¸·¶µ´²±°¯®-
«ª©¨§¥¤£¢¡Ÿž□œ›™˜—–”“‘’‚□Ž□‹Š^^†…„„□□
~}{zxwvtsqpnmkjigfdcb`_]\[YXWUTRRPONMLJIHGFE
DCBBA@?>==<<;:::9988888887778888999::;<<=>>?@
ABBDEFGHIJKLNOQRSTVWXZ[]^`acdfgiklnoqrtuwxz{
}~□□„„†^‰Š‹Œ□□□‘’“”•˜™™ššš›››œœœœœœœ›››››šš
™˜˜•”“’‘□‹Š‰‡†ƒ‚€~}{zxvurqonljhfdca_]ZYWUSRPNLJ
IGECA@>=;:865421//,+*)('&%%$$##""!!!!!!!!!!""#$$%
&&'()*+,./0234689<=?@BDFHKLNPSUWY[]`bdgiknpst
wy{}€,…†‰‹□□‘“•—™›□Ÿ ¢£¤¥§¨ª«®¯°±²³
´µ¶·¸,,,¹¹¹ººº¹¹¹,,,...¶µ´³²°°®¬«©¨¥¤¢ žœ›™•'Š‰†„„~zwtrol
igda^[YVSPMKHEC@=;7530.+)'$##################
######################%(*0259;>ADHKNQTX[^ceh
lotvz}€„‡‹□‘•˜œ £¦©¬
´·¸½ÀÃÄÅÈËÎÐÓÖ×ÙÛÝßáâåçêëìíîñòôõö÷øùúûüüýþþÿÿÿ
ÿÿÿÿÿÿÿÿÿþþýýüüûûúùø÷öõôóòñðïîíìëêèçæãâáàÞÜÛÙ×ÖÕÓÒ
ÐÎÍËÊÈÆÄÃÁ¾¼º¹¸µ²±¯«©¦¥¢¢Ÿ□›™—•'□ŽŒŠ^…„„□
~ywusqomkigdb`^\ZXVTRQNMKHGEDBA?=<:97553210/.-++*))("&&%%%%%%%%%%%&&"())*+,-
./01345789<=>@BCEGIKMOQSUWY[]`bdgikloqsuxz|
~€,…†‰‰ŒŽ□’”–˜š›□ž ¢£¤¦§©ª«¬®¯°±²³´´´µµµµµµ
´´´³³²±°¯®¬ª©¨§¦¤¢¡Ÿ□›™—–”‘□□‹‰†„„□|
zxuspmjhgc`^[XVSPNKGFC@><9742/-+)&$"
################################ #

Texte décrypté

ÿÿÿÿÿÿÿÿÿ

Transmission d'une image

Image originale

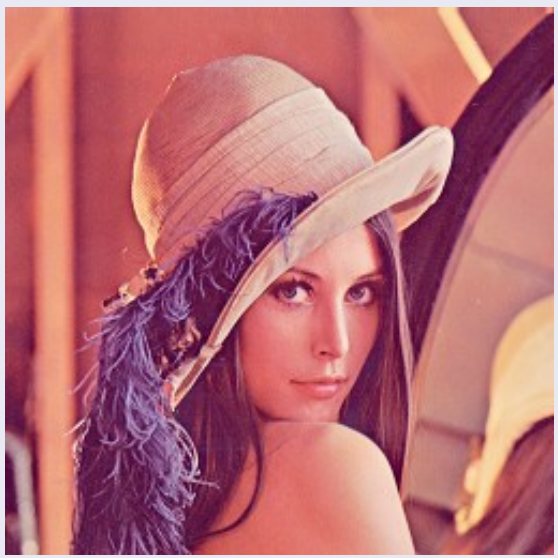
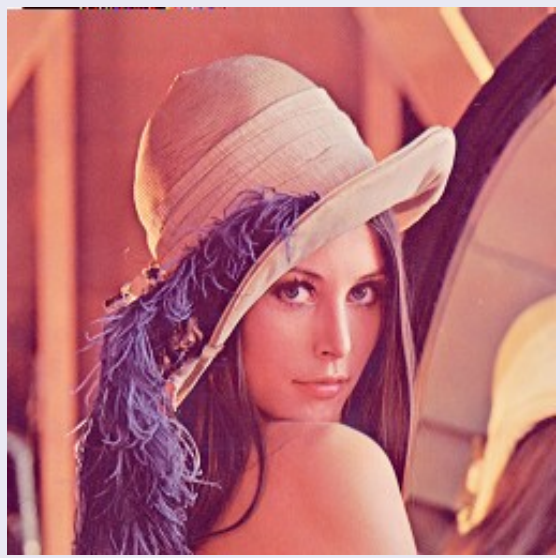


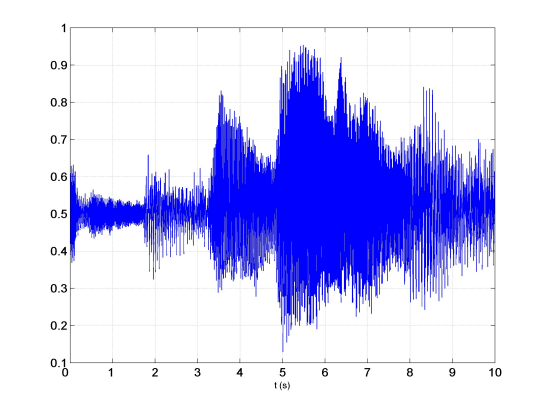
Image cryptée

Image reconstruite



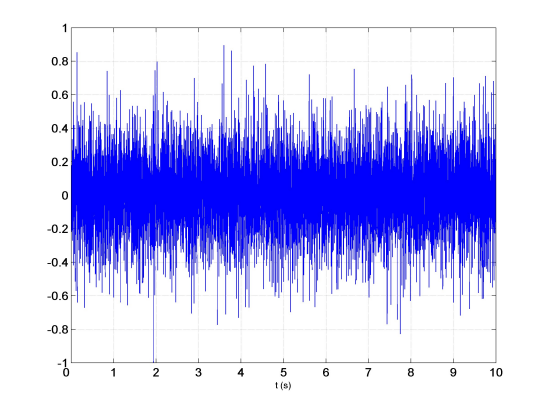
Transmission d'un son

Son original



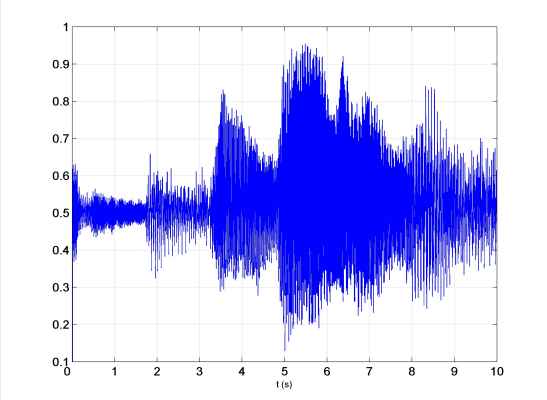
Son original

Son crypté



Son crypté

Son reconstruit



Son décrypté

Plan de la présentation

Sécurité de la synchronisation

Attaques par des techniques de reconstruction à retard

- Signal chaotique différent d'un bruit blanc
- Propriétés géométriques caractéristiques de chaque type d'attracteur
- Signature de chaque émetteur chaotique (au niveau temporel et spectral)

Sécurité de la synchronisation

Attaques par des techniques de reconstruction à retard

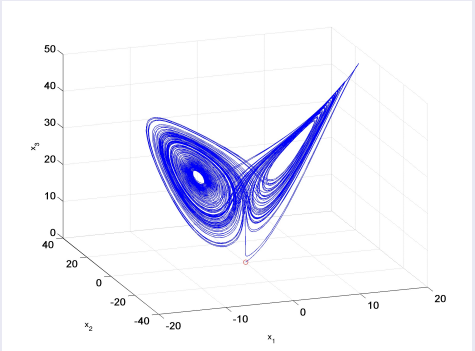
- Signal chaotique différent d'un bruit blanc
- Propriétés géométriques caractéristiques de chaque type d'attracteur
- Signature de chaque émetteur chaotique (au niveau temporel et spectral)

Sécurité de la synchronisation

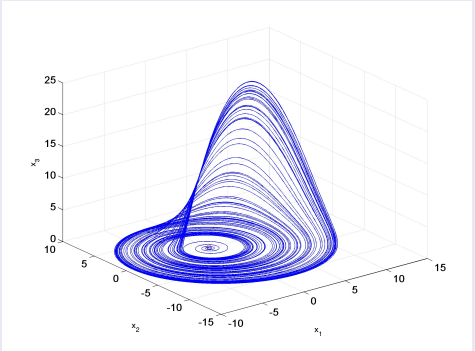
Attaques par des techniques de reconstruction à retard

- Signal chaotique différent d'un bruit blanc
- Propriétés géométriques caractéristiques de chaque type d'attracteur
- Signature de chaque émetteur chaotique (au niveau temporel et spectral)

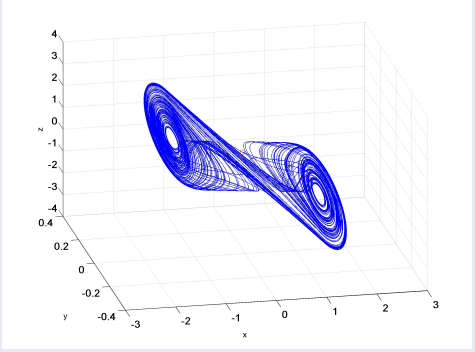
Système de Lorenz



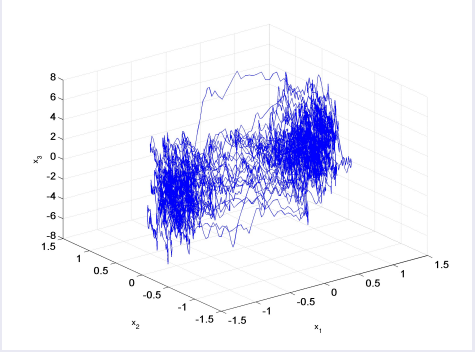
Système de Rössler



Circuit de Chua



Système à retard

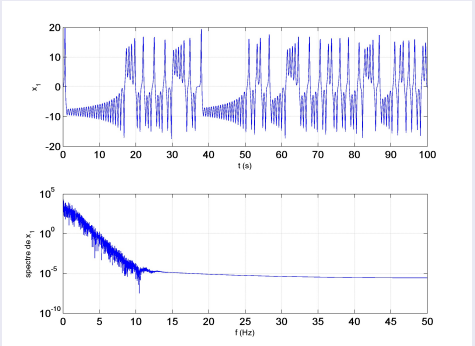


Sécurité de la synchronisation

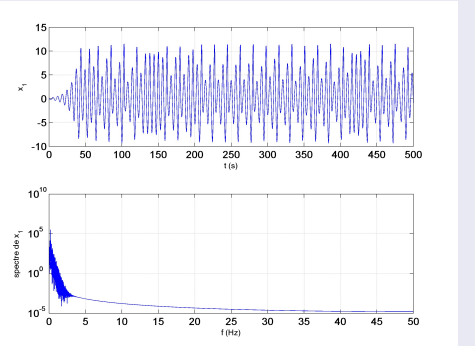
Attaques par des techniques de reconstruction à retard

- Signal chaotique différent d'un bruit blanc
- Propriétés géométriques caractéristiques de chaque type d'attracteur
- Signature de chaque émetteur chaotique (au niveau temporel et spectral)

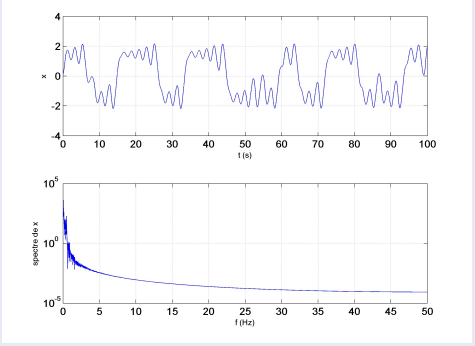
Système de Lorenz



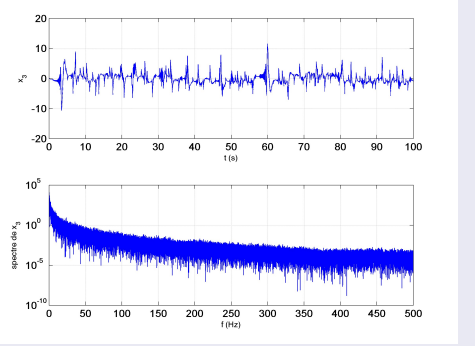
Système de Rössler



Circuit de Chua



Système à retard



Nouvelle famille de systèmes chaotiques

Multimodèles linéaires

- Modèle non linéaire $\dot{x}(t) = f(x(t))$
- p modèles linéaires de base
  $\dot{x}_i(t) = A_i x_i(t)$

$\Rightarrow$ multimodèle

$$\dot{x}(t) = \sum_{i=1}^{p} \mu_i(\xi(t)) A_i x(t)$$

- avec $\begin{cases} \sum_{i=1}^{p} \mu_i(\xi) = 1 \\ 0 \leq \mu_i(\xi) \leq 1 \ \forall i = 1, p \end{cases}$

Multimodèles chaotiques

- p modèles chaotiques
  $\dot{x}_i(t) = A_i x_i(t) + f_i(x_i(t))$

$\Rightarrow$ multimodèle chaotique

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{p} \mu_i(y(t)) \left(A_i x(t) + f_i(x(t))\right) \\ y(t) = Cx(t) \end{cases}$$

- avec $\begin{cases} \sum_{i=1}^{p} \mu_i(y) = 1 \\ 0 \leq \mu_i(y) \leq 1 \ \forall i = 1, p \end{cases}$

Nouvelle famille de systèmes chaotiques

Multimodèles linéaires

- Modèle non linéaire $\dot{x}(t) = f(x(t))$
- p modèles linéaires de base
  $\dot{x}_i(t) = A_i x_i(t)$

$\Rightarrow$ multimodèle

$$\dot{x}(t) = \sum_{i=1}^{p} \mu_i(\xi(t)) A_i x(t)$$

- avec $\begin{cases} \sum_{i=1}^{p} \mu_i(\xi) = 1 \\ 0 \leq \mu_i(\xi) \leq 1 \ \forall i = 1, p \end{cases}$

Multimodèles chaotiques

- p modèles chaotiques
  $\dot{x}_i(t) = A_i x_i(t) + f_i(x_i(t))$

$\Rightarrow$ multimodèle chaotique

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{p} \mu_i(y(t)) \left(A_i x(t) + f_i(x(t))\right) \\ y(t) = Cx(t) \end{cases}$$

- avec $\begin{cases} \sum_{i=1}^{p} \mu_i(y) = 1 \\ 0 \leq \mu_i(y) \leq 1 \ \forall i = 1, p \end{cases}$

Exemple 1

Multimodèle à base de circuits de Chua

Modèle de base :

$$\begin{cases} \dot{x_1} = -\alpha x_1 + \alpha x_2 - \alpha f(x_1) \\ \dot{x_2} = x_1 - x_2 + x_3 \\ \dot{x_3} = -\beta x_2 - \gamma x_3 \end{cases}$$

avec $f(x_1) = bx_1 + \frac{1}{2}(a-b)\left(|x_1+1| - |x_1-1|\right)$

Exemple 1

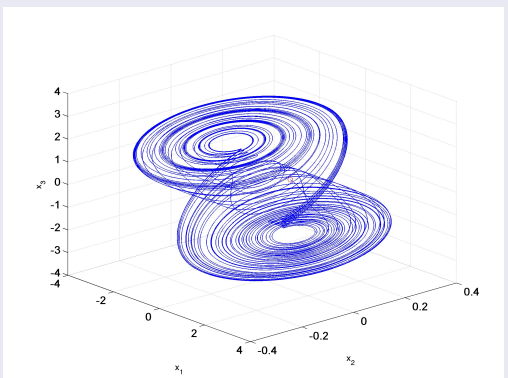
Multimodèle à base de circuits de Chua

Modèle de base :

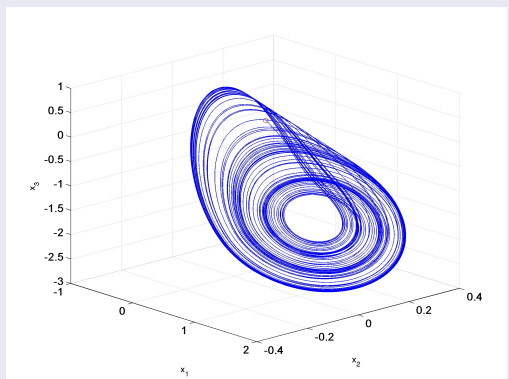
$$\begin{cases} \dot{x_1} = -\alpha x_1 + \alpha x_2 - \alpha f(x_1) \\ \dot{x_2} = x_1 - x_2 + x_3 \\ \dot{x_3} = -\beta x_2 - \gamma x_3 \end{cases}$$

avec $f(x_1) = bx_1 + \frac{1}{2}(a-b)\left(|x_1+1| - |x_1-1|\right)$

Premier modèle



Second modèle



Exemple 1

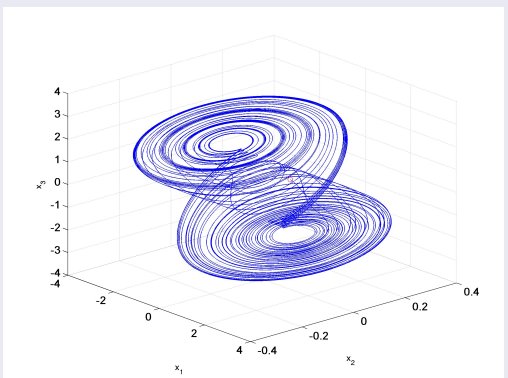
Multimodèle à base de circuits de Chua

Modèle de base :

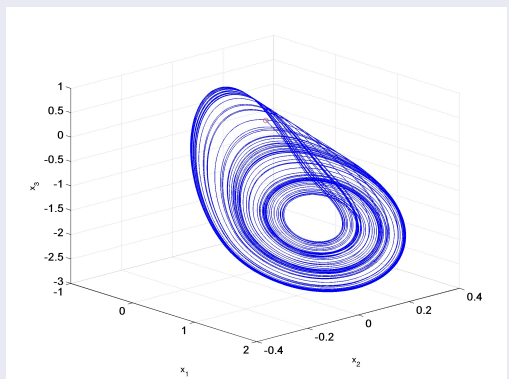
$$\begin{cases} \dot{x_1} = -\alpha x_1 + \alpha x_2 - \alpha f(x_1) \\ \dot{x_2} = x_1 - x_2 + x_3 \\ \dot{x_3} = -\beta x_2 - \gamma x_3 \end{cases}$$

avec $f(x_1) = bx_1 + \frac{1}{2}(a-b)\left(|x_1+1| - |x_1-1|\right)$

Premier modèle



Second modèle



Multimodèle

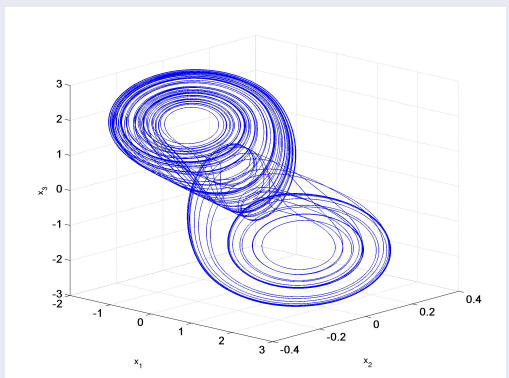


Diagramme de bifurcations

Fonction d'activation μ

$$\mu(y) = \frac{1 + \tanh(\omega y)}{2}$$

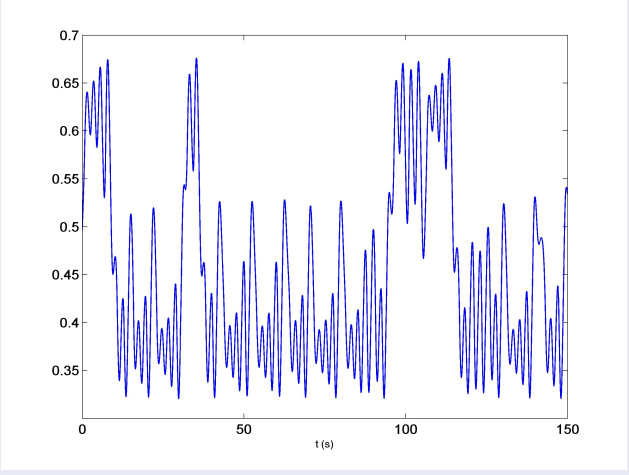
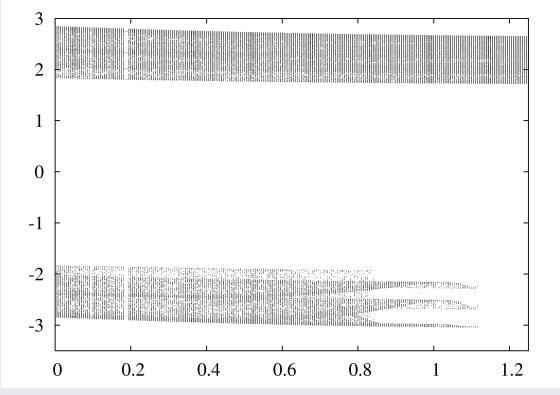
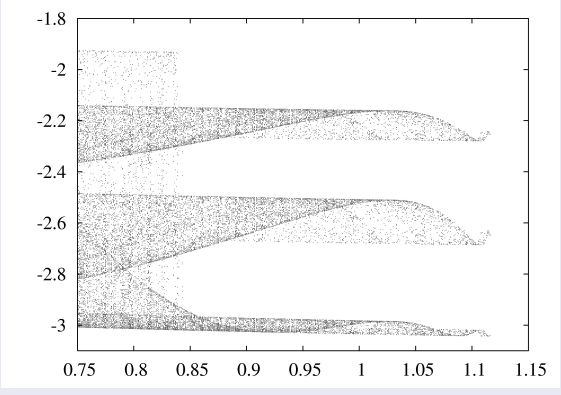


Diagramme de bifurcations (par rapport à ω)



$\omega \in [0; 1,25]$



Zoom : $\omega \in [0,75; 1,15]$

Exemple 2

Multimodèle à base de systèmes de Lorenz et Chua

Modèle de base :

$$\begin{cases} \dot{x}_1 = -\sigma x_1 + \sigma x_2 \\ \dot{x}_2 = \gamma x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 = x_1 x_2 - \beta x_3 \end{cases}$$

avec $\mu(y(t)) = \dfrac{1 + \tanh(\omega y(t) + \nu)}{2}$, $\omega = -0.01$, $\nu = 0.2$

Exemple 2

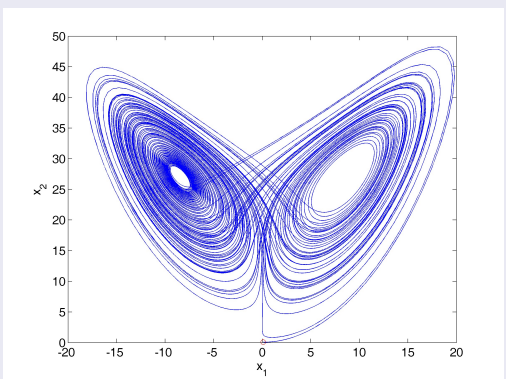
Multimodèle à base de systèmes de Lorenz et Chua

Modèle de base :

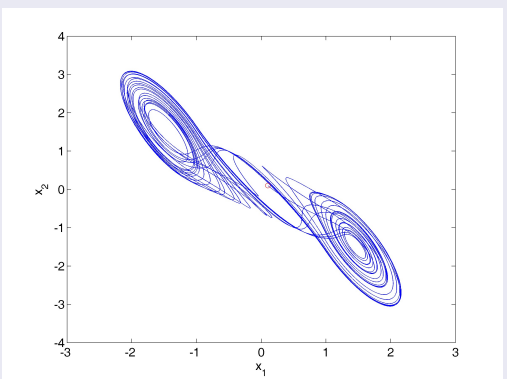
$$\begin{cases} \dot{x}_1 = -\sigma x_1 + \sigma x_2 \\ \dot{x}_2 = \gamma x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 = x_1 x_2 - \beta x_3 \end{cases}$$

avec $\mu(y(t)) = \dfrac{1 + \tanh(\omega y(t) + \nu)}{2}$, $\omega = -0.01$, $\nu = 0.2$

Premier modèle : Lorenz



Second modèle : Chua



Exemple 2

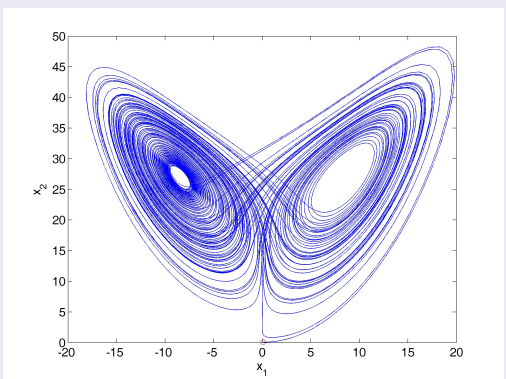
Multimodèle à base de systèmes de Lorenz et Chua

Modèle de base :

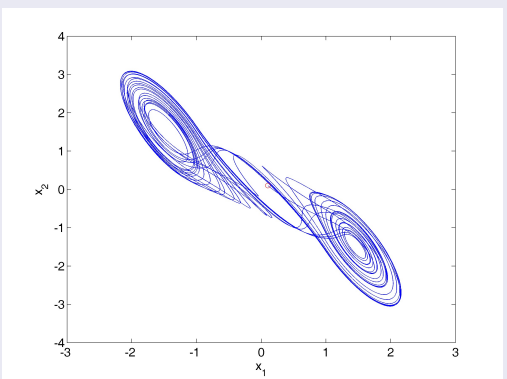
$$\begin{cases} \dot{x}_1 = -\sigma x_1 + \sigma x_2 \\ \dot{x}_2 = \gamma x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 = x_1 x_2 - \beta x_3 \end{cases}$$

avec $\mu(y(t)) = \dfrac{1 + \tanh(\omega y(t) + \nu)}{2}$, $\omega = -0.01$, $\nu = 0.2$

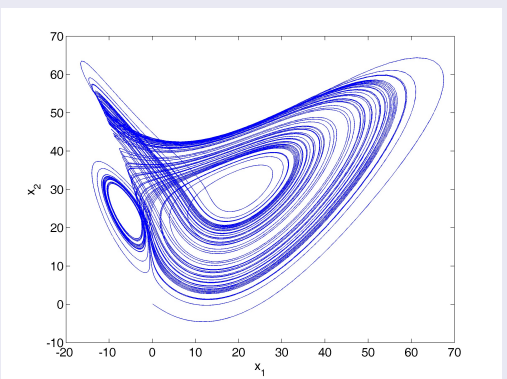
Premier modèle : Lorenz



Second modèle : Chua



Multimodèle



Exemple 3

Multimodèle à retard

Modèle de base :

$$\begin{cases} \dot{x}_1 &= -\alpha x_1 + \alpha x_1 - \alpha\delta \tanh(x_1) \\ \dot{x}_2 &= x_1 - x_2 + x_3 \\ \dot{x}_3 &= -\beta x_2 - \gamma x_3 + \varepsilon \sin(\sigma x_{1\tau}) \end{cases}$$

avec $\mu(y) = \dfrac{1 + \tanh(\omega y)}{2}$

Exemple 3

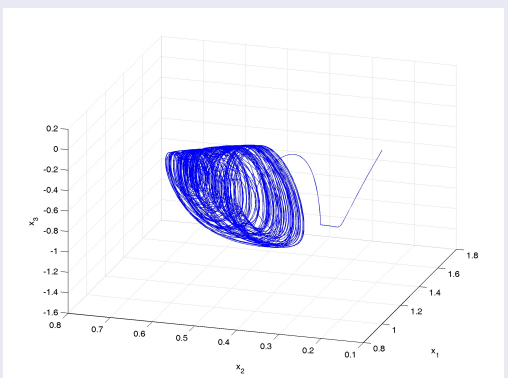
Multimodèle à retard

Modèle de base :

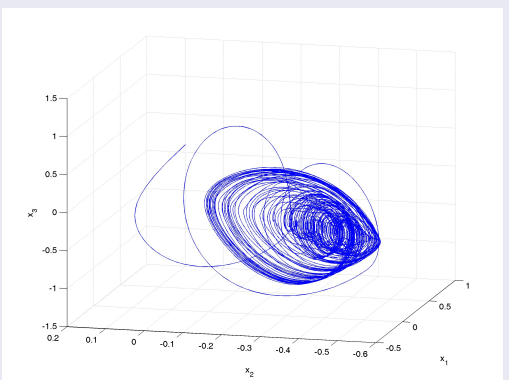
$$\begin{cases} \dot{x}_1 &= -\alpha x_1 + \alpha x_1 - \alpha\delta \tanh(x_1) \\ \dot{x}_2 &= x_1 - x_2 + x_3 \\ \dot{x}_3 &= -\beta x_2 - \gamma x_3 + \varepsilon \sin(\sigma x_{1\tau}) \end{cases}$$

avec $\mu(y) = \dfrac{1 + \tanh(\omega y)}{2}$

Premier modèle



Second modèle



Exemple 3

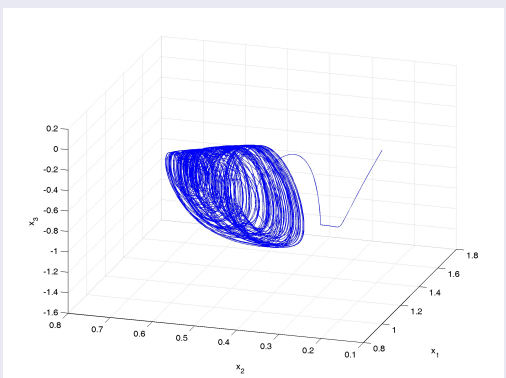
Multimodèle à retard

Modèle de base :

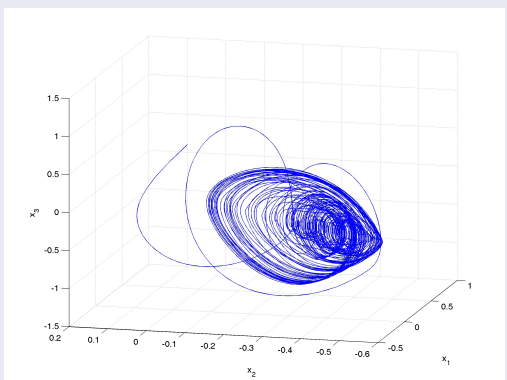
$$\begin{cases} \dot{x}_1 &= -\alpha x_1 + \alpha x_1 - \alpha\delta \tanh(x_1) \\ \dot{x}_2 &= x_1 - x_2 + x_3 \\ \dot{x}_3 &= -\beta x_2 - \gamma x_3 + \varepsilon \sin(\sigma x_{1\tau}) \end{cases}$$

avec $\mu(y) = \dfrac{1 + \tanh(\omega y)}{2}$

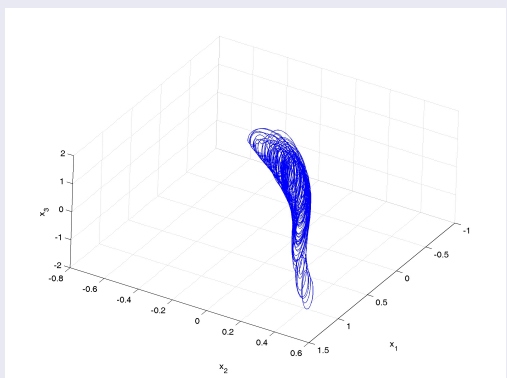
Premier modèle



Second modèle



Multimodèle



Synchronisation des multimodèles chaotiques

- Émetteur = multimodèle chaotique
- Récepteur = observateur spécifique :

$$\dot{\hat{x}}(t) = \sum_{i=1}^{p} \mu_i(y(t)) \Big(A_i \hat{x}(t) + f_i(\hat{x}(t)) + K_i(y(t) - C\hat{x}(t)) \Big)$$

Théorème

S'il existe une matrice symétrique définie positive P, des matrices définies positives Q et Q_i, $i = 1, p$ et p gains K_i tels que, pour $i = 1, p$:

$$\begin{pmatrix} (A_i - K_i C)^T P + P (A_i - K_i C) + k_{f_i} I + Q_i & P \\ P & -\frac{1}{k_{f_i}} I \end{pmatrix} < 0$$

et

$$Q_i < Q$$

alors l'erreur de synchronisation $e(t) = x(t) - \hat{x}(t)$ converge exponentiellement vers zéro, selon la formule $\|e(t)\| \leqslant \rho \|e(0)\| e^{-\frac{\nu}{2} t}$ avec $\rho = \sqrt{\frac{\lambda_M(P)}{\lambda_m(P)}}$ et $\nu = \frac{\lambda_m(Q)}{\lambda_M(P)}$

Synchronisation des multimodèles chaotiques

- Émetteur = multimodèle chaotique
- Récepteur = observateur spécifique :

$$\dot{\hat{x}}(t) = \sum_{i=1}^{p} \mu_i(y(t)) \Big(A_i \hat{x}(t) + f_i(\hat{x}(t)) + K_i(y(t) - C\hat{x}(t)) \Big)$$

Théorème

S'il existe une matrice symétrique définie positive P, des matrices définies positives Q et Q_i, $i = 1, p$ et p gains K_i tels que, pour $i = 1, p$:

$$\begin{pmatrix} (A_i - K_i C)^T P + P (A_i - K_i C) + k_{f_i} I + Q_i & P \\ P & -\frac{1}{k_{f_i}} I \end{pmatrix} < 0$$

et

$$Q_i < Q$$

alors l'erreur de synchronisation $e(t) = x(t) - \hat{x}(t)$ converge exponentiellement vers zéro, selon la formule $\|e(t)\| \leqslant \rho \|e(0)\| e^{-\frac{\nu}{2} t}$ avec $\rho = \sqrt{\frac{\lambda_M(P)}{\lambda_m(P)}}$ et $\nu = \frac{\lambda_m(Q)}{\lambda_M(P)}$

Plan de la présentation

Conclusion

Cryptosystème chaotique

- problème d'estimation d'état pour une classe de systèmes non linéaires chaotiques à retard
- problème de restauration d'entrées inconnues

Solution proposée : cryptosystème chaotique par modulation de phase

- choix d'un émetteur : système chaotique à retard
- conception du récepteur : synchronisation à base d'observateurs non linéaires
  - observateur d'ordre plein
  - observateur d'ordre réduit
  - observateur robuste
- cryptage : par modulation de phase chaotique, transmission double
- extension aux multimodèles chaotiques

Conclusion

Cryptosystème chaotique

- problème d'estimation d'état pour une classe de systèmes non linéaires chaotiques à retard
- problème de restauration d'entrées inconnues

Solution proposée : cryptosystème chaotique par modulation de phase

- choix d'un émetteur : système chaotique à retard
- conception du récepteur : synchronisation à base d'observateurs non linéaires
  - observateur d'ordre plein
  - observateur d'ordre réduit
  - observateur robuste
- cryptage : par modulation de phase chaotique, transmission double
- extension aux multimodèles chaotiques

Perspectives

Sur le plan pratique

- expérimentation : dispositif électronique
- robustesse au bruit de transmission : observateur robuste, tests sur carte dSpace

Sur le plan théorique

- approfondissement des multimodèles
- cas du temps discret
- extension des résultats $\longrightarrow$ diagnostic

Perspectives

Sur le plan pratique

- expérimentation : dispositif électronique
- robustesse au bruit de transmission : observateur robuste, tests sur carte dSpace

Sur le plan théorique

- approfondissement des multimodèles
- cas du temps discret
- extension des résultats $\longrightarrow$ diagnostic