Observateurs non linéaires de multimodèles. Application à la synchronisation et aux communications

Estelle Cherrier [,**], Mohamed Boutayeb [**], José Ragot [*]*

[*] *CRAN UMR CNRS 7039*
INPL 2 Avenue de la Forêt de Haye
54516 Vandoeuvre-lès-Nancy Cedex

[**] *LSIIT UMR CNRS 7005*
ULP Bd Brandt BP 10413
67412 Illkirch

CIFA 2006
Conférence Internationale Francophone d'Automatique
Bordeaux, France, 30 mai - 1 juin 2006

❒Plan

- ❒ Introduction
  - ❒ Synchronisation
  - ❒ Systèmes de communication
- ❒ Multimodèles :
  - ❒ Choix de l'émetteur : multimodèle chaotique
  - ❒ Conception du récepteur : synthèse de l'observateur et analyse de la synchronisation
- ❒ Système de communication
- ❒ Simulations
- ❒ Conclusion et perspectives

Introduction

Synchronisation

- **Synchronisation** : observée au XVIe siècle (Huygens)
  ⊗ concerne les systèmes périodiques

a priori incompatible

- **Systèmes chaotiques** :
  - Déterministes
  - Sensibilité aux conditions initiales
  - Existence d'UPO denses dans l'attracteur

} apériodiques

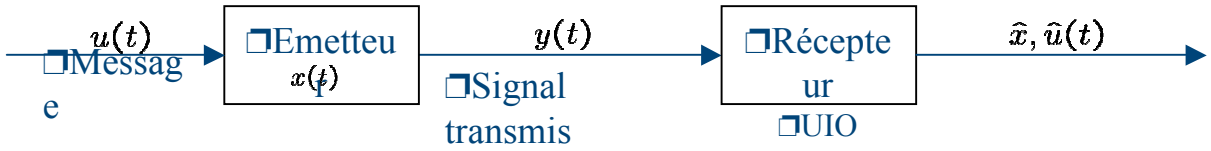
Synchronisation

- Dans les années 1990 :
  - théorie du contrôle du chaos
  - synchronisation des systèmes chaotiques :
    - Pecora et Carroll ⇒ *principe maître-esclave* (1990)
    - Décomposition active-passive (1995)
    - Approche utilisant les observateurs (1997)

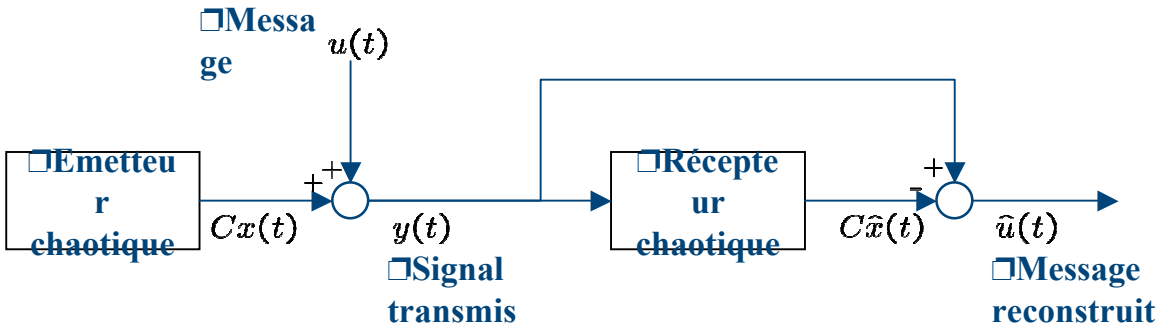
- ⊗ principale application : systèmes de communications

❒Les techniques de cryptage (1)

- ❒ Technique générale de reconstruction d'entrées inconnues
  - ❒ Observateurs à entrées inconnues

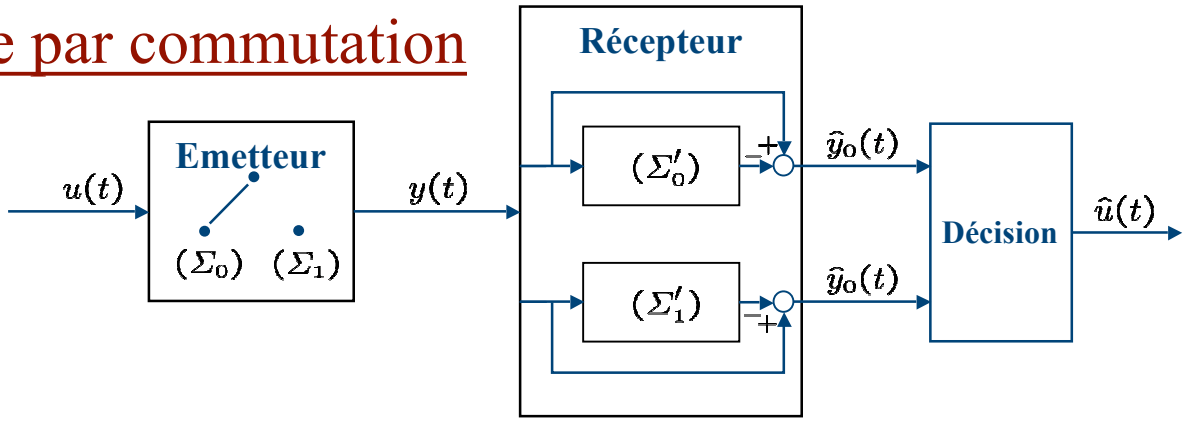


- ❒ Techniques spécifiques adaptées aux systèmes chaotiques
  - ❒ Cryptage par addition

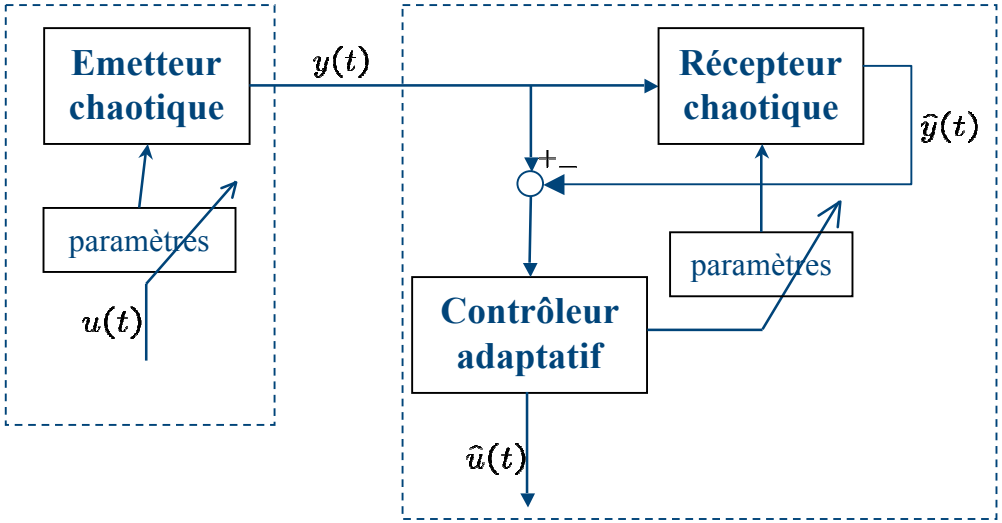


Les techniques de cryptage (2)

Cryptage par commutation

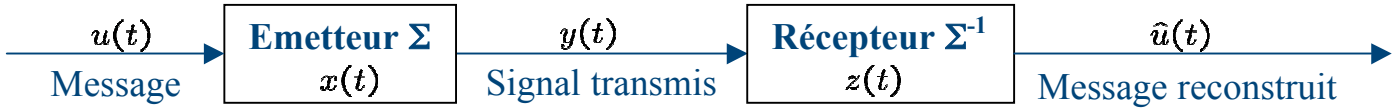


Cryptage par modulation

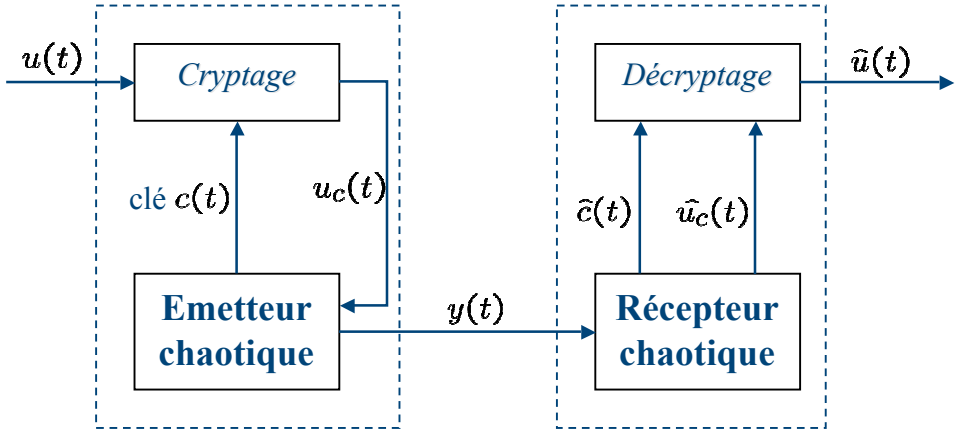


Les techniques de cryptage (3)

Cryptage par inversion



Cryptosystèmes



La synchronisation des multimodèles chaotiques

Multimodèles chaotiques

❒ p modèles linéaires locaux
⇒ multimodèle :

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{p} \mu_i(\xi(t)) \, (A_i x(t)) \\ y(t) = Cx(t) \end{cases}$$

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

ω p systèmes chaotiques
à retard :

$$\dot{x} = A_i x + f_i(x) + g_i(x_\tau), i = 1, p$$

Emetteur
= multimodèle chaotique

$$\begin{cases} \dot{x} = \sum_{i=1}^{p} \mu_i(y) \, (A_i x + f_i(x) + g_i(x_\tau)) \\ y = Cx \end{cases} \quad (1)$$

Récepteur
= observateur

$$\dot{\hat{x}} = \sum_{i=1}^{p} \mu_i(y) \, (A_i \hat{x} + f_i(\hat{x}) + g_i(\hat{x}_\tau) - K_i(y - C\hat{x})) \quad (2)$$

Conditions de synchronisation

❒ **Théorème**

Si les conditions suivantes sont vérifiées:

(i) les fonctions f_i et g_i sont Lipschitziennes de constantes respectives k_{fi} et k_{gi}

(ii) il existe $\xi > 0$, une matrice $P = P^T > 0$ et p matrices K_i tq

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

$$\begin{pmatrix} (k_{gi} - \xi) I & P \\ P & -\frac{1}{k_{gi}} I \end{pmatrix} < 0 \quad \text{pour i=1,p}$$

alors le système (2) est un observateur du multimodèle chaotique (1).

Démonstration

⊗On utilise la théorie de Lyapunov-Krasovskii pour déterminer les gains K_i

❒ Vecteur d'erreur de synchronisation $e = x - \hat{x}$

$$\Rightarrow \dot{e} = \sum_{i=1}^{p} \mu_i(y) \left((A_i - K_i C)e + \tilde{f}_i + \tilde{g}_i \right)$$

❒avec $\tilde{f}_i = f_i(x) - f_i(\hat{x})$
$\tilde{g}_i = g_i(x_\tau) - g_i(\hat{x}_\tau)$

❒ Fonctionnelle de Lyapunov-Krasovskii :

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

❒ On montre que :(i) $V \geqslant 0$

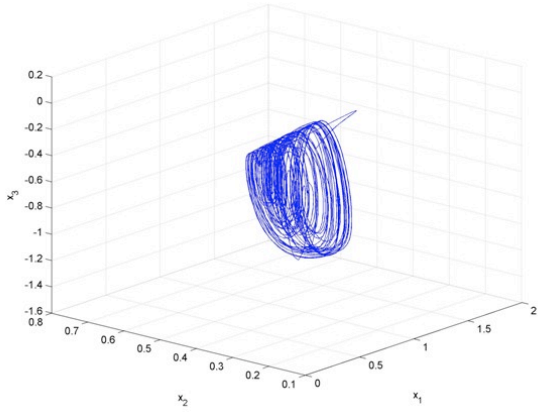
(ii) $\dot{V} \leqslant 0$

❒si $\begin{cases} \mathcal{M}^T P + P\mathcal{M} + \sum_{i=1}^{p} \mu_i(y) k_{fi} P^2 + \left(\sum_{i=1}^{p} \mu_i(y) k_{gi} + \xi \right) I < 0 \\ k_{gi} P^2 + (k_{gi} - \xi) I < 0 \end{cases}$ $\quad \mathcal{M} = \sum_{i=1}^{p} \mu_i(y) (A_i - K_i C)$

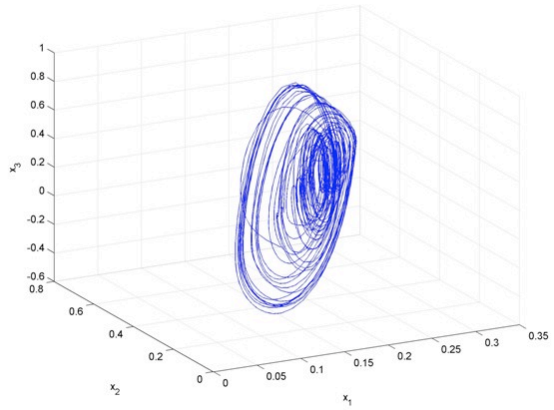
Simulations

Multimodèle chaotique émetteur

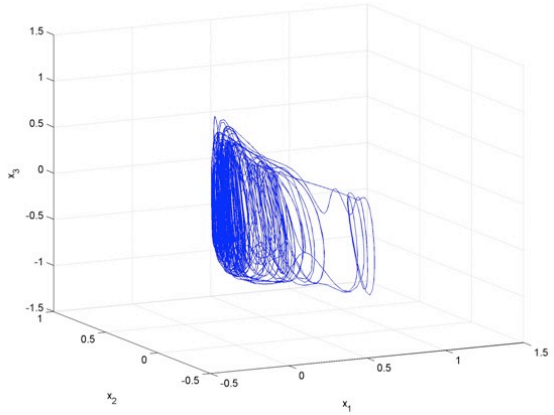
❒ Modèle dynamique : $\begin{cases} \dot{x}_1 = -\alpha x_1 + \alpha x_2 - \alpha\delta \tanh(x_1) \\ \dot{x}_2 = x_1 - x_2 + x_3 \\ \dot{x}_3 = -\beta x_2 - \gamma x_3 + \varepsilon \sin(\sigma x_{1\tau}) \end{cases}$



$\alpha_1 = 40,\ \beta_1 = 35,$
$\gamma_1 = 20,\ \delta_1 = -1,$
$\varepsilon_1 = 10,\ \sigma_1 = 10,$
$\tau_1 = 1$

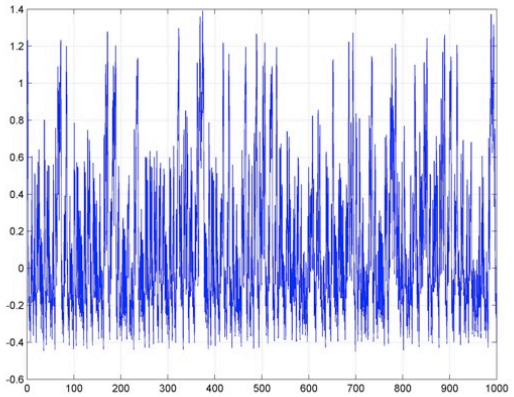


$\alpha_2 = 20,\ \beta_2 = 15,$
$\gamma_2 = 5,\ \delta_2 = 1,$
$\varepsilon_2 = 10,\ \sigma_2 = 10,$
$\tau_2 = 1$

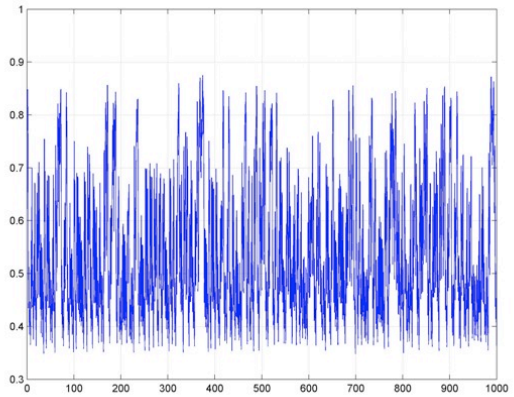


multimodèle

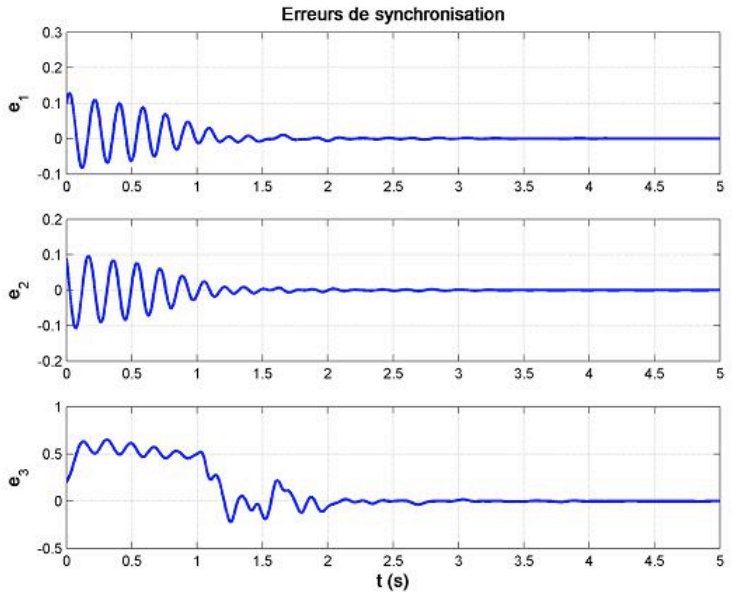
Synchronisation du récepteur



Message transmis



Fonction de transition $\mu(t)$



Composantes de l'erreur de synchronisation $e(t)$

❒Application au cryptage

❒ On envoie un deuxième signal chaotique généré par l'émetteur, avec un retard dépendant du message :

$$y_2(t) = x_3(t - T_u u(t))$$

❒ Après approximation au premier ordre de la formule de Taylor-Lagrange, on obtient :

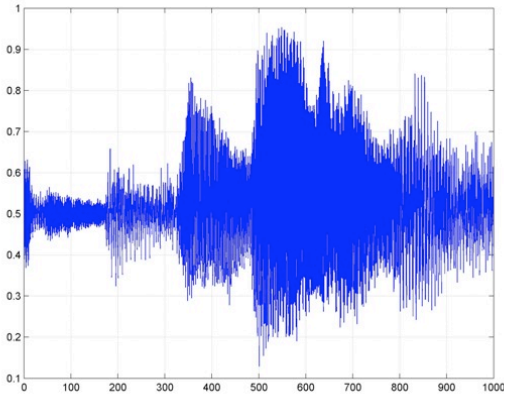
$$x_3(t) - y_2(t) = x_3(t) - x_3(t - T_u u(t)) = \dot{x}_3 T_u u(t)$$

❒ D'où la formule de décryptage :

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

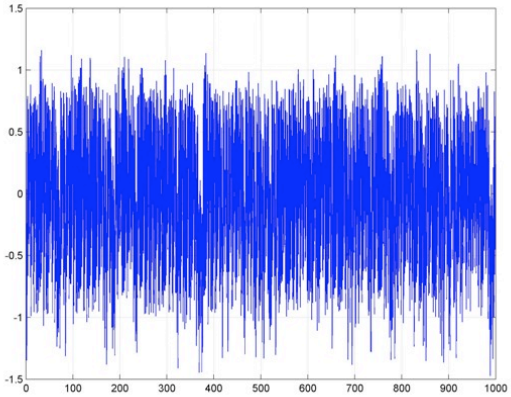
Simulations : cryptage / décryptage

❒ Message original :



$u(t) \in [0, 1]$

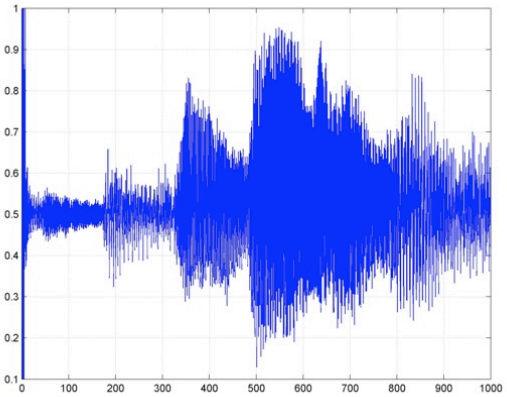
❒ Message crypté :



$y_2(t) = x_3(t - T_u u(t))$

$T_u = 0.01$

ω Message décrypté :



$\hat{u}(t)$

Conclusion

- Synchronisation de multimodèles chaotiques :
  - émetteur = multimodèle chaotique à retard
  - récepteur = observateur
- Application au cryptage :
  on envoie un deuxième signal chaotique
- Simulations :
  message = image, son …

Perspectives

- Approfondir l'étude du multimodèle chaotique
- Développer d'autres techniques de synchronisation
- Comparaison avec d'autres techniques de cryptage, étude de la sécurité