



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

Estelle Cherrier, Mohamed Boutayeb, José Ragot

► To cite this version:

Estelle Cherrier, Mohamed Boutayeb, José Ragot. Observateurs non linéaires de multimodèles. Application à la synchronisation et aux communications. Conférence Internationale Francophone d'Automatique, CIFA'2006, May 2006, Bordeaux, France. pp.CDROM. hal-00118548

HAL Id: hal-00118548

<https://hal.science/hal-00118548>

Submitted on 5 Dec 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

Estelle CHERRIER^{1,2}, Mohamed BOUTAYEB², José RAGOT¹

¹ CRAN UMR CNRS 7039

INPL/UHP, 2 Avenue de la Forêt de Haye, 54516 Vandoeuvre-lès-Nancy Cedex

²LSIIT UMR CNRS 7005

ULP, Pôle API, Bd Sébastien Brandt - BP 10413, 67412 Illkirch

cherrier@eavr.u-strasbg.fr, mohamed.boutayeb@ipst-ulp.u-strasbg.fr,
jragot@ensem.inpl-nancy.fr

Résumé— Cet article est consacré à la synthèse d'observateurs pour une classe de systèmes non linéaires. Des multimodèles non linéaires sont définis à partir de deux (ou plus généralement $p > 0$) systèmes chaotiques comportant un retard. Des conditions suffisantes de synchronisation basée observateur sont établies pour cette classe de systèmes, sous la forme d'Inégalités Matricielles Linéaires (LMIs). Cette méthode de synchronisation est intégrée dans un processus de communications, dont l'efficacité est testée à travers le cryptage/décryptage d'un signal sonore.

Mots-clés— Observateurs non linéaires, multimodèles, systèmes chaotiques, synchronisation, communications.

I. INTRODUCTION

L'utilisation du chaos dans le domaine de la synchronisation et, plus généralement, dans le domaine des communications (sécurisées) est relativement récente. Pendant longtemps, les phénomènes chaotiques ont été étroitement liés à l'étude des systèmes non linéaires. Parmi les scientifiques qui ont consacré une part importante de leurs travaux aux manifestations du chaos, certains sont restés célèbres, comme Poincaré, et ont même donné leur nom à des types d'attracteurs comme Van der Pol, Lorenz, Rössler, Chua... Ils ont contribué à la caractérisation des systèmes chaotiques en établissant quelques propriétés fondamentales qu'ils doivent vérifier : les systèmes chaotiques présentent une très grande sensibilité aux conditions initiales (plus connue sous le nom d'*effet papillon*) ; il existe des UPOs (Unstable Periodic Orbits : orbites périodiques instables) denses dans l'attracteur ; et enfin ce sont des systèmes déterministes. L'extrême sensibilité dans les conditions initiales est restée un inconvénient majeur des systèmes chaotiques jusqu'en 1990. Les travaux novateurs de Pecora et Carroll [1] ont constitué une révolution dans l'étude de la synchronisation, et ont été le point de départ de recherches toujours en cours, notamment des applications dans le domaine des communications sécurisées. Ils ont prouvé que deux systèmes chaotiques identiques, de conditions initiales différentes, peuvent se synchroniser selon le principe de *drive-response*. Plus récemment, [2] et [3] ont relié le processus de synchronisation à un problème

classique d'estimation d'état, linéaire ou non linéaire. Depuis, la plupart des schémas de synchronisation reposent sur la construction d'un observateur d'état adapté à la classe de systèmes chaotiques étudiés [4], [5], [6], [7]... Une vue d'ensemble des différentes techniques utilisées peut être trouvée dans [8].

Dans cet article, nous proposons une méthode de synchronisation basée observateur pour une classe de systèmes non linéaires, qui sera ensuite appliquée à un processus de communications. L'émetteur est un multimodèle non linéaire, construit à partir de systèmes chaotiques comportant un retard : une méthode systématique (reposant sur la résolution de LMIs : Inégalités Matricielles Linéaires) est développée pour synthétiser des observateurs pour cette classe de systèmes.

La théorie des multimodèles est assez récente. [9] est un ouvrage de référence qui fait un tour d'horizon sur ce sujet. Des problèmes plus spécifiques de stabilité par exemple sont abordés dans [10], [11]. L'existence d'un multimodèle est liée à celle d'un système non linéaire, qui a été linéarisé autour de plusieurs points de fonctionnement, et dont le comportement général à chaque instant est approché par la somme pondérée de chacun de ces modèles locaux. Ainsi, dans le cas de systèmes autonomes :

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

avec

$$\begin{cases} \sum_{i=1}^p \mu_i(\xi) = 1 \\ 0 \leq \mu_i(\xi) \leq 1 \quad \forall i = 1, p \end{cases} \quad (2)$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, et $y \in \mathbb{R}^m$ représente le vecteur des sorties mesurées, les matrices A_i , $i = 1, p$ and C étant de dimensions appropriées.

μ est la fonction d'interpolation, dans le sens où, à chaque instant, sa valeur détermine la façon dont chaque modèle local agit dans la dynamique du multimodèle (1). En effet, s'il existe $i \in \{1, \dots, p\}$ tel que $\mu_i(\xi) = 1$, d'après (1) et (2), seul le i^{me} modèle est actif, tandis que si $0 < \mu_i(\xi) < 1$, alors il existe $j \in \{1, \dots, p\}$, $j \neq i$ tel que $\mu_j(\xi) > 0$, donc

au moins deux modèles locaux sont actifs.
La variable ξ dépend généralement de l'état x , ou des mesures y .

Ici nous n'adoptons pas un point de vue classique sur les multimodèles : le même procédé de somme pondérée est utilisé pour créer un nouveau multimodèle, à partir de p systèmes chaotiques comportant un retard :

$$\begin{cases} \dot{x} = \sum_{i=1}^p \mu_i(y) (A_i x + f_i(x) + g_i(x_\tau)) \\ y = Cx \end{cases} \quad (3)$$

en utilisant la notation standard $x_\tau(t) = x(t - \tau)$, où $\tau > 0$ est un retard connu.

Les fonctions $f_i, g_i : \mathbb{R}^n \rightarrow \mathbb{R}^n$ sont des fonctions non linéaires garantissant que chaque modèle local $\dot{x} = A_i x + f_i(x) + g_i(x_\tau)$, $i = 1, p$, se comporte de manière chaotique (se reporter à [12], [7] pour des exemples de cette classe de systèmes). En général, ces fonctions f_i, g_i vérifient la condition de Lipschitz, qui sera détaillée ultérieurement.

La fonction μ réalise une sorte de mixage entre la dynamique des p modèles chaotiques locaux, ce qui peut protéger le processus de synchronisation contre les attaques reposant sur des techniques de *delay-reconstruction* [13]. En effet, ces techniques tirent profit du fait que le signal y envoyé par l'émetteur constitue une série temporelle d'un état d'un attracteur particulier sur un laps de temps assez long pour pouvoir le reconstruire géométriquement. Ici, le signal y envoyé au récepteur est une interpolation variable (dans le temps) de chaque modèle local, et ne correspond donc pas à une série temporelle d'un attracteur connu.

Cet article présente une méthode de synchronisation basée observateur pour la classe de systèmes définie par (3). Il est organisé comme suit. La partie II est consacrée à l'élaboration de conditions suffisantes garantissant la synchronisation, sous forme de LMIs, en utilisant la théorie de Lyapunov-Krasovskii. Ces conditions sont tout d'abord établies dans le cas d'un multimodèle composé de deux modèles locaux, puis généralisée au cas de p sous-modèles chaotiques. L'efficacité de la méthode est ensuite testée dans la partie III sur l'exemple d'un multimodèle composé de deux systèmes chaotiques à retard. Enfin, la partie IV constitue une application de cette méthode de synchronisation à un procédé de communications, par l'intermédiaire du cryptage/décryptage d'un signal sonore.

II. SYNCHRONISATION À BASE D'OBSERVATEUR DE MULTIMODÈLES

Cette partie détaille tout d'abord la définition du multimodèle construit à partir de deux systèmes chaotiques comportant un retard, puis la construction d'un observateur pour ce multimodèle. Ensuite on établit une condition suffisante garantissant la synchronisation de l'observateur, sous la forme d'une LMI. Cette démarche systématique est finalement étendue au cas général d'un multimodèle s'appuyant sur $p > 0$ systèmes chaotiques retardés.

A. Multimodèle composé de deux systèmes

On considère deux systèmes chaotiques, de dynamiques respectives :

$$\dot{x} = A_1 x + f_1(x) + g_1(x_\tau) \quad (4)$$

et :

$$\dot{x} = A_2 x + f_2(x) + g_2(x_\tau) \quad (5)$$

On définit alors le multimodèle suivant, à partir de (4) et (5):

$$\begin{cases} \dot{x} = \mu(y)(A_1 x + f_1(x) + g_1(x_\tau)) \\ \quad + (1 - \mu(y))(A_2 x + f_2(x) + g_2(x_\tau)) \\ y = Cx \in \mathbb{R} \end{cases} \quad (6)$$

La fonction μ doit vérifier $\mu \in [0, 1]$. On a choisi $\xi(t) = y(t)$ dans l'expression (2), car y est le seul signal disponible au niveau du récepteur.

Nous allons établir les conditions garantissant la synchronisation à base d'observateur du multimodèle (6). On cherche à construire un observateur du système (6), dont la dynamique est la suivante :

$$\begin{aligned} \dot{\hat{x}} = & \mu(y) (A_1 \hat{x} + f_1(\hat{x}) + g_1(\hat{x}_\tau) - K_1(y - C\hat{x})) \\ & + (1 - \mu(y)) (A_2 \hat{x} + f_2(\hat{x}) + g_2(\hat{x}_\tau) - K_2(y - C\hat{x})) \end{aligned} \quad (7)$$

Nous allons indiquer la procédure pour trouver les gains K_1 et K_2 . Le vecteur d'erreur de synchronisation est défini par $e = x - \hat{x}$. Par dérivation, il vient :

$$\begin{aligned} \dot{e} = & \mu(y) ((A_1 - K_1 C)e + f_1(x) - f_1(\hat{x}) + g_1(x_\tau) \\ & - g_1(\hat{x}_\tau)) + (1 - \mu(y)) ((A_2 - K_2 C)e \\ & + f_2(x) - f_2(\hat{x}) + g_2(x_\tau) - g_2(\hat{x}_\tau)) \end{aligned} \quad (8)$$

Pour alléger les notations, on pose :

$$\mathcal{M} = \mu(y)(A_1 - K_1 C) + (1 - \mu(y))(A_2 - K_2 C) \quad (9)$$

et

$$\begin{aligned} \tilde{f}_i &= f_i(x) - f_i(\hat{x}), \quad i = 1, 2 \\ \tilde{g}_i &= g_i(x_\tau) - g_i(\hat{x}_\tau) \end{aligned} \quad (10)$$

Le théorème suivant énonce les conditions suffisantes de synchronisation de l'observateur (7) avec le multimodèle (6) :

Théorème 1:

Si les conditions suivantes sont vérifiées :

1. Les fonctions f_i, g_i , $i = 1, 2$, sont lipschitziennes, de constantes de Lipschitz respectives k_{fi} et k_{gi} , $i = 1, 2$:

$$\left. \begin{aligned} \|f_i(x) - f_i(y)\| &\leq k_{fi} \|x - y\| \\ \|g_i(x) - g_i(y)\| &\leq k_{gi} \|x - y\| \end{aligned} \right\}, \quad \forall x, y \in \mathbb{R}^n \quad (11)$$

2. Il existe une matrice symétrique, définie positive P , deux matrices K_1, K_2 et $\xi > 0$ solution des LMIs suivantes ($i = 1, 2$) :

$$\left(\begin{array}{cc} (A_i - K_i C)^T P + P(A_i - K_i C) + (\xi + k_{fi})I & -\frac{P}{k_{fi}}I \\ P & -\frac{1}{k_{fi}}I \end{array} \right) < 0 \quad (12)$$

et

$$\left(\begin{array}{cc} (k_{gi} - \xi)I & P \\ P & -\frac{1}{k_{gi}}I \end{array} \right) < 0 \quad (13)$$

alors (7) est un observateur de l'état du système (6) : $\hat{x}(t) \rightarrow x(t)$ quand $t \rightarrow \infty$.

Preuve: Pour analyser la convergence de l'observateur, on introduit la fonction de Lyapunov-Krasovskii :

$$V = V(e(t), e_\tau(t)) = e^T P e + \xi \int_{-\tau}^0 e(t+\theta)^T e(t+\theta) d\theta \quad (14)$$

où P est une matrice symétrique, définie positive et $\xi > 0$. L'erreur de synchronisation converge asymptotiquement vers zéro si [14] :

(i) $V(e, e_\tau) \geq 0$

(ii) $\dot{V}(e, e_\tau) \leq 0$

La première condition est facilement vérifiée puisque $P > 0$ et $\xi > 0$.

Les équations (8), (9), (10) mènent à :

$$\dot{V} = e^T (\mathcal{M}^T P + P \mathcal{M} + \xi I) e + 2e^T P (\mu \tilde{f}_1 + (1 - \mu) \tilde{f}_2) + 2e^T P (\mu \tilde{g}_1 + (1 - \mu) \tilde{g}_2) - \xi e_\tau^T e_\tau \quad (15)$$

Si on applique successivement les inégalités de Cauchy-Schwarz et de Young, on obtient :

$$2\mu(y)e^T P \tilde{f}_1 \leq \mu(y)(k_{f1}e^T P P e + k_{f1}e^T e) \quad (16)$$

$$2(1 - \mu(y))e^T P \tilde{f}_2 \leq (1 - \mu(y))(k_{f2}e^T P P e + k_{f2}e^T e)$$

$$2\mu(y)e^T P \tilde{g}_1 \leq \mu(y)(k_{g1}e_\tau^T P P e_\tau + k_{g1}e_\tau^T e_\tau) \quad (17)$$

$$2(1 - \mu(y))e^T P \tilde{g}_2 \leq (1 - \mu(y))(k_{g2}e_\tau^T P P e_\tau + k_{g2}e_\tau^T e_\tau)$$

ce qui implique :

$$\begin{aligned} \dot{V} \leq & e^T (\mathcal{M}^T P + P \mathcal{M} + (\mu(y)k_{f1} + (1 - \mu(y))k_{f2})P^2 \\ & + (\mu(y)k_{f1} + (1 - \mu(y))k_{f2} + \xi)I) e \\ & + e_\tau^T ((\mu(y)k_{g1} + (1 - \mu(y))k_{g2})P^2 \\ & + (\mu(y)k_{g1} + (1 - \mu(y))k_{g2} - \xi)I) e_\tau \end{aligned} \quad (18)$$

Par conséquent, en utilisant (9) et (2), si les équations suivantes, de type Riccati, sont vérifiées :

$$(A_i - K_i C)^T P + P(A_i - K_i C) + k_{fi}P^2 + (\xi + k_{fi})I < 0, \quad i = 1, 2 \quad (19)$$

ainsi que

$$k_{gi}P^2 + (k_{gi} - \xi)I < 0, \quad i = 1, 2 \quad (20)$$

on arrive à :

$$\dot{V} \leq 0 \quad (21)$$

L'utilisation du complément de Schur permet de mettre (19) et (20) sous une forme LMI, et on obtient ainsi respectivement (12) et (13), ce qui complète la démonstration : le vecteur d'erreur de synchronisation e converge bien vers 0, et l'observateur (7) est asymptotiquement convergent. ■

Remarque 2:

Les LMIs (12), pour $i = 1, 2$, peuvent être résolues numériquement. Si on note $L_i = PK_i$ (ce qui équivaut à $K_i = P^{-1}L_i$ puisque P est inversible), on obtient d'après (19) :

$$\begin{aligned} (A_i - K_i C)^T P + P(A_i - K_i C) + (\xi + k_{fi})I \\ = A_i^T P + P A_i - C^T L_i^T - L_i C + (\xi + k_{fi})I \end{aligned} \quad (22)$$

Le membre de droite est linéaire en P et L_i , donc les LMIs (12) et (13), $i = 1, 2$, peuvent être facilement résolues par un algorithme standard d'optimisation convexe.

B. Généralisation à p modèles chaotiques

Les résultats précédents peuvent s'étendre au cas général d'un multimodèle composé de $p > 0$ systèmes chaotiques retardés, défini de manière analogue à (6) :

$$\begin{cases} \dot{x} = \sum_{i=1}^p \mu_i(y) (A_i x + f_i(x) + g_i(x_\tau)) \\ y = Cx \end{cases} \quad (23)$$

avec

$$\sum_{i=1}^p \mu_i(y) = 1, \quad 0 \leq \mu_i \leq 1 \quad (24)$$

De la même manière qu'à l'équation (7), la dynamique de l'observateur de (23) est choisie de la forme :

$$\dot{\hat{x}} = \sum_{i=1}^p \mu_i(y) (A_i \hat{x} + f_i(\hat{x}) + g_i(\hat{x}_\tau) - K_i(y - C\hat{x})) \quad (25)$$

Le théorème 1 peut aussi être généralisé :

Théorème 3:

Si les conditions suivantes sont remplies :

1. Les fonctions f_i , et g_i , $i = 1, p$ sont respectivement k_{fi} - et k_{gi} -lipschitziennes (voir (11));
2. Il existe $\xi > 0$, une matrice symétrique, définie positive P et p matrices K_i , $i = 1, p$ solutions des $2p$ LMIs :

$$\begin{pmatrix} (A_i - K_i C)^T P + P(A_i - K_i C) + k_{fi}I & P \\ P & -\frac{1}{k_{fi}}I \end{pmatrix} < 0 \quad (26)$$

et

$$\begin{pmatrix} (k_{gi} - \xi)I & P \\ P & -\frac{1}{k_{gi}}I \end{pmatrix} < 0 \quad (27)$$

alors dans ce cas, (25) est un observateur du multimodèle (23): $\hat{x}(t) \rightarrow x(t)$ quand $t \rightarrow \infty$.

Preuve: La démonstration est analogue à celle du Théorème 1. Si on introduit la notation

$$\mathcal{M} = \sum_{i=1}^p \mu_i(y) (A_i - K_i C) \quad (28)$$

les équations de type Riccati (19) se généralisent sous la forme :

$$\mathcal{M}^T P + P \mathcal{M} + \sum_{i=1}^p \mu_i(y) k_{fi} P^2 + \left(\sum_{i=1}^p \mu_i(y) k_{gi} + \xi \right) I < 0 \quad (29)$$

III. CAS DE DEUX SYSTÈMES CHAOTIQUES À RETARD

On teste la synchronisation utilisant des observateurs mise au point dans la partie précédente. Pour cela, on choisit un multimodèle composé de deux systèmes chaotiques comportant un retard (selon le modèle détaillé dans [7]), ces deux systèmes définissant deux attracteurs chaotiques différents.

A. Description du multimodèle

La dynamique des modèles retenus est donnée par :

$$\begin{cases} \dot{x}_1 &= -\alpha x_1 + \alpha x_2 + f(x_1) \\ \dot{x}_2 &= x_1 - x_2 + x_3 \\ \dot{x}_3 &= -\beta x_2 - \gamma x_3 + g(x_{1\tau}) \end{cases} \quad (30)$$

où les nonlinéarités f et g sont données par (les paramètres de ces fonctions, ainsi que le retard, sont connus) :

$$\begin{aligned} f(x_1) &= -\alpha \delta \tanh(x_1) \\ g(x_1(t)) &= \varepsilon \sin(\sigma x_1(t - \tau)) \end{aligned} \quad (31)$$

On remarque que les fonctions f et g vérifient la condition de Lipschitz, pour des constantes égales respectivement à $|\alpha\delta|$ et $|\varepsilon\sigma|$.

Deux ensembles de paramètres ont été choisis, l'ensemble 1 :

$$\alpha_1 = 40, \beta_1 = 35, \gamma_1 = 20, \delta_1 = -1, \tau_1 = 1, \varepsilon_1 = 10, \sigma_1 = 10 \quad (32)$$

et l'ensemble 2:

$$\alpha_2 = 20, \beta_2 = 15, \gamma_2 = 5, \delta_2 = 1, \tau_2 = 1, \varepsilon_2 = 10, \sigma_2 = 10 \quad (33)$$

Les attracteurs correspondants aux paramètres 1 et 2 sont tracés sur les figures 1 et 2. On construit alors le multi-

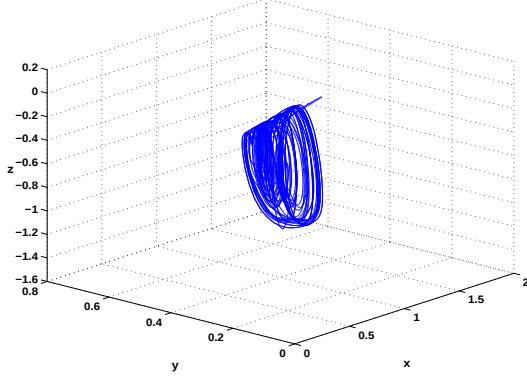


Fig. 1. Système chaotique retardé 1

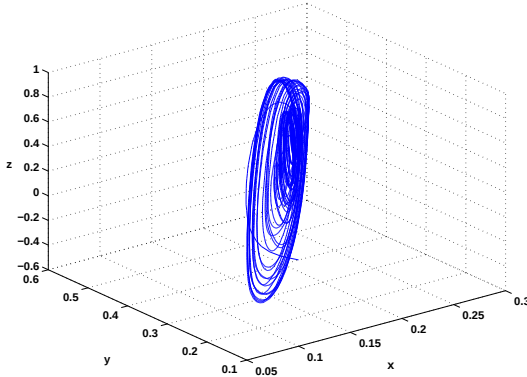


Fig. 2. Système chaotique retardé 2

modèle (6) à partir de ces systèmes. La fonction $\mu(\cdot)$ est choisie de la forme

$$\mu(y) = \frac{1 + \tanh(\eta y)}{2} \quad (34)$$

le paramètre η garantissant une réelle transition continue entre les deux modèles, et pas seulement une alternance entre les deux. Cela évite que la fonction $\mu(\cdot)$ privilégie une valeur (voire quelques valeurs particulières) entre 0 et 1. La démonstration des Théorèmes 1 et 3 est indépendante du choix de la fonction $\mu(\cdot)$, il faut seulement que les conditions (2) soient vérifiées.

Remarque 4:

Pour réduire la valeur des constantes de Lipschitz k_{fi} et k_{gi} , $i = 1, 2$, on choisit la matrice d'observation suivante dans (6) :

$$C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix} \quad (35)$$

avec ζ assez petit, $0 < \zeta < 1$, et dans ce cas, on peut écrire (avec $h = f$ ou g) :

$$\begin{aligned} \|h(x_1) - h(\hat{x}_1)\| &= \|h(y - \zeta x_2) - h(y - \zeta \hat{x}_2)\| \\ &\leq k|\zeta| \|x_2 - \hat{x}_2\| \end{aligned} \quad (36)$$

On constate que les nouvelles constantes de Lipschitz sont toutes multipliées par ζ . Ici on a pris $\zeta = 0.01$, donc on obtient pour les paramètres correspondant à (32) et (33) : $k_{f1} = 0.4$, $k_{f2} = 0.2$, et $k_{g1} = k_{g2} = 1$. Ce réglage du paramètre ζ a pour but de rendre applicable le Théorème 1, dont les hypothèses ne peuvent être vérifiées si les constantes de Lipschitz sont trop grandes.

La figure 3 montre l'attracteur résultant de la simulation du multimodèle.

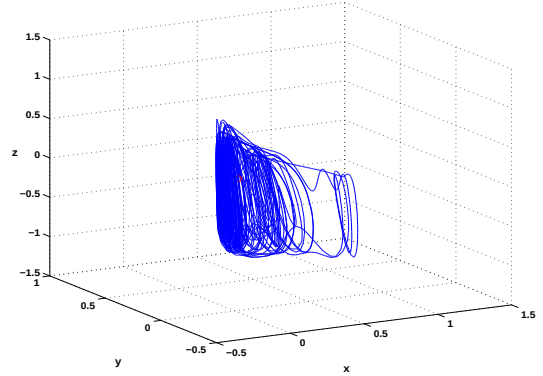


Fig. 3. Multimodèle

B. Simulations

Les simulations suivantes vont illustrer l'efficacité de la méthode proposée de synchronisation à base d'observateurs pour les multimodèles.

La procédure de résolution des LMIs donne les gains suivants pour construire l'observateur :

$$K_1 = \begin{pmatrix} -22.73009924194811 \\ 41.15127226834878 \\ 13.21359829809531 \end{pmatrix} \quad (37)$$

$$K_2 = \begin{pmatrix} -8.89211050110927 \\ 23.15660169589151 \\ 8.79844323851249 \end{pmatrix} \quad (38)$$

la matrice P est donnée en (39), et $\xi = 2$.

Les conditions initiales pour le multimodèle sont :

$$\begin{pmatrix} 0.1 & 0.1 & 0.1 \end{pmatrix}^T \quad (40)$$

et pour l'observateur

$$\begin{pmatrix} 0 & 0.01 & -0.1 \end{pmatrix}^T \quad (41)$$

La fonction $\mu(y(t))$ est tracée figure 4, sachant que $\eta = 0.7$ dans (34). Cette courbe montre qu'il y a bien transition entre les deux modèles chaotiques, la dynamique du multimodèle est influencée à chaque instant par celle des deux systèmes qui le définissent, et pas successivement par l'un puis par l'autre.

L'erreur de synchronisation de chaque état est tracée sur la figure 5.

$$P = \begin{pmatrix} 0.66711349131098 & -0.24680949689941 & 0.12692206278854 \\ -0.24680949689941 & 0.72345874659580 & -0.21169486677705 \\ 0.12692206278854 & -0.21169486677705 & 0.29023507485856 \end{pmatrix} \quad (39)$$

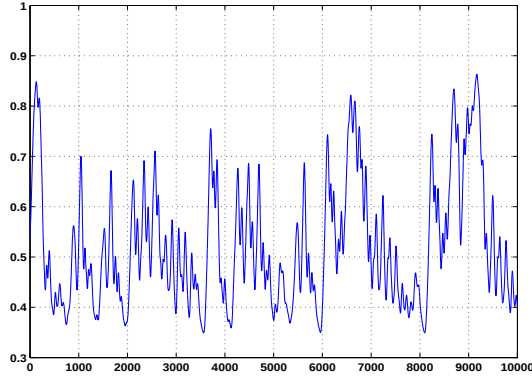


Fig. 4. Trajectoire de la fonction μ

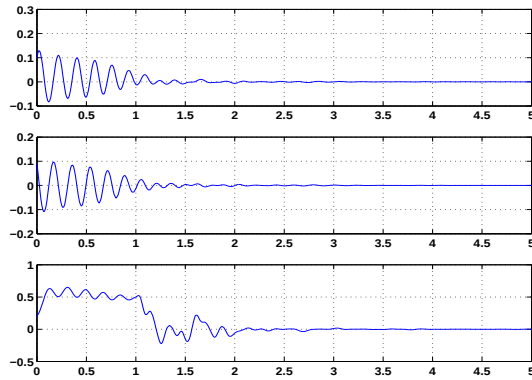


Fig. 5. Erreurs de synchronisation

IV. APPLICATION AUX COMMUNICATIONS

Dans cette partie, nous allons appliquer le schéma de synchronisation précédent à un processus de cryptage/décryptage, détaillé dans [7].

A. Description de la méthode de cryptage

Un second signal chaotique y_2 est envoyé au récepteur, ce signal étant généré de façon totalement indépendante de y . $y_2(t)$ est défini à partir du troisième état $x_3(t)$ du multimodèle-émetteur (30), auquel on ajoute un retard dépendant du message $u(t)$ (on suppose que $u \in [0, 1]$) :

$$y_2(t) = x_3(t - T_u u(t)) \quad (42)$$

En pratique, pour permettre la reconstruction de u , on suppose que $0 < T_u < T_e$, où T_e est le pas de l'intégration numérique des équations différentielles mises en jeu.

Si on applique la formule de Taylor-Lagrange à l'expression (42), et après une approximation au premier ordre, on obtient (se référer à [7] pour les détails) :

$$x_3(t) - y_2(t) = \dot{x}_3(t) T_u u(t) \quad (43)$$

En supposant que la condition $\dot{x}_3(t) \neq 0$ est vérifiée (dans le cas contraire, on fait une approximation à l'ordre deux

de la formule de Taylor), on peut inverser (43), et il vient :

$$u(t) = \frac{x_3(t) - y_2(t)}{T_u \dot{x}_3(t)} \quad (44)$$

La formule de décryptage se déduit facilement de (44) :

$$\hat{u}(t) = \frac{\hat{x}_3(t) - y_2(t)}{T_u \dot{\hat{x}}_3(t)} \quad (45)$$

En remplaçant $\dot{\hat{x}}_3$ par son expression tirée de (30) et (7), (45) se met sous la forme (47), avec les notations

$$K_i = \begin{pmatrix} \kappa_{i,1} \\ \kappa_{i,2} \\ \kappa_{i,3} \end{pmatrix} \quad (46)$$

$i = 1, 2$ et $\hat{y} = C\hat{x} = \hat{x}_1 + \zeta\hat{x}_2$.

Remarque 5: En pratique, la formule (47) peut toujours être appliquée, même si, a priori, elle comporte un dénominateur qui ne doit pas s'annuler.

Remarque 6: On ne s'intéresse pas ici aux problèmes qui peuvent survenir au niveau du canal de transmission. Par exemple, un retard de transmission semble inévitable. Dans ce cas, s'il s'agit d'un retard constant ς , il existe des techniques pour l'estimer [15]. La formule (45) permet alors de reconstruire $(u(t) + \varsigma)$, et il suffit de soustraire l'estimation de ς , réalisée avant l'envoi du signal utile. Le cas d'un retard variable apparaissant sur la ligne de transmission semble plus délicat, et reste un problème ouvert.

B. Simulations

Le message choisi est un signal sonore (voir figure 6), qui est normalisé pour obtenir $u(t) \in [0, 1]$, $\forall t > 0$. La méthode d'intégration numérique est une méthode de Runge-Kutta d'ordre quatre, et de pas variable inférieur à 0.01 seconde. La figure 7 représente le message crypté envoyé au récepteur, et la figure 8 représente le message décrypté. L'erreur de décryptage est tracée à la figure 5 : on constate que la reconstruction n'est pas parfaite au départ, en effet la formule (45) n'est valable que lorsque la synchronisation est bien établie entre l'émetteur et le récepteur, ce qui nécessite quelques instants. Ce laps de temps préalable dépend en particulier des valeurs des paramètres du modèle. D'un point de vue pratique, l'utilisateur peut facilement estimer la durée nécessaire a priori, pour un ensemble de paramètres fixé. Dans l'exemple proposé ici, le temps de synchronisation est d'environ cinq secondes, et ensuite le message peut être injecté.

V. CONCLUSION

Dans cet article, nous développons une méthode de synchronisation utilisant des observateurs pour une classe de systèmes non linéaires. Il s'agit de multimodèles non linéaires, définis à partir de plusieurs systèmes chaotiques comportant un retard. Des conditions suffisantes

$$\hat{u}(t) = \frac{1}{T_u} \frac{-(\hat{x}_3(t) - y_2(t))}{\mu (\beta_1 \hat{x}_2 + \gamma_1 \hat{x}_3 + \varepsilon_1 \sin(\sigma_1 \hat{x}_{1,\tau_1}) + \kappa_{1,3}(y - \hat{y})) + (1 - \mu) (\beta_2 \hat{x}_2 + \gamma_2 \hat{x}_3 + \varepsilon_2 \sin(\sigma_2 \hat{x}_{1,\tau_2}) + \kappa_{2,3}(y - \hat{y}))} \quad (47)$$

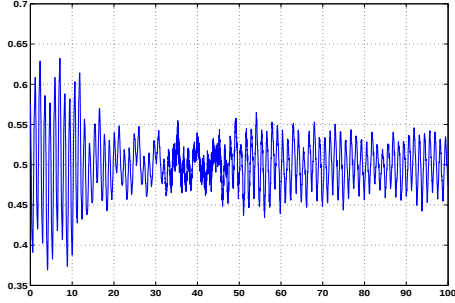


Fig. 6. Signal sonore à transmettre

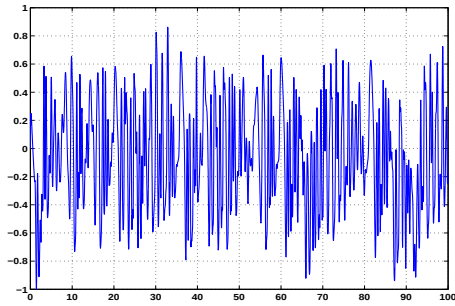


Fig. 7. Signal crypté

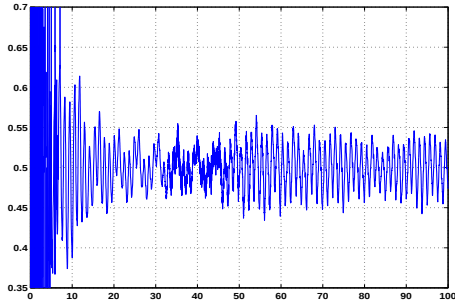


Fig. 8. Signal décrypté

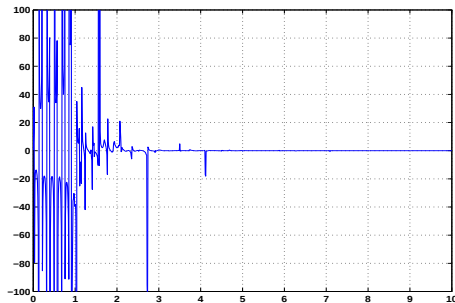


Fig. 9. Erreur de reconstruction

de la sécurité du schéma de communications, ou l'étude du caractère chaotique du multimodèle, par exemple en étudiant les exposants de Lyapunov du multimodèle.

RÉFÉRENCES

- [1] L.M. Pecora et T.L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64(8):821–824, 1990.
- [2] O. Morgül et E. Solak. Observer based synchronization of chaotic systems. *Phys. Rev. E*, 54(5):4803–4811, 1996.
- [3] H. Nijmeijer et I.M.Y. Mareels. An observer looks at synchronization. *IEEE Trans. Circuit Syst. I*, 44(10):882–890, 1997.
- [4] G. Millerioux et J. Daafouz. Global chaos synchronization and robust filtering in noisy context. *IEEE Trans. Circuit Syst. I*, 48(10):1170–1176, 2001.
- [5] M. Boutayeb, M. Darouach, et H. Rafaralahy. Generalized state-space observers for chaotic synchronization and secure communication. *IEEE Trans. Circuit Syst. I*, 49(3):345–349, 2002.
- [6] S. Celikovský et G. Chen. Secure synchronization of a class of chaotic systems from a nonlinear observer approach. *IEEE Trans. Automatic Control*, 50(1):76–82, 2005.
- [7] E. Cherrier, M. Boutayeb, et J. Ragot. Observers based synchronization and input recovery for a class of chaotic models. *Proceedings of the Joint 44th IEEE Conference on Decision and Control and European Control Conference, Seville, Spain*, 2005.
- [8] S. Boccaletti, J. Kurths, G. Osipov, D.L. Valladares, et C.S. Zhou. The synchronization of chaotic systems. *Phys. Reports*, 366:1–101, 2002.
- [9] R. Murray-Smith et T.A. Johansen. *Multiple Model Approaches to Modeling and Control*. Taylor and Francis, 1997.
- [10] Y. Wang, Q.L. Zhang, et W.Q. Liu. Stability analysis and design for t-s fuzzy descriptor. *Proceedings of the 40th IEEE Conference on Decision and Control, Orlando, Florida, USA*, pages 3962–3967, 2001.
- [11] M. Chadli, J. Ragot, et D. Maquin. Multiquadratic stability and stabilization of continuous-time multiple-model. *11th IFAC Symposium on Automation in Mining, Mineral and Metal processing, Nancy, France*, 2004.
- [12] X.F. Wang, G.-Q. Zhong, K.-S. Tang, K.F. Man, et Z.-F. Liu. Generating Chaos in Chua's Circuit via Time-Delay Feedback. *IEEE Trans. Circuit Syst. I*, 48(9):1151–1156, 2001.
- [13] H.D.I. Abarbanel, R. Brown, J.J. Sidorowich, et L.Sh. Tsimring. The analysis of observed data in physical systems. *Rev. Mod. Phys.*, 65(4):1331–1392, 1993.
- [14] K. Gu, V.L. Kharitonov, et J. Chen. *Stability of time-delay systems*. Birkhäuser, 2003.
- [15] C.E. García, J.F. Postigo, A. Castro, R. Carelli, et B. Kuchen. On-line estimation of communication time delay in a robotic teleoperation system. *Lat. Am. Appl. Res.*, 33(4):371–377, 2003.

de synchronisation sont établies, permettant la synthèse d'observateurs non linéaires grâce à la résolution de LMIs. Cette méthode de synchronisation est testée sur un exemple, puis intégrée dans un processus de communications, lui-même illustré par le cryptage/décryptage d'un signal sonore. Ce travail pourra être approfondi par l'étude