République Algérienne Démocratique et Populaire

Ministère de L'Enseignement Supérieur et de la Recherche Scientifique

Université de Jijel

Faculté des Sciences et de la Tech

Département d'Automatique

Projet de Fin d'Etudes

Pour L'obtention du Diplôme Master en Automatique

Option:
Automatique et Informatique Industrielle

THEME

Systèmes de communication sécurisés basés sur les systèmes chaotiques à retard

Encadré par :
Mlle. Meriem HALIMI

Réalisé par :
Mr. Khaled BENKOUIDER

Juin 2015

REMERCIEMENT

Avant tout, je remercie Dieu, le miséricordieux, qui m'a donné la force, le courage et la réussite et qui a mis à ma disposition des gens merveilleux qui m'ont supporté et soutenu tout au long de mes études.

Je remercie très chaleureusement mon encadreuse, Mlle HALIMI Meriem, Maitre assistant à l'Université de Jijel, pour avoir dirigé mes travaux. Merci pour vos échanges scientifiques, vos conseils et votre rigueur. Merci pour votre soutien scientifique et humain. Je voudrais aussi vous remercier d'avoir cru en mes capacités et de m'avoir fourni d'excellentes conditions me permettant d'aboutir à la production de ce mémoire de fin d'étude. Ce mémoire n'aurait vu le jour sans votre confiance et votre générosité.

Je tiens également à remercier les membres du jury pour m'avoir honoré par leur présence et pour avoir accepté d'évaluer ce modeste travail.

Enfin, il me serait impossible de terminer sans adresser une pensée chaleureuse à mes parents pour leur soutien et leurs encouragements pendant de longues années, sans qui, je n'aurais pu arriver à ce niveau d'études.

K. Benkouider

TABLE DES MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

ACRONYMES

LPV	Linear Parameter Varying
LMI	Linear Matrix Inegalities
UIO	Unknown Input Observer
CSK	Chaotic Switch Keying
DSCK	Differential Chaotic Switch Keying
FM	Frequent Modulation
GAS	Globalement Asymptotiquement Stable

NOTATIONS

$\mathbb{R}$	Ensemble des nombres réels
$\mathbb{R}^n$	Ensemble des nombres réels de dimension n
$\mathbb{R}_+$	Ensemble des nombres réels non négatifs
$\mathbb{N}$	Ensemble des entiers
$A(\rho_k)$, $\mathcal{A}_l(\rho_k)$	Matrice dynamique à description polytopique
$B, \mathcal{B}$	Matrice de commande
$C, \mathcal{C}$	Matrice d'observation
n	Dimension du vecteur x_k
M	Dimension du vecteur $X_k^{(l)}$
x_k	Vecteur d'état d'un système dynamique en temps discret
u_k	Entrée de commande
y_k	Vecteur de sortie d'un système dynamique en temps discret
Ω	Attracteur chaotique
Ω_ρ	Ensemble compact auquel appartient ρ_k
λ_L	Exposant de Lyapunov
ρ_k	Vecteur des paramètres variant d'un système à description polytopique
D_ρ	Polytope auquel appartient ρ_k
D_ρ^*	Polytope minimal auquel appartient ρ_k
L_ρ	Dimension de ρ_k

$\mathcal{L}_l(\rho_k)$	Gain à temps variant de l'observateur polytopique O_l
$\mathcal{P}_l(\rho_k)$	Matrice définie positive à temps variant
ρ_{o_i}	Sommets du polytope D_ρ
Φ	Ensemble convexe,$\Phi = \left\{\xi_k \in \mathbb{R}^N, \xi_k = \left[\xi_k^{(1)}, \cdots, \xi_k^{(N)}\right], \xi_k^{(i)} \geq 0 \; \forall \; k \; et \; \sum_{i=1}^{N} \xi_k^{(i)} = 1\right\}$
D_A	Polytope auquel appartient $A(\rho_k)$
$A^{(i)}$	Sommet du polytope D_A
$\hat{Y}_k^{(l)}$	Vecteur de sortie de l'observateur O_l
$\hat{X}_k^{(l)}$	Vecteur d'état de l'observateur O_l
m_k	Signal d'information
$\hat{m}_k$	Signal d'information reconstruit
x_0	Ensemble des conditions initiales
$P_i^{(l)}$	Matrices définies positives
$\mathcal{P}$	Fonction de Lyapunov
I_n	Matrice identité de dimension n
$\mathbf{0}$	Matrice nulle de dimension appropriée
$\|.\|$	Valeur absolue
Y	Matrice arbitraire
$rang(M)$	Rang de la matrice M
$ln(.)$	Logarithme népérien
f	Fonction d'état
k	Temps discret
N	Nombre de sommets du polytope
$e_k^{(l)}$	Erreur de reconstruction d'état de l'observateur O_l
$(\blacksquare)$	Bloc d'une matrice induit par symétrie

A^T	Transposé de la matrice A
A^+	Inverse généralisée de A satisfaisant A^+A symétrique, AA^+ symétrique, $AA^+A = A$ et $A^+AA^+ = A^+$
$\tau(k)$	Retard inconnu associé au vecteur d'état, $\tau(k) \in \{0, \dots, \alpha\}$
$\hat{\tau}(k)$	Retard reconstruit
O_l	Observateur l
S_l	Sous système l

Introduction Générale

Depuis l'antiquité, l'homme n'a pas cessé de chercher les différents moyens pour transmettre un message à son correspondant et pouvoir ainsi communiquer avec lui en toute sécurité. Il a fourni, à travers des époques successives, des efforts autant physiques qu'intellectuels pour pouvoir trouver une technique de communication efficace et appropriée.

La cryptographie a depuis des siècles été une histoire de conflit qui oppose deux camps, un qui cherche à cacher une information et un autre qui essaie de trouver ce qu'on lui cache. Ainsi à chaque fois que le premier trouve un moyen de chiffrer ses messages le second essaie et, avec le temps et les moyens dont il dispose, réussit à trouver la méthode pour le décrypter. La cryptographie ancienne utilisait différents outils pour dissimuler une information ou un texte secret. Certains remplaçaient des mots par des nombres, d'autres mélangeaient, décalaient ou permutaient les lettres, comme dans la substitution alphabétique inverse, pour rendre la lecture du message difficile voire impossible.

La cryptographie actuelle cherche à transformer de façon mathématique et algorithmique un message clair pour obtenir un autre chiffré et qui, à première vue, semble aléatoire. Plus l'inversion de la transformation est difficile plus la sécurité est élevée et vice versa. On cherche alors un phénomène d'apparence aléatoire mais qui est déterministe à l'origine pour le masquage d'information.

Il existe plusieurs systèmes présentant ce comportement, ils sont dits chaotiques, ils sont régis par des lois déterministes, dépendent d'un ou de plusieurs paramètres et leur évolution dans le temps est imprévisible. L'étude de tels systèmes est liée à la théorie du chaos qui a connu un grand essor à partir de 1960 grâce aux travaux de plusieurs chercheurs notamment ceux de Lorenz et à la découverte de nouveaux outils de calculs.

La cryptographie chaotique est ainsi née par inclusion du chaos dans les télécommunications et systèmes de transmission. L'idée consiste à noyer un message dans un

signal chaotique pour faire face aux éventuelles tentatives de piratage. L'utilisation du chaos dans les systèmes de communication a été inspirée de la découverte de Pecora-Carroll en 1990 [Pecora and Caroll, 1990]. Ils ont montré que deux systèmes chaotiques identiques avec des conditions initiales différentes peuvent se synchroniser.

Depuis, le développement des systèmes de communication utilisant le chaos a commencé par des schémas de synchronisation très simples de circuits électroniques, visant pour le cryptage et la reconstruction simultanée d'un signal d'information. Par la suite, de nombreuses techniques de cryptage par addition, par commutation, par modulation, ... etc, ont été mises au point pour inclure le message clair dans un signal porteur chaotique, voire dans la dynamique même de l'émetteur.

Pour la cryptographie chaotique, un des concepts les plus importants est la synchronisation, c'est à dire que le récepteur essaie de reconstruire les états de l'émetteur à partir du signal transmis, considéré comme la sortie du système à observer et ensuite de récupérer le message crypté considéré comme une entrée inconnue. Du point de vue de l'automatique, cette technique peut être classée dans le domaine de la conception d'observateurs [Nijmeijer and Mareels, 1997].

Même si les techniques de cryptage par le chaos sont en plein essor, des attaques spécifiques ont été développées en parallèle, ouvrant ainsi une nouvelle voie dans la cryptanalyse, qui s'oppose à la cryptographie. Par conséquent, la proposition d'une nouvelle façon de transmettre un message, en exploitant la synchronisation et les propriétés des systèmes chaotiques, doit s'accompagner d'une réflexion sur la sécurité du processus.

Au cours des deux dernières décennies, il y a eu un intérêt croissant pour les systèmes chaotiques à retard dans les communications sécurisées. En effet, les retards augmentent la dimension du système, ce qui est intéressant pour améliorer la complexité des dynamiques [Zheng et al., 2008] et rendent le décryptage de l'information claire plus complexe. Dans ce contexte, l'estimation du retard est un enjeu important puisqu'il peut jouer le rôle de clé secrète dans une communication sécurisée. Un travail pionnier qui traite des systèmes de communication optoélectroniques a été d'abord rapporté dans [Mirasso et al., 1996]. Depuis, les performances ont été améliorées et de nos jours, des systèmes de communication très haut débit peuvent être conçus.

Le travail que nous allons réaliser dans ce mémoire s'inscrit dans ce contexte particulier. Notre objectif est d'étudier deux systèmes de transmission plus sécurisés et plus robustes aux attaques. Pour le premier système de transmission, l'émetteur est composé d'un système chaotique en temps discret où l'information secrète est injectée comme retard dans le vecteur d'état de l'émetteur. Pour le deuxième système de transmission, le retard sur le vecteur d'état de l'émetteur est une clé secrète qui permet d'augmenter la complexité de la transmission, et l'information secrète est injectée par inclusion dans l'émetteur. Nous allons proposer pour chaque cas une méthode permettant d'estimer le retard et éventuellement l'information. Pour cela, on fera appel à des observateurs polytopiques. Ceci constitue notre contribution dans ce mémoire, car la conception d'observateurs pour les systèmes chaotiques à retard est plus complexe. Une technique très utile, permettant à la fois, d'estimer le retard inconnu et le message crypté, qui repose sur la conception d'observateurs, sera étudiée dans ce mémoire.

Ce mémoire est organisé de la façon suivante :

Le premier chapitre fera l'objet d'un rappel sur les systèmes chaotiques et les systèmes de chiffrement fondés sur le chaos. Il énoncera quelques concepts et définitions introductifs à la théorie du chaos suivis par quelques exemples des plus célèbres des systèmes chaotiques. La synchronisation et la cryptographie chaotique, sera ensuite détaillée. En effet, on va parcourir d'abord les différents types de la synchronisation du chaos. Ensuite, on va rappeler les principaux schémas de la transmission chaotique.

Le deuxième chapitre est consacré à la technique de modélisation LPV (Linéaire à Paramètres Variant) polytopique. On expliquera dans un premier temps le principe de cette description puis on rappellera comment un système chaotique à non linéarité polynomiale pouvait être réécrit sous cette forme. Ce choix de modélisation est motivé par les méthodes de *décryptage, utilisées dans les chapitres 3 et 4, qui font appel à des observateurs polytopiques.*

Le troisième chapitre est dédié à l'étude du premier système de communication chaotique où l'information secrète est injectée comme retard dans le vecteur d'état de l'émetteur. On expliquera comment l'émetteur (qui devient un système chaotique autonome à retard) pouvait être réécrit sous une forme LPV polytopique. Ensuite, on rappellera le principe d'une formulation hybride qui va nous permettre de passer d'un système à retard à un système sans retard en augmentant la dimension du vecteur d'état. Nous allons ensuite s'intéresser à la méthode de conception des observateurs LPV polytopiques fondée sur

l'utilisation des LMIs pour assurer la stabilité poly-quadratique de l'erreur de reconstruction d'état. Une procédure complète permettant de reconstruire l'information secrète au niveau du récepteur sera proposée dans ce chapitre. Finalement, on termine avec un exemple illustratif, portant sur la transmission d'un message binaire, qui permet d'illustrer l'efficacité de la méthode.

Le quatrième chapitre est dédié à l'étude du deuxième système de communication chaotique où l'information secrète est injectée par inclusion, et le retard joue le rôle de la clé secrète. On expliquera comment l'émetteur (qui devient un système chaotique non autonome à retard) pouvait être réécrit sous une forme LPV polytopique. Ensuite, on utilisera la formulation hybride du chapitre précédent pour éliminer le retard. La méthode de conception des observateurs LPV polytopiques à entrée inconnue fondée sur l'utilisation des LMIs sera ensuite introduite. Après, une procédure complète permettant d'estimer à la fois le retard et l'information cryptée sera proposée. Plusieurs applications seront données à la fin de ce chapitre afin de montrer l'efficacité de cette procédure.

Le mémoire se termine par une conclusion générale et quelques perspectives.

Chapitre 1

Systèmes de Chiffrement Chaotique

1.1 Introduction

Les systèmes chaotiques possèdent des caractéristiques particulières exploitables dans le domaine de la télécommunication, pour la sécurisation des transmissions. Comme le chaos déterministe peut générer des comportements dynamiques d'apparences aléatoires, ces derniers ont été utilisés comme porteuses d'informations en télécommunication.

En 1990, *L. M. Pecora* et *T. L. Caroll* ont introduit la notion de synchronisation de deux systèmes chaotiques identiques [Pecora and Caroll, 1990]. Trois ans plus tard, le premier dispositif de communication entre deux systèmes chaotiques de Lorenz identiques a été présenté par *Cuomo* et *Oppenheim* [Cuomo et al., 1993]. En 1997 *Kolumban*, *Kennedy* et *Chua* réalisèrent des communications numériques à base de deux circuits de Chua identiques. Plus tard, le domaine du chaos attira l'attention de la communauté scientifique et plusieurs systèmes de communication symétriques furent présentés.

Dans le cadre de ce projet de fin d'étude, nous nous sommes intéressés à l'étude des systèmes de transmission sécurisés à base des systèmes chaotiques à retard. Cependant, dans un premier temps, nous allons rappeler brièvement les phénomènes chaotiques.

1.2 Systèmes chaotiques

Un système est dit être chaotique lorsqu'il présente la propriété particulière de sensibilité aux conditions initiales. Cette dernière se traduit par le fait que la distance entre deux trajectoires tend à augmenter de manière exponentielle au cours du temps, pouvant atteindre une distance limite qui est de l'ordre du diamètre de l'attracteur.

1.2.1 Caractéristiques du chaos

Dans ce qui suit, nous allons rappeler quelques caractéristiques permettant de comprendre les points marquants de ces systèmes [Devancy, 1992].

a) Non-linéarité

Un système chaotique est un système dynamique non linéaire. Ainsi, un système linéaire ne peut pas être chaotique.

b) *Sensibilité aux conditions initiales*

La sensibilité aux conditions initiales communément appelée effet papillon a été popularisée par le météorologue Edward Lorenz. Elle se caractérise par le fait que la distance entre deux trajectoires de phase initialement voisines, tend à augmenter de manière drastique (souvent exponentielle) au cours du temps. Ainsi, la moindre erreur ou simple imprécision sur la condition initiale interdit de décider quelle sera la trajectoire effectivement suivie à long terme et en conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système, bien que l'on traite de systèmes déterministes.

En simulation, les erreurs d'arrondis peuvent être à l'origine de ce phénomène. Ceci est illustré dans la Figure 1.1. On affecte au système chaotique de Lorenz (donné ci-après) deux conditions initiales très proches. Dans un premier temps, on remarque que les deux signaux évoluent de la même manière, mais, très vite, leur comportement devient différent.

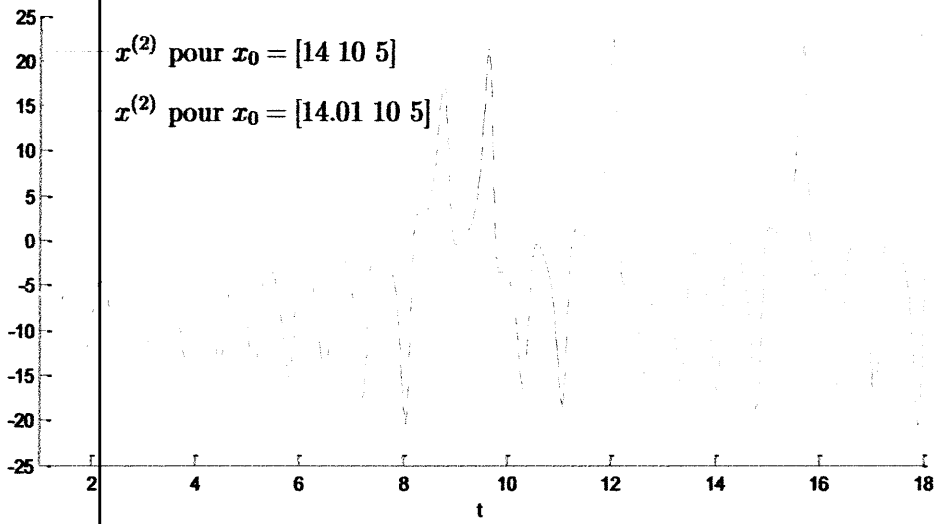


Figure 1.1 Evolution dans le temps pour deux conditions initiales très proches

c) Aspect aléatoire

Une autre caractéristique des systèmes chaotiques peut être observée sur les courbes de la Figure 1.1. En effet, un système chaotique évolue d'une manière qui semble être aléatoire. La Figure 1.2 permet de comparer l'évolution périodique et donc prédictible d'un

système classique avec l'évolution plus complexe, non périodique et non prédictible du système chaotique de Lorenz.

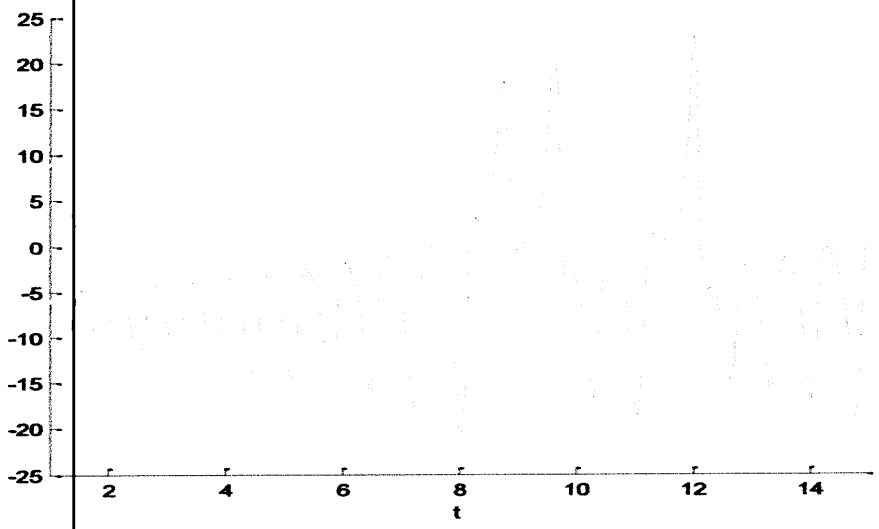


Figure 1.2 Evolution dans le temps d'un système chaotique, comparé à une sinusoïde

d) Déterminisme

La notion de déterminisme signifie la capacité de prédire le futur d'un phénomène à partir d'un évènement passé ou présent. L'évolution irrégulière du comportement d'un système chaotique est due aux non linéarités.

Dans les phénomènes aléatoires, il est absolument impossible de prévoir la trajectoire d'une quelconque particule. À l'opposé, un système chaotique a des règles fondamentales déterministes et non probabilistes.

e) Attracteur étrange

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires de l'espace des phases, c'est-à-dire, une situation ou un ensemble de situations vers lesquelles évolue un système, quelles que soient ses conditions initiales.

Un attracteur chaotique, appelé aussi attracteur étrange, possède la propriété particulière suivante : la trajectoire ne repasse jamais par un même état. Ce qui signifie, entre autres, que cette trajectoire passe par une infinité d'états.

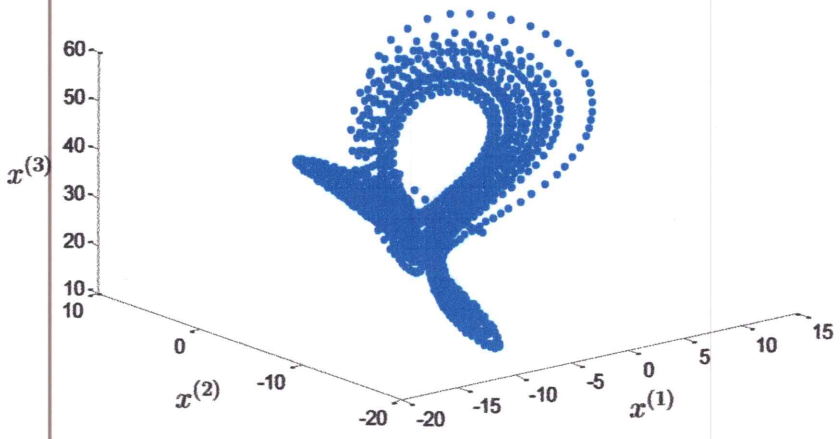


Figure 1.3 Attracteur chaotique

1.2.2 Exposant de Lyapunov

Le mathématicien russe Alexander Lyapunov s'est penché sur le phénomène de sensibilité aux conditions initiales et a proposé une grandeur permettant de la qualifier. Cette grandeur est appelée "exposant de Lyapunov". Ainsi, l'exposant de Lyapunov permet de caractériser quantitativement le caractère chaotique d'un système. Considérons un système dynamique, à une dimension, défini par

$$x_{k+1} = f(x_k) \tag{1.1}$$

où $x_k \in \mathbb{R}$ est le vecteur d'état et $f: \mathbb{R} \to \mathbb{R}$ une fonction non linéaire. La suite $x_0, x_1, \cdots$ est appelée orbite ou trajectoire de phase.

Supposons que la condition initiale x_0 de (1.1) soit affectée d'une erreur infinitésimale E_0. Après k itérations, l'erreur initiale E_0 sera donc amplifiée d'un facteur $\left|\frac{E_k}{E_0}\right|$.

Notons que l'erreur diminue lorsque le facteur est inférieur à 1 et augmente s'il est supérieur à 1. On a la formule suivante :

$$\left|\frac{E_k}{E_0}\right| = \left|\frac{E_k}{E_{k-1}}\right| \cdot \left|\frac{E_{k-1}}{E_{k-2}}\right| \cdot \left|\frac{E_{k-2}}{E_{k-3}}\right| \cdots \left|\frac{E_2}{E_1}\right| \cdot \left|\frac{E_1}{E_0}\right| \tag{1.2}$$

d'où

$$ln\left(\left|\frac{E_k}{E_0}\right|\right) = \sum_{i=1}^{k} ln\left(\left|\frac{E_i}{E_{i-1}}\right|\right) \tag{1.3}$$

Il suffit alors de calculer ce produit pour déterminer la façon dont s'amplifie l'erreur initiale. Lyapunov a découvert ensuite que cette erreur tendait vers une limite donnée par la formule suivante :

$$\lambda_L = \lim_{k\to\infty} \frac{1}{k} \sum_{i=1}^{k} ln\left(\left|\frac{df(x_{i-1})}{dx_{i-1}}\right|\right) \in \mathbb{R} \qquad (1.4)$$

- Si $\lambda_L < 0$: l'orbite est attractive vers un point fixe ou une orbite périodique. Il caractérise les systèmes dissipatifs. Ce type de système exhibe une stabilité asymptotique.
- Si $\lambda_L = 0$: les orbites issues de conditions initiales différentes, gardent une séparation constante, ni ne convergent, ni ne divergent l'une par rapport à l'autre. Un système physique avec un tel exposant est dit conservatif.
- Si $\lambda_L > 0$: l'orbite est instable et chaotique.

Ce résultat a été étendu à des systèmes à n dimensions comme l'illustre le Tableau 1.1 [Eckmann and Ruelle, 1992].

Exposants de Lyapunov	Régime permanent	Attracteur
$0 > \lambda_{L1} \geq \cdots \geq \lambda_{Ln}$	Point d'équilibre	Point
$\lambda_{L1} = 0$ $0 > \lambda_{L2} \geq \cdots \geq \lambda_{Ln}$	Périodique	Courbe fermée
$\lambda_{L1} = \cdots = \lambda_{Li} = 0$ $0 > \lambda_{Li+1} \geq \cdots \geq \lambda_{Ln}$	Quasi – périodique	tore
$\lambda_{L1} > 0$ $0 > \lambda_{L2} \geq \cdots \geq \lambda_{Ln}$	Chaotique	fractale

Tableau 1.1 Classification des régimes permanents en fonction des exposants de Lyapunov

1.3 Exemples de systèmes chaotiques

1.3.1 Exemples de systèmes à temps continu

a) Système de Lorenz

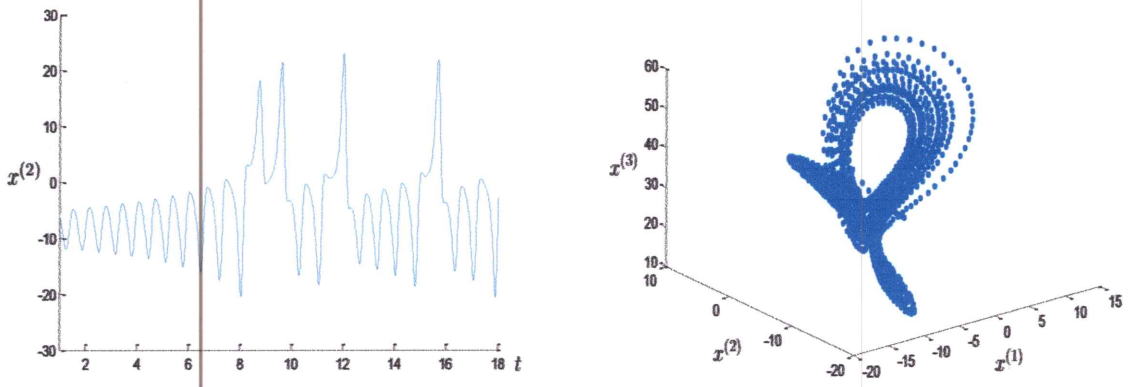
Le physicien *Edward Lorenz* travaillait sur un modèle mathématique dont le but était de prédire la température. Il utilisa un modèle à trois variables dynamiques $x^{(1)}$, $x^{(2)}$ et $x^{(3)}$.

Le système de Lorenz est un exemple célèbre de système différentiel au comportement chaotique pour certaines valeurs de paramètres, son système est composé de trois équations différentielles [Cuomo et al., 1993] :

$$\begin{cases} \dot{x}^{(1)} = \sigma\left(x^{(2)} - x^{(1)}\right) \\ \dot{x}^{(2)} = rx^{(1)} - x^{(2)} - x^{(1)}x^{(3)} \\ \dot{x}^{(3)} = -bx^{(3)} + x^{(1)}x^{(2)} \end{cases} \tag{1.5}$$

σ , r et b représentent des paramètres.

L'attracteur chaotique de Lorenz est donné sur la Figure 1.4 (b) pour les valeurs numériques σ = 10, r = 28, et b = $\frac{8}{3}$. La Figure 1.4 (a) représente la variation de la coordonnée $x^{(2)}$.



(a) Evolution de $x^{(2)}$ (b) Attracteur chaotique de Lorenz

Figure 1.4 Système chaotique de Lorenz

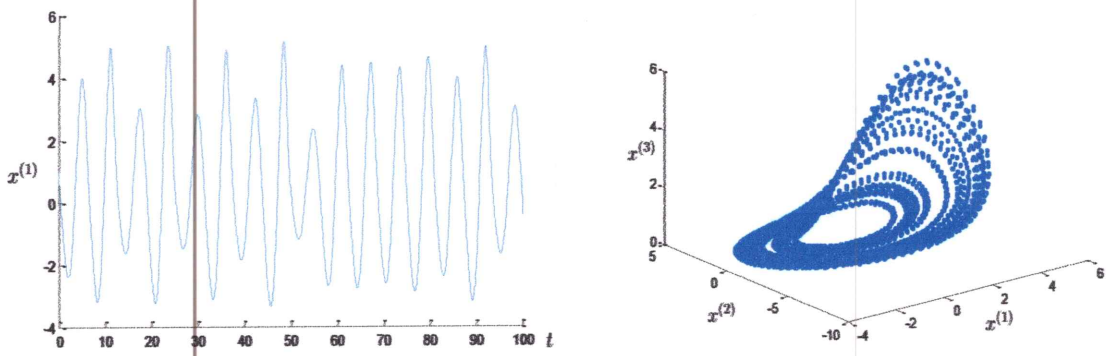
b) Système de Rössler

Le système de Rössler, proposé par l'Allemand Otto Rössler, est lié à l'étude de l'écoulement des fluides. Il découle des équations de Navier-Stokes. Les équations de ce système ont été découvertes à la suite de travaux en cinétique chimique. Ce système est défini par les équations suivantes [Rössler, 1976] :

$$\begin{cases} \dot{x}^{(1)} = -\left(x^{(2)} + x^{(3)}\right) \\ \dot{x}^{(2)} = x^{(1)} + ax^{(2)} \\ \dot{x}^{(3)} = b + x^{(3)}(x^{(1)} - c) \end{cases} \tag{1.6}$$

a, *b* et *c* représentent des paramètres.

L'attracteur chaotique de Rössler est donné sur la Figure 1.5 (b) pour les valeurs numériques a = 0.398, b = 2 et c = 4. La Figure 1.5 (a) représente la variation de la coordonnée $x^{(1)}$.



(a) Evolution de $x^{(1)}$ (b) Attracteur chaotique de Rössler.

Figure 1.5 Système chaotique de Rössler

1.3.2 Exemples de systèmes à temps discret

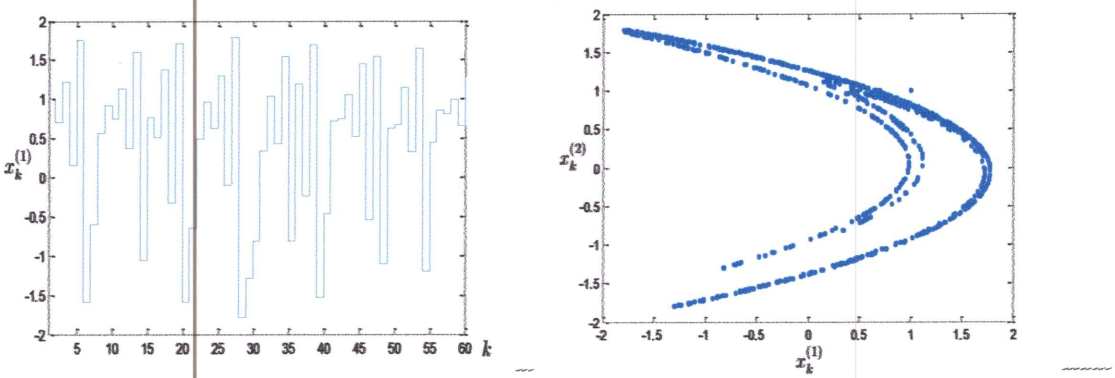
a) Récurrence de Henon

Le système de Hénon est un modèle proposé en 1976 par le mathématicien *Michel Hénon*. Le modèle d'état associé est [Douglas, 1992] :

$$\begin{cases} x_{k+1}^{(1)} = \alpha - \left(x_k^{(1)}\right)^2 + bx_k^{(2)} \\ x_{k+1}^{(2)} = x_k^{(1)} \end{cases} \tag{1.7}$$

a et b représentent des paramètres.

L'attracteur chaotique de Hénon est donné sur la Figure 1.6 (b) pour les valeurs numériques a =1.4 et b = 0.3. La Figure 1.6 (a) représente la variation de la coordonnée $x^{(1)}$.



(a) Evolution de $x^{(1)}$ (b) Attracteur chaotique de Henon.

Figure 1.6 Récurrence chaotique de Henon.

Il est à noter qu'il ya un autre système chaotique discret, qui est le système de Lozi, qu'on l'obtient en remplaçons $\left(x_k^{(1)}\right)^2$ dans le système (1.7) par $\left|x_k^{(1)}\right|$.

b) Suite logistique

La suite logistique est un modèle simplifié de l'évolution d'une population d'une espèce animale. Elle est définie par l'équation [May, 1976] :

$$x_{k+1} = \theta\, x_k(1 - x_k) \tag{1.8}$$

θ représente un paramètre.

La grandeur x_k représente le pourcentage de cette espèce dans son environnement à l'année k, et θ un facteur de proportionnalité.

La figure suivante représente l'évolution de la fonction logistique en fonction des itérations k pour différentes valeurs de θ, pour la condition initiale $x_0 = 0.15$:

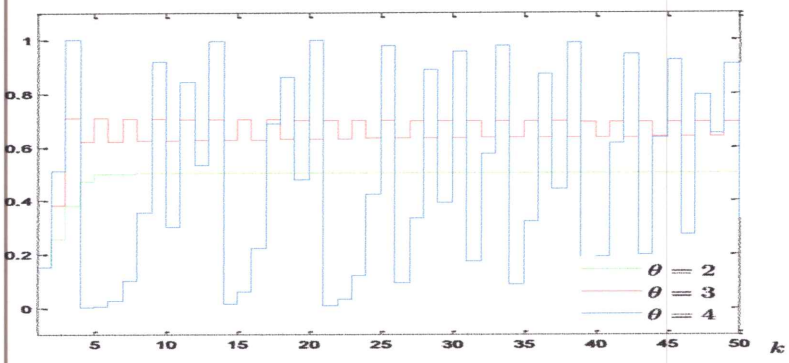


Figure 1.7 Evolution de la suite logistique pour différentes valeurs de θ

L'attracteur chaotique de la suite logistique est donné sur la Figure 1.8 pour la valeur numérique $\theta = 4$.

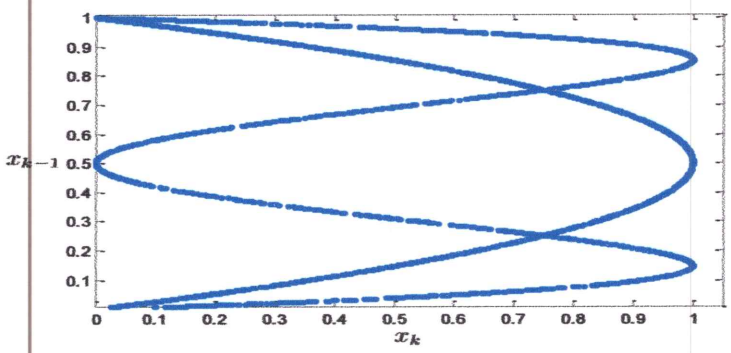


Figure 1.8 Attracteur chaotique de la suite logistique

1.4 Principe de la communication sécurisée à base du chaos

Le diagramme principal de la communication sécurisée par le chaos est montré sur la Figure 1.9. Le principe consiste à masquer une information par des signaux chaotiques au niveau de l'émetteur et de l'envoyer par la suite vers le récepteur via un canal public. L'information cryptée est récupérée au niveau du récepteur.

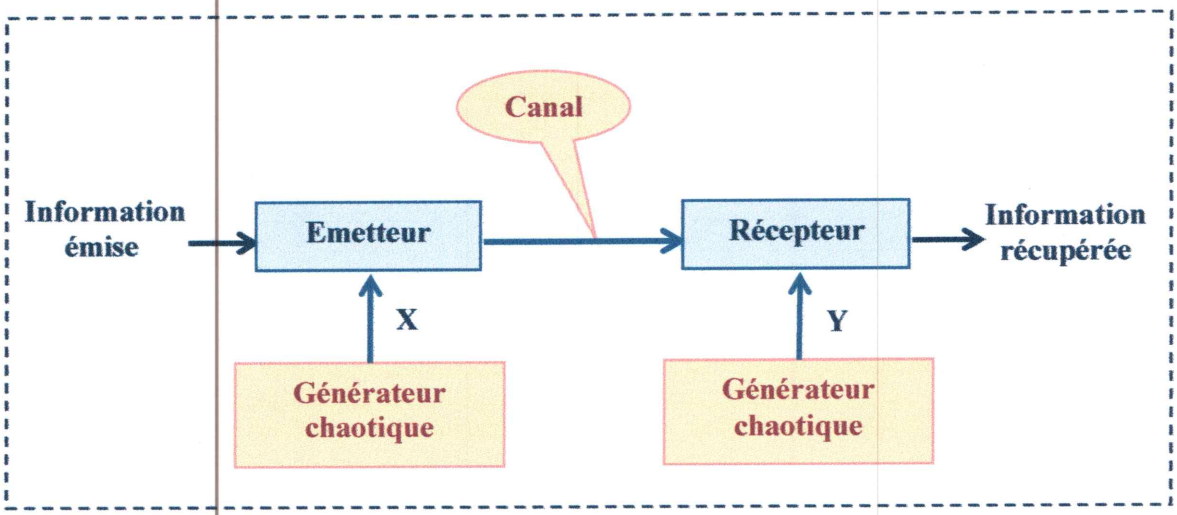


Figure 1.9 Principe de la communication sécurisée à base du chaos

1.5 Propriétés des systèmes de communication à base du chaos

Dans cette partie, des propriétés des systèmes de communication chaotiques seront étudiées et comparées aux propriétés des systèmes classiques.

1.5.1 Spectre à large bande

Les systèmes chaotiques ont spécifiquement un spectre à large bande. Cette propriété est bénéfique pour les applications qui nécessitent une importante robustesse face aux interférences et une faible probabilité de détection [Tenny, 2003].

Ces problèmes ont été pris en compte par les premiers systèmes de transmission en utilisant des spectres larges et des modulations par saut de fréquences. Cependant malgré le recours à ces moyens, la synchronisation entre l'émetteur et le récepteur reste une tâche qui n'est pas toujours triviale. En effet les schémas de transmission qui utilisent un saut de fréquence requièrent une nouvelle synchronisation à chaque changement de fréquence de la porteuse. Donc l'utilisation des systèmes chaotiques permet la transmission des signaux à large bandes, ainsi la synchronisation entre l'émetteur et le récepteur est plus simple.

1.5.2 Signal non périodique

La périodicité, dans la communication sécurisée engendre des pics spectraux indésirables. Par contre, un signal chaotique est non périodique et son évolution ne peut être prédite sur un long intervalle de temps. Par conséquent, il y a absence des pics spectraux. De plus il est plus difficile de développer un modèle de prévisions pour les dynamiques non périodiques [Tenny, 2003].

1.5.3 Implémentation analogique simple

Les systèmes de communication à base du chaos peuvent être implémentés en utilisant des dispositifs électriques ou optiques. Dans les schémas traditionnels par exemple, la transmission par saut de fréquences nécessite la numérisation des données, ceci impliques des circuits indépendants plus complexes [Tenny, 2003].

1.6 Synchronisation des systèmes chaotiques

Pour que deux systèmes chaotiques identiques puissent se synchroniser, il faut que leur attracteur soit le même. Ils doivent donc avoir les mêmes équations, les mêmes paramètres et le même point de repos. L'opération de synchronisation consiste à rapprocher les trajectoires des deux systèmes jusqu'à ce qu'elles finissent par être confondues.

Le système global comporte un circuit émetteur, et un circuit récepteur. Synchroniser les deux systèmes revient à injecter dans le récepteur une grandeur proportionnelle à la différence des deux trajectoires. De cette façon la trajectoire du récepteur finit par être confondue avec celle de l'émetteur. Ce principe est détaillé par le schéma bloc de la Figure 1.10.

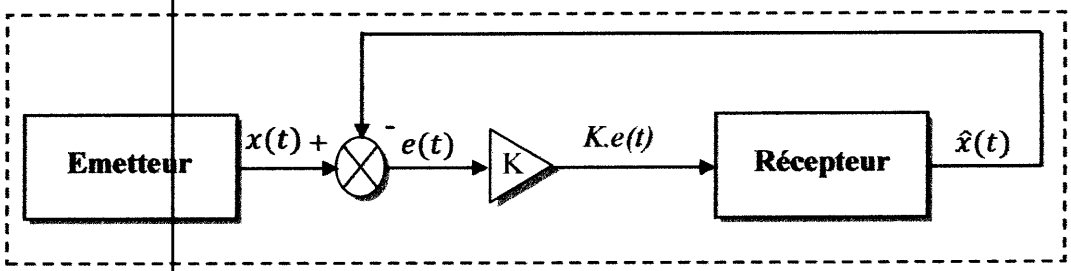


Figure 1.10 Schéma bloc illustrant le principe de la synchronisation.

Dans le domaine de la communication, la synchronisation consiste à forcer un système esclave à se synchroniser avec un système maître. Plusieurs types de synchronisation existent, et dans ce qui suit nous allons citer les cinq types principaux de

synchronisations. Il est à noter que même ces cinq types de synchronisations ne sont pas totalement séparables.

1.6.1 Synchronisation basée sur la partition du système

Cette approche de synchronisation des systèmes a été proposée par *Pecora* et *Carrol* [Pecora and Carroll, 1990]. Considérons un système chaotique de dimension $n \geq 3$ suivant :

$$\dot{x} = f(x) \tag{1.9}$$

Et supposons qu'il peut être divisé en deux sous systèmes :

$$\begin{cases} \dot{x}_R = f_R(x_R) \\ \dot{x}_T = f_T(x_R, x_T) \end{cases} \tag{1.10}$$

Où : $x_R \in \mathbb{R}^{n_R}$, $x_T \in \mathbb{R}^{n_T}$ et $n_R + n_T = n$.

Le premier sous système s'appelle le système conducteur, et le second est appelé le système de réponse. Ensuite, nous pouvons encore diviser le sous système conducteur de (1.10) en deux autres sous systèmes comme suit :

$$\begin{cases} \begin{cases} \dot{x}_{R1} = f_{R1}(x_{R1}, x_{R2}) \\ \dot{x}_{R2} = f_{R2}(x_{R1}, x_{R2}) \end{cases} \\ \dot{x}_T = f_T(x_R, x_T) \end{cases} \tag{1.11}$$

La synchronisation du système (1.9) est basée sur la stabilité du sous système de réponse (1.10), qui ne peut pas être déterminée de manière globale par la stabilité de sa matrice Jacobinne (J_{fT}), car celle ci dépend évidemment de l'état x_R. Ainsi, le comportement de ce sous système dépend de l'exposant de Lyapunov du système (1.11), qui s'appelle l'exposant exponentiel conditionnel.

Il est prouvé que, si tous les exposants sont négatifs, la stabilité asymptotique du sous système de réponse peut être garantie. Mais les évidences sont trouvées que deux systèmes chaotiques couplés avec les exposants exponentiels conditionnels négatifs peuvent désynchroniser [Heidari-Bateni et al., 1992].

1.6.2 Synchronisation par la boucle fermée

Une autre technologie de la synchronisation est basée sur la boucle fermée qui peut être illustrée en Figure 1.11, où l'erreur entre l'émetteur et le récepteur est employée afin de *corriger le comportement du récepteur pour but d'atteindre la synchronisation.*

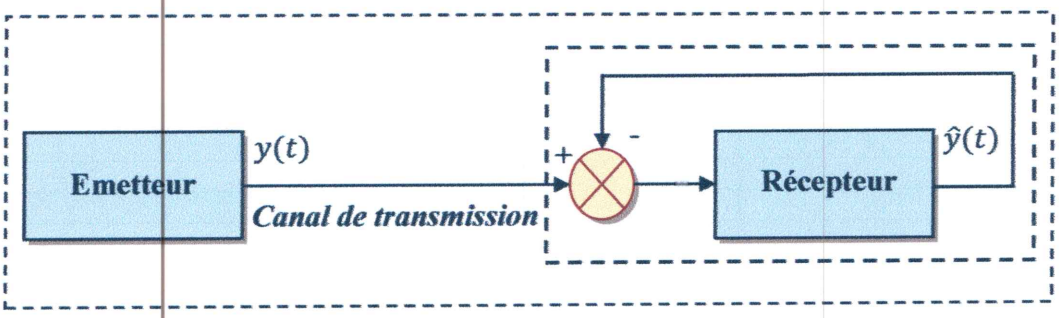


Figure 1.11 Synchronisation par un contrôle en boucle fermée

Supposons que l'émetteur s'écrit comme suit :

$$\begin{cases} \dot{x} = f(x) \\ y = h(x) \end{cases} \tag{1.12}$$

Et que le récepteur peut être décrit comme suit :

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) + g(y - \hat{y}) \\ \hat{y} = h(\hat{x}) \end{cases} \tag{1.13}$$

Où g est une fonction de l'erreur entre y et $\hat{y}$, et que cette fonction est choisie afin de garantir la synchronisation entre l'émetteur et le récepteur.

En fait, ce genre de récepteur peut être considéré comme la conception d'un observateur. Celle-ci sera présentée dans la section suivante. Ensuite, nous pouvons également appliquer quelques stratégies adaptatives quand nous employons l'erreur entre l'émetteur et le récepteur pour piloter le récepteur.

1.6.3 Synchronisation à l'aide d'observateur

Les systèmes chaotiques sont généralement décrits par une équation différentielle non linéaire. Il s'avère cependant intéressant de séparer la dynamique du système en une *partie linéaire et une partie non-linéaire.*

La synchronisation peut également être réalisée en employant un observateur. L'observateur est une méthode typique afin d'estimer les états inconnus d'un système dynamique qui ne peuvent pas être mesurés directement : soit inaccessible, soit pas économique.

Considérons l'émetteur comme suit :

$$\begin{cases} \dot{x} = f_\theta(x) = Ax + f(x) \\ y = h_\theta(x) = Cx \end{cases} \tag{1.14}$$

Où $x \in \mathbb{R}^n$ et $y \in \mathbb{R}$ représentent respectivement le vecteur d'état et la sortie du système d'émission.

A et C : Deux matrices constantes

$f: \mathbb{R}^n \to \mathbb{R}^n$: Fonction vectorielle réelle.

Le récepteur est conçu sur la base d'un observateur où y correspond à l'entrée de commande. L'observateur peut être conçu de la façon suivante :

$$\begin{cases} \dot{\hat{x}} = f_\theta(\hat{x}) = A\hat{x} + f(\hat{x}) + K(y - \hat{y}) \\ \hat{y} = h_\theta(\hat{x}) = C\hat{x} \end{cases} \tag{1.15}$$

Où $\hat{x}$ est le vecteur d'état associé au récepteur, et $K \in \mathbb{R}^n$ est un gain d'observateur.

En définissant l'erreur de synchronisation $e = x - \hat{x}$, nous pouvons obtenir :

$$\dot{e} = (A - KC)e + f(x) - f(\hat{x}) \tag{1.16}$$

Dans ce cas, le problème de la synchronisation devient celui de la stabilité au voisinage du point fixe 0, du système (1.16). Si la fonction *f(x)* vérifie la condition Lipschitz, et si nous pouvons trouver un gain approprié *K* afin de garantir la stabilité du système (1.16), alors la synchronisation entre l'émetteur et le récepteur peut être réalisée.

Cette approche peut également être regardée comme un type de synchronisation par la boucle fermée, puisque le récepteur est conduit également par l'erreur des signaux de sortie de l'émetteur et du récepteur. Il est à noter que l'observateur discuté ci-dessus est un des types d'observateurs, appelé l'observateur grand gain [Ghanes et al., 2005].

1.6.4 Synchronisation par l'inversion du système

Toutes les approches mentionnées jusqu'à présent ont pour but de synchroniser seulement les états du système, et elles ne concernent pas la synchronisation (ou plus exactement l'estimation) des entrées inconnues du système. Cependant, la possibilité d'estimer les entrées inconnues est évidemment essentielle à la transmission chaotique de données puisque l'entrée inconnue est généralement le message confidentiel. Naturellement, il existe également certains observateurs à entrée inconnue qui permettent d'accomplir l'estimation de ces dernières.

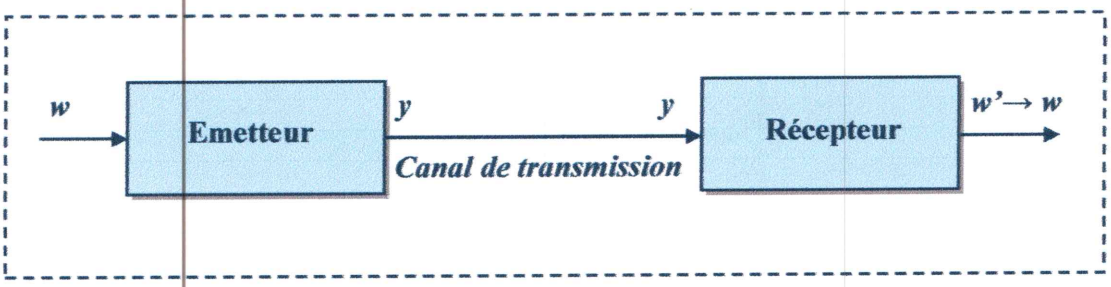


Figure 1.12 Synchronisation par l'inversion du système

Une autre méthode proposée est basée sur la solubilité du problème d'inversion à gauche afin d'achever les synchronisations des états et entrées inconnues du système. Celle-ci peut être décrite en Figure 1.12, où l'émetteur peut être écrit de la façon suivante :

$$\begin{cases} \dot{x} = f(x) + g(x)m \\ y = h(x) \end{cases} \tag{1.17}$$

Où :

$x \in \mathbb{R}^n$: Vecteur des états du système,

$m \in \mathbb{R}^m$: Vecteur des entrées inconnues,

$f : \mathbb{R}^n \to \mathbb{R}^n, g : \mathbb{R}^n \to \mathbb{R}^{n\times m}, h : \mathbb{R}^n \to \mathbb{R}^P$: Vecteurs des fonctions analytiques.

Pour le récepteur, son vecteur d'entrée est le vecteur de sortie de l'émetteur. Nous essayons de concevoir un récepteur tel que son vecteur de sortie convergera au moins asymptotiquement vers le vecteur d'entrée de l'émetteur. Ce problème s'appelle l'inversion à gauche du système. Il est à noter que l'inversion du système exige des conditions additionnelles par rapport au problème d'observabilité, telles que le degré relatif. Ensuite, pour la conception du récepteur, nous pouvons construire un observateur, dans lequel nous pouvons appliquer des stratégies adaptatives, autrement dit cette approche est aussi reliée aux autres approches.

1.6.5 Synchronisation impulsive

Dans un schéma de transmission usuel, un des états du système dynamique est transmis afin de réaliser la synchronisation par le récepteur. Dans le but de réduire la redondance du signal transmis, c.-à-d., envoyer le signal minimum possible, la synchronisation impulsive (ce concept est analogue à la synchronisation échantillonnée) a été proposée en [Heidari-Bateni and McGillem, 1994].

Dans cette approche, en raison de l'introduction d'un opérateur de Dirac, le problème de synchronisation entre l'émetteur et le récepteur devient celui de stabiliser un système impulsionnel.

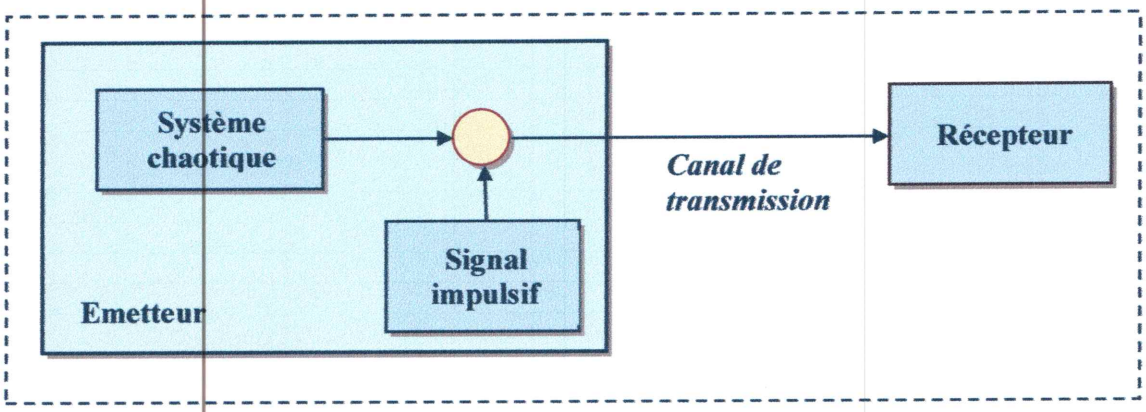


Figure 1.13 Synchronisation impulsive

A l'exception de ce type de synchronisations évoque ci-dessus, quelques autres types de synchronisations des systèmes chaotiques ont également été étudiées, telles que la synchronisation généralisée, la synchronisation de phase et bien d'autres.

1.7 Systèmes de chiffrement chaotique

La plupart des approches de synchronisation discutées précédemment peuvent être directement appliquées dans la transmission de données, ainsi ici nous rappellerons quelque schémas principaux : l'addition chaotique, la commutation chaotique, la modulation chaotique, méthode par inclusion et l'injection du retard.

1.7.1 Addition chaotique

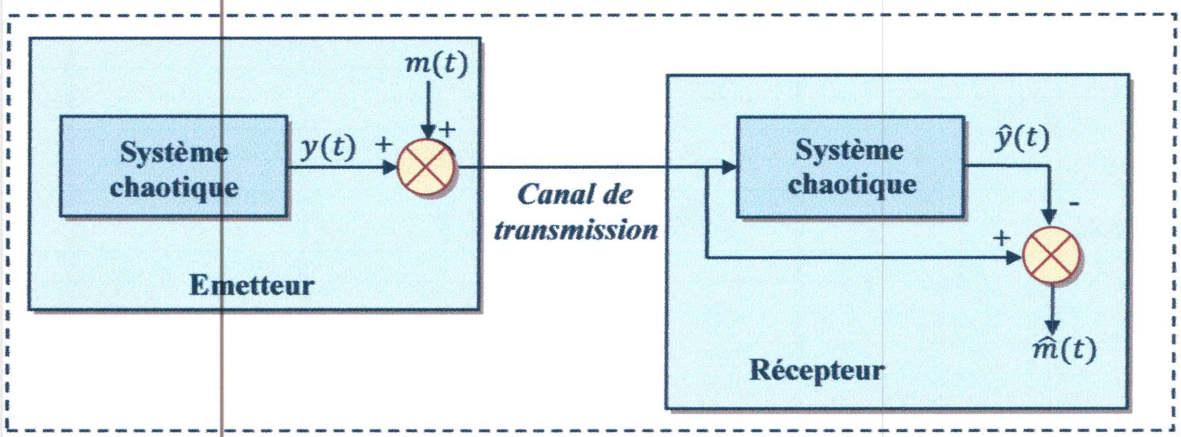


Figure 1.14 Schéma de l'addition chaotique

Le schéma par addition chaotique a été proposé pour appliquer le chaos dans la transmission de données (Figure 1.14). Avec cette méthode, le message confidentiel est additionné à un signal chaotique (la sortie d'un système chaotique), et le signal résultant est envoyé au récepteur pour la synchronisation. En conséquence, après la synchronisation, le message confidentiel peut être récupéré par une simple opération de soustraction entre la sortie du récepteur et le signal émis sur le canal public.

Il est à noter que, dans ce schéma, l'attracteur étrange du système chaotique n'est pas modifié par le message confidentiel, mais dans les deux schémas suivants, nous verrons que les attracteurs étranges modifies par des messages confidentiels.

1.7.2 Commutation chaotique

Un autre schéma de transmission chaotique de données est la commutation chaotique (CSK : Chaotique Switch Keying), qui exige que le message soit binaire, et elle s'inspire de la modulation à saut de fréquence (SFK). Le diagramme de cette approche est illustré en Figure 1.15, où une opération de commutation est employée selon la valeur du message binaire :

- Si $m(t) = 0$, le système chaotique f est choisi et sa sortie est transmise vers le récepteur ;
- Si $m(t) = 1$, le système chaotique g est choisi et sa sortie est transmise vers le récepteur.

Dans ce sens, le message binaire commute l'émetteur entre deux attracteurs étranges correspondants à deux systèmes chaotiques.

Du coté du récepteur, il y a deux sous systèmes chaotiques f_0 et g_0 qui correspondent respectivement à f et g. Supposons que le canal est parfait, alors :

- Si $m(t) = 0$, le système chaotique f_0 se synchronisera avec le système chaotique f, mais le sous système g_0 ne pourra pas être synchronisé;
- Si $m(t) = 1$, le système chaotique g_0 se synchronisera avec le système chaotique g, mais le sous système f_0 ne pourra pas être synchronisé.

Par conséquent, selon les erreurs de synchronisation, le signal peut être récupéré avec succès.

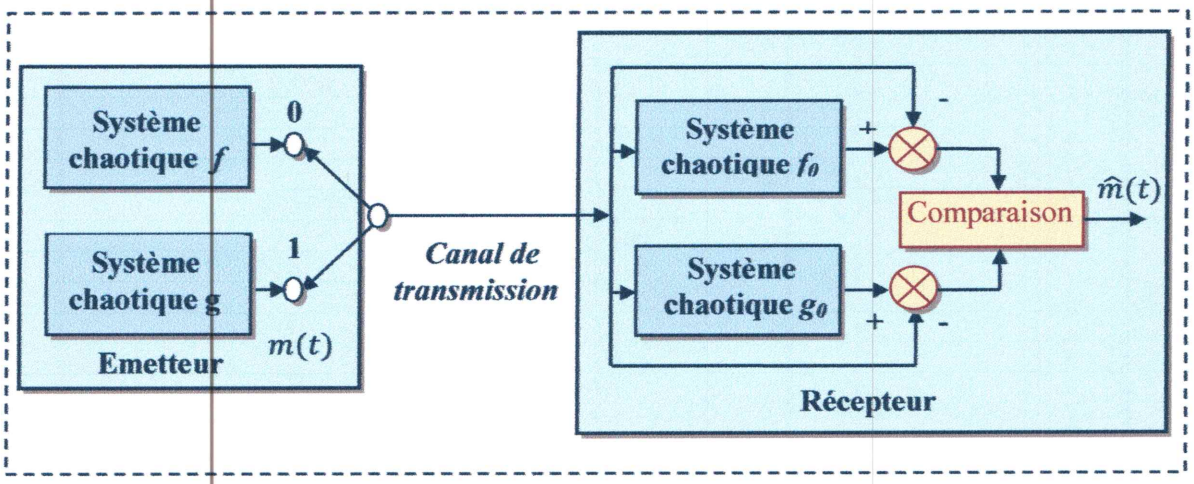


Figure 1.15 Schéma de la commutation chaotique

Il est à noter que la méthode CSK est basée sur la démodulation cohérente. Une modification de la méthode CSK pour la démodulation non cohérente a été également proposée en distinguant l'énergie de bit de deux systèmes chaotiques. Parfois, seulement un système chaotique est employé pour générer deux différentes énergies de bit, par exemple par amplificateur, ou par en retard, la méthode s'appelle alors DCSK (Differential CSK) , et FM-DCSK (Frequent Modulation DCSK).

1.7.3 Modulation chaotique

Une autre idée utilise le message pour modifier directement l'attracteur étrange du système chaotique. Ces méthodes s'appellent la modulation chaotique, et elle peut se *décomposer en deux types de méthodes : la modulation chaotique de paramètre, celle-ci* modifie le paramètre du système chaotique, et la modulation chaotique d'état, qui modifie l'état du système chaotique. Mais ces deux méthodes font bouger directement l'attracteur étrange du système (Figure 1.16).

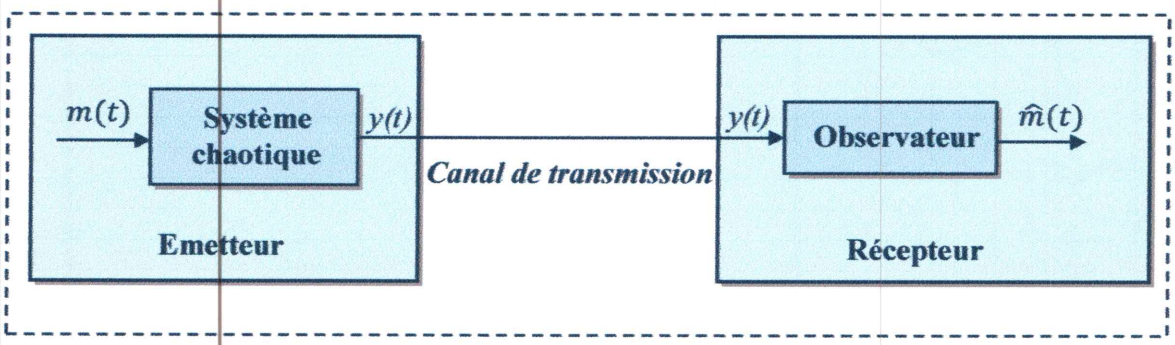


Figure 1.16 Schéma de modulation chaotique

Pour le récepteur, afin de synchroniser l'émetteur, nous pouvons employer la technique de la synchronisation par le contrôle en boucle fermé, ou la synchronisation par l'observateur, de même la synchronisation par inversion à gauche du système si l'émetteur est inversible.

1.7.4 Injection du retard

L'utilisation des systèmes chaotiques à retard dans les communications sécurisées a suscité récemment beaucoup d'attention afin d'améliorer la complexité des dynamiques, *notamment dans les communications optoélectroniques [Zheng et al., 2008]. Cependant, la* plupart des systèmes de chiffrement chaotique qui ont été proposés utilisent des systèmes chaotiques à retard à temps continu. Nous allons, dans ce mémoire de fin d'étude, étudier le système de chiffrement fondé sur l'injection du retard pour les systèmes chaotiques à temps discret. Le schéma est représenté sur la Figure 1.17.

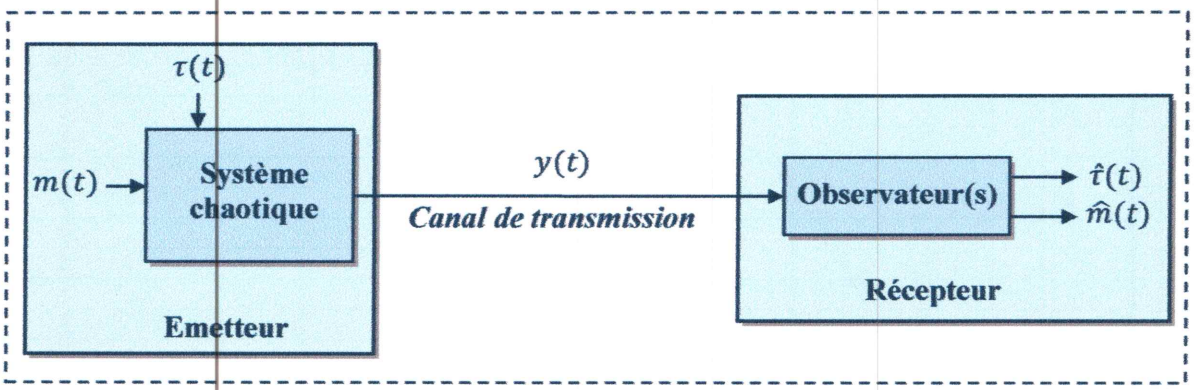


Figure 1.17 Schéma de l'injection du retard

Où $m(t)$ est le message secret et $\tau(t)$ est le retard variable ou constant. Le récepteur doit dans un premier temps délivrer un estimé $\hat{\tau}(t)$ de $\tau(t)$ pour retrouver ensuite $m(t)$:

$$\hat{m}(t) = m(t) \text{ lorsque } \hat{\tau}(t) = \tau(t) \qquad (2.18)$$

1.8. Conclusion

Au cours de ce chapitre, nous avons présenté d'abord des généralités sur des systèmes chaotiques. Le chaos est un comportement imprédictible dans un système déterministe en raison d'une grande sensibilité à des conditions initiales. La dynamique chaotique apparaît dans un système non linéaire si deux points de départs proches divergent exponentiellement. Cette propriété nous permet théoriquement de générer un nombre infini

de signaux chaotiques d'un même système en utilisant différentes valeurs initiales. Ensuite, nous avons présenté l'application du chaos pour la sécurisation des transmissions de données (cryptographie). On a commencé par la définition du principe de cryptage par le chaos pour illustrer l'importance des systèmes chaotiques dans la sécurisation des transmissions, ce principe consiste à mélanger l'information que nous voulons la transmettre avec un signal chaotique, cette information sera déchiffrée au niveau du récepteur qui lui connaît les caractéristiques du générateur du chaos. Après nous avons vu les différentes approches de synchronisation des systèmes chaotiques. Et nous avons terminé avec quelques exemples des transmissions basées sur la synchronisation du chaos.

Dans le cadre de ce travail, nous nous sommes intéressés aux systèmes de transmission sécurisés par le chaos, impliquant des systèmes chaotiques à retard à temps discret. Par conséquent, les chapitres suivants seront consacrés uniquement aux systèmes à temps discret.

Chapitre 2

Description LPV Polytopique pour les Systèmes Chaotiques

2.1 Introduction

De nombreux systèmes chaotiques à temps discret sont décrits par des équations d'état admettant pour fonction de transition et fonction de sortie des non-linéarités polynomiales. Nous rappellerons dans ce chapitre comment un système chaotique à non linéarité polynomiale, peut être réécrit comme un système Linéaire à Paramètres Variant (LPV) c'est-à-dire un modèle linéaire dont la représentation d'état dépend d'un vecteur de paramètres qui peut varier dans le temps. Ces techniques de modélisation LPV ont suscité beaucoup d'intérêt car elles fournissent une procédure systématique pour concevoir les observateurs LPV polytopiques [Bara et al., 2001].

Avant d'expliquer la réécriture d'un système chaotique sous la forme d'un modèle LPV polytopique, nous allons d'abord faire quelques rappels sur les modèles LPV.

2.2 Forme LPV

Un système LPV peut être donné par la forme suivante :

$$\begin{cases} x_{k+1} = A(\rho_k)x_k + Bu_k \\ y_k = C\,x_k \end{cases} \tag{2.1}$$

où $x_k \in \mathbb{R}^n$ est le vecteur d'état, $u_k \in \mathbb{R}^m$ est l'entrée, $y_k \in \mathbb{R}^p$ est le vecteur de sortie, $A \in \mathbb{R}^{n\times n}$ est la matrice dynamique qui dépend linéairement du vecteur de paramètres variant dans le temps $\rho_k = \Psi(x_k) = [\rho_k^{(1)}, \rho_k^{(2)}, \cdots, \rho_k^{(L_\rho)}] \in \mathbb{R}^{L_\rho}$, $B \in \mathbb{R}^{n\times m}$ est la matrice d'entrée et $C \in \mathbb{R}^{p\times n}$ est la matrice de sortie.

Dans le cas ou le système (2.1) est chaotique, l'état interne x_k évolue dans un ensemble borné Ω. Nous supposons que ρ_k est borné quand x_k l'est. Par conséquent, ρ_k

appartient également à un ensemble borné $\Omega_\rho \subset \mathbb{R}^{L_\rho}$ et donc peut être intégré dans un polytope D_ρ dont les sommets sont $\rho_{o_1}, \cdots, \rho_{o_N} \in \mathbb{R}^{L_\rho}$, de telle sorte que :

$$\rho_k = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k)\ \rho_{o_i} \tag{2.2}$$

où N est le nombre de sommets du polytope D_ρ et ξ_k appartient à l'ensemble compact Φ définie comme suit :

$$\Phi = \left\{ \xi_k \in \mathbb{R}^N, \xi_k = \left[\xi_k^{(1)}, \cdots, \xi_k^{(N)}\right], \xi_k^{(i)} \geq 0 \ \forall\, k \ et \sum_{i=1}^{N} \xi_k^{(i)} = 1 \right\} \tag{2.3}$$

La dépendance de $A(\rho_k)$ par rapport à ρ_k peut prendre plusieurs formes, en particulier, polytopique. La décomposition polytopique de la matrice $A(\rho_k)$ est donnée par :

$$A(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) A^{(i)}, \qquad \xi_k \in \Phi \tag{2.4}$$

Où :

$$A^{(i)} = A\left(\rho_{o_i}\right) \tag{2.5}$$

En raison de la convexité de Φ, l'ensemble des matrices $\left\{A^{(1)}, \cdots, A^{(N)}\right\}$ définit un polytope noté D_A et les matrices $A^{(i)}$ correspondent aux sommets de D_A.

Ci-après, la notation $\xi_k^{(i)}$ sera utilisée à la place de $\xi_k^{(i)}(\rho_k)$ pour des raisons de simplicité et chaque fois que possible, la dépendance des paramètres $\xi_k^{(i)}$ de ρ_k sera omis.

2.3 Recherche du polytope minimal

Pour des raisons de conservatisme, on s'intéresse à l'obtention d'un polytope minimal. Etant donné que nous pouvons obtenir, par simulation ou expérimentalement, un nombre suffisant de vecteurs ρ_k, collectés dans un ensemble fini Γ_ρ, pour décrire l'ensemble Ω_ρ avec une précision adéquate, le polytope minimal D_ρ^* dans lequel Ω_ρ est intégré peut ainsi être considéré comme l'enveloppe convexe de l'ensemble des points Γ_ρ. Nous rappelons qu'un élément d'un ensemble fini de points est un point extrême, s'il n'est pas une combinaison

convexe des autres points de cet ensemble. Par conséquent, trouver D_ρ^* revient à trouver les points extrêmes de Γ_ρ.

Plusieurs méthodes permettant de calculer ce polytope ont été proposées [Graham, 1973]. Cependant, dans le cadre de ce travail, on s'intéresse uniquement à l'algorithme "*Quick hull*" qui est fondé sur l'approche "diviser pour régner" [Eddy, 1977]. Un tel algorithme utilise la propriété que, étant donné un triangle formé par trois points de l'ensemble d'origine, les points strictement à l'intérieur de ce triangle n'appartiennent pas à l'enveloppe convexe. Par conséquent, ils peuvent être ignorés. Ce principe est illustré sur la Figure 2.1.

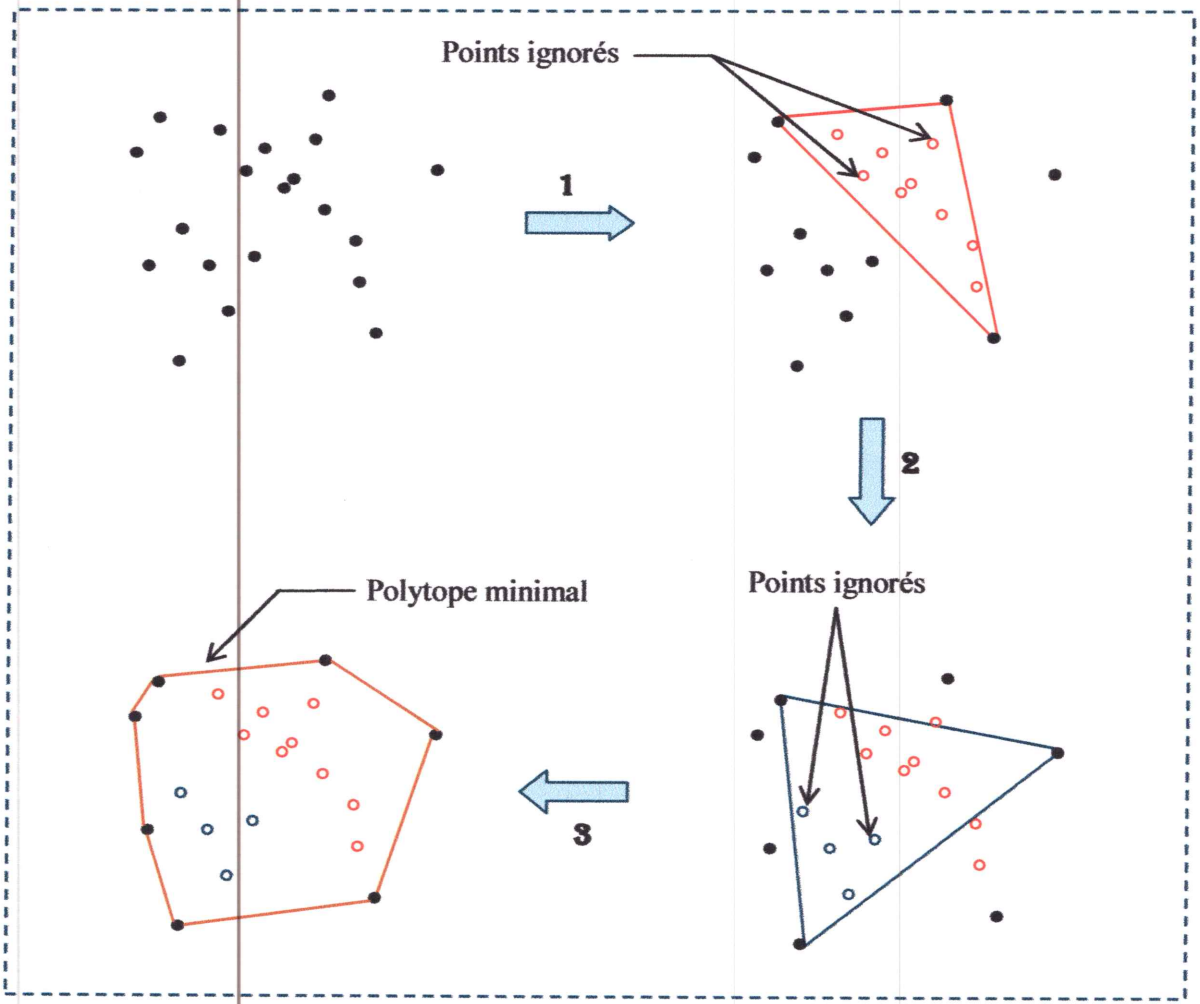


Figure 2.1 Principe de fonctionnement de l'algorithme "*Quick hull*"

L'algorithme Quick hull est celui qui est incorporé dans la fonction *convhull* du logiciel MATLAB.

Grace à l'algorithme "Quick hull", on peut trouver les sommets ρ_{o_i} du polytope minimal D_ρ^*. On rappelle que le paramètre variant ρ_k peut s'écrire sous forme LPV polytopique donnée par (2.2). Ce paramètre ρ_k étant fonction de l'état x_k, il est accessible à chaque instant. Connaissant ρ_k et $\rho_{o_i}, i = 1, \cdots, N$, il faut déterminer le vecteur ξ_k à chaque instant, ce qui fait l'objet de la section suivante.

2.4 Décomposition polytopique

Le problème revient à chercher le vecteur $\xi_k = \left[\xi_k^{(1)}, \cdots, \xi_k^{(N)}\right]^T$ tel que, à chaque instant :

$$W_k = Z \times \xi_k \qquad (2.6)$$
$$\xi_k^{(i)} \geq 0, \qquad i = 1, \cdots, N$$

Où

$$W_k = \left[\rho_k^{(1)}, \cdots, \rho_k^{(L_\rho)}, 1\right]$$

et

$$Z = \begin{bmatrix} \rho_{o_1}^{(1)} & \cdots & \rho_{o_N}^{(1)} \\ \vdots & \cdots & \vdots \\ \rho_{o_1}^{(L_\rho)} & \cdots & \rho_{o_N}^{(L_\rho)} \\ 1 & \cdots & 1 \end{bmatrix}$$

Etant donné que les éléments ρ_{o_i} (sommets du polytope D_ρ) sont donnés, la matrice Z de dimension $(L_\rho + 1) \times N$ est de ce fait constante et connue. En effet, il est supposé que ρ_k est accessible, hypothèse usuelle dans le cadre des systèmes LPV et retenue ici.

2.5 Réécriture sous la forme LPV d'un système chaotique

Les systèmes chaotiques à temps discret à non-linéarité polynomiale peuvent être modélisés par des systèmes LPV sous certaines conditions [Bruzelius, 2004]. Considérons le système chaotique à temps discret :

$$x_{k+1} = g(x_k, u_k) \qquad (2.7)$$

où $x_k \in \mathbb{R}^n$ est le vecteur d'état et $u_k \in \mathbb{R}^m$ est l'entrée.

L'objectif est de réécrire le système (2.7) sous la forme d'un système LPV donné par la (2.1).

Théorème 1 [Bruzelius, 2004] Le système (2.7) admet une description LPV exacte sous la forme de (2.1) si les conditions suivantes sont respectées :

- Il existe une fonction $\rho: \mathbb{R}^n \rightarrow \mathbb{R}^{L_\rho}$ de telle sorte que $A(\rho(x_k))x_k + B\,u_k = g(x_k, u_k)$;
- $\rho_k = \rho(x_k)$ ne dépend que de signaux mesurés ;
- $\rho_k = \rho(x_k)$ est borné lorsque x_k est borné.

2.6 Exemples illustratifs

Dans cette section, deux exemples sont considérés. Le premier exemple illustre la méthode qui permet d'obtenir une description polytopique LPV d'un système chaotique à non linéarité polynomiale, le choix d'une fonction appropriée ρ_k ainsi que la méthode de recherche du polytope minimal D_ρ^*. L'exemple 2 est consacré à un cas particulier où le polytope minimal D_ρ^* contient uniquement deux sommets.

2.6.1 Exemple 1

Considérons la récurrence chaotique, avec le vecteur d'état $(x_k^{(1)}, x_k^{(2)}, x_k^{(3)}, x_k^{(4)})$, donnée par :

$$\begin{cases} x_{k+1}^{(1)} = \left(x_k^{(1)}\right)^2 - \left(x_k^{(2)}\right)^2 + a x_k^{(1)} + b x_k^{(2)} \\ x_{k+1}^{(2)} = 2x_k^{(1)} x_k^{(2)} + c x_k^{(1)} + d x_k^{(2)} \\ x_{k+1}^{(3)} = 0.1 b x_k^{(2)} - 0.1\left(x_k^{(2)}\right)^2 + 0.1 x_k^{(3)} \\ x_{k+1}^{(4)} = 0.5 x_k^{(1)} - 0.1 x_k^{(2)} + 0.3 x_k^{(4)} \\ y_k^{(1)} = x_k^{(1)} \\ y_k^{(2)} = x_k^{(2)} \end{cases} \tag{2.8}$$

avec $a = 0.9$, $b = -0.6013$, $c = 2$ et $d = 0.5$.

Pour ces valeurs typiques de paramètres, le système (2.8) présente un comportement chaotique. Une projection de l'attracteur chaotique correspondant dans

l'espace de dimension 3 $(x_k^{(1)}, x_k^{(2)}, x_k^{(4)})$ est illustrée sur la Figure 2.2. L'évolution de la première coordonnée $x_k^{(1)}$ du système est représentée sur la Figure 2.3.

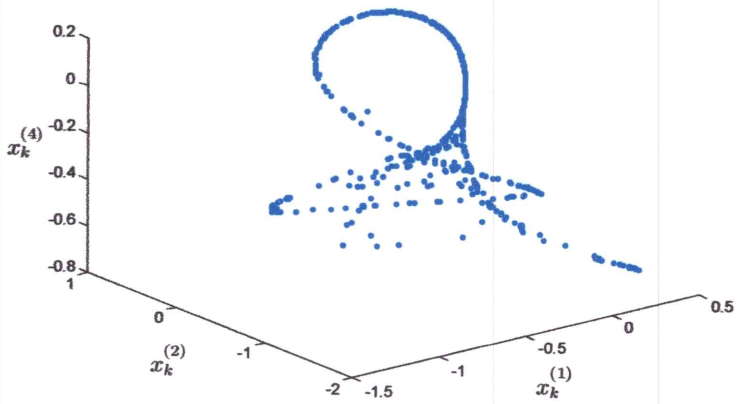


Figure 2.2 Attracteur chaotique Ω dans l'espace de dimension 3 $(x_k^{(1)}, x_k^{(2)}, x_k^{(4)})$

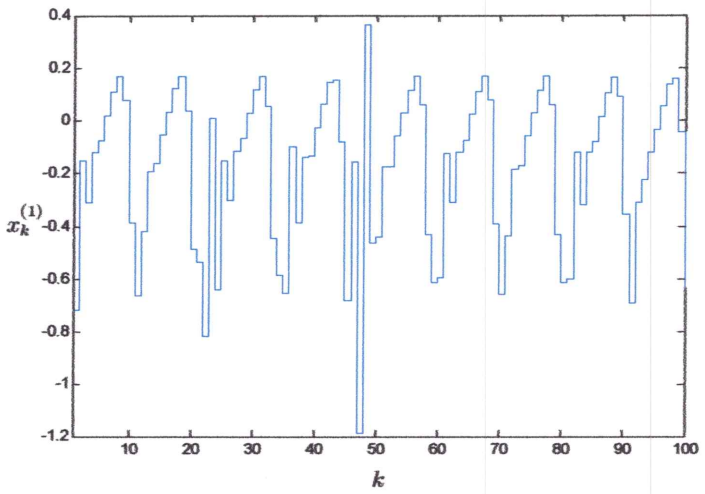


Figure 2.3 Evolution de la première cordonnée $x_k^{(1)}$

Notre objectif est de réécrire (2.8) sous la forme LPV (2.1) polytopique (2.4) et de construire le polytope D_ρ^*. A cette fin, nous choisissons ρ_k comme le vecteur de paramètres obéissant à :

$$\begin{aligned} \rho_k^{(1)} &= a + x_k^{(1)} \\ \rho_k^{(2)} &= b - x_k^{(2)} \end{aligned} \tag{2.9}$$

On remarque que ρ_k dépend que de signaux mesurés puisque $\rho_k^{(1)} = a + y_k^{(1)}$ et $\rho_k^{(2)} = b - y_k^{(2)}$. De plus, ρ_k reste borné tant que x_k l'est aussi.

Par conséquent, le système (2.8) peut être réécrit sous la forme LPV (2.1) polytopique (2.4) avec :

$$A(\rho_k) = \begin{bmatrix} \rho_k^{(1)} & \rho_k^{(2)} & 0 & 0 \\ c & d + 2(\rho_k^{(1)} - a) & 0 & 0 \\ 0 & 0.1\rho_k^{(2)} & 0.1 & 0 \\ 0.5 & 0.1 & 0 & 0.3 \end{bmatrix}$$

Et

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

La matrice B est nulle puisque le système (2.8) est autonome.

Après la simulation du système (2.8) à partir de la condition initiale $x_0 = [-0.72 \; -0.64 \; 0.1 \; 0]^T$ qui appartient a l'attracteur chaotique, nous recueillons 1000 vecteurs ρ_k qui constituent l'ensemble des données Γ_ρ. Ensuite, l'approche «Quick hull», correspondant à la fonction «*convhull*» du logiciel MATLAB, est utilisée pour trouver le polytope minimal D_ρ^* qui englobe les données de Γ_ρ. Il s'avère que 45 sommets ρ_{o_i} ont été trouvés ($N = 45$). L'ensemble Ω_ρ et le polytope minimal D_ρ^* sont représentés sur la Figure 2.4.

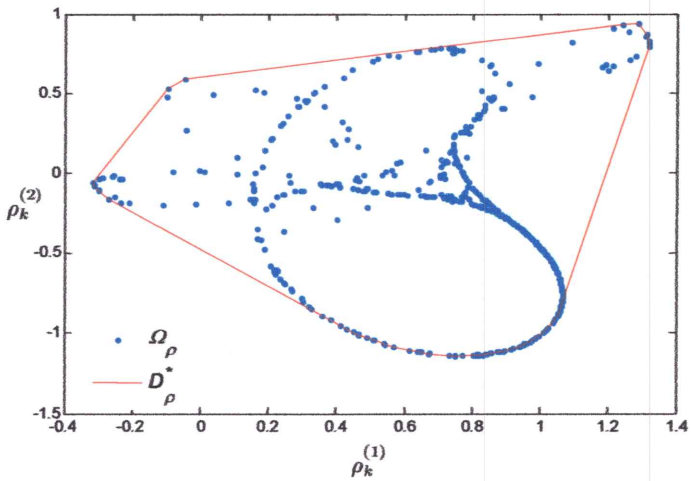


Figure 2.4 Ensemble Ω_ρ et polytope minimal D_ρ^*

2.6.2 Exemple 2

Considérons la récurrence chaotique, avec vecteur d'état $(x_k^{(1)}, x_k^{(2)})$, donnée par :

$$\begin{cases} x_{k+1}^{(1)} = -1.4\left(x_k^{(1)}\right)^2 + x_k^{(2)} + 1 + 0.1m_k \\ x_{k+1}^{(2)} = 0.3x_k^{(1)} \\ y_k = 0.4x_k^{(1)} \end{cases} \tag{2.10}$$

où m_k est l'entrée inconnue qui joue le rôle de l'information à crypter.

On doit tout d'abord réécrire le système (2.10) sous une forme polynomiale. Pour cela, on procède à une augmentation du vecteur d'état. Ainsi, on définit une nouvelle variable $x_k^{(3)} = 1$. *Le système (2.10) peut être réécrit sous la forme :*

$$\begin{cases} x_{k+1}^{(1)} = -1.4\left(x_k^{(1)}\right)^2 + x_k^{(2)} + x_k^{(3)} + 0.1m_k \\ x_{k+1}^{(2)} = 0.3x_k^{(1)} \\ x_{k+1}^{(3)} = x_k^{(3)} \\ y_k = 0.4x_k^{(1)} \end{cases} \tag{2.11}$$

Ensuite, nous choisissons ρ_k comme :

$$\rho_k = -1.4\, x_k^{(1)} \tag{2.12}$$

On remarque que ρ_k dépend que d'un signal mesuré puisque $\rho_k = -3.5\, y_k$. De plus, ρ_k reste borné tant $x_k^{(1)}$ l'est aussi.

Par conséquent, le système (2.11) peut être réécrit comme un système LPV de la forme (2.1) polytopique (2.4) avec :

$$A(\rho_k) = \begin{bmatrix} \rho_k & 1 & 1 \\ 0.3 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad C = [0.4 \quad 0 \quad 0], \quad B = \begin{bmatrix} 0.1 \\ 0 \\ 0 \end{bmatrix}$$

Le vecteur ρ_k appartient à l'intervalle $[min(\rho_k)\ max(\rho_k)]$. Par conséquent, le polytope minimal D_ρ^* contient deux (02) sommets ρ_{o_1} et ρ_{o_2} $(N = 2)$ qui correspondent respectivement à $min(-1.4\, x_k^{(1)})$ et $max(-1.4\, x_k^{(1)})$.

Les matrices correspondantes $A^{(1)}$ et $A^{(2)}$ sont calculées à partir de (2.5) :

$$A^{(1)} = A(\rho_{o_1}) = \begin{bmatrix} \rho_{o_1} & 1 & 1 \\ 0.3 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

et

$$A^{(2)} = A(\rho_{o_2}) = \begin{bmatrix} \rho_{o_2} & 1 & 1 \\ 0.3 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

2.7 Conclusion

Dans ce chapitre, nous avons rappelé comment un système chaotique à non linéarité polynomiale pouvait être réécrit sous une forme LPV polytopique. Nous avons vu que le choix du vecteur de paramètres ρ_k n'est pas arbitraire. En effet, ρ_k doit dépendre que de signaux mesurés (sorties du système) et doit être borné afin de pouvoir l'incorporé dans un polytope minimal D_ρ^*.

Cette modélisation LPV des systèmes chaotiques nous donne une procédure systématique pour concevoir les observateurs LPV polytopiques et les observateurs LPV polytopiques à entrée inconnue que nous allons voir dans les chapitres suivants.

Chapitre 3

Application des Observateurs Polytopiques à l'Estimation des Retards Variables

3.1 Introduction

Au cours des deux dernières décennies, il y a eu un intérêt croissant pour les systèmes chaotiques à retard dans les communications sécurisées. En effet, les retards augmentent la dimension du système, ce qui est intéressant pour améliorer la complexité des dynamiques.

Dans ce contexte, on s'intéresse à l'étude du système de communication chaotique à retard illustré sur la Figure 3.1.

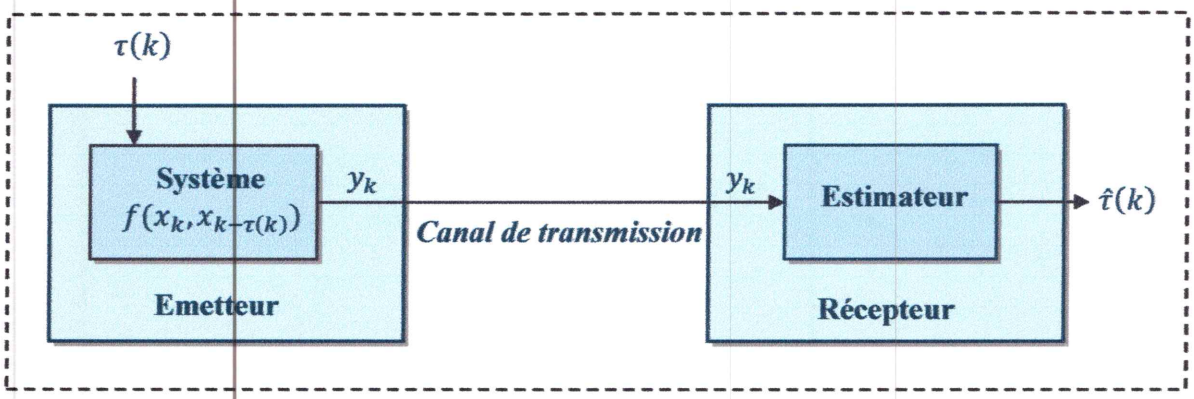


Figure 3.1 Schéma de la transmission par injection du retard

où $\tau(k)$ est l'information à crypter, injectée comme retard dans le vecteur d'état du système chaotique. Cette quantité prend des valeurs dans un ensemble fini supposé connu (cas d'un *signal binaire par exemple*). *On note que l'injection du retard modifie l'attracteur chaotique* de l'émetteur (voir l'exemple de la section 3.7)

Le but est de reconstruire l'information cryptée au niveau du récepteur, qui n'est rien d'autre que le retard variable. Nous proposerons dans ce chapitre une méthode fondée sur l'utilisation des observateurs polytopiques (au niveau du bloc estimateur de la Figure 3.1), permettant d'estimer ce retard variable. Le point central de cette méthode est le passage par une formulation hybride qui sera expliquée dans ce qui suit. Cependant, nous allons tout

d'abord s'intéresser à l'écriture LPV polytopique des systèmes chaotiques à retard. Cette écriture est nécessaire pour l'utilisation des observateurs polytopiques.

3.2 Ecriture LPV polytopique des systèmes à retard autonome

L'émetteur de la transmission sécurisée de la Figure 3.1 est un système chaotique qui possède la forme suivante :

$$x_{k+1} = f(x_k, x_{k-\tau(k)}) \tag{3.1}$$

La quantité $\tau(k)$ est le retard variable dans le vecteur d'état du système chaotique, qui prend des valeurs dans un ensemble fini supposé connu : $\tau(k) \in \{0,1,\cdots,\alpha\}$.

A partir du Théorème 1 vu dans le chapitre 2, on introduit la proposition suivante.

Proposition 1 *Si les conditions suivantes sont vérifiées :*

- Il existe une fonction $\rho : \mathbb{R}^n \to \mathbb{R}^{L_\rho}$ de telle sorte que $A(\rho(x_k))x_k + G(\rho(x_k))x_{k-\tau(k)} = f(x_k, x_{k-\tau(k)})$;
- $\rho_k = \rho(x_k)$ ne dépend que de signaux mesurés ;
- $\rho_k = \rho(x_k)$ est borné lorsque x_k est borné.

alors le système (3.1) peut être réécrit sous la forme LPV polytopique suivante :

$$\begin{cases} x_{k+1} = A(\rho_k)x_k + G(\rho_k)x_{k-\tau(k)} \\ y_k = C\,x_k \end{cases} \tag{3.2}$$

où $k \in \mathbb{N}$ représente le temps discret, $x_k \in \mathbb{R}^n$ est le vecteur d'état, $y_k \in \mathbb{R}^p$ est la sortie, les matrices $A(\rho_k) \in \mathbb{R}^{n\times n}$, $G(\rho_k) \in \mathbb{R}^{n\times n}$ et $C \in \mathbb{R}^{p\times n}$ sont respectivement les matrices dynamiques et la matrice de sortie. La quantité $\rho_k = [\rho_k^{(1)}, \rho_k^{(2)}, \cdots, \rho_k^{(L_\rho)}] \in \mathbb{R}^{L_\rho}$ est le vecteur de paramètres variant dans le temps donné par (2.2) :

$$\rho_k = \sum_{i=1}^{N} \xi_k^{(i)}\, \rho_{o_i} \tag{3.3}$$

On propose maintenant de réécrire (3.2) sous une forme hybride.

3.3 Formulation hybride

Afin d'éliminer le retard, on procède à une augmentation du vecteur d'état du système (3.2). Définissons :

$$X_k = \begin{bmatrix} x_k \\ x_{k-1} \\ \vdots \\ x_{k-\alpha} \end{bmatrix} \quad \text{et} \quad Y_k = y_k$$

Le système (3.2) peut être réécrit comme :

$$\begin{cases} X_{k+1} = \mathcal{A}_{\tau(k)}(\rho_k) X_k \\ Y_k = \mathcal{C}\, X_k \end{cases} \tag{3.4}$$

où $X_k \in \mathbb{R}^M$ avec $M = (\alpha + 1)n$, $Y_k \in \mathbb{R}^p$, $\mathcal{A}_{\tau(k)} \in \mathbb{R}^{M \times M}$ et $\mathcal{C} \in \mathbb{R}^{p \times M}$.

Les matrices d'état de (3.4) obéissent à la construction suivante :

$$\mathcal{A}_{\tau(k)}(\rho_k) = \begin{bmatrix} A(\rho_k) + \kappa(\tau(k))G(\rho_k) & \psi_1(\tau(k)) & \cdots & \psi_\alpha(\tau(k)) \\ I_n & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & I_n & \cdots & \mathbf{0} \\ \vdots & \vdots & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & & \mathbf{0} \end{bmatrix} \tag{3.5}$$

$$\mathcal{C} = [C \quad \mathbf{0} \quad \cdots \quad \mathbf{0}]$$

Où κ est défini comme :

$$\kappa(\tau(k)) = \begin{cases} 1 & si\ \tau(k) = 0 \\ 0 & si\ \tau(k) \neq 0 \end{cases}$$

ψ_i est défini pour $i = 1, \cdots, \alpha$ comme :

$$\psi_i(\tau(k)) = \begin{cases} G(\rho_k) & si\ \tau(k) = i \\ \mathbf{0} & si\ \tau(k) \neq i \end{cases}$$

A partir de l'équation (2.4) et (2.5), la dépendance polytopique de $\mathcal{A}_{\tau(k)}(\rho_k)$ par rapport à ρ_k est donnée par :

$$\mathcal{A}_{\tau(k)}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)} A_{\tau(k)}^{(i)} \tag{3.6}$$

Où :

$$A_{\tau(k)}^{(l)} = \mathcal{A}_{\tau(k)}(\rho_{o_l}) \tag{3.7}$$

Pour clarifier cette construction, considérons par exemple le système (3.2) avec $\tau(k) \in \{0,1,2\}$. Ce système peut être réécrit sous la forme (3.4) avec :

$$X_k = \begin{bmatrix} x_k \\ x_{k-1} \\ x_{k-2} \end{bmatrix} \text{ et } Y_k = y_k$$

$$\mathcal{A}_0(\rho_k) = \begin{bmatrix} A(\rho_k) + G(\rho_k) & \mathbf{0} & \mathbf{0} \\ I_n & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I_n & \mathbf{0} \end{bmatrix} \qquad \mathcal{A}_1(\rho_k) = \begin{bmatrix} A(\rho_k) & G(\rho_k) & \mathbf{0} \\ I_n & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I_n & \mathbf{0} \end{bmatrix},$$

$$\mathcal{A}_2(\rho_k) = \begin{bmatrix} A(\rho_k) & \mathbf{0} & G(\rho_k) \\ I_n & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I_n & \mathbf{0} \end{bmatrix}$$

et

$$\mathcal{C} = [C \quad \mathbf{0} \quad \mathbf{0}]$$

Ainsi, le système chaotique à retard (3.2) avec $\tau(k) \in \{0, \cdots, \alpha\}$, et donc l'émetteur (3.1), est équivalent au système hybride (3.4) qui commute entre $(\alpha + 1)$ sous systèmes S_l $(l \in \{0, \cdots, \alpha\})$ *en fonction de la valeur actuelle du retard* $\tau(k)$.

Dans ce contexte, on propose d'utiliser $(\alpha + 1)$ observateurs O_l $(l \in \{0, \cdots, \alpha\})$ au niveau du récepteur, tel que chaque observateur O_l correspond à un sous système S_l de (3.4). Puisque le retard $\tau(k)$ ne peut prendre qu'une seule valeur à la fois, seul l'observateur $O_{\tau(k)}$ (qui correspond au sous système $S_{\tau(k)}$) peut être synchronisé avec l'émetteur. Cela implique que la valeur du retard, et donc l'information cryptée, peut être récupérée en calculant l'erreur de synchronisation de chaque observateur.

Etant donné que le système (3.4) est donné sous une forme LPV polytopique, nous allons utiliser des observateurs polytopiques. La structure de ces observateurs est donnée ci-dessous.

3.4 Observateurs LPV polytopiques

L'observateur polytopique O_l correspondant au sous système S_l de (3.4) obéit à la description suivante :

$$\begin{cases} \hat{X}_{k+1}^{(l)} = \mathcal{A}_l(\rho_k)\hat{X}_k^{(l)} + \mathcal{L}_l(\rho_k)\left(y_k - \hat{Y}_k^{(l)}\right) \\ \hat{Y}_k^{(l)} = \mathcal{C}\,\hat{X}_k^{(l)} \end{cases} \tag{3.8}$$

où $\hat{X}_k^{(l)} \in \mathbb{R}^M$ est le vecteur d'état de l'observateur, $\hat{Y}_k^{(l)} \in \mathbb{R}^p$ est la sortie de l'observateur et $\mathcal{L}_l(\rho_k)$ est une matrice de gain à temps variant fonction de ρ_k qui vérifie :

$$\mathcal{L}_l(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)} L_l{}^{(i)} \tag{3.9}$$

Les grandeurs $\xi_k^{(i)}$ dans (3.9) coïncident, pour chaque instant discret k, avec ceux qui sont impliqués dans la décomposition polytopique (3.6) de $\mathcal{A}_{\tau(k)}(\rho_k)$.

A partir de (3.4) et (3.8), l'erreur de reconstruction de l'observateur O_l est donnée par :

$$e_k^{(l)} = X_k - \hat{X}_k^{(l)} \tag{3.10}$$

Dans le cas où $\tau(k) = l$, cela signifie que l'observateur O_l correspond au sous système actif S_l et l'erreur (3.10) est gouvernée par la dynamique :

$$e_{k+1}^{(l)} = (\mathcal{A}_l(\rho_k) - \mathcal{L}_l(\rho_k)\,\mathcal{C})e_k^{(l)} \tag{3.11}$$

La dynamique de l'erreur de reconstruction d'état est non linéaire puisque $\mathcal{A}_{\tau(k)}$ et $\mathcal{L}_{\tau(k)}$ dépendent de ρ_k. Toutefois, (3.11) peut être considérée comme un système LPV polytopique autonome avec le vecteur d'état $e_k^{(l)} \in \mathbb{R}^M$. En effet, à partir de (3.6) et (3.9), sachant que $\tau(k) = l$ et en tenant compte de la coïncidence entre les $\xi_k^{(i)}$ impliqués dans ces équations, nous obtenons :

$$e_{k+1}^{(l)} = \sum_{i=1}^{N} \xi_k^{(i)} \left(A_l^{(i)} - L_l^{(i)}\,\mathcal{C}\right)e_k^{(l)} \tag{3.12}$$

La stabilité asymptotique globale (GAS) de (3.11) autour du point d'équilibre zéro peut être assurée par un choix approprié des gains $L_l^{(i)}$ $(i = 1, \cdots, N)$ impliqués dans (3.9). Ceci fait l'objet du théorème suivant.

Théorème 2 [Daafouz et al., 2002] S'il existe des matrices symétriques $P_l^{(l)}$, des matrices $G_i^{(l)}$ et des matrices $F_i^{(l)}$ vérifiant, $\forall(i,j) \in \{1, \cdots, N\} \times \{1, \cdots, N\}$, les LMIs :

$$\begin{bmatrix} P_i^{(l)} & (\blacksquare)^T \\ G_i^{(l)} A_l^{(i)} - F_i^{(l)} \mathcal{C} & G_i^{(l)^T} + G_i^{(l)} - P_j^{(l)} \end{bmatrix} > 0 \tag{3.13}$$

alors l'observateur polytopique (3.8) avec le gain $\mathcal{L}_l(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)} L_l{}^{(i)}$ et $L_l^{(i)} = G_i^{(l)^{-1}} F_i^{(l)}$ garantit que le système (3.12) soit globalement asymptotiquement stable.

La preuve détaillée de ce théorème est donnée dans [Daafouz et al., 2002]. Il est démontré que les LMIs (3.13) assure l'existence d'une fonction de Lyapunov V_l: $\mathbb{R}^M \times \mathbb{R}^{L_\rho} \rightarrow \mathbb{R}_+$ définie par $V_l\left(e_k^{(l)}, \rho_k\right) = e_k^{(l)^T} \mathcal{P}_l(\rho_k) e_k^{(l)}$ avec $\mathcal{P}_l(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)} P_i^{(l)}$, appelée fonction de Lyapunov poly-quadratique, vérifiant pour tout $e_k^{(l)} \in \mathbb{R}^M$:

$$V_l\left(e_{k+1}^{(l)}, \rho_{k+1}\right) - V_l\left(e_k^{(l)}, \rho_k\right) < 0 \tag{3.14}$$

Cette fonction assure la stabilité poly-quadratique de (3.12) qui est suffisante pour la stabilité asymptotique globale.

3.5 Reconstruction du retard

D'après l'étude effectuée ci-dessus, on propose un schéma détaillé de la transmission de la Figure 3.1. Ce dernier est illustré sur la Figure 3.2

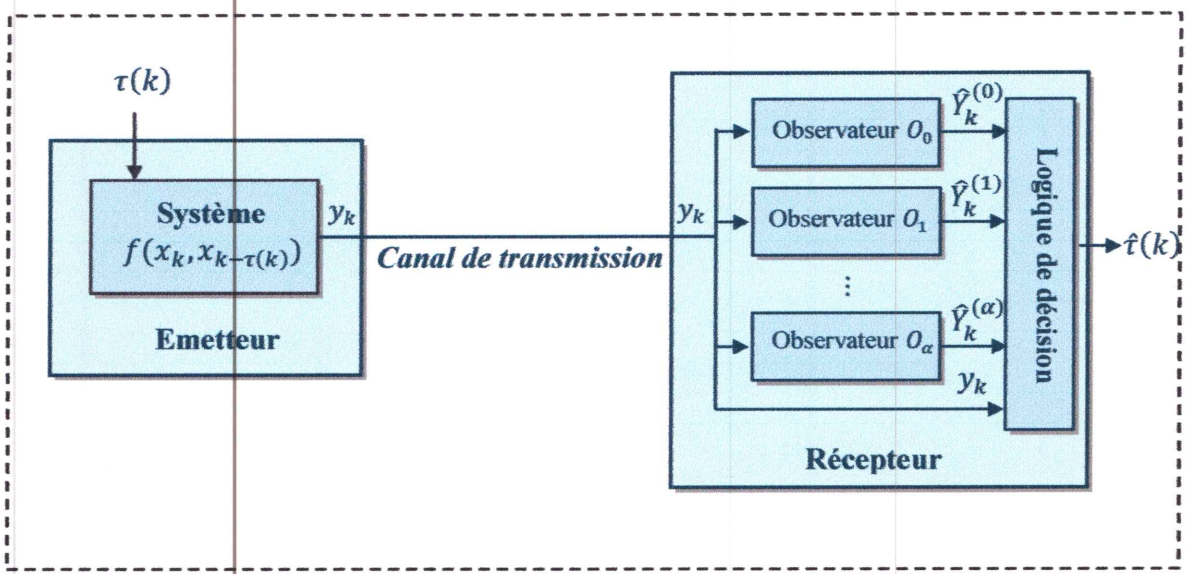


Figure 3.2 Schéma détaillé de la transmission par injection du retard

La valeur du retard est estimée en calculant l'erreur de synchronisation entre la sortie $\hat{Y}_k^{(l)}$ de chaque observateur O_l avec $l \in \{0, \cdots, \alpha\}$ et la sortie de l'émetteur y_k (le bloc *logique de décision* de la figure précédente). En effet :

$$\hat{\tau}(k) = \begin{cases} 0 & si \quad y_k - \hat{Y}_k^{(0)} = 0 \\ 1 & si \quad y_k - \hat{Y}_k^{(1)} = 0 \\ & \vdots \\ \alpha & si \quad y_k - \hat{Y}_k^{(\alpha)} = 0 \end{cases} \tag{3.15}$$

3.6 Procédure globale de la reconstruction du retard

Cette section a pour objectif de donner, en récapitulant les résultats précédents, une description détaillée de la procédure globale nécessaire pour l'estimation du retard variable pour le système (3.1).

Etape 1 - Forme LPV polytopique

Réécrire le système (3.1) sous la forme (3.2).

Etape 2 - Polytope minimal D_ρ^*

Recherche du polytope minimal D_ρ^* qui englobe Ω_ρ avec l'approche *Quick hull*, incorporée dans la fonction *convhull* du logiciel MATLAB.

Etape 3 - Formulation hybride

Réécrire le système (3.2) sous la forme (3.4).

Etape 4 - Détermination des matrices sommets $A_l^{(i)}$

Pour chaque valeur du retard $\tau(k) = l \in \{0, \cdots, \alpha\}$, calculer les matrices sommets $A_l^{(i)}$ qui correspond aux sommets du polytope minimal D_ρ^* à l'aide de l'équation (3.7).

Etape 5 - Calcul des gains $L_l{}^{(i)}$

Pour chaque valeur du retard $\tau(k) = l \in \{0, \cdots, \alpha\}$, calculer les gains $L_l{}^{(i)}$ de l'observateur O_l en résolvant les LMIs (3.13) sachant que les matrices $A_l^{(i)}$ ont été déjà calculées précédemment.

Etape 6 - Calcul du vecteur ξ_k

Calculer le vecteur ξ_k à chaque instant à l'aide de l'équation (2.6).

Etape 7 - Calcul du gain $\mathcal{L}_l(\rho_k)$

Pour chaque valeur du retard $\tau(k) = l \in \{0, \cdots, \alpha\}$, calculer le gain $\mathcal{L}_l(\rho_k)$ de l'observateur O_l avec l'équation (3.9) sachant que les vecteurs ξ_k et $L_l{}^{(i)}$ ont été calculés précédemment.

Etape 8 - Calcul des vecteurs $\hat{X}_k^{(l)}$ et $\hat{Y}_k^{(l)}$

Pour chaque valeur du retard $\tau(k) = l \in \{0, \cdots, \alpha\}$, calculer le vecteur $\hat{X}_k^{(l)}$ et $\hat{Y}_k^{(l)}$ avec l'équation (3.8).

Etape 9 - Reconstruction du retard $\hat{\tau}(k)$

Calculer la valeur estimée du retard $\hat{\tau}(k)$ à l'aide de l'équation (3.15).

3.7 Exemple illustratif

Considérons le système de transmission chaotique de la Figure 3.2 où l'émetteur est la récurrence chaotique, avec le vecteur d'état $(x_k^{(1)}, x_k^{(2)}, x_k^{(3)}, x_k^{(4)})$, donnée par :

$$\begin{cases} x_{k+1}^{(1)} = \left(x_k^{(1)} + 0.9\right)x_k^{(1)} - \left(x_k^{(2)} + 0.6013\right)x_k^{(2)} - 0.1x_k^{(3)} - 0.05x_{k-\tau(k)}^{(1)} \\ x_{k+1}^{(2)} = \left(2 + 2x_k^{(2)}\right)x_k^{(1)} + 0.5x_k^{(2)} - 0.3x_k^{(4)} - 0.1x_{k-\tau(k)}^{(2)} \\ x_{k+1}^{(3)} = \left(0.09 - 0.1x_k^{(2)}\right)x_k^{(2)} + 0.1x_k^{(3)} \\ x_{k+1}^{(4)} = 0.5x_k^{(1)} - 0.1x_k^{(2)} + 0.3x_k^{(4)} \\ y_k^{(1)} = 4x_k^{(1)} \\ y_k^{(2)} = 3x_k^{(2)} \end{cases} \tag{3.16}$$

L'information $\tau(k)$ est injectée comme retard dans le vecteur d'état et prend deux valeurs 0 ou 1 ($\tau(k) \in \{0,1\}$). La variation de $\tau(k)$ est donnée sur la Figure 3.3.

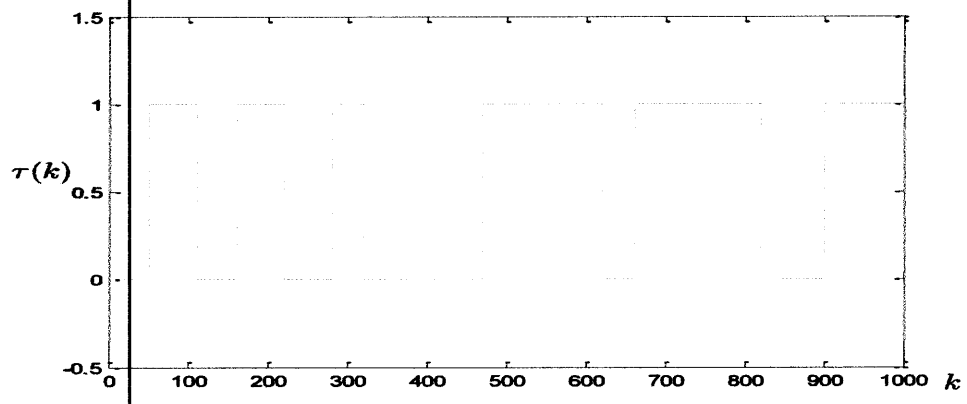


Figure 3.3 Variation du retard $\tau(k)$

L'injection du retard dans un système chaotique modifie son attracteur. Afin d'illustrer cette propriété, on fait la simulation du système (3.16) à partir de la condition initiale $x_0 = [-0.72 \quad -0.64 \quad 0.1 \quad 0]^T$ avec et son retard. La projection de l'attracteur chaotique correspondant Ω dans l'espace de dimension 3 $(x_k^{(1)}, x_k^{(2)}, x_k^{(4)})$ ainsi que l'évolution de la première cordonnée $x_k^{(1)}$ sont données sur la Figure 3.4 et la Figure 3.5 respectivement.

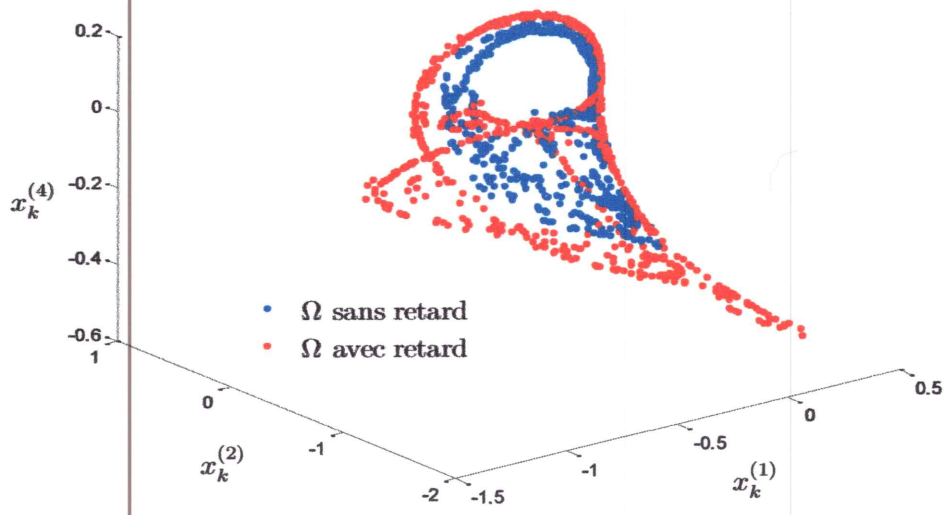


Figure 3.4 Attracteur chaotique Ω

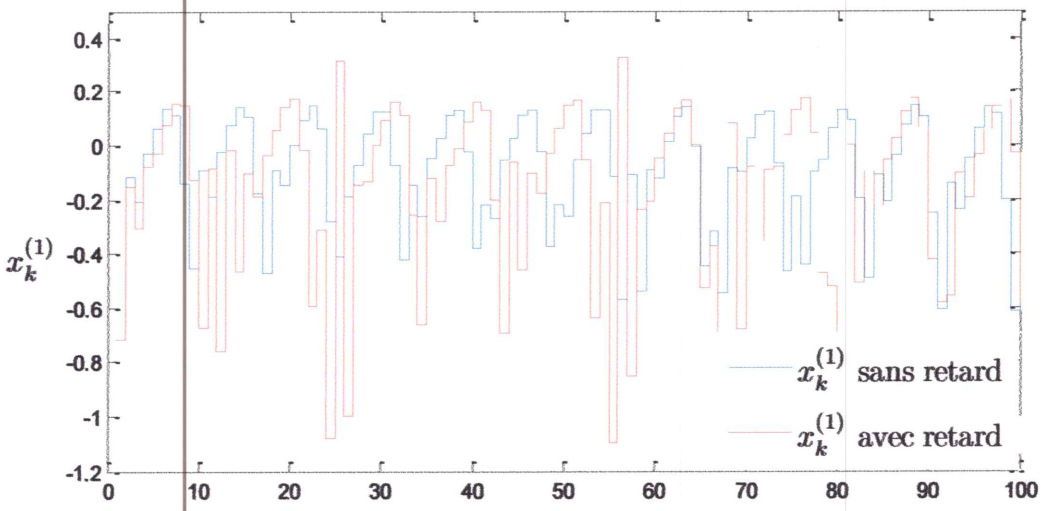


Figure 3.5 Evolution de la première cordonnée $x_k^{(1)}$

D'après les deux figures on remarque que l'injection du retard a modifié le comportement du système chaotique ainsi que son attracteur Ω.

Maintenant, afin de reconstruire l'information $\tau(k)$, nous allons suivre les étapes de la Section 3.6.

Etape 1 - Forme LPV polytopique

Afin de réécrire le système (3.16) sous la forme (3.2), on définie le vecteur ρ_k comme :

$$\begin{cases} \rho_k^{(1)} = x_k^{(1)} = \dfrac{y_k^{(1)}}{4} \\ \rho_k^{(2)} = x_k^{(2)} = \dfrac{y_k^{(2)}}{3} \end{cases}$$

Par conséquent, le système (3.16) peut être réécrit sous la forme (3.2) avec :

$$A(\rho_k) = \begin{bmatrix} \rho_k^{(1)} + 0.9 & -\rho_k^{(2)} - 0.6013 & -0.1 & 0 \\ 2 + 2\rho_k^{(2)} & 0.5 & 0 & -0.3 \\ 0 & 0.09 - 0.1\rho_k^{(2)} & 0.1 & 0 \\ 0.5 & -0.5 & 0 & 0.3 \end{bmatrix} \quad (3.17)$$

$$G(\rho_k) = \begin{bmatrix} -0.05 & 0 & 0 & 0 \\ 0 & -0.1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{bmatrix}$$

Etape 2 - Polytope minimal D_ρ^*

Le polytope minimal D_ρ^* qui englobe Ω_ρ est calculé avec la fonction MATLAB *convhull*.

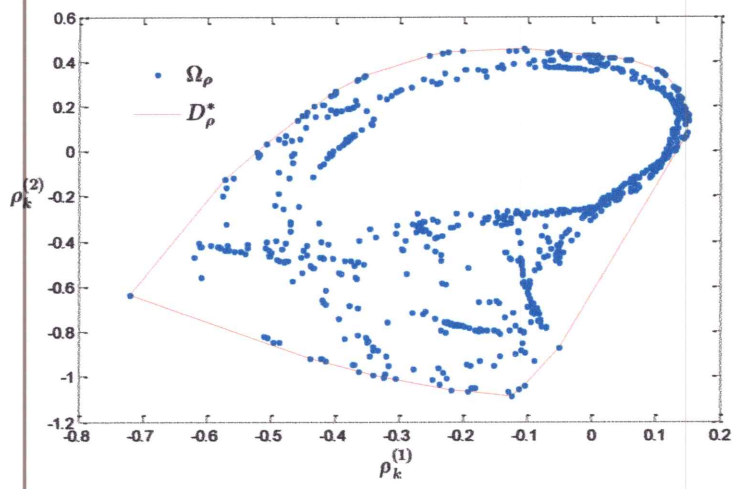


Figure 3.6 Ensemble Ω_ρ et polytope minimal D_ρ^*

Il s'avère que 33 sommets ρ_{o_i} ont été trouvés ($N = 33$). L'ensemble Ω_ρ et le polytope minimal D_ρ^* sont représentés sur la Figure 3.6.

Etape 3 - Formulation hybride

Le système (3.17) peut être réécrit sous la forme (3.4) avec les matrices :

$$\mathcal{A}_0(\rho_k) = \begin{bmatrix} A(\rho_k) + G(\rho_k) & \mathbf{0} \\ I_4 & \mathbf{0} \end{bmatrix}, \quad \mathcal{A}_1(\rho_k) = \begin{bmatrix} A(\rho_k) & G(\rho_k) \\ I_4 & \mathbf{0} \end{bmatrix}, \quad \mathcal{C} = [C \quad \mathbf{0}]$$

et

$$X_k = \begin{bmatrix} x_k \\ x_{k-1} \end{bmatrix}, Y_k = y_k$$

Etape 4 - Détermination des matrices sommets $A_l^{(i)}$

Pour chaque valeur du retard $\tau(k) = l \in \{0,1\}$, on calcule les matrices sommets $A_l^{(i)}$ avec (3.7). On trouve :

$$A_0^{(i)} = \mathcal{A}_0(\rho_{o_i}) = \begin{bmatrix} A(\rho_{o_i}) + G(\rho_{o_i}) & \mathbf{0} \\ I_4 & \mathbf{0} \end{bmatrix}, \quad A_1^{(i)} = \mathcal{A}_1(\rho_{o_i}) = \begin{bmatrix} A(\rho_{o_i}) & G(\rho_{o_i}) \\ I_4 & \mathbf{0} \end{bmatrix}$$

Etape 5 - Calcul des gains $L_l{}^{(i)}$

Pour chaque valeur du retard $\tau(k) = l \in \{0,1\}$, on calcule les gains $L_l{}^{(i)}$ de l'observateur O_l en résolvant les LMIs (3.13). On trouve que ces LMIs sont faisables pour les deux observateurs O_0 et O_1.

Etape 6 - Calcul du vecteur ξ_k

On Calcule le vecteur ξ_k à chaque instant à l'aide de l'équation (2.6).

Etape 7 - Calcul du gain $\mathcal{L}_l(\rho_k)$

Pour chaque valeur du retard $\tau(k) = l \in \{0,1\}$, on calcule le gain $\mathcal{L}_l(\rho_k)$ de l'observateur O_l avec l'équation (3.9).

Etape 8 - Calcul des vecteurs $\hat{X}_k^{(l)}$ et $\hat{Y}_k^{(l)}$

On calcule les vecteurs d'état et de sortie $\hat{X}_k^{(0)}$, $\hat{Y}_k^{(0)}$ et $\hat{X}_k^{(1)}$ et $\hat{Y}_k^{(1)}$ avec l'équation (3.8), qui correspondent respectivement aux observateurs O_0 et O_1. Les résultats de synchronisation entre ces observateurs et l'émetteur (3.16) sont illustrés sur le Figures 3.7, 3.8, 3.9 et 3.10.

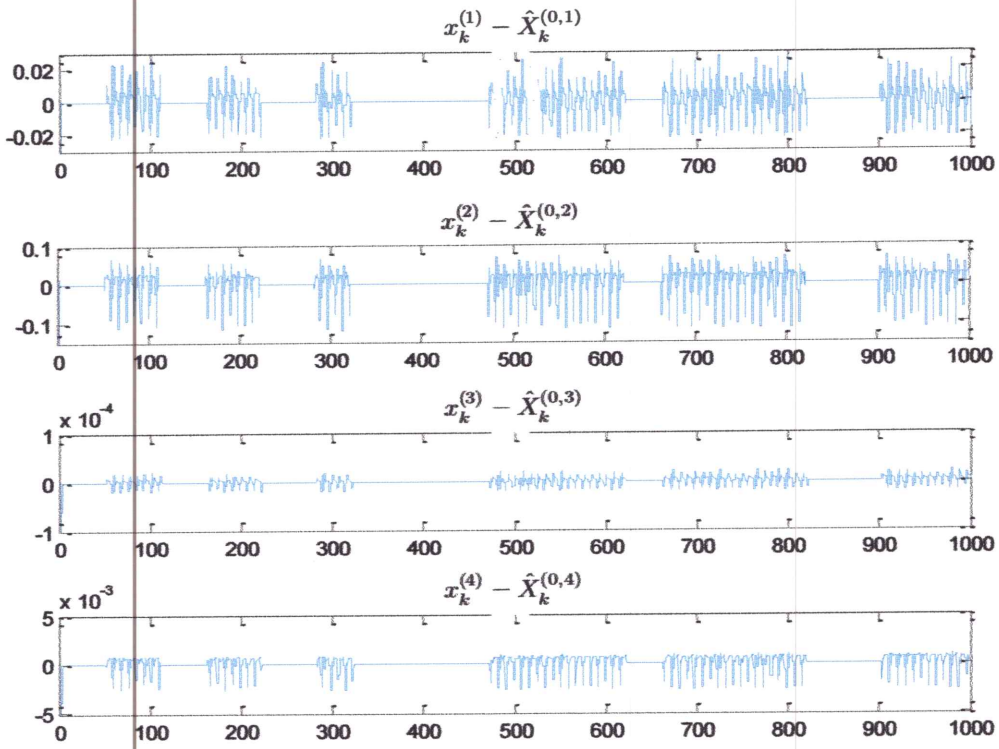


Figure 3.7 Erreur de synchronisation du vecteur d'état de O_0 $x_k - \hat{X}_k^{(0)}$

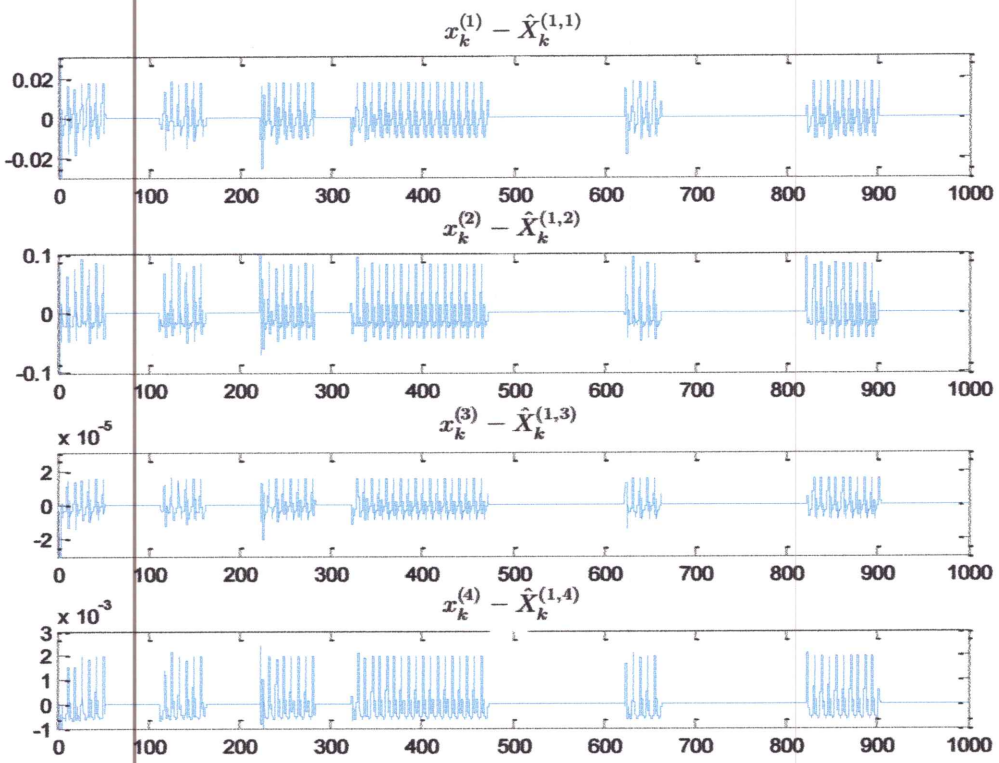


Figure 3.8 Erreur de synchronisation du vecteur d'état de O_1 $x_k - \hat{X}_k^{(1)}$

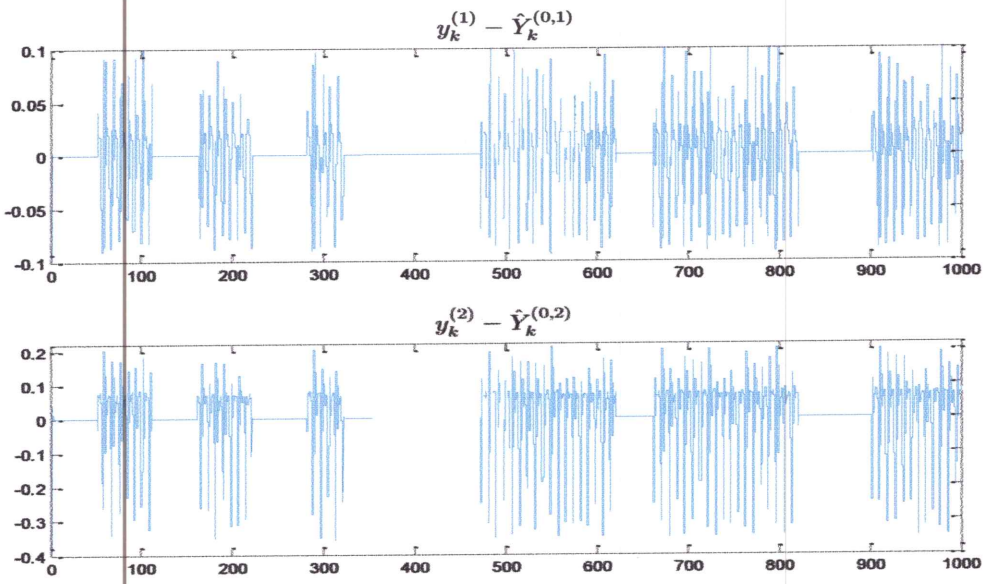


Figure 3.9 Erreur de synchronisation de la sortie de O_0 $y_k - \hat{Y}_k^{(0)}$

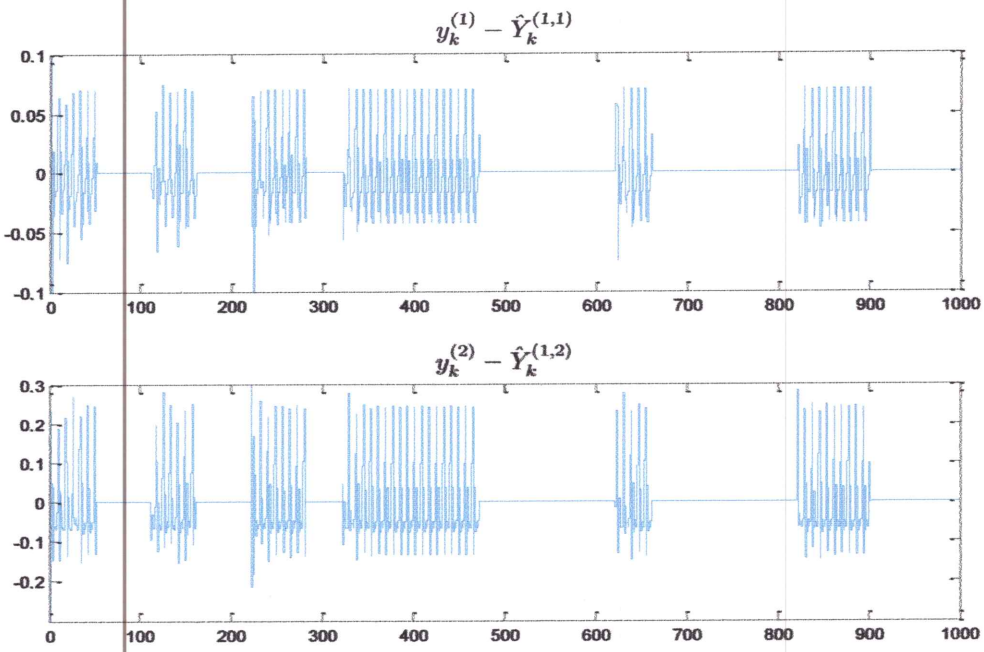


Figure 3.10 Erreur de synchronisation de la sortie de O_1 $y_k - \hat{Y}_k^{(1)}$

Les résultats de simulation montrent bien qu'un seul observateur à la fois peut se synchroniser avec l'émetteur. En effet, on remarque bien que lorsque le vecteur d'état du premier observateur O_0 est synchronisé avec le vecteur d'état de l'émetteur ($x_k - \hat{X}_k^{(0)} = 0$),

celui du deuxième observateur O_1 ne l'est pas ($x_k - \hat{X}_k^{(1)} \neq 0$), et vice versa. De la même façon, lorsque la sortie du premier observateur O_0 est synchronisée avec la sortie de l'émetteur ($y_k - \hat{Y}_k^{(0)} = 0$), celle du deuxième observateur O_1 ne l'est pas ($y_k - \hat{Y}_k^{(1)} \neq 0$), et vice versa.

On note que, dans des petits intervalles de temps, les erreurs de synchronisation entre les observateurs et l'émetteur sont toutes différentes de zéro ($x_k - \hat{X}_k^{(0)} \neq 0$ et $x_k - \hat{X}_k^{(1)} \neq 0$). Ce résultat est logique puisque la convergence des observateurs est asymptotique, ce qui signifie que chaque observateur passe par un état transitoire avant d'être synchronisé avec l'émetteur. Cela signifie que cette méthode de reconstruction exige que la variation du retard $\tau(k)$ soit suffisamment lente pour pouvoir estimer ce retard.

Etape 9 - Reconstruction du retard $\hat{\tau}(k)$

A l'aide de l'équation (3.15) on calcule la valeur estimée de l'information $\hat{\tau}(k)$:

$$\hat{\tau}(k) = \begin{cases} 0 & si \quad y_k - \hat{Y}_k^{(0)} = 0 \\ 1 & si \quad y_k - \hat{Y}_k^{(1)} = 0 \end{cases}$$

Le résultat est montré sur la Figure 3.11.

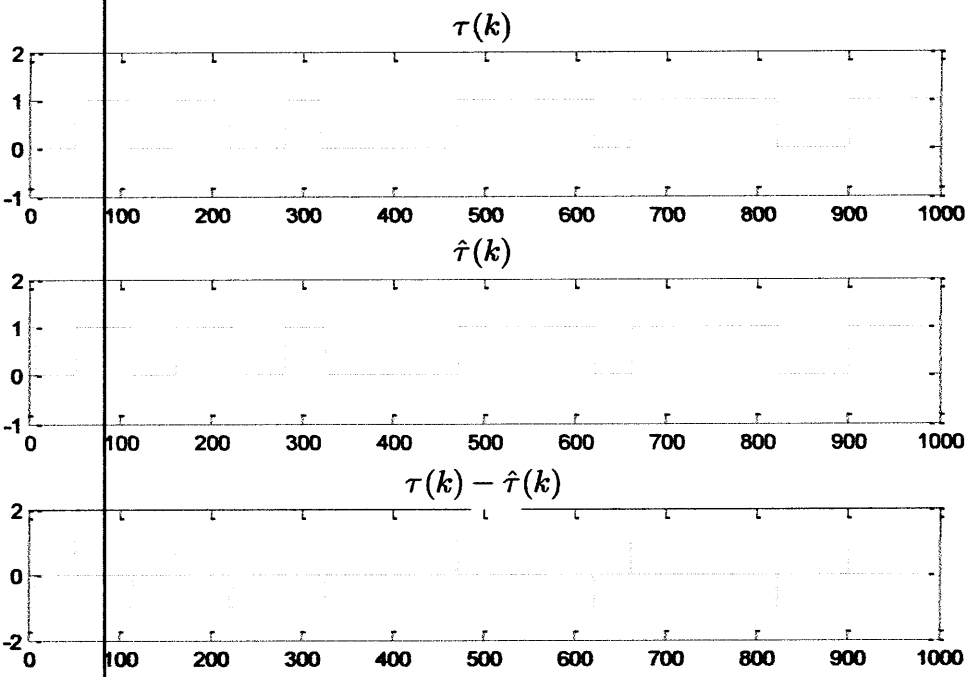


Figure 3.11 Information $\tau(k)$ et information reconstruite $\hat{\tau}(k)$

On remarque que l'erreur de reconstruction converge rapidement vers zéro au début de la reconstruction et à chaque fois que l'information change de valeur. Cela est dû à l'état transitoire de la convergence des observateurs comme on l'a expliqué précédemment.

D'après la figures précédentes, on remarque que retard reconstruit suit le signal du retard injecté au niveau de l'émetteur (information secrète). Les résultats de simulation montrent l'efficacité de cette méthode pour l'estimation de l'information $\tau(k)$.

3.8 Conclusion

Dans ce chapitre, nous avons étudié un système de transmission chaotique où l'information à transmettre est injectée comme retard dans le vecteur d'état de l'émetteur. Nous avons montré que la reconstruction de cette information au niveau de récepteur peut être assurée en faisait appel à des observateurs polytopiques. Ainsi, nous avons rappelé le principe de la synthèse des observateurs LPV polytopiques reposant sur l'utilisation des LMIs et garantissant la stabilité, en particulier polyquadratique. Après une étude détaillée du problème, nous avons développé une procédure globale permettant de reconstruire l'information cryptée au niveau du récepteur. Pour vérifier l'efficacité de la méthode de reconstruction, nous avons terminé par un exemple illustratif. Les résultats de simulation obtenus montrent l'efficacité de cette méthode pour la reconstruction des retards ayant une variation suffisamment lente.

Chapitre 4

Application des UIO Polytopiques aux Transmissions Sécurisées à Retard

4.1 Introduction

Le système de communication auquel on s'intéresse dans ce chapitre est illustré dans la Figure 4.1.

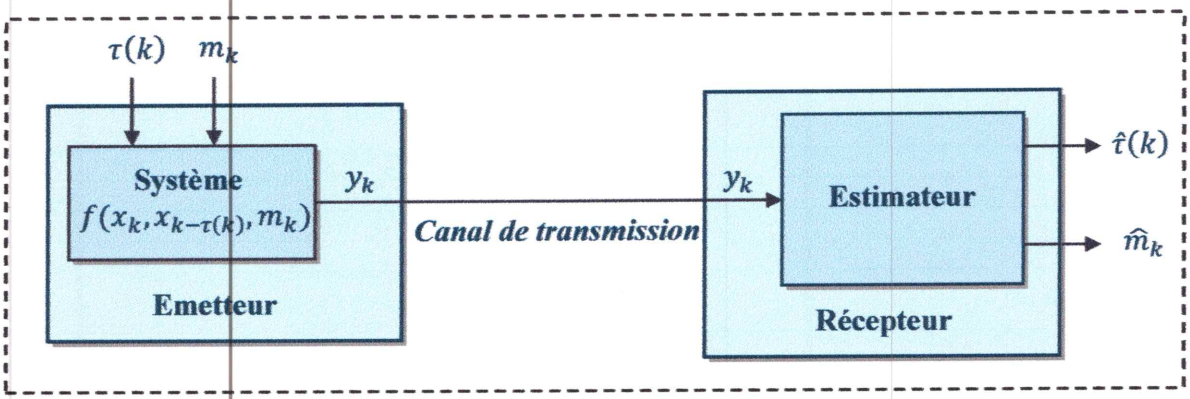


Figure 4.1 Schéma de la transmission chaotique à retard

où $\tau(k)$ est le retard injecté dans le vecteur d'état du système chaotique afin d'augmenter la sécurité de la transmission. Cette quantité prend des valeurs dans un ensemble fini supposé connu. Le signal m_k est l'information secrète qu'on cherche à crypter au niveau de l'émetteur.

Le but est de reconstruire l'information cryptée m_k au niveau du récepteur. Cependant, cette reconstruction nécessite la connaissance du retard $\tau(k)$. Nous proposerons dans ce chapitre une méthode fondée sur l'utilisation des observateurs polytopiques à entrée inconnue (au niveau du bloc estimateur de la Figure 4.1), permettant d'estimer à la fois le retard inconnu et l'information cryptée.

Le point central de cette méthode est le passage par la formulation hybride expliquée dans le chapitre précédent, qui sera étendue aux cas des systèmes chaotiques non autonomes.

4.2 Ecriture LPV polytopique des systèmes à retard non autonome

L'émetteur de la transmission sécurisée de la Figure 4.1 est un système chaotique qui possède la forme suivante :

$$x_{k+1} = f(x_k, x_{k-\tau(k)}, m_k) \tag{4.1}$$

La quantité $\tau(k)$ est le retard variable dans le vecteur d'état du système chaotique, qui prend des valeurs dans un ensemble fini supposé connu : $\tau(k) \in \{0,1,\cdots,\alpha\}$ et $m_k \in \mathbb{R}^m$ est une entrée.

A partir du Théorème 1 vu dans le chapitre 2, on introduit la proposition suivante.

Proposition 2 Si les conditions suivantes sont vérifiées :

- Il existe une fonction $\rho : \mathbb{R}^n \to \mathbb{R}^{L_\rho}$ de telle sorte que $A(\rho(x_k))x_k + G(\rho(x_k))x_{k-\tau(k)} + B\, m_k = f(x_k, x_{k-\tau(k)}, m_k)$;
- $\rho_k = \rho(x_k)$ ne dépend que de signaux mesurés ;
- $\rho_k = \rho(x_k)$ est borné lorsque x_k est borné.

alors le système (4.1) peut être réécrit sous la forme LPV polytopique suivante :

$$\begin{cases} x_{k+1} = A(\rho_k)x_k + G(\rho_k)x_{k-\tau(k)} + Bm_k \\ y_k = C\, x_k \end{cases} \tag{4.2}$$

où $k \in \mathbb{N}$ représente le temps discret, $x_k \in \mathbb{R}^n$ est le vecteur d'état, $y_k \in \mathbb{R}^p$ est la sortie, $m_k \in \mathbb{R}^m$ est l'entrée, les matrices $A(\rho_k) \in \mathbb{R}^{n\times n}$, $G(\rho_k) \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$ et $C \in \mathbb{R}^{p\times n}$ sont respectivement les matrices dynamiques et la matrice de sortie. La quantité $\rho_k = [\rho_k^{(1)}, \rho_k^{(2)}, \cdots, \rho_k^{(L_\rho)}] \in \mathbb{R}^{L_\rho}$ est le vecteur de paramètres variant dans le temps donné par (2.2) et (3.3). On propose maintenant de réécrire (4.2) sous forme une forme hybride.

4.3 Formulation hybride

Le système (4.2) peut être réécrit comme :

$$\begin{cases} X_{k+1} = \mathcal{A}_{\tau(k)}(\rho_k)X_k + \mathcal{B}\, M_k \\ Y_k = \mathcal{C}\, X_k \end{cases} \tag{4.3}$$

où $X_k \in \mathbb{R}^M$ avec $M = (\alpha + 1)n$, $Y_k \in \mathbb{R}^p$, $M_k \in \mathbb{R}^m$, $\mathcal{A}_{\tau(k)} \in \mathbb{R}^{M \times M}$, $\mathcal{B} \in \mathbb{R}^{M \times m}$ et $\mathcal{C} \in \mathbb{R}^{p \times M}$. Avec :

$$X_k = \begin{bmatrix} x_k \\ x_{k-1} \\ \vdots \\ x_{k-\alpha} \end{bmatrix}, M_k = m_k \ et \ Y_k = y_k$$

Les matrices d'état de (4.3) $\mathcal{A}_{\tau(k)}(\rho_k)$ et $\mathcal{C}$ obéissent à la construction donnée par (3.5) et la matrice $\mathcal{B}$ est donnée par :

$$\mathcal{B} = \begin{bmatrix} B \\ \mathbf{0} \end{bmatrix}$$

A partir de l'équation (2.4) et (2.5), la dépendance polytopique de $\mathcal{A}_{\tau(k)}(\rho_k)$ par rapport à ρ_k est donnée par :

$$\mathcal{A}_{\tau(k)}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)} A_{\tau(k)}^{(i)} \tag{4.4}$$

Où :

$$A_{\tau(k)}^{(i)} = \mathcal{A}_{\tau(k)}(\rho_{o_i}) \tag{4.5}$$

Ainsi, le système chaotique à retard (4.2) avec $\tau(k) \in \{0, \cdots, \alpha\}$, et donc l'émetteur (4.1), est équivalent au système hybride (4.3) qui commute entre $(\alpha + 1)$ sous systèmes S_l $(l \in \{0, \cdots, \alpha\})$ en fonction de la valeur actuelle du retard $\tau(k)$.

Dans ce contexte, étant donnée que l'entrée m_k est l'information secrète, non accessible côté récepteur, on propose d'utiliser $(\alpha + 1)$ observateurs à entrée inconnue O_l $(l \in \{0, \cdots, \alpha\})$ au niveau du récepteur, tel que chaque observateur O_l correspond à un sous système S_l de (4.3). Puisque le retard $\tau(k)$ ne peut prendre qu'une seule valeur à la fois, seul l'observateur à entrée inconnue $O_{\tau(k)}$ (qui correspond au sous système $S_{\tau(k)}$) peut être synchronisé avec l'émetteur. Cela implique que la valeur du retard, peut être récupérée en calculant l'erreur de synchronisation de chaque observateur. Une fois le retard estimé, on pourra procéder à la reconstruction de l'information cryptée.

Etant donné que le système (4.3) est donné sous une forme LPV polytopique, nous allons utiliser des observateurs polytopiques à entrée inconnue. La structure de ces observateurs est donnée ci-dessous.

4.4 Observateurs LPV polytopiques à entrée inconnue

L'observateur polytopique à entrée inconnue O_l correspondant au sous système S_l de (4.3) obéit à la description suivante :

$$\begin{cases} \hat{X}_{k+1}^{(l)} = (\mathcal{Z}\mathcal{A}_l(\rho_k) - \mathcal{L}_l(\rho_k)\mathcal{C})\hat{X}_k^{(l)} + \mathcal{L}_l(\rho_k)y_k + Qy_{k+1} \\ \hat{Y}_{k\ k}^{(l)} = \mathcal{C}\,\hat{X}_k^{(l)} \end{cases} \tag{4.6}$$

où $\hat{X}_k^{(l)} \in \mathbb{R}^M$ est le vecteur d'état de l'observateur, $\hat{Y}_k^{(l)} \in \mathbb{R}^p$ est la sortie de l'observateur et $\mathcal{L}_l(\rho_k)$ est une matrice de gain à temps variant fonction de ρ_k donnée par (3.9).

$$\mathcal{Z} = I_n - Q\mathcal{C} \tag{4.7}$$

et

$$Q = \mathcal{B}(\mathcal{C}\mathcal{B})^+ + Y(I_m - (\mathcal{C}\mathcal{B})(\mathcal{C}\mathcal{B})^+) \tag{4.8}$$

où Y une matrice arbitraire.

A partir de (4.3) et (4.6), l'erreur de reconstruction de l'observateur O_l est donnée par :

$$e_k^{(l)} = X_k - \hat{X}_k^{(l)} \tag{4.9}$$

Dans le cas où $\tau(k) = l$, cela signifie que l'observateur O_l correspond au sous système actif S_l et l'erreur (4.9) est gouvernée par la dynamique :

$$e_{k+1}^{(l)} = (\mathcal{Z}\mathcal{A}_l(\rho_k) - \mathcal{L}_l(\rho_k)\mathcal{C})e_k + \mathcal{Z}\mathcal{B}m_k \tag{4.10}$$

La dynamique de l'erreur de reconstruction d'état est non linéaire puisque $\mathcal{A}_{\tau(k)}$ et $\mathcal{L}_{\tau(k)}$ dépendent de ρ_k. A partir de (4.4) et (3.9), sachant que $\tau(k) = l$, et en tenant compte de la coïncidence entre les $\xi_k^{(i)}$ impliqués dans ces équations, nous obtenons :

$$e_{k+1}^{(l)} = \sum_{i=1}^{N} \xi_k^{(i)} \left(\mathcal{Z}A_l^{(i)} - L_l^{(i)}\mathcal{C}\right)e_k + \mathcal{Z}\mathcal{B}m_k \tag{4.11}$$

La stabilité asymptotique globale (GAS) de (4.11) autour du point d'équilibre zéro peut être assurée par un choix approprié des gains $L_l^{(i)}$ $(i = 1, \cdots, N)$ impliqués dans (3.9). Le théorème suivant nous permet de calculer ces gains.

Théorème 3 [Millérioux and Daafouz, 2006] La stabilité asymptotique globale autour du point d'équilibre zéro est assurée si les deux conditions suivantes sont vérifiées:

- $rang(\mathcal{CB}) = rang(\mathcal{B}) = m$;
- Il existe des matrices symétriques $P_i^{(l)}$, des matrices $F_i^{(l)}$ et $G_i^{(l)}$ vérifiant, $\forall (i,j) \in \{1, \cdots, N\} \times \{1, \cdots, N\}$, les LMIs :

$$\begin{bmatrix} P_i^{(l)} & (\blacksquare)^T \\ G_i^{(l)} \mathcal{Z} A_l^{(i)} - F_i^{(l)} \mathcal{C} & G_i^{(l)^T} + G_i^{(l)} - P_j^{(l)} \end{bmatrix} > 0 \qquad (4.12)$$

Alors l'observateur polytopique à entrée inconnue (4.6) avec le gain $\mathcal{L}_l(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)} L_l^{(i)}$ et $L_l^{(i)} = G_i^{(l)^{-1}} F_i^{(l)}$ garantit que le système (4.11) soit globalement asymptotiquement stable.

La preuve détaillée de ce théorème est donnée dans [Millérioux and Daafouz, 2006].

Si les conditions du Théorème 3 sont vérifiées, l'entrée inconnue peut être estimée avec l'équation suivante :

$$\hat{m}_k^{(l)} = (\mathcal{CB})^{+}\left(y_{k+1} - \mathcal{C}\mathcal{A}_l(\rho_k)\hat{X}_k^{(l)}\right) + Y(1 - (\mathcal{CB})^{+}(\mathcal{CB})) \qquad (4.13)$$

4.5 Reconstruction du retard et de l'information

D'après l'étude effectuée ci-dessus, on propose un schéma détaillé de la transmission de la Figure 4.1. Ce dernier est illustré sur la Figure 4.2.

La valeur du retard est estimée en calculant l'erreur de synchronisation entre la sortie $\hat{Y}_k^{(l)}$ de chaque observateur O_l avec $l \in \{0, \cdots, \alpha\}$ et la sortie de l'émetteur y_k (le bloc *logique de décision 1* de la Figure 4.2). En effet :

$$\hat{\tau}(k) = \begin{cases} 0 & si \quad y_k - \hat{Y}_k^{(0)} = 0 \\ 1 & si \quad y_k - \hat{Y}_k^{(1)} = 0 \\ & \vdots \\ \alpha & si \quad y_k - \hat{Y}_k^{(\alpha)} = 0 \end{cases} \qquad (4.14)$$

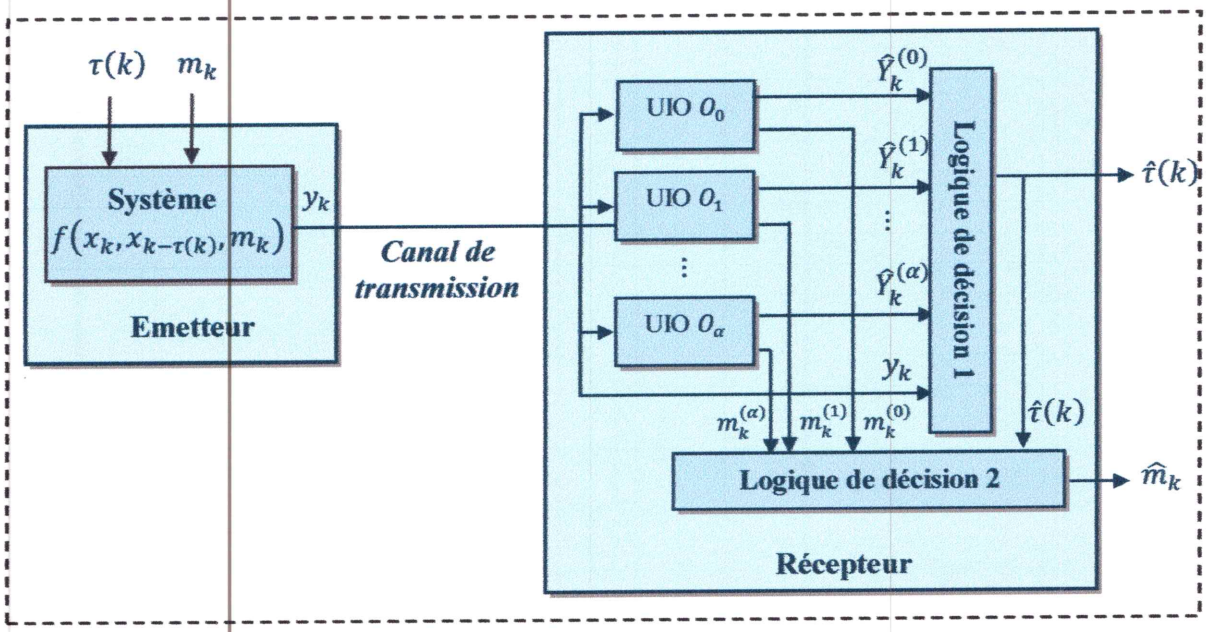


Figure 4.2 Schéma détaillé de la transmission chaotique à retard

Une fois la valeur du retard estimée, l'information cryptée est reconstruite en considérant l'information estimée par l'observateur à entrée inconnue qui correspond à la valeur de ce retard (le bloc *logique de décision 2* de la figure précédente). En effet :

$$\hat{m}(k) = \begin{cases} \hat{m}_k^{(0)} & si \quad \hat{\tau}(k) = 0 \\ \hat{m}_k^{(1)} & si \quad \hat{\tau}(k) = 1 \\ \vdots & \\ \hat{m}_k^{(\alpha)} & si \quad \hat{\tau}(k) = \alpha \end{cases} \tag{4.15}$$

4.6 Procédure globale de la reconstruction de l'information et du retard

Cette section a pour objectif de donner, en récapitulant les résultats précédents, une description détaillée de la procédure globale nécessaire pour l'estimation du retard variable et la reconstruction de l'information cryptée du système (4.1).

Etape 1 - Forme LPV polytopique

Réécrire le système (4.1) sous la forme (4.2).

Etape 2 - Polytope minimal D_ρ^*

Recherche du polytope minimal D_ρ^* qui englobe Ω_ρ avec l'approche *Quick hull*, incorporée dans la fonction *convhull* du logiciel MATLAB.

Etape 3 - Formulation hybride

Réécrire le système (4.2) sous la forme (4.3).

Etape 4 - Détermination des matrices sommets $A_l^{(i)}$

Pour chaque valeur du retard $\tau(k) = l \in \{0, \cdots, \alpha\}$, calculer les matrices sommets $A_l^{(i)}$ qui correspond aux sommets du polytope minimal D_ρ^* à l'aide de l'équation (4.5).

Etape 5 - Calcul des gains $L_l{}^{(i)}$

Pour chaque valeur du retard $\tau(k) = l \in \{0, \cdots, \alpha\}$, calculer les gains $L_l{}^{(i)}$ de l'observateur O_l en résolvant les LMIs (4.12) sachant que les matrices $A_l^{(i)}$ ont été déjà calculées précédemment.

Etape 6 - Calcul du vecteur ξ_k

Calculer le vecteur ξ_k à chaque instant à l'aide de l'équation (2.6).

Etape 7 - Calcul du gain $\mathcal{L}_l(\rho_k)$

Pour chaque valeur du retard $\tau(k) = l \in \{0, \cdots, \alpha\}$, calculer le gain $\mathcal{L}_l(\rho_k)$ de l'observateur O_l avec l'équation (3.9) sachant que les vecteurs ξ_k et $L_l{}^{(i)}$ ont été calculés précédemment.

Etape 8 - Calcul des vecteurs $\hat{X}_k^{(l)}$ et $\hat{Y}_k^{(l)}$

Pour chaque valeur du retard $\tau(k) = l \in \{0, \cdots, \alpha\}$, calculer le vecteur $\hat{X}_k^{(l)}$ et $\hat{Y}_k^{(l)}$ avec l'équation (4.6).

Etape 9 - Reconstruction du retard $\hat{\tau}(k)$

Calculer la valeur estimée du retard $\hat{\tau}(k)$ à l'aide de l'équation (4.14).

Etape 10 - Reconstruction de l'information $\hat{m}(k)$

Calculer la valeur estimée de l'information $\hat{m}(k)$ à l'aide de l'équation (4.15).

4.7 Exemples illustratifs

Dans cette section, trois applications seront étudiées afin de tester l'efficacité de cette méthode. Pour le premier exemple, l'information secrète à crypter est un signal sinusoïdal qu'on cherche à récupérer au niveau du récepteur. Le deuxième et le troisième exemple concernent la transmission d'une image et d'un texte respectivement.

4.7.1 Exemple 1 : Transmission d'un signal sinusoïdal

Considérons le système de transmission chaotique de la Figure 4.2 où l'émetteur est la récurrence chaotique, avec le vecteur d'état $(x_k^{(1)}, x_k^{(2)}, x_k^{(3)}, x_k^{(4)})$, donnée par :

$$\begin{cases} x_{k+1}^{(1)} = \left(x_k^{(1)} + 0.9\right)x_k^{(1)} - \left(x_k^{(2)} + 0.6013\right)x_k^{(2)} - 0.1x_k^{(3)} - 0.05x_{k-\tau(k)}^{(1)} - 0.01m_k \\ x_{k+1}^{(2)} = \left(2 + 2x_k^{(2)}\right)x_k^{(1)} + 0.5x_k^{(2)} - 0.3x_k^{(4)} - 0.1x_{k-\tau(k)}^{(2)} \\ x_{k+1}^{(3)} = \left(0.09 - 0.1x_k^{(2)}\right)x_k^{(2)} + 0.1x_k^{(3)} \\ x_{k+1}^{(4)} = 0.5x_k^{(1)} - 0.1x_k^{(2)} + 0.3x_k^{(4)} \\ y_k^{(1)} = 4x_k^{(1)} \\ y_k^{(2)} = 3x_k^{(2)} \end{cases} \quad (4.16)$$

La quantité $\tau(k)$ est un retard variable dans le vecteur d'état qui appartient à l'ensemble $\tau(k) \in \{0,1\}$. La variation de $\tau(k)$ est donnée sur la Figures 4.3

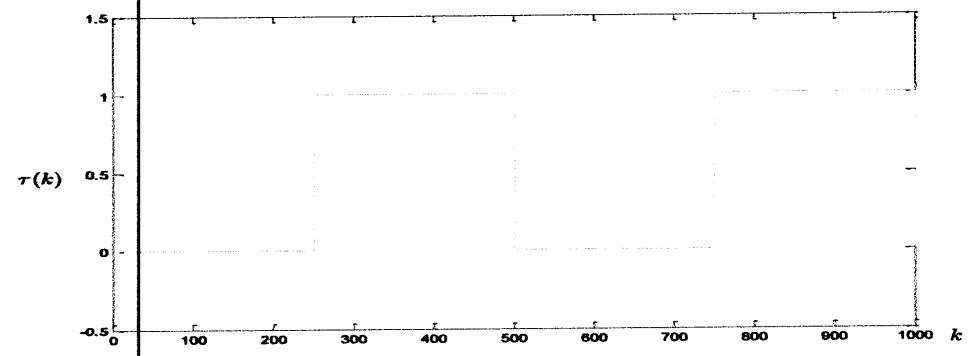


Figure 4.3 Variation du retard $\tau(k)$

Le signal m_k est l'information secrète illustrée sur la Figure 4.4.

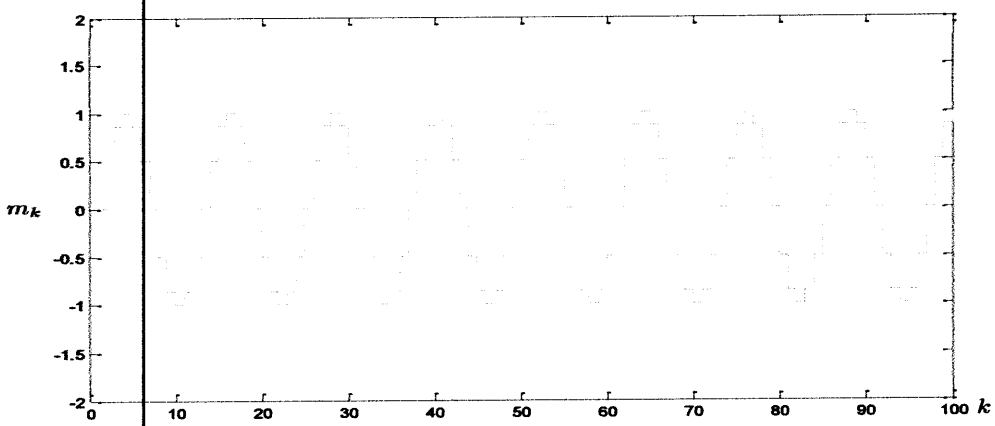


Figure 4.4 Information originale m_k

On fait la simulation du système (4.16) à partir de la condition initiale $x_0 = [-0.72 \quad -0.64 \quad 0.1 \quad 0]^T$. La projection de l'attracteur chaotique correspondant Ω dans l'espace de dimension 3 $(x_k^{(1)}, x_k^{(2)}, x_k^{(4)})$ est donnée sur la Figure 4.5.

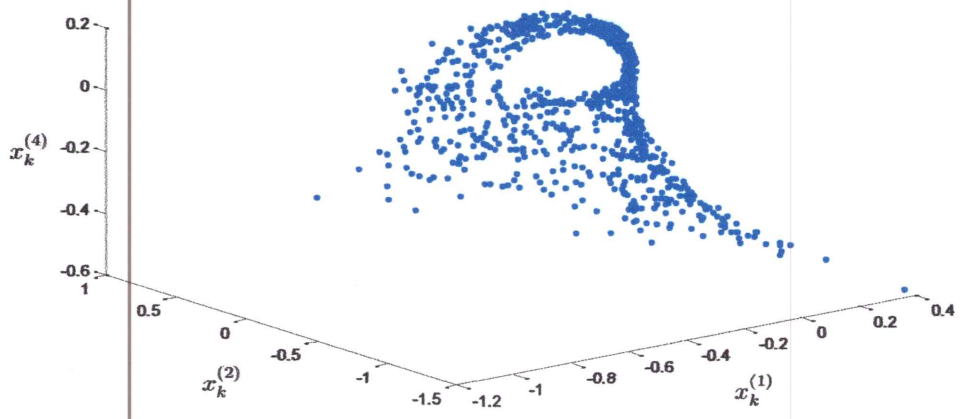


Figure 4.5 Attracteur chaotique Ω

Maintenant, afin de reconstruire l'information cryptée m_k, nous allons suivre les étapes de la Section 4.6.

Etape 1 - Forme LPV polytopique

On définie le vecteur ρ_k comme :

$$\begin{cases} \rho_k^{(1)} = x_k^{(1)} = \dfrac{y_k^{(1)}}{4} \\ \rho_k^{(2)} = x_k^{(2)} = \dfrac{y_k^{(2)}}{3} \end{cases}$$

Par conséquent, le système (4.16) peut être réécrit sous la forme (4.2) avec :

$$A(\rho_k) = \begin{bmatrix} \rho_k^{(1)} + 0.9 & -\rho_k^{(2)} - 0.6013 & -0.1 & 0 \\ 2 + 2\rho_k^{(2)} & 0.5 & 0 & -0.3 \\ 0 & 0.09 - 0.1\rho_k^{(2)} & 0.1 & 0 \\ 0.5 & -0.5 & 0 & 0.3 \end{bmatrix} \qquad (4.17)$$

$$G(\rho_k) = \begin{bmatrix} -0.05 & 0 & 0 & 0 \\ 0 & -0.1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, B = \begin{bmatrix} -0.01 \\ 0 \\ 0 \\ 0 \end{bmatrix} \text{ et } C = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{bmatrix}$$

Etape 2 - Polytope minimal D_ρ^*

Le polytope minimal D_ρ^* qui englobe Ω_ρ est calculé avec la fonction MATLAB *convhull*.

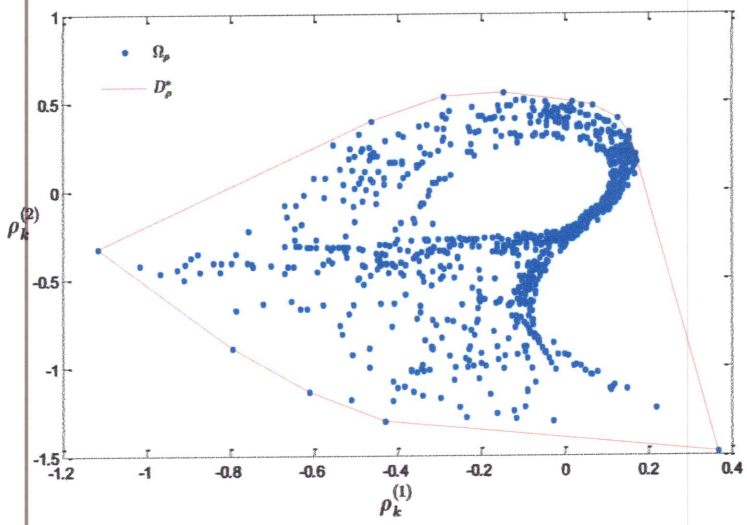


Figure 4.6 Ensemble Ω_ρ et polytope minimal D_ρ^*

Il s'avère que 14 sommets ρ_{o_i} ont été trouvés ($N = 14$). L'ensemble Ω_ρ et le polytope minimal D_ρ^* sont représentés sur la Figure 4.6.

Etape 3 - Formulation hybride

Le système (4.17) peut être réécrit sous la forme (4.4) avec les matrices :

$$\mathcal{A}_0(\rho_k) = \begin{bmatrix} A(\rho_k) + G(\rho_k) & \mathbf{0} \\ I_4 & \mathbf{0} \end{bmatrix}, \quad \mathcal{A}_1(\rho_k) = \begin{bmatrix} A(\rho_k) & G(\rho_k) \\ I_4 & \mathbf{0} \end{bmatrix}, \quad \mathcal{B} = \begin{bmatrix} B \\ \mathbf{0} \end{bmatrix},$$
$$\mathcal{C} = [C \quad \mathbf{0}]$$

et

$$X_k = \begin{bmatrix} x_k \\ x_{k-1} \end{bmatrix}, Y_k = y_k$$

Etape 4 - Détermination des matrices sommets $A_l^{(i)}$

Pour chaque valeur du retard $\tau(k) = l \in \{0,1\}$, on calcule les matrices sommets $A_l^{(i)}$ avec (4.5). On trouve :

$$A_0^{(i)} = \mathcal{A}_0(\rho_{o_i}) = \begin{bmatrix} A(\rho_{o_i}) + G(\rho_{o_i}) & \mathbf{0} \\ I_4 & \mathbf{0} \end{bmatrix}, \quad A_1^{(i)} = \mathcal{A}_1(\rho_{o_i}) = \begin{bmatrix} A(\rho_{o_i}) & G(\rho_{o_i}) \\ I_4 & \mathbf{0} \end{bmatrix}$$

Etape 5 - Calcul des gains $L_l^{(i)}$

Pour chaque valeur du retard $\tau(k) = l \in \{0,1\}$, on calcule les gains $L_l^{(i)}$ de l'observateur O_l en résolvant les LMIs (4.12). On trouve que ces LMIs sont faisables pour les deux observateurs à entrée inconnue O_0 et O_1.

Etape 6 - Calcul du vecteur ξ_k

On Calcule le vecteur ξ_k à chaque instant à l'aide de l'équation (2.6).

Etape 7 - Calcul du gain $\mathcal{L}_l(\rho_k)$

Pour chaque valeur du retard $\tau(k) = l \in \{0,1\}$, on calcule le gain $\mathcal{L}_l(\rho_k)$ de l'observateur O_l avec l'équation (3.9).

Etape 8 - Calcul des vecteurs $\hat{X}_k^{(l)}$et $\hat{Y}_k^{(l)}$

On calcule les vecteurs d'état et de sortie $\hat{X}_k^{(0)}$, $\hat{Y}_k^{(0)}$ et $\hat{X}_k^{(1)}$ et $\hat{Y}_k^{(1)}$ avec l'équation (4.6), qui correspondent respectivement aux observateurs O_0 et O_1. Les résultats de synchronisation entre ces observateurs et l'émetteur (4.16) sont illustrés sur le Figures 4.7, 4.8, 4.9 et 4.10.

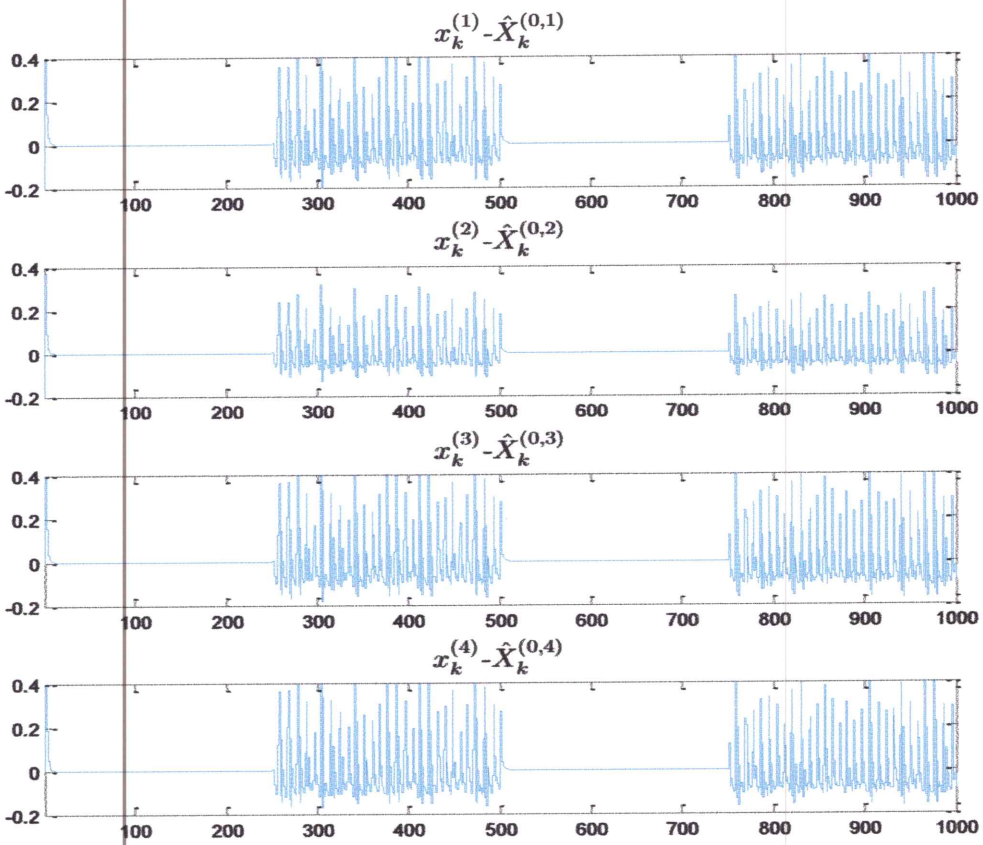


Figure 4.7 Erreur de synchronisation du vecteur d'état de O_0 $x_k - \hat{X}_k^{(0)}$

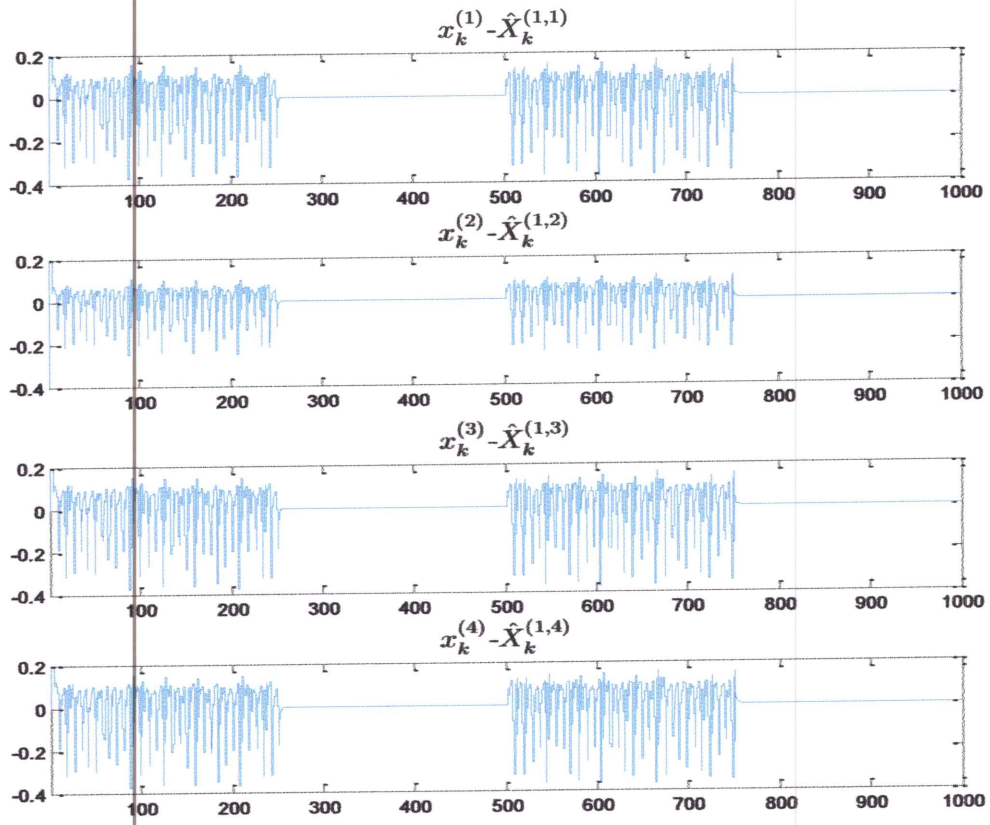


Figure 4.8 Erreur de synchronisation du vecteur d'état de O_1 $x_k - \hat{X}_k^{(1)}$

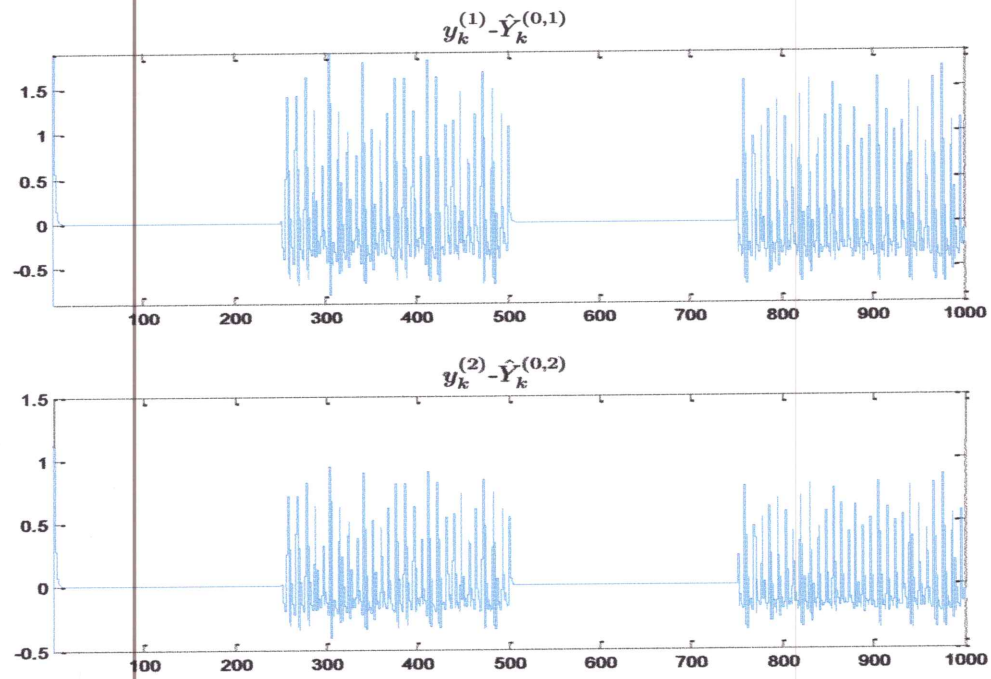


Figure 4.9 Erreur de synchronisation de la sortie de O_0 $y_k - \hat{Y}_k^{(0)}$

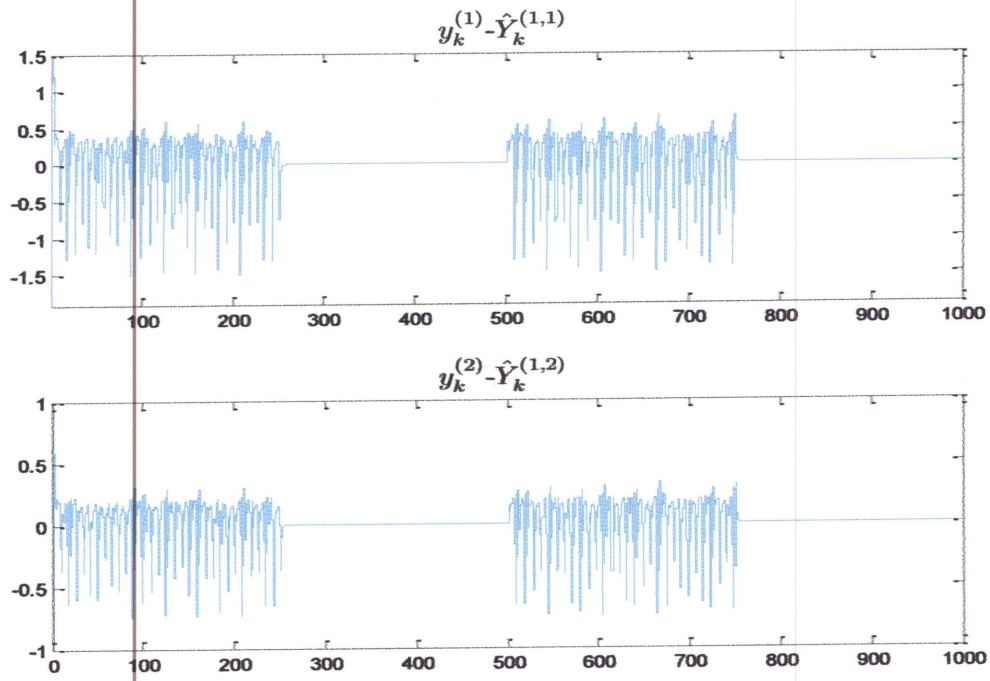


Figure 4.10 Erreur de synchronisation de la sortie de O_1 $y_k - \hat{Y}_k^{(1)}$

Les résultats de simulation montrent bien qu'un seul observateur à entrée inconnue à la fois peut se synchroniser avec l'émetteur. En effet, on remarque bien que lorsque le vecteur d'état du premier observateur O_0 est synchronisé avec le vecteur d'état de l'émetteur ($x_k - \hat{X}_k^{(0)} = 0$), celui du deuxième observateur O_1 ne l'est pas ($x_k - \hat{X}_k^{(1)} \neq 0$), et vice versa. De la même façon, lorsque la sortie du premier observateur O_0 est synchronisée avec la sortie de l'émetteur ($y_k - \hat{Y}_k^{(0)} = 0$), celle du deuxième observateur O_1 ne l'est pas ($y_k - \hat{Y}_k^{(1)} \neq 0$), et vice versa.

Etape 9 - Reconstruction du retard $\hat{\tau}(k)$

A l'aide de l'équation (4.14) on calcule la valeur estimée du retard $\hat{\tau}(k)$:

$$\hat{\tau}(k) = \begin{cases} 0 & si \quad y_k - \hat{Y}_k^{(0)} = 0 \\ 1 & si \quad y_k - \hat{Y}_k^{(1)} = 0 \end{cases}$$

Le résultat est montré sur la Figure 4.11.

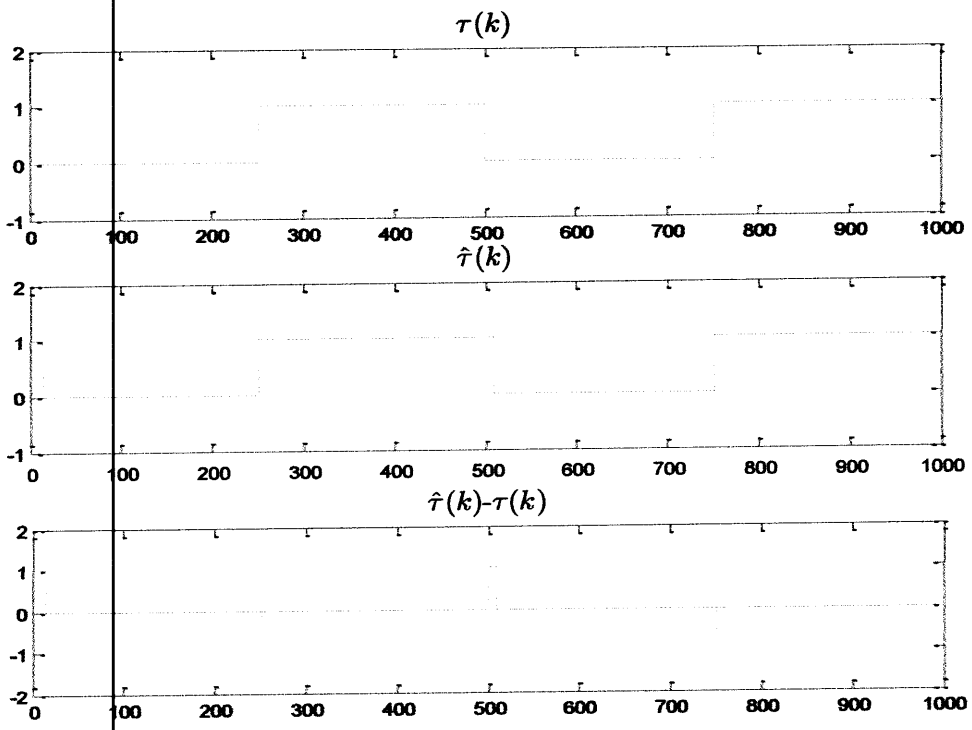


Figure 4.11 Retard $\tau(k)$ et retard reconstruit $\hat{\tau}(k)$

On remarque que l'erreur de reconstruction du retard converge rapidement vers zéro au début de la reconstruction et à chaque fois que ce retard change de valeur. Cela est dû à la convergence asymptotique des observateurs comme on l'a expliqué dans le chapitre précédent.

Etape 10 - Reconstruction de l'information $\hat{m}(k)$

A l'aide de l'équation (4.15) on reconstruit l'information $\hat{m}(k)$:

$$\hat{m}(k) = \begin{cases} \hat{m}_k^{(0)} & si \quad \hat{\tau}(k) = 0 \\ \hat{m}_k^{(1)} & si \quad \hat{\tau}(k) = 1 \end{cases}$$

Les entrées reconstruites $\hat{m}_k^{(0)}$ et $\hat{m}_k^{(1)}$ par les deux observateurs à entrée inconnue O_0 et O_1 respectivement sont illustrées sur la Figure 4.12.

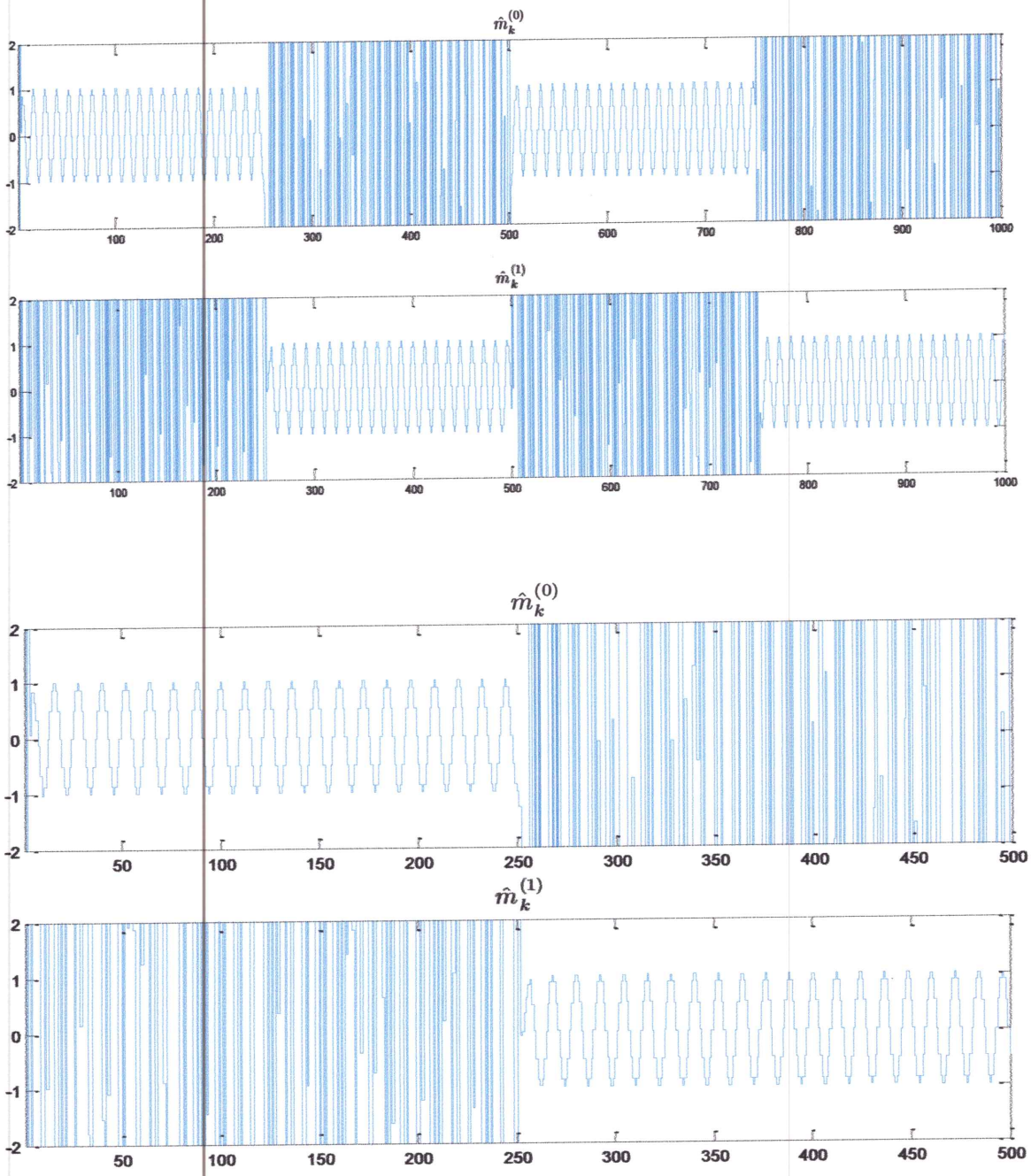


Figure 4.12 Entrées reconstruites $\hat{m}_k^{(0)}$ et $\hat{m}_k^{(1)}$

La reconstruction de l'information $\hat{m}_k$ est donnée sur la Figure 4.13.

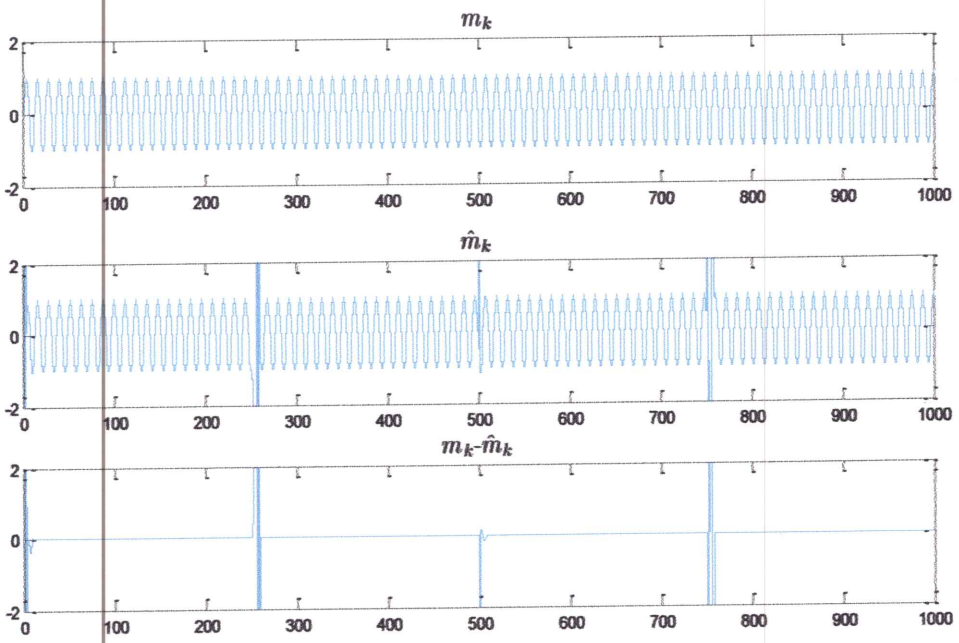


Figure 4.13 Information reconstruite $\hat{m}_k$ et erreur de reconstruction $m_k - \hat{m}_k$

D'après les deux figures précédentes, on remarque que le signal reconstruit suit le signal transmis. L'erreur de reconstruction de l'information m_k converge rapidement vers zéro au début de la reconstruction et à chaque fois que le retard change de valeur. Ces états transitoires correspondent à la commutation entre les deux observateurs.

Les résultats de simulation montrent l'efficacité de cette méthode, à la fois pour l'estimation du retard variable $\tau(k)$ et l'information cryptée m_k.

4.7.2 Exemple 2 : Transmission d'une image

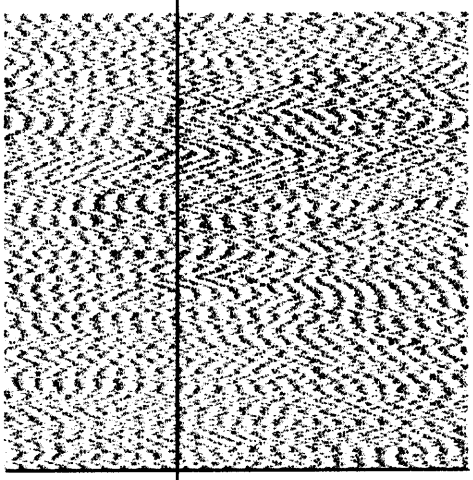
On garde les mêmes paramètres de simulation qu'à l'exemple précédent, cependant, on considère que le retard $\tau(k)$ prend une seule valeur qui vaut 1 ($\tau(k) = 1$). L'image originale, la célèbre photographie du *Cameraman* couramment utilisée en traitement d'image, est représentée sur la Figure 4.14.

Cette photographie est définie comme une matrice de 256 lignes et 256 colonnes. Pour pouvoir l'injecter comme entrée m_k du système de transmission de la Figure 4.2, on génère un signal à une dimension : les lignes de cette matrice sont concaténées pour former un seul vecteur. Ainsi, on obtient un vecteur de 65535 pixels. Ensuite, les coefficients de ce vecteur sont normalisés, pour obtenir un signal $m_k \in [0,1]$.

Figure 4.14 Photographie du cameraman

La Figure 4.15 (a) montre l'image cryptée correspondant au signal transmis au récepteur après l'injection de m_k (première sortie de l'émetteur $y_k^{(1)}$).

Afin de reconstruire l'image cryptée, on suit les mêmes étapes que celles de l'exemple précédent. Il s'avère que les LMIs sont faisables pour les deux observateurs à entrée inconnue O_0 et O_1. A partir de l'information reconstruite $\widehat{m}_k$, on applique le processus inverse et on obtient l'image décryptée. Elle est illustrée sur la Figure 4.15 (b).



(a) Image cryptée

(b) Image décryptée

Figure 4.15 Reconstruction de l'image

Nous constatons bien que cette image reconstruite au niveau du récepteur est identique à celle de l'image originale transmise au niveau de l'émetteur. Elle présente seulement

quelques pixels incorrects dans les premiers points (en haut à gauche). Ces premiers pixels ont été reconstruits avant que l'observateur à entrée inconnue O_1 soit synchronisé avec l'émetteur ce qui explique cette erreur. Ces résultats permettent d'affirmer la performance de la méthode utilisée.

4.7.3 Exemple 3 : Transmission d'un texte

Les paramètres de simulation précédemment indiqués sont toujours conservés. Le texte à transmettre est indiqué sur la Figure 4.16.

> message vide message vide Il existe un comportement entre la régularité rigide et l'aspect aléatoire. Ce comportement s'appelle : chaos. On a longtemps supposé que c'était de l'aléatoire et la vaste théorie de la probabilité et des statistiques est appliquée. En fait, c'est un champ nouveau d'investigation qui s'ouvrait en même temps qu'une nouvelle manière d'appréhender des effets parfois méconnus depuis longtemps

Figure 4.16 Texte original

Pour pouvoir injecter ce texte comme entrée m_k du système de transmission de la Figure 4.2, et à l'aide du code ASCII, on génère un vecteur dont les composantes sont des entiers compris entre 0 et 255. Ensuite, on normalise ce vecteur pour obtenir un signal $m_k \in [0,1]$.

Après le processus de cryptage, le texte correspondant au signal de sortie $y_k^{(1)}$ transmis au récepteur est montré sur la Figure 4.17.

> Žƒlupvwf]NDNQUN_XVdTfcag^jm[I=8PKSQ_[jx†˜š—
> Ž‹™‹ ™‰ŽŠ~lqsyxeVHTS\]gl[odUNG6=CM@EJPRNF
> JZSP_NcU^f\LCA?;:CYWLYcf\mqlej{†wl€zjit„˜›˜š'†ˆ Š
> vrhXbmhZ_n}™•‹ zsx‰wxqkrsgUE6#%.+&2@>6:CPZb
> iiddplb_z}tw}toplmngxmZI8(#2>+=2@22<GLOPRU[acl
> mg[[elbX\fmhcYj^aecVa[V˜S]]bTZf^YgWd_Xh^UiqbU
> fk_OD>JTFMeq€tny€tlgjotjlsdwd^O[ZL`_F;/-
> =4&#3*0;8FBEUFL`TRgcYgo `viyb} ln, pƒt{~·s·lx‹

Figure 4.17 Texte crypté

Afin de reconstruire le texte crypté, on suit les mêmes étapes que celles du premier exemple précédent. Il s'avère que les LMIs sont faisables pour les deux observateurs à entrée inconnue O_0 et O_1. A partir de l'information reconstruite $\hat{m}_k$, on applique le processus inverse avec le code ASCII et on obtient le texte décrypté. La figure 4.18 montre le texte correspondant à l'information décryptée $\hat{m}_k$.

drr`fduhcdldsrage vide Il existe un comportement entre la régularité rigide et l'aspect aléatoire. Ce comportement s'appelle : chaos. On a longtemps supposé que c'était de l'aléatoire et la vaste théorie de la probabilité et des statistiques est appliquée. En fait, c'est un champ nouveau d'investigation qui s'ouvrait en même temps qu'une nouvelle manière d'appréhender des effets parfois méconnus depuis longtemps

Figure 4.18 Texte décrypté

On remarque que le texte reconstruit au niveau du récepteur présente seulement quelques mots qui ne sont pas correcte (au début du texte). Ces derniers ont été reconstruits avant que l'observateur à entrée inconnue O_1 ne soit synchronisé avec l'émetteur ce qui explique cette erreur. Cependant, grâce à l'ajout d'un message vide, la reconstitution du texte est parfaite pour cette simulation.

4.8 Conclusion

Dans ce chapitre, nous avons étudié un système de transmission chaotique à retard. Contrairement aux méthodes de synchronisations traditionnelles, l'émetteur et le récepteur ne possèdent pas la même structure. Nous avons injecté un retard variable dans le vecteur d'état de l'émetteur afin d'augmenter la complexité de la transmission puis nous avons injecté l'information à crypter. Nous avons montré que la reconstruction de l'information cryptée nécessite la connaissance de ce retard. Ceci a été assuré en faisant appel à des observateurs à entrée inconnue. Par conséquent, la synthèse des observateurs polytopiques à entrée inconnue a été introduite.

Après une étude détaillée du problème, nous avons développé une procédure globale permettant à la fois la reconstruction du retard inconnu et de l'information cryptée au niveau du récepteur. Finalement, nous avons illustré l'efficacité de cette méthode via trois

applications différentes : transmission d'un signal, transmission d'une image et la transmission d'un texte.

Conclusion Générale

Ce mémoire a porté sur les systèmes de communication sécurisés à base des systèmes chaotiques à retard à temps discret.

Dans un premier temps, nous avons évoqué quelques notions sur les systèmes chaotiques. Ces systèmes présentent plusieurs caractéristiques dont l'exploitation serait intéressante pour la transmission de données. Parmi ces caractéristiques, on peut citer le déterminisme qui signifie que ces systèmes sont régis par des règles fondamentales non probabilistes. Il est alors possible de reproduire le comportement chaotique. Une autre propriété intéressante de ces systèmes, est la sensibilité aux conditions initiales. En effet, un moindre écart ou imprécision dans les conditions initiales engendre des évolutions totalement différentes. Ceci implique l'impossibilité de prédiction à long terme du comportement du système chaotique. Puis, nous avons donné le schéma général de la transmission sécurisée à base du chaos. Le principe est de crypter l'information utile dans un signal ou dans une combinaison de signaux chaotiques puis l'envoyer sur un canal public vers le récepteur qui récupère l'information par décryptage. A ce stade, la synchronisation de l'émetteur et du récepteur s'impose pour obtenir une « copie » identique du système chaotique de l'émetteur à la réception. Après, nous avons introduit le concept de synchronisation des systèmes chaotiques et rappelé les différentes techniques de synchronisation proposées dans la littérature et nous avons présenté quelques systèmes de transmission chaotiques.

Le schéma de transmission choisi dans ce travail est la transmission par injection du retard, où le retard, joue soit le rôle de l'information qui doit être masquée (système de transmission étudié dans le chapitre 3), ou bien le rôle d'une clé secrète qui sert à augmenter la sécurité de la transmission (système de transmission étudié dans le chapitre 4). Afin de pouvoir récupérer ce retard variable, nous avons opté pour la méthode de synchronisation par observateur LPV polytopique.

Pour cette raison, nous avons expliqué comment les systèmes chaotiques à non linéarité polynomiale peuvent se réécrire sous forme LPV polytopique. La méthode utilisée est basée sur la recherche du polytope minimal englobant les paramètres variant. Ces techniques de modélisation LPV ont suscité beaucoup d'intérêt car elles fournissent une procédure systématique pour concevoir les observateurs LPV polytopiques.

Pour les systèmes de transmission étudiés dans les chapitre 3 et 4, nous avons montré, à l'aide d'une formulation hybride, que la reconstruction du retard, et éventuellement de l'information secrète, et donc le décryptage, peut être assurée en faisait appel, soit à des observateurs LPV polytopiques, soit à des observateurs LPV polytopiques à entrée inconnue. La synthèse de ces observateurs est fondée sur la vérification des LMIs qui assurent la convergence asymptotique globale de l'erreur de reconstruction d'état.

L'efficacité des méthodes de décryptage utilisées, fondées sur l'utilisation d'observateurs polytopiques, a été testée à travers différentes applications. Les résultats obtenus ont montré l'efficacité de ces méthodes.

Dans le cadre de ce mémoire, nous n'avons pas pris en considération les perturbations qui peuvent influencées l'émetteur. Comme perspective de ce travail, on pourrait considérer une adaptation des procédures données dans le contexte stochastique.

BIBLIOGRAPHIE

[Bara et al., 2001] G. I. Bara, J. Daafouz, F. Kratz, and J. Ragot, "Parameter-dependent state observer design for affine LPV systems" 74(16) , Pages 1601--1611, 2001.

[Bruzelius, 2004] F. Bruzelius, "Linear Parameter-Varying Systems : an approach to gain scheduling". PhD thesis, Department of Signals and Systems, Chalmers University of Technology, Goteborg, Sweden, 2004.

[Cuomo et al.,1993] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz. "Synchronization of Lorenz based chaotic circuits with applications to communications". IEEE Trans. Circuits Syst. II, 40(10), Pages 626--633, 1993.

[Daafouz et al., 2002] J. Daafouz, G. Millérioux, and C. Iung, "A polyquadratic stability based approach for switched systems". International Journal of Control, 75, Pages 1302--1310, 2002.

[Devancy, 1992] R. L. Devancy, "A first course in chaotic dynamical systems". Addison-Wesley, New York, 1992.

[Douglas, 1992] E. Douglas, "Internetworking with TCP/IP: principles, protocols, architecture". Prentice-Hall International, New Jersey, USA, 1992.

[Eckmann and Ruelle, 1992] J. P. Eckmann, and D. Ruelle, "Fundamental limitations for estimating dimensions and Lyapunov exponents in dynamical systems". Physica D, 56, Pages 185-187.

[Eddy, 1977] W. F. Eddy, "A new convex hull algorithm for planar sets". ACM Transactions on Mathematical Software, 3, Pages 398--403, 1977.

[Ghanes et al., 2005] M. Ghanes, J. DeLeon and A. Glumineau "Validation of an Interconnected High Gain Observer for Sensorless Induction Motor On Low

Frequencies Benchmark: Application to an Experimental Set-up", IEEE Proc. Control Theory and Applications, 152(4), Pages 371--378, 2005.

[Graham, 1973] R. L. Graham, "An efficient algorithm for determining the convex hull of a finite planar set". Information Processing Letters, 2(1), Pages 132--133, 1973.

[Heidari-Bateni et al., 1992] G. Heidari-Bateni, C. C. McGillem and M. F. Tenorio, "A novel multiple address digital communication system using chaotic signals", ICC, 1992.

[Heidari-Bateni and McGillem, 1994] G. Heidari-Bateni, and C. C. McGillem,"A chaotic direct-sequence spread-spectrum communication system". IEEE Trans on communications, 42, Pages1524--1527, 1994.

[May, 1976] R. May, "Simple mathematical models with complicated dynamics". Nature, 261, Pages 459--470, 1976.

[Millérioux and Daafouz, 2006] G. Millérioux and J. Daafouz, "Performances of unknown input observers for chaotic lpv maps in a stochastic context". Nonlinear Dynamics, 44, Pages 205--212, 2006

[Pecora and Carroll, 1990] L. M. Pecora et T. L. Carroll, "Synchronization in chaotic system". Phys. Rev. Lett., 64 (11), Pages 1196--1199, 1990.

[Rössler, 1976] O. E. Rössler, "An Equation for Continuous Chaos". Physics Letters 57A (5), Pages 397--398,1976.

[Tenny, 2003] R. Tenny, "Symmetric and Asymmetric Secure Communication Schemes". Thèse de Doctorat, University of California, San Diego, 2003.

[Zheng et al., 2008] G. Zheng, D. Boutat, T. Floquet, and J.-P. Barbot, "Secure data transmission based on multi-input multi-output delayed chaotic system". International Journal of Bifurcation and Chaos, 18(7), Pages 2063--2072, 2008.