Synchronisation des systèmes chaotiques par observateurs et applications à la transmission d'informations

Habib Dimassi

Université Paris Sud XI – Université Tunis El-Manar
ÉCOLES DOCTORALES : STITS (France) – STI ENIT (Tunisie)

Synchronisation des systèmes chaotiques par observateurs et applications à la transmission d'informations

THÈSE DE DOCTORAT PAR

Habib DIMASSI

Soutenue publiquement le 09 Novembre 2012 pour obtenir le grade de Docteur en Physique de l'Université Paris Sud 11 – Docteur en Génie Électrique de l'École Nationale d'Ingénieurs de Tunis

Composition de jury

Présiedent de Jury:	Jamal DAAFOUZ	Professeur à l'Université de Lorraine
Rapporteurs:	Jean Pierre BARBOT	Professeur à l'Université de Cergy-Pontoise
	Naceur BENHADJ BRAIEK	Professeur à l'Ecole Polytechnique de Tunisie
Examinateurs:	Mohamed BENREJEB	Professeur à l'ENIT
	Antonio LORIA	Directeur de recherches au CNRS
	Safya BELGHITH	Professeur à l'ENIT.

L2S / SUPELEC – SYS'COM / ENIT
Université Paris Sud XI – Université Tunis El-Manar

Remerciements

Avant tout, je remercie infiniment 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 d'abord, je tiens à remercier chaleureusement mes directeurs de thèse M. Antonio Loria et Mme. Safya Belghith :

Je suis très reconnaissant envers M. Antonio Loria, directeur de recherches au CNRS pour son soutient, sa générosité, sa disponibilité et sa patience. Je suis reconnaissant envers lui pour tout ce qu'il m'a apporté sur le plan scientifique et tout ce que j'ai appris de lui au laboratoire L2S-Supelec. Merci pour tous les échanges scientifiques et les conseils précieux. Il étais toujours présent pour moi tout au long de la thèse malgré ses nombreuses responsabilités et a fortement contribué à mon évolution scientifique. Je salue toutes ses qualités humaines : sa modestie, sa générosité, etc, et pour l'affection qu'il portait pour moi. J'adresse par l'occasion mon profond respect à sa femme Mme. Elena.

Je suis très reconnaissant envers Mme. Safya Belghith, professeur à l'école nationale d'ingénieurs de Tunis (ENIT) qui m'a adopté dans son équipe au laboratoire Sys'Com à l'ENIT depuis mon stage de mastère de recherche et m'a initié au monde de recherche : elle m'a fait découvrir ce domaine de recherche passionnant qui couvre les thèmes de l'automatique et de télécommunication et a continué à me diriger dans le cadre de ce travail de thèse en cotutelle. Merci pour tout son soutient, sa confiance et sa générosité. Toute ma reconnaissance pour tout ce qu'elle m'a apporté sur les plans scientifique et humain et toute mon admiration pour ses qualités humaines.

Je remercie chaleureusement les membres de Jury qui m'ont fait l'honneur d'évaluer mon travail de thèse :

En particulier, je tiens à remercier chaleureusement M. Jean Pierre Barbot , professeur à l'ENSEA et M. Naceur Benhadj Braiek, professeur à l'école polytechnique de Tunisie qui ont fait le travail délicat et minutieux de rapporter mon mémoire de thèse et pour leurs commentaires et remarques précieux.

Je remercie chaleureusement M. Jamal Daafouz, professeur à l'université de Lorraine et M. Mohamed Benrejeb , professeur l'école nationale d'ingénieurs de Tunis (ENIT) qui m'ont fait l'honneur d'examiner mon travail de thèse.

Mes sentiments amicales s'adressent aux collègues du laboratoire L2S-Supelec, en particulier à ma collègue du bureau LeHavy et à mes compatriotes Sami, Ali, Islam, Leila et Sarra avec qui je ne me sens pas trop loin de la patrie : Notre chère Tunisie ! ! !.

Mes salutations vont également à mes amis en Tunisie Makram, Elyes, Hassen, Moez, Zied, Mohamed, Slah, Belhassen, etc. Un grand merci à Moez pour son soutient logistique ! ! !

Enfin, je remercie mon père et surtout ma mère qui, sans elle, je n'aurais pas atteint ce niveau d'études : elle m'a appris à aimer la science depuis mon enfance malgré son niveau de scolarisation très moyen. Mes remerciements s'adressent également à ma sœur et mon frère (mes salutations à sa femme et sa belle famille) et grand bisou à ses enfants Alaa et Ahmed ! !

À ma mère,

À ma mère,

À ma mère,

À mon père,

À ma sœur, mon frère et sa femme,

À Alaa et Ahmed,
À tous ceux que j'aime et je respecte.

Université Paris Sud XI – Université Tunis El-Manar
ÉCOLES DOCTORALES : STITS (France) – STI ENIT (Tunisie)

Résumé

L2S / SUPELEC – SYS'COM / ENIT
Université Paris Sud XI – Université Tunis El-Manar

Docteur en Physique – Docteur en Génie Électrique

par Habib DIMASSI

Dans ce travail de thèse, nous développons des méthodes de synchronisation des systèmes chaotiques pour les applications de transmission d'informations. La première méthode de synchronisation que nous proposons est basée sur les observateurs adaptatifs à entrées inconnues pour une classe des systèmes chaotiques présentant des incertitudes paramétriques et des perturbations dans leurs dynamiques et du bruit dans les signaux de sortie (bruit dans le canal de communication). La méthode développée repose sur les techniques adaptatives pour la compensation des non-linéarités et des incertitudes paramétriques et pour la restauration des messages transmis. Elle se base également sur les méthodes de synthèse d'observateurs à entrées inconnues pour supprimer l'influence des perturbations et du bruit. Ensuite, nous développons une deuxième méthode de synchronisation utilisant un observateur adaptatif à "modes glissants" pour une classe des systèmes chaotiques présentant des entrées inconnues et dont les signaux de sortie sont bruités. La synthèse de l'observateur s'appuie sur la théorie des modes glissants, les techniques de synthèse d'observateurs singuliers et les techniques adaptatives dans le but d'estimer conjointement l'état et les entrées inconnues malgré la présence du bruit dans les équations de sortie. Cette approche de synchronisation est ensuite employée dans un nouveau schéma de communication chaotique sécurisée dont l'objectif est d'augmenter le nombre et l'amplitude des messages transmis, améliorer le niveau de sécurité ainsi que la robustesse aux bruits présents dans le canal de communication. En outre, le scénario de présence des retards de transmission est étudié en élaborant une troisième approche de synchronisation à base d'observateurs adaptatifs pour une classe des systèmes chaotiques de Lur'e avec des non-linéarités à pente restreinte et des signaux de sortie retardés. En se basant sur la théorie de Lyapunov-Krasovskii et en utilisant une hypothèse d'excitation persistante, l'observateur adaptatif proposé garantit la synchronisation maitre-esclave et la restauration des informations transmises malgré l'existence des retards de transmission. Les résultats théoriques obtenus dans ce travail de thèse sont vérifiés à travers des applications de transmission d'informations utilisant différents modèles des systèmes chaotiques tout en étudiant les différents scénarios et cas de figure pouvant se présenter en pratique et en analysant les aspects de sécurité de ces systèmes.

Table des matières

Table des figures

Liste des tableaux

Abréviations

$\mathbb{R}$	Ensemble des nombres réels.
$\mathbb{R}^+$	Ensemble des nombres réels positifs.
$\mathbb{R}^n$	Espace réel euclidien de dimension n.
$\mathbb{R}^{n\times m}$	Ensemble des matrices réelles de dimension $n \times m$.
L_∞	Ensemble des vecteurs fonctions bornées.
L_2	Ensemble des vecteurs fonctions carrées intégrables.
C^1	Ensemble des fonctions continuellement différentiables.
$\mathcal{C}([q,r],\mathbb{R}^n)$	Ensemble des fonctions continues sur $[q,r]$ dans $\mathbb{R}^n$.
$\mathcal{C}_h$	Ensemble des fonctions continues sur $[-h,0]$.
$\|\cdot\|$	Norme euclidienne pour les vecteurs et norme induites pour les matrices.
s_m (s_M)	la plus petite et la plus grande valeur propre de S, respectivement.
M^T	Transposée de la matrice M.
M^{-1}	Inverse de la matrice M.
$M > 0$ $(M \geq 0)$	Matrice M symétrique définie (resp. semi-définie) positive.
$M < 0$ $(M \leq 0)$	Matrice M symétrique définie (resp. semi-définie) négative.
I_q (I)	Matrice identité de dimension $q \times q$ (resp. de dimension appropriée).
MIMO	Entrée multiple sortie multiple (Multiple Input Multiple Output).
ISS	Entrée-État stable (Input-to-State stable).
UIO	Observateur à entrées inconnues (Unknown Input Observer).
SNR	Rapport Signal-Bruit (Signal to noise ratio).
LMI	Inégalité matricielle linéaire (Linear Matrix Inequality).
SISO	Entrée simple sortie simple (Single Input Single Output).

Références Personnelles

I. Revues internationales avec comité de lecture :

1. H. Dimassi, A. Loria, Adaptive Unknown input Observers-based Synchronization of Chaotic Systems for Telecommunicaion, **IEEE Transactions on Circuits and Systems I : Regular papers**, vol. 58, pp 800–812, 2011. (publié)

2. H. Dimassi, A. Loria and S. Belghith, Continuously-implemented Sliding-mode Adaptive Unknown-input Observers under Noisy Measurements, **Systems & control Letters**, 2012. (accepté)

3. H. Dimassi, A. Loria and S. Belghith, A new secured transmission scheme based on chaotic synchronization via smooth adaptive unknown-input observers, **Communications in Nonlinear Science and Numerical Simulations Systems**, vol 17, pp 3727–3739, 2012. (publié)

II. Conférences internationales avec actes et comité de lecture :

4. H. Dimassi, A. Loria and S. Belghith, An Adaptive "Sliding-mode" Observer for Nonlinear Systems with Unknown Inputs and Noisy measurements, **18th IFAC World Congress**, pp 1837–1842, Milan, Italia 2011. (présenté et publié)

5. H. Dimassi, A. Loria and S. Belghith, A Robust Adaptive Observer for Nonlinear Systems with Unknown Inputs and Disturbances, **49th IEEE Conference on Decision and Control**, pp 2602–2607, Atlanta, USA 2010. (présenté et publié)

6. H. Dimassi, A. Loria and S. Belghith, Adaptive observers-based synchronization of a class of Lur'e systems with delayed outputs for chaotic communications, **IFAC Conference on Analysis and Control of Chaotic Systems**, Cancun, Mexico 2012. (presenté)

7. H. Dimassi, A. Loria and S. Belghith, Adaptive state estimation for a class of uncertain nonlinear systems with output time-delays, **51th IEEE Conference on Decision and Control**, Hawaii, USA 2012. (accepté)

III. Communications nationales :

8. H. Dimassi, A.Loria and S.Belghith, Synchronisation des systèmes chaotiques par observateurs, Applications à la transmission sécurisée d'informations, Journées de doctorants du laboratoire des signaux et systèmes L2S, JDD-L2S, Saint-Rémy-Les-Chevreuses, Juin 2011.

IV. Articles soumis dans des revues et conférences internationales avec actes et comité de lecture :

9. H. Dimassi, A. Loria and S. Belghith, Observers-based Synchronization of Lur'e Systems for chaotic communications with transmission delays, **IEEE Transactions on Circuits and Systems I : Regular papers**. (soumis)

Introduction générale

0.1 Contexte et motivations

Ce travail de thèse porte sur la synchronisation des systèmes chaotiques à base d'observateurs non linéaires et ses applications dans les systèmes de transmission d'informations.
Le phénomène de synchronisation peut être décrit comme étant un processus d'ajustement des rythmes des évènements répétitifs par l'intermédiaire des faibles interactions. Ce phénomène a été observé pour la première fois par Huygens, en 1673, en étudiant un système de deux pendules couplées. Depuis le constat de Huygens, la synchronisation des systèmes dynamiques a trouvé ses applications en théorie et en pratique et plusieurs types de synchronisation ont été distingués tels que l'auto-synchronisation qui se manifeste par les interactions internes entre les systèmes considérés et la synchronisation commandée qui nécessite une intervention externe pour forcer deux ou plusieurs systèmes dynamiques à se synchroniser. La synchronisation maître-esclave appartient à la catégorie de la synchronisation commandée, pour laquelle on dispose d'un système dominant (le système maître) qui impose son rythme à un second système (le système esclave). Pendant les deux dernières décennies, la configuration maître-esclave a été appliquée avec succès, dans les systèmes de communication sécurisée basés sur la synchronisation des systèmes chaotiques où un émetteur chaotique (le système maître) génère un signal d'information chiffré transmis dans le canal de communication vers un système récepteur (le système esclave) qui a pour objectif de synchroniser avec l'émetteur et de restaurer le signal d'information. L'utilisation du chaos dans les applications de communication sécurisée est motivée par les propriétés des systèmes chaotiques qui sont des systèmes déterministes, à comportement complexe et qui sont caractérisés par une forte sensibilité aux conditions initiales et aux variations paramétriques. Par ailleurs, plusieurs similitudes entre les systèmes chaotiques et les systèmes cryptographiques ont été constatées par la communauté scientifique, notamment les propriétés de confusion, de diffusion et de possession d'une clé secrète. Le premier travail de recherche ayant suggéré une réponse à la question de synchronisation des systèmes chaotiques a été réalisé en 1990 par les chercheurs Pecora et Caroll qui ont réussi à synchroniser deux systèmes chaotiques maître et esclave en utilisant la méthode de décomposition en sous-systèmes.

D'autre part, en 1997, Nijmeijer et Mareels ont démontré que la synchronisation maître-esclave peut être considérée comme étant un problème d'estimation d'état où le système esclave est conçu à base d'un estimateur d'état (observateur) pour le système maître. Depuis ce constat, la théorie

des *observateurs non linéaires* a joué un rôle fondamental dans le développement des méthodes de synchronisation des systèmes chaotiques et ses applications dans les systèmes de transmission sécurisée d'informations.

Le problème d'estimation d'état et de synthèse d'observateurs pour les systèmes dynamiques est un domaine de recherche qui a été abordé depuis les années soixante et qui reste actuellement un domaine très actif. En effet, le besoin d'estimation d'état est motivé par de nombreuses applications telles que la détection de défauts, la commande, l'identification (modélisation), la synchronisation des systèmes dynamiques, etc.
Il s'agit de concevoir un système dynamique appelé *observateur* dont l'objectif est de reconstruire l'état du système à partir des informations partielles accessibles telles que les signaux d'entrée et de sortie. Dans ce contexte, diverses stratégies de synthèse d'observateurs pour différentes classes des systèmes linéaires et non linéaires ont été développées, telles que les systèmes *Lipschitziens*, les systèmes satisfaisant les propriétés de secteur et de restriction de pente, les systèmes ayant des formes particulières telles que la forme canonique et la forme normale de l'observabilité, et pour lesquelles plusieurs types d'observateurs linéaires et non linéaires ont été proposés tels que l'observateur de Luenberger, le filtre de Kalman, l'observateur à grand gain, l'observateur de Thau, l'observateur d'Arcak, etc. Ces observateurs ont été utilisés et réalisés avec succès dans les conditions idéales, cependant en pratique, on se trouve souvent face à des situations particulières pour lesquelles ces stratégies ne réussissent pas à estimer parfaitement l'état du système. Il s'agit des contraintes et des incertitudes qui sont imposées par l'environnement extérieur et les imperfections des circuits électroniques et qui se manifestent sous la forme d'incertitudes paramétriques, d'erreurs de modélisation, de perturbations, des dynamiques non modélisées, d'entrées inconnues, de défauts, du bruit de mesure, de retards, etc. Afin d'améliorer la performance de l'estimateur d'état dans des telles conditions, les chercheurs ont développé des stratégies de plus en plus avancées qui tiennent compte des considérations pratiques : des stratégies robustes et adaptatives. Ainsi, les *observateurs à entrées inconnues* ont donc été développés dans le but d'estimer l'état du système tout en découplant les entrées inconnues, les *observateurs à modes glissants* basés sur la théorie de la commande à structure variable sont des observateurs robustes et permettent l'estimation conjointe de l'état et de l'entrée inconnue et les observateurs adaptatifs ont été développés dans l'objectif de reconstruire simultanément l'état et les paramètres inconnus.

Plus particulièrement, ces imperfections se produisent fréquemment dans le contexte de la synchronisation maître-esclave et ses applications dans les systèmes de communication où elles sont souvent négligées ou uniquement analysées et quantifiées.

Par ailleurs, les systèmes de communication traditionnels basés sur la synchronisation des systèmes chaotiques sont caractérisés par un faible niveau de sécurité et de confidentialité. En effet, plusieurs techniques d'attaques ont été développées, telles que la technique d'analyse spectrale, la méthode d'identification paramétrique, la synchronisation généralisée, les attaques cryptographiques, etc. Ces systèmes présentent également plusieurs autres limites telles que les restrictions sur l'amplitude, le

nombre et la nature des informations à transmettre ; ces restrictions sont imposées par les propriétés structurelles du système émetteur et les techniques de synchronisation et de cryptage utilisées.

0.2 Objectifs de la thèse

L'objectif principal de cette thèse est d'apporter à partir du domaine de l'*automatique* et plus précisément, à partir de la théorie des observateurs non linéaires, des solutions aux problèmes rencontrés dans les applications de communications basées sur la synchronisation des systèmes chaotiques :

a. Développement de méthodes de synchronisation à base d'observateurs non linéaires en tenant compte de différents scénarios qui peuvent exister en pratique.

b. Application des méthodes de synchronisation dans des systèmes de transmission à base du chaos qui sont soumis aux imperfections, incertitudes, bruit présent dans le canal de communication, etc.

c. Amélioration de performances en termes de sécurité, relaxation des restrictions et élimination des limitations des systèmes de communication traditionnels.

d. Développement de méthodes de synchronisation pour la transmission d'informations dans le cas de présence de retards de communication.

0.3 Organisation du mémoire et contributions

La structure de ce mémoire se présente comme suit. Le chapitre 1 est consacré aux systèmes chaotiques et cryptographiques dans les applications de transmission sécurisée d'informations basées sur la synchronisation de systèmes chaotiques. Après avoir bien établi la connexion entre le problème de synchronisation et le problème d'estimation d'état, nous faisons un tour d'horizon des méthodes de synthèse d'observateurs non linéaires, et en particulier celles qui sont en liaison avec ce travail de thèse.

Dans le chapitre 2, nous présentons une méthode de synchronisation robuste et adaptative basée sur les observateurs adaptatifs à entrées inconnues et son application dans un système de communication chaotique. Le système maître considéré est un système chaotique présentant dans sa dynamique des paramètres inconnus constants par morceaux ainsi que des perturbations externes. Pour la transmission de l'information, nous utilisons la technique de modulation paramétrique : le message à transmettre (supposé constant par morceaux) module l'un des paramètres du système maître. L'équation de sortie est également affectée par un bruit (le bruit présent dans le canal de communication). Les différents signaux utilisés (perturbations, bruit, signal d'information, etc) sont supposés bornés. Le système esclave proposé est un observateur adaptatif à entrées inconnues qui a pour objectif de synchroniser avec le système maître, rejeter le bruit présent dans le canal de

transmission et les perturbations présentes dans la dynamique du système et reconstruire l'information transmise. Nous présentons les conditions nécessaires et suffisantes pour la synchronisation maître-esclave et les conditions de convergence paramétrique (reconstruction du message envoyé et des paramètres inconnues), notamment la condition d'excitation persistante. Pour mettre en relief notre contribution, nous présentons des exemples de simulation dans une application de transmission d'informations tout en mettant l'accent sur les avantages de notre approche par rapport à la méthode traditionnelle utilisant les observateurs adaptatifs classiques (sans élimination des perturbations et du bruit).

Dans le chapitre 3, une méthodologie de synchronisation à base d'un *observateur adaptatif par modes glissants* est développée. Les systèmes considérés sont des systèmes non linéaires couvrant une large classe des systèmes chaotiques dont on peut appliquer la technique de *transformation de Lipschitz* sous l'hypothèse de bornitude des solutions du système. La dynamique du système en considération présente également des entrées inconnues bornées et la sortie mesurée est contaminée par un bruit borné. L'observateur que nous proposons est un observateur adaptatif par modes glissants dont la réalisation ne dépend pas de la connaissance des bornes supérieures des états, des entrées inconnues et du bruit dans l'équation de sortie, ni la valeur exacte de la constante de Lipschitz qui peut prendre des grandes valeurs. La méthode proposée est basée sur les techniques de conception d'observateurs singuliers, la théorie de commande par modes glissants et la commande adaptative. Nous présentons les étapes de construction de l'observateur et les conditions nécessaires et suffisantes garantissant la stabilité pratique et la convergence de l'erreur d'estimation vers un ensemble compact centré autour de l'origine et qu'on peut réduire arbitrairement en agissant convenablement sur les paramètres de l'observateur.

La méthode de synchronisation à base d'observateurs adaptatifs à modes glissants est ensuite exploitée dans un nouveau schéma de communication sécurisée basé sur la synchronisation maître-esclave des systèmes chaotiques. L'approche proposée est compatible avec des informations de type analogiques/numériques et de grandes amplitudes et garantit un bon niveau de sécurité et une robustesse aux différentes attaques spécifiques aux systèmes de communication analogiques. L'idée principale est de séparer les opérations de cryptage et de synchronisation en utilisant deux systèmes chaotiques en cascade. Nous démontrons que le schéma de transmission proposé résiste aux attaques basées sur l'analyse des caractéristiques du signal de texte chiffré et les attaques basées sur l'identification de la structure et des paramètres du système émetteur. Une analyse de la clé secrète a été également réalisée pour évaluer la robustesse du schéma proposé aux attaques cryptographiques. Le schéma est également robuste au bruit affectant le canal de communication.

Dans le chapitre 4, nous présentons une méthode de synchronisation à base d'observateurs adaptatifs pour une classe des systèmes de Lur'e avec des non-linéarités à pente restreinte en présence d'un retard de transmission à temps variant. La technique de transmission chaotique employée est la technique de modulation paramétrique et les messages à transmettre sont supposés constants par morceaux. En se basant sur l'approche de Lyapunov-Krasovskii, nous démontrons que pour des valeurs de la borne supérieure du retard suffisamment petites, l'estimation d'état et la restauration des informations transmises sont obtenues sous une hypothèse d'excitation persistante et après la

résolution d'un problème convexe d'optimisation. Ensuite, nous généralisons ce résultat au cas des longs retards de transmission en présentant un schéma de synchronisation à base d'observateurs en cascade. La performance de l'approche proposée est testée à l'aide des applications des systèmes de communication présentant des retards de transmission. En particulier, un nouveau schéma de communication sécurisée garantissant à la fois un niveau élevé de sécurité et une robustesse aux retards de transmission, a été développé en combinant cette méthode de synchronisation avec des techniques cryptographiques.

Chapitre 1

Etat de l'art

1.1 Introduction

Dans ce chapitre, nous présentons dans une première partie les notions relatifs à la théorie du chaos et au problème de synchronisation des systèmes chaotiques. Ensuite, nous faisons un tour d'horizon des techniques de transmission d'informations utilisées dans les systèmes de communications analogiques basés sur la synchronisation de systèmes chaotiques. Après avoir bien expliqué la connexion entre le problème de synchronisation et le problème d'estimation d'état, nous présentons, dans une deuxième partie, un état de l'art de la théorie des observateurs en exposant une liste de méthodes de synthèse d'observateurs non linéaires tout en analysant les conditions nécessaires et suffisantes de convergence et de stabilité. Nous commençons par présenter des exemples d'observateurs pour des systèmes non affectés par des incertitudes ni par des perturbations, puis nous étudions des exemples d'observateurs adaptatifs et robustes pour des systèmes incertains et perturbés tels que l'observateur adaptatif, l'observateur à modes glissants et l'observateur à entrées inconnues.

1.2 Systèmes de communications basés sur la synchronisation des systèmes chaotiques

1.2.1 Les systèmes chaotiques

Pendant plusieurs siècles de l'histoire de la science et jusqu'à la fin du dix-neuvième siècle, les scientifiques interprétaient les phénomènes naturelles par la *physique déterministe*. Dans la conception déterministe, l'état présent d'un phénomène physique est l'effet d'un état antérieur et la cause d'un état futur. Néanmoins, plusieurs comportements complexes qui existaient à cette époque tels que les phénomènes météorologiques ne trouvaient pas d'explication avec cette vision déterministe. Au début du vingtième siècle, Henri Poincaré a expliqué ces phénomènes par leur sensibilité aux conditions initiales. En 1967, Edwards Lorenz a présenté un système dynamique déterministe ayant un

comportement complexe manifesté par un attracteur étrange et caractérisé par une forte sensibilité aux conditions initiales. Quatre ans plus tard, James Yorke a introduit pour la première fois le terme *chaos* pour décrire les systèmes déterministes et imprévisibles. Depuis ces découvertes, la théorie du chaos a trouvé diverses applications en mathématiques, en physique, en électronique, en biologie, en médecine et plus récemment en télécommunications.
Un système chaotique est caractérisé par :
-*Un comportement apériodique à long terme* : la trajectoire d'un système chaotique dans l'espace de phase ne converge vers aucun point fixe ni orbite périodique lorsque le temps tend vers l'infini.
-*Son déterminisme* : le comportement irrégulier provient des non-linéarités intrinsèques plutôt que des bruits aléatoires. Un système chaotique ne présente pas des paramètres stochastiques (probabilistes).
-*Sa forte sensibilité aux conditions initiales* : deux trajectoires initialisées à deux valeurs très proches divergent exponentiellement.
-*Des solutions globalement bornées*.

On trouve dans la littérature plusieurs définitions mathématiques du chaos, mais jusqu'à présent, il n'existe aucune définition mathématique universelle du chaos. Les nouvelles méthodes d'analyse des systèmes dynamiques qui ont été développées considèrent les systèmes chaotiques comme étant des systèmes non linéaires présentant des trajectoires globalement bornées et localement instables.

Définition 1.1. [1] On considère le système dynamique continu suivant

$$\dot{x} = f(x); \quad x \in \mathbb{R}^n. \tag{1.1}$$

Le système (1.1) est dit chaotique s'il existe un ensemble compact $\Omega \in \mathbb{R}^n$ et un ensemble ouvert Ω_0 tels que toutes les trajectoires $x(t)$ du système (1.1) initialisées à $x(0) \in \Omega_0$ et définies $\forall t \geq 0$ vérifient la condition suivante :

$$\lim_{t\to\infty} \inf_{\omega\in\Omega} |x(t) - \omega| = 0, \tag{1.2}$$

et que toute trajectoire $X(t, 0, X(0))$ commençant dans Ω est instable au sens de Lyapunov.

Remarque 1.2. On peut interpréter cette définition comme suit. Un système chaotique possède au moins un attracteur borné Ω. L'instabilité au sens de Lyapunov des trajectoires met l'accent sur la propriété de sensibilité aux conditions initiales qui caractérise les systèmes chaotiques.

Pour mettre en évidence les caractéristiques d'un système chaotique, prenons comme exemple le modèle de Rössler :

$$\dot{x}_1 = -(x_2 + x_3), \tag{1.3a}$$
$$\dot{x}_2 = x_1 + ax_2, \tag{1.3b}$$
$$\dot{x}_3 = b + x_3(x_1 - c). \tag{1.3c}$$
$$\tag{1.3d}$$

Pour les valeurs des paramètres ($a = 0.398$, $b = 2$ et $c = 4$), le système de Rössler fonctionne en régime chaotique.

La figure 1.1 représente l'évolution en fonction du temps des trajectoires chaotiques du système de Rössler et illustre une évolution complexe, non périodique et imprévisible. C'est l'aspect aléatoire des systèmes chaotiques.

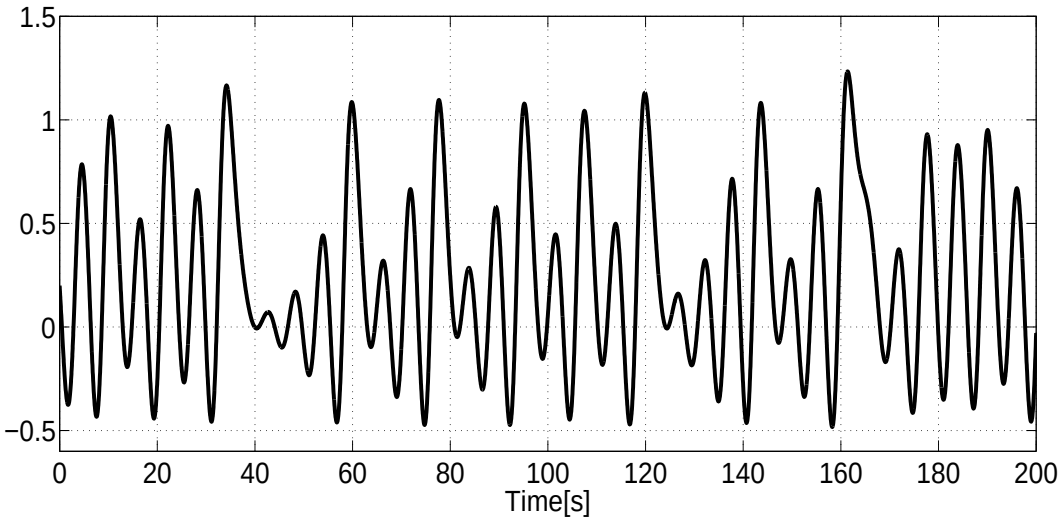

FIGURE 1.1: Évolution dans le temps de la solution $x_2(t)$

L'évolution dans le temps d'une trajectoire chaotique au cours du temps apparaît comme aléatoire, cependant l'observation de la trajectoire dans l'espace des phases, lorsque t tend vers l'infini, décrit une forme particulière qui présente une structure fractale : c'est l'attracteur étrange – voir la figure 1.2.

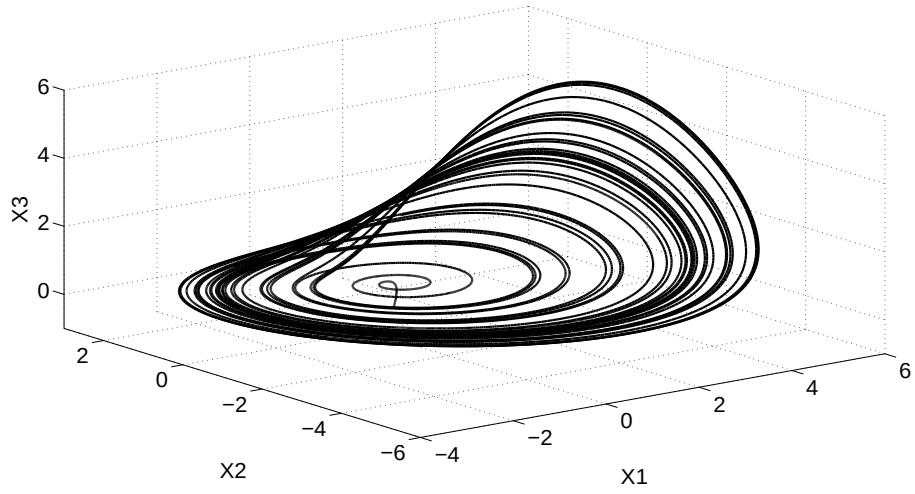

FIGURE 1.2: Attracteur du systèmes chaotique de Rössler

Dans le domaine fréquentiel, le spectre d'une solution chaotique a une large gamme de fréquences comme montré dans la figure 1.3. Le système chaotique de Rössler se caractérise par une transformée de Fourier ou spectre de puissance illustrant l'aspect non périodique de la trajectoire chaotique.

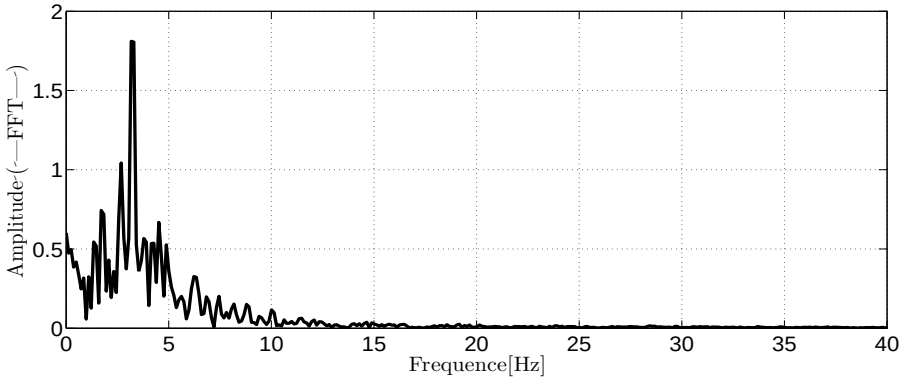

FIGURE 1.3: Spectre du systèmes chaotique de Rössler

Il existe plusieurs autres modèles des systèmes chaotiques qui possèdent des caractéristiques similaires au système de Rössler. A titre d'exemple nous citons le modèle de Lorenz, le modèle de Chua, l'oscillateur de Duffing, le système de Van Der Pol, le système de Lü, etc.

La sensibilité aux conditions initiales, l'attracteur étrange, l'évolution aléatoire et le spectre sont mises en évidence par simulation ou expérimentalement pour caractériser le comportement des systèmes chaotiques. Afin de répondre aux besoins de quantifier le chaos et mesurer la sensibilité des systèmes aux conditions initiales et les taux de divergence des trajectoires, une méthode analytique basée sur le calcul des exposants de Lyapunov a été développée. On considère une trajectoire "référence" $\bar{x}(t)$ du système (1.1) commençant avec la condition initiale $\bar{x}(0)$. La linéarisation de (1.1) autour de $\bar{x}(0)$ donne

$$\frac{dw(t)}{dt} = \frac{\partial f}{\partial x}(x(t))w(t)\Big|_{x(t)=\bar{x}(0)}, \tag{1.4}$$

avec $w(t) = x(t) - \bar{x}(t)$. Le taux d'accroissement exponentiel de $|w(t)|$ dans la direction de $w(0)$ est caractérisé par un nombre λ tel que

$$|w(t)| = e^{\lambda t} |w(0)|, \tag{1.5}$$

et par conséquent, on a :

$$\lambda = \frac{1}{t} \log \frac{|w(t)|}{|w(0)|}. \tag{1.6}$$

Définition 1.3. [2] Soit $w(t)$ la solution de l'équation (1.4). Soient $x(0)$ et $w(0)$ les conditions initiales de $x(t)$ et $w(t)$. L'exposant de Lyapunov *dans la direction de w(0)* est l'indice caractéristique

défini par

$$\lambda(x(0), w(0)) = \lim_{t\to\infty} \frac{1}{t} \log \frac{|w(t)|}{|w(0)|}, \tag{1.7}$$

dans la mesure où la limite existe.

Remarque 1.4. Le nombre des exposants de Lyapunov est un nombre fini. D'ailleurs, il existe une base $\{b_i, i = 1, \ldots, n\}$ telle que $\lambda(x(0), b_i) = \lambda_i, i = 1, \ldots, n$ et $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$.
Une fois les exposants de Lyapunov calculés, on peut définir la nature des systèmes en considération. Si les exposants sont tous négatifs ou nuls et que leur somme est négative donc l'attracteur est non chaotique. Par contre, s'il existe au moins un exposant de Lyapunov positif alors que la somme des exposants est négative, alors il s'agit d'un attracteur chaotique [3]. En particulier, les système hyperchaotiques tels que le système de Chen possèdent plus qu'un exposant de lyapunov positif.

Le comportement complexe des systèmes chaotiques a attiré l'attention des chercheurs travaillant, dans le domaine de la télécommunication, sur les méthodes de transmission sécurisée d'informations basées sur les techniques de la cryptographie. Depuis l'année 1990, plusieurs analogies entre les systèmes chaotiques et cryptographiques ont été constatées, ce qui a ouvert une grande voie pour l'utilisation du chaos dans les systèmes de communication sécurisée. Dans la section suivante, nous rappelons les notions de base de la cryptographie tout en mettant en relief l'analogie entre les systèmes chaotiques et les systèmes cryptographiques.

1.2.2 Analogie entre les systèmes chaotiques et les systèmes cryptographiques

La cryptographie est l'étude des méthodes de cryptage d'informations et les aspects associés tels que la sécurité, la confidentialité, l'intégrité, l'authentification, etc. Nous rappelons ici les principes et les notions de base liées à la cryptographie.
Un cryptosystème défini par $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{D}, \mathcal{E})$ est illustré par la figure 1.4.

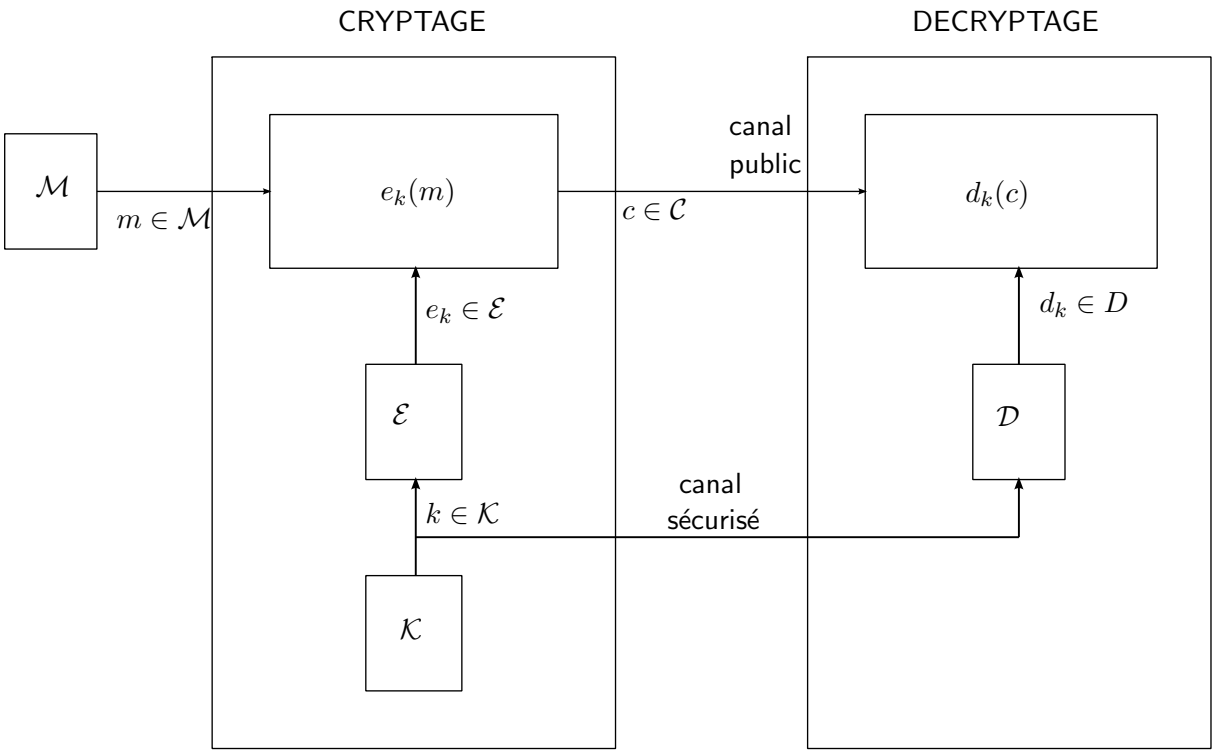

FIGURE 1.4: Schéma représentatif d'un cryptosystème

L'*espace texte clair* $\mathcal{P}$ est un ensemble fini des textes clairs possibles (messages) , l'*espace texte chiffré* $\mathcal{C}$ est un ensemble fini des textes chiffrés possibles et l'*espace clé* $\mathcal{K}$ est un ensemble fini des clés possibles. $\mathcal{E} = \{e_k : k \in \mathcal{K}\}$ et $\mathcal{D} = \{d_k : k \in \mathcal{K}\}$ représentent les ensembles des fonctions du cryptage et du décryptage, respectivement. Pour chaque clé $k \in \mathcal{K}$, il existe une fonction de cryptage $e_k : \mathcal{P} \to \mathcal{C} \in \mathcal{E}$ et une fonction de décryptage $d_k : \mathcal{P} \to \mathcal{C} \in \mathcal{D}$ tels que $d_k(e_k(p)) = p$, pour tout texte clair $p \in \mathcal{P}$ – voir [4].

Les cryptosystèmes peuvent être classifiés en deux catégories. La première catégorie repose sur le *cryptage symétrique* (à clé privée) dont on utilise la même clé secrète au niveau du cryptage et au niveau du décryptage. Ces cryptosystèmes possèdent une grande vitesse de transmission, ce qui leurs permet de transmettre des quantités considérables d'informations. Contrairement au cryptage symétrique, le principe due *cryptage asymétrique* (à clé publique) consiste à attribuer à chaque récepteur deux clés : une clé publique connue de tous les émetteurs potentiels et une autre clé gardée privée. L'inconvénient des cryptosystèmes à cryptage asymétrique est leur faible vitesse de transmission.

Plusieurs similitudes entre les systèmes cryptographiques et les systèmes chaotiques ont été constatées par la communauté scientifique, ce qui a motivé les chercheurs à exploiter des propriétés cryptographiques du chaos dans les applications de télécommunication et de transmission sécurisée d'informations. Le tableau 1.1 illustre l'analogie entre les systèmes cryptographiques et chaotiques –voir [5]. Bien que les systèmes chaotiques présentent des caractéristiques cryptographiques appropriées pour la transmission sécurisée d'informations, il est très difficile de concevoir deux circuits chaotiques

Système cryptographique	*Système chaotique*
Diffusion avec une légère modification dans le texte clair ou la clé secrète	Hypersensibilité aux conditions initiales
Confusion : complexité de la relation entre la clé secrète et le texte chiffré	Ergodicité : caractéristiques macroscopiques de l'attracteur étrange
Déterminisme des générateurs pseudo-aléatoires	Déterminisme des systèmes chaotiques
Complexité des algorithmes de cryptage	Comportements complexes
Clé secrète	Paramètres de bifurcation comme clés secrètes

TABLE 1.1: Analogie entre les systèmes cryptographiques et chaotiques

identiques à cause de leur hypersensibilité aux conditions initiales et aux variations paramétriques. La synchronisation entre l'émetteur et le récepteur chaotiques dans les systèmes de communications analogiques est un thème de recherche très actif qui a fait l'objet des nombreux travaux pendant les deux dernières décennies.

1.2.3 Synchronisation des systèmes chaotiques

Parallèlement aux grandes avancées réalisées dans la théorie de chaos, les perspectives de l'utilisation du chaos dans diverses applications, notamment en télécommunication, ont motivé les chercheurs à étudier la question de l'éventuelle possibilité de synchroniser le chaos.
La synchronisation des oscillateurs non linéaires est un phénomène qui a attiré l'attention des chercheurs depuis le constat et la description de ce phénomène par Huygens en 1673, dans un exemple de deux systèmes mécaniques couplés. Le phénomène de synchronisation est manifesté lorsque deux systèmes dynamiques évoluent d'une manière identique en fonction de temps. L'une des configurations de synchronisation les plus populaires est la configuration maître-esclave pour laquelle un système dynamique, appelé système esclave suit le rythme et la trajectoire imposés par un autre système dynamique, appelé système maître. D'où la définition suivante :

Définition 1.5. [6] On dit qu'un système esclave :

$$\dot{x}_s = f_s(x_s), \quad x_s \in \mathbb{R}^n \tag{1.8}$$

se synchronise avec un système maître :

$$\dot{x}_m = f_m(x_m), \quad x_m \in \mathbb{R}^n, \tag{1.9}$$

si pour toute paire de conditions initiales $(x_m(0), x_s(0))$,

$$\lim_{t\to\infty} |x_s(t) - x_m(t)| = 0. \tag{1.10}$$

L'un de premiers travaux de recherche proposant une approche de synchronisation maître-esclave a été réalisé par Pecora et Caroll en 1990 [7]. L'idée de base de leur approche consiste à trouver une décomposition appropriée du vecteur d'état $x = (x_1; x_2)$ du système maître (émetteur) : $\dot{x} = f(x)$, couplé par l'intermédiaire de x_1 avec un système esclave (récepteur) : $\dot{y}_2 = f_2(x_1, y_2)$, de telle manière que les exposants de Lyapunov (dits *conditionnels*) de la dynamique du système esclave soient négatives.
Depuis cette découverte innovatrice, différents régimes de synchronisation ont été distingués tels que la synchronisation identique [7], [8] (Voir définition 1.1), la synchronisation généralisée [9], la synchronisation retardée [10], la synchronisation projective [11], la synchronisation impulsive [12], la synchronisation de phase [13] et la synchronisation adaptative [14], nous rappelons ici brièvement les principales caractéristiques de ces régimes de synchronisation :
1- On dit que deux systèmes (1.8) et (1.9) se synchronisent au sens généralisé s'il existe un difféomorphisme D tel que $\lim_{t\to\infty} |x_1(t) - Dx_2(t)| = 0$, ainsi la synchronisation identique appelée aussi "synchronisation complète" est un cas particulier de la synchronisation généralisée.
2- La synchronisation projective est une autre forme spéciale de la synchronisation généralisée, elle est établie s'il existe une constante α telle que $\lim_{t\to\infty} |x_1(t) - \alpha x_2(t)| = 0$. Par ailleurs, la synchronisation retardée entre deux systèmes (1.8) et (1.9) est réalisée s'il existe un retard $\tau > 0$ tel que $lim_{t\to\infty}|x_1(t) - x_2(t-\tau)| = 0$.
3- Pour réaliser la synchronisation impulsive, un signal de sortie $y(t)$ du système maître de la forme (1.8) est envoyé au système esclave sous forme d'impulsions aux instants discrets prédéfinis.
4-La synchronisation adaptative concerne les systèmes maîtres présentant des incertitudes paramétriques ou des paramètres inconnus ; dans ce cas, l'objectif est de synchroniser les systèmes maître et esclave d'une manière adaptative et robuste en dépit de ces incertitudes.

La théorie de *commande des systèmes* a joué un rôle fondamental dans le développement des méthodes de synchronisation des systèmes chaotiques. Parmi ces techniques, on cite notamment la technique de synchronisation avec commande par retour d'état [15], la synchronisation par "backstepping" [16] et la synchronisation par observateurs [14], [17], [18]. L'approche de synchronisation par observateurs est l'approche qui nous intéresse particulièrement dans ce travail de thèse. La deuxième partie 1.3 de ce chapitre sera exclusivement consacrée à la théorie des observateurs non linéaires et leurs méthodes de synthèse. La connexion entre le problème de synchronisation et le problème d'estimation d'état a été bien mise en relief dans les références [19] et [20]. En effet, en examinant la définition de synchronisation maître-esclave 1.5, si on considère le système (1.9) comme étant un estimateur d'état (observateur) pour le système (1.8) conformément à la définition d'observation d'état donnée plus loin dans la section 1.3.1, alors on constate bien la liaison entre les deux définitions. Ainsi, le problème de synchronisation peut être examiné de ce point de vue comme étant un problème d'estimation d'état. Cette connexion entre les deux problèmes a ouvert la voie pour des nombreux travaux de recherche exploitant les propriétés des observateurs non linéaires dans les applications de

synchronisation des systèmes dynamiques, et plus particulièrement dans les applications de synchronisation des systèmes chaotiques pour la transmission sécurisée d'informations. Dans ce travail de thèse, nous avons développé différentes méthodologies de synchronisation de systèmes chaotiques à base d'observateurs non linéaires appliquées aux systèmes de communications dans divers scénarios pouvant exister en pratique tels que la présence de perturbations, d'incertitudes paramétriques, du bruit dans le canal public, de retards de transmission, etc. Comme nous allons voir dans les prochains chapitres, les techniques de synchronisation élaborées sont robustes et adaptatives et s'appuient sur différents types d'observateurs : des observateurs à entrées inconnues, des observateurs adaptatifs, des observateurs à modes glissants, des observateurs singuliers, etc. Dans la section suivante, nous nous intéressons au principe de transmission d'informations basé sur la synchronisation des systèmes chaotiques et nous faisons un tour d'horizon des techniques de communications traditionnelles.

1.2.4 Systèmes de communications basés sur la synchronisation des systèmes chaotiques

Dans cette section, on s'intéresse aux techniques de transmission sécurisée d'informations qui reposent sur le principe de synchronisation chaotique. Le point commun constaté dans la majorité des techniques développées dans la littérature est l'utilisation de la configuration maître-esclave pour laquelle on dispose d'un émetteur chaotique (système maître) qui génère le signal du texte chiffré transmis dans le canal de communication vers un système récepteur (système esclave) qui a pour objectif de synchroniser avec le système maître et de restaurer le signal d'information. Parmi les techniques de communications traditionnelles à base du chaos, on cite : le masquage chaotique [21], la modulation paramétrique [21], [22], la commutation chaotique [23], [24], le cryptage par injection [25], la transmission à deux voies [26] et le cryptage combiné [27].

1.2.4.1 Le masquage chaotique

Le masquage chaotique [21] est la technique de transmission d'information la plus simple et la plus élémentaire. La figure 1.5 illustre le principe de base de cette technique. Le signal d'information $M(t)$ de nature binaire ou analogique est additionné à un signal porteur chaotique $X(t)$ généré par le système émetteur. Le signal du texte chiffré $T(t)$ ainsi obtenu est transmis à travers le canal de transmission vers le système récepteur qui se synchronise identiquement avec le système maître. Le signal d'information reconstruit $M'(t)$ est obtenu après la soustraction entre le signal chiffré (transmis) $T(t)$ et le signal porteur estimé $X'(t)$.

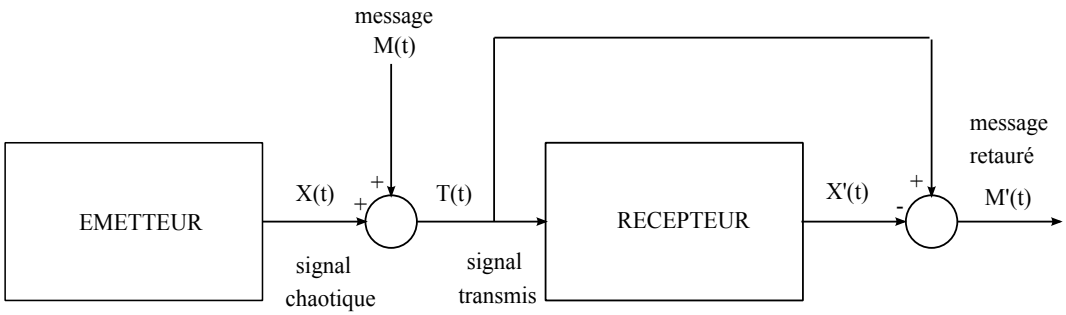

FIGURE 1.5: Schéma représentatif de la technique de masquage chaotique

Ce système est efficace seulement en absence du bruit de canal. Par ailleurs, la puissance du signal d'information doit être de 35 à 65 db moins élevée que le signal porteur en absence de bruit de canal et le spectre de fréquences du signal chaotique porteur doit être plus large que celui du signal du texte clair. En revanche, en utilisant un canal de transmission bruité et si l'émetteur chaotique présente des incertitudes paramétriques, les performances du système se dégradent considérablement et on peut même perdre la synchronisation entre les systèmes maître et esclave. De plus, du point de vue sécurité, il s'est avéré que cette technique est très fragile par rapport à diverses méthodes d'attaques.

1.2.4.2 La modulation paramétrique

Le principe de modulation paramétrique consiste à utiliser le signal d'information, généralement de nature binaire, pour moduler l'un des paramètres du système chaotique émetteur – voir [21], [22]. La figure 1.6 représente le schéma d'un système de communication utilisant cette technique. Le système récepteur synchronise d'une manière adaptative avec l'émetteur chaotique et le signal d'information est restauré par l'intermédiaire d'une loi d'adaptation. Cette technique peut être interprétée comme étant un problème d'estimation conjointe des états et des paramètres inconnus : le système récepteur est conçu à l'aide d'un observateur adaptatif pour le système émetteur.

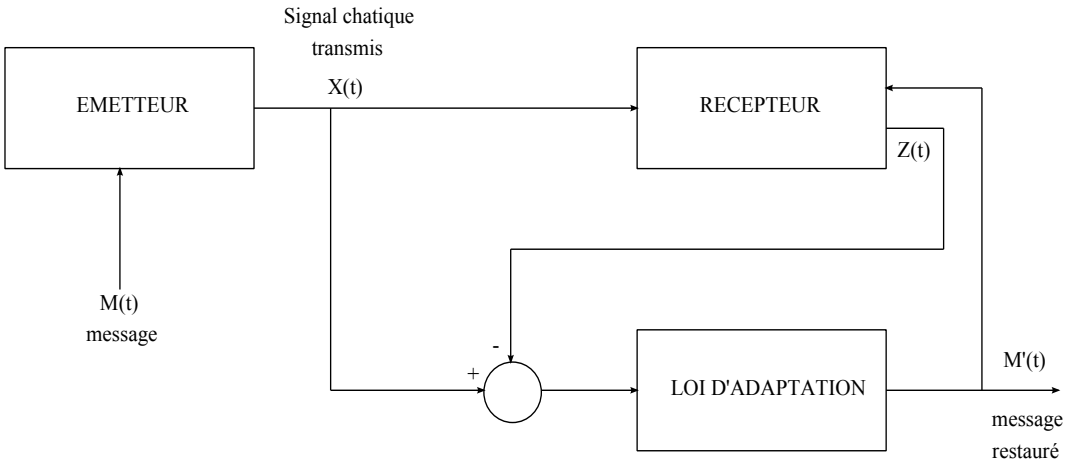

FIGURE 1.6: Schéma représentatif de la technique de modulation paramétrique

Afin de préserver le comportement chaotique du système maître, l'amplitude du signal d'information ne doit pas dépasser certaines valeurs limites. Notons également que la durée d'un bit du signal d'information doit être suffisamment long puisque la convergence du système récepteur passe par une période transitoire à chaque changement de bit. Cette technique s'est avérée également sensible à quelques techniques d'attaques [28]. Dans les chapitres 2 et 4, nous allons voir avec plus de détails comment des techniques similaires à la modulation paramétrique seront utilisées conjointement avec des méthodes de synchronisation à base d'observateurs adaptatifs pour garantir la transmission et la réception des messages de type binaire et constants par morceaux.

1.2.4.3 La commutation chaotique

Le schéma de principe de cette technique est représenté par la figure 1.7. Au niveau de l'émetteur, on dispose de deux oscillateurs générant les signaux chaotiques $A(t)$ et $B(t)$. Le signal d'information de type binaire $M(t)$ est utilisé pour commuter entre $A(t)$ encodant le bit 1 et $B(t)$ encodant le bit 0. Le signal résultant $X(t)$ est transmis à travers le canal de transmission vers le système récepteur constitué de deux système esclaves. Le premier système esclave synchronise exclusivement avec le premier oscillateur (correspondant au signal chaotique $A(t)$) de telle façon que le bit 1 est détecté par la convergence de l'erreur de synchronisation vers zéro et par conséquent le signal d'information peut être enfin restauré à la fin du processus de détection.

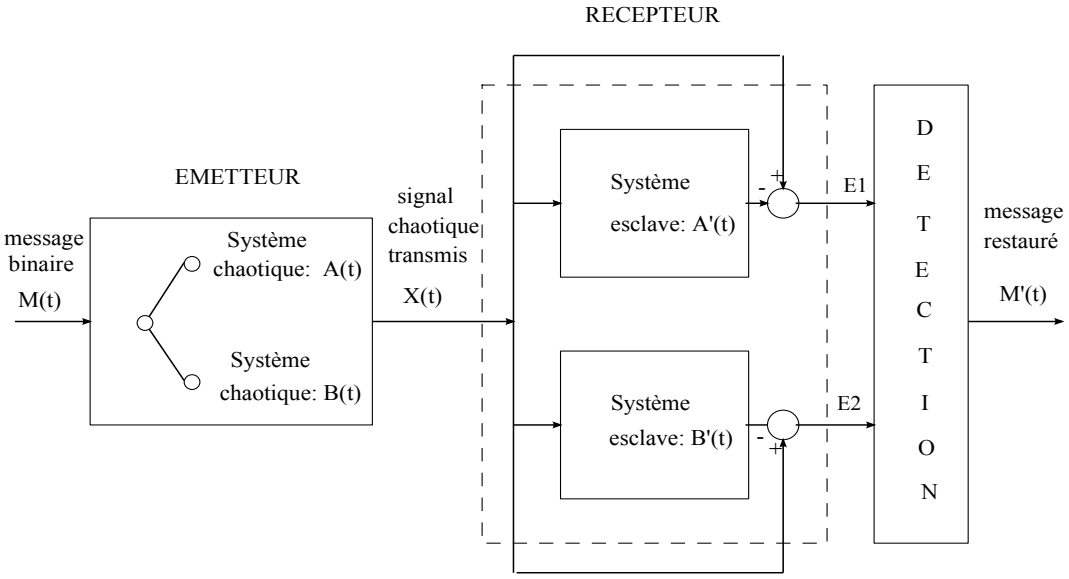

FIGURE 1.7: Schéma repréentatif de la technique de commutation chaotique

Comparée à la technique de masquage chaotique, la commutation chaotique présente relativement plus de robustesse au bruit de canal ; néanmoins, les cryptosystèmes utilisant cette technique possèdent une faible vitesse de transmission car à chaque changement de bit on doit tenir compte du temps de convergence nécessaire pour la mise en place de la synchronisation. Cette méthode est caractérisée par un faible niveau de sécurité puisqu'à chaque changement du niveau binaire, on peut

observer la modification du signal du texte chiffré, surtout lorsque les deux oscillateurs utilisés au niveau de l'émetteur possèdent deux attracteurs très différents – voir [23], [24].

1.2.4.4 Cryptage par injection

Le schéma de principe de cette technique est représenté dans la figure 1.8. Il s'agit d'injecter le signal d'information dans la dynamique de l'émetteur chaotique. Le récepteur a pour but de synchroniser avec l'émetteur et de reconstruire le signal d'information. Conformément au constat de Nijmeijer et Mareels [19], le système esclave peut être conçu sous la forme d'un observateur à entrées inconnues ou un observateur à modes glissants – Voir les sections 1.3.5 et 1.3.6.

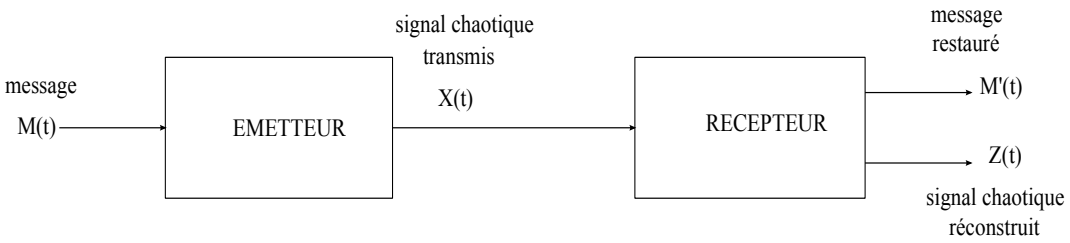

FIGURE 1.8: Schéma représentatif de la technique de cryptage par injection

Cette technique est valable pour transmettre un message de nature binaire ou analogique, mais la puissance de ce dernier doit être suffisamment petite pour ne pas détériorer le comportement chaotique du système maître. Cette technique présente un niveau de sécurité nettement élevé par rapport aux techniques précédentes puisque le signal d'information est masqué dans la dynamique du système maître et que le signal chaotique disponible dans le canal public ne porte pas l'information d'une manière directe comme dans le cas de la technique de masquage chaotique. Pour plus de détails, le lecteur peut consulter la référence [25].

1.2.4.5 Transmission à deux voies

Le schéma de principe de la transmission à deux voies est illustré dans la figure 1.9. L'idée de base consiste à séparer les tâches de synchronisation et de cryptage en utilisant deux voies de communication [26]. L'émetteur chaotique génère un signal chaotique $Y(t)$ transmis dans un premier canal de communication (Canal 1) vers le récepteur qui doit synchroniser avec le système maître. L'émetteur génère également un autre signal chaotique $X(t)$ utilisé par une fonction de cryptage qui produit le signal du texte chiffré $C(t)$ transmis dans un deuxième canal de transmission (Canal 2).

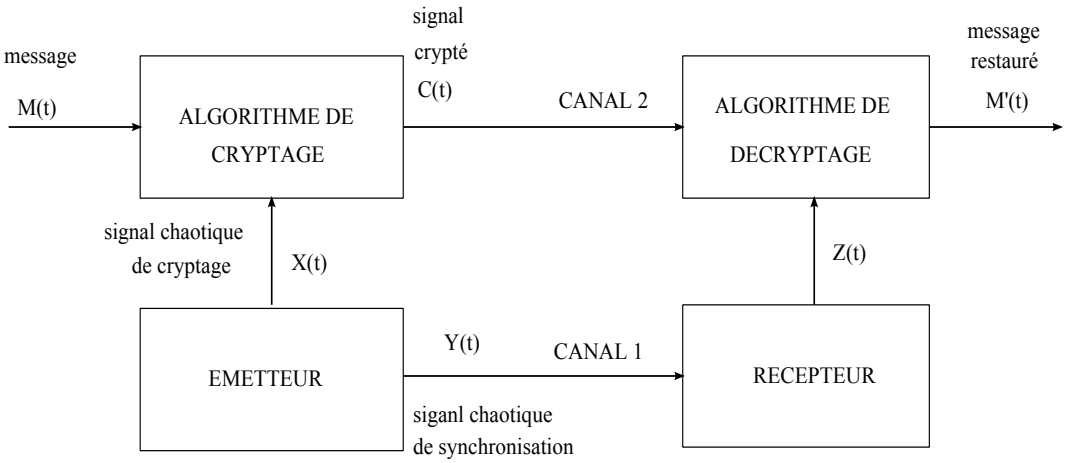

FIGURE 1.9: Schéma représentatif de la technique de transmission à deux voies

Grâce de cette indépendance entre les tâches de synchronisation et de cryptage, il n'y a pas de contrainte à imposer sur l'amplitude du signal d'information puisque dans ce cas, ce dernier n'agit ni sur la dynamique de l'émetteur chaotique ni sur le signal transmis $Y(t)$ contrairement aux autres techniques. De plus, le signal d'information n'a aucune influence sur l'opération de synchronisation qui s'établit d'une façon idéale, ce qui permet de garantir une meilleure qualité de l'image récupérée au niveau du récepteur. D'un autre côté, cette méthode garantit un meilleur niveau de sécurité par rapport aux autres techniques puisque la séparation entre les opérations de cryptage et de synchronisation permet de concevoir une fonction de cryptage de plus en plus complexe sans se soucier de détériorer l'aspect chaotique de l'émetteur ou de perdre la synchronisation entre les systèmes maître et esclave. Cependant, cette technique présente des mauvaises performances en présence du bruit de transmission puisque l'effet du bruit est doublé en agissant à la fois sur le signal transmis $Y(t)$ dans la première voie et également sur le signal du texte chiffré $C(t)$ présent dans la deuxième voie de transmission. Dans le chapitre 3, la technique de transmission à deux voies sera combinée avec la technique de cryptage par injection dans un système de communication utilisant des observateurs adaptatifs à modes glissants. Afin d'améliorer la sécurité du système, des modifications appropriées ont été apporté au niveau de l'architecture du schéma de communication tout en exploitant les avantages de deux techniques et en proposant une remède au problème de robustesse au bruit présent dans le canal public, qui représente l'inconvénient majeur de la technique de transmission à deux voies.

1.2.4.6 Cryptage combiné

Cette technique est un mixage entre les systèmes cryptographiques classiques et les systèmes de communication reposant sur le principe de synchronisation des systèmes chaotiques (voir la référence [27]). Le principe de cette méthode est illustré dans la figure 1.10. La fonction de cryptage utilise le signal d'information $M(t)$ et un signal chaotique de cryptage $X(t)$ généré par l'émetteur chaotique pour produire le signal crypté $C(t)$ réinjecté dans la dynamique de l'émetteur chaotique. Au niveau de la réception, un système esclave se synchronise avec le système maître et génère les signaux

$C'(t)$ et $Z(t)$ qui représentent les estimations respectives des signaux $C(t)$ et $X(t)$. Enfin, un algorithme de décryptage utilise les signaux obtenus pour restaurer le signal d'information en générant le signal $M'(t)$. Dans le chapitre 4, l'idée du cryptage combiné sera exploitée dans un système de communication sécurisée présentant des retards de transmission, tout en apportant quelques améliorations par rapport à l'architecture de base.

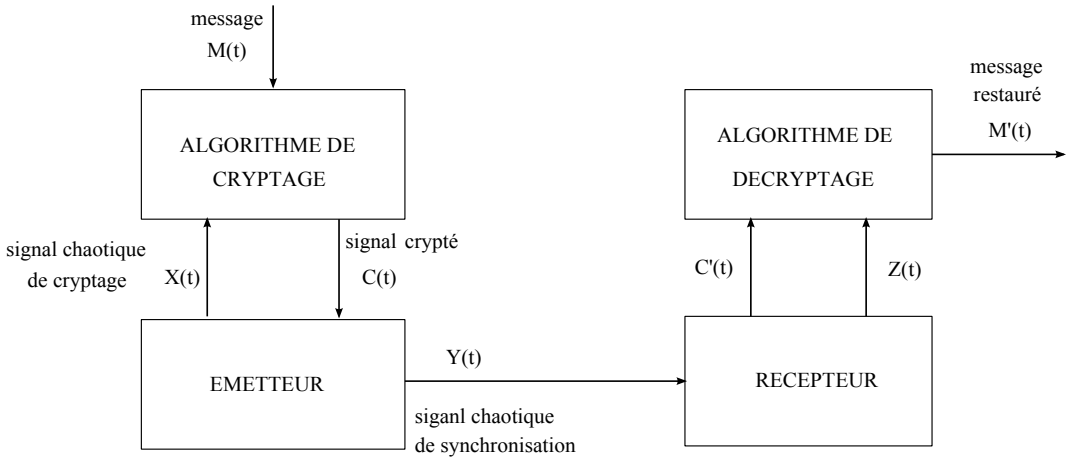

FIGURE 1.10: Schéma représentatif de la technique de cryptage combiné

Cette technique présente un bon niveau de sécurité grâce à la complexité de l'algorithme de cryptage, et plus de robustesse aux attaques cryptographiques.

1.2.5 Analyse de sécurité

1.2.5.1 Cryptanalyse et attaques cryptographiques

L'analyse de la sécurité (cryptanalyse) est une étape indispensable pour tester la robustesse du cryptosystème aux différentes attaques possibles, évaluer le niveau de sécurité du cryptosystème et corriger les éventuelles défaillances. Un cryptosystème doit avoir deux propriétés cryptographiques fondamentales : la confusion et la diffusion. La confusion consiste à rendre la relation entre le clé et le texte chiffré la plus complexe possible. La diffusion signifie qu'un petit changement dans le texte clair ou dans la clé, induit un grand changement dans le texte chiffré. Selon la référence [4], on considère quatre nivaux d'attaques :

1. *Attaque utilisant le texte chiffré choisi* : L'intrus accède temporairement aux algorithmes de décryptage, ainsi il peut choisir un texte chiffré $y \in \mathcal{C}$ et obtenir le texte clair correspondant $x \in \mathcal{P}$.

2. *Attaque utilisant le texte clair choisi* : L'intrus accède temporairement aux algorithmes de cryptage, il peut choisir un texte clair $x \in \mathcal{P}$ et obtenir le texte chiffré correspondant $y \in \mathcal{C}$.

3. *Attaque utilisant le texte clair connu* : L'intrus accède à un ou à plusieurs textes clairs $x_1, x_2, \ldots, x_n \in \mathcal{P}$ et les textes chiffrés correspondants $y_1, y_2, \ldots, y_n \in \mathcal{C}$.

4. *Attaque utilisant le texte chiffré uniquement* : L'intrus a accès uniquement à un ou plusieurs textes chiffrés $y_1, y_2, \ldots, y_n \in \mathcal{C}$.

L'objectif de chacune des ces attaques est de restaurer la clé secrète $k \in \mathcal{K}$. Selon le principe de Kerckhoff [29], la sécurité d'un cryptosystème doit dépendre uniquement de sa clé secrète. Un cryptosystème de bon niveau de sécurité doit posséder une clé secrète bien définie et ayant un espace clé suffisamment large. L'analyse de la clé secrète représente une tâche centrale dans la conception de tout système de communication sécurisée.
Tout d'abord, la clé secrète doit être définie d'une manière très précise. Ensuite, une caractérisation de l'espace clé doit être réalisée. La taille de l'espace clé $\mathcal{K}$ est définie par le nombre des paires des clés au niveau du cryptage et du décryptage. Ainsi, l'espace clé $\mathcal{K} = \{k_1, k_2, \ldots, k_r\}$ représente l'ensemble fini de clés possibles k_i, pour $i = 1..r$. La sécurité du cryptosystème dépend étroitement de la taille de l'espace clé. Une taille suffisamment large de l'espace clé représente une condition nécessaire (mais pas suffisante) pour détenir un système de communication sécurisée et robuste aux attaques à "force brute".
Dans [30], l'auteur définit trois critères de base que doit satisfaire un cryptosystème de " bon niveau de sécurité". Le premier critère est la sensibilité par rapport aux clés, $i.e$: modifier un bit dans une clé génère un texte chiffré complètement différent sachant que le texte clair restant inchangé. Le deuxième critère est la sensibilité par rapport au texte clair. Enfin, le troisième critère consiste à produire à partir du texte clair, un texte chiffré statistiquement aléatoire. Les deux premiers critères correspondent à la propriété de diffusion et le troisième critère correspond à la propriété de confusion.

1.2.5.2 Cryptanalyse spécifique aux systèmes de communications analogiques à base des systèmes chaotiques

Diverses méthodes d'attaques spécifiques au cryptosystèmes chaotiques analogiques ont été développées. Elles peuvent être classées en deux catégories :
1. *Les attaques basées sur l'analyse des caractéristiques du signal du texte chiffré* : parmi ces attaques, il y a celles qui permettent l'extraction directe du signal correspondant au texte clair (message) à partir du signal du texte chiffré disponible dans le canal public, ou bien celles qui permettent la restauration de la porteuse chaotique à partir du signal du texte chiffré afin d'extraire indirectement le texte clair.
2. *Les attaques basées sur l'identification de la structure et des paramètres du système émetteur* : le principe de ces attaques consiste à identifier les paramètres secrets de l'émetteur chaotique à partir du signal correspondant au texte chiffré disponible dans le canal de communication.

Parmi ces attaques, on cite la technique d'analyse de la puissance spectrale [31], [32], la méthode du plan de retour [33], la technique de synchronisation généralisée [34], etc.
La technique d'*analyse de puissance spectrale* est une méthode basique et efficace qui peut être appliquée à tout cryptosystème chaotique analogique puisqu'elle agit uniquement sur le signal du texte

chiffré et ne nécessite pas la connaissance de la structure du système émetteur. L'objectif de cette analyse est de vérifier si le spectre du signal d'information (texte clair) est constitué des fréquences moins élevées que celles retrouvées dans le spectre du signal porteur et que la densité de puissance de ce dernier est plus élevée que celle du signal d'information. De cette manière, le spectre du signal d'information est bien masqué par celui du signal porteur. Si ces conditions ne sont pas satisfaites, le cryptosystème n'est pas sécurisé et il est facile d'extraire le message par les techniques de filtrage.

Dans la technique de *plan de retour*, on trace le plan de phase (plan de retour) de $A_n = \frac{X_n+Y_n}{2}$ par rapport à $B_n = X_n - Y_n$, où X_n et Y_n représentent respectivement le n-ième maximum local et le n-ième minimum local du signal transmis du texte chiffré y. L'examen de l'attracteur ainsi tracé permet de détecter les éventuelles défaillances de sécurité. Par exemple, dans les systèmes de communication utilisant la technique de modulation paramétrique, il a été démontré dans [31], qu'une petite modification dans un paramètre de bifurcation entraîne deux bandes parallèles séparées par une fente dans le plan de phase, et par conséquent, il est possible de distinguer les variations paramétriques et d'extraire le message transmis. Cette méthode est également applicable sur les systèmes de communication à commutation (CSK) et les cryptosystèmes basés sur la technique de masquage chaotique.

La technique d'attaque basée sur la *synchronisation généralisée* introduite pour la première fois dans [34], contrairement aux méthodes précédentes, doit supposer la connaissance de la structure du système émetteur sans accéder aux valeurs exactes des paramètres, généralement utilisés comme clé secrètes. Dans la référence [28], cette technique a été utilisée pour attaquer un système de communication basé sur la technique de modulation paramétrique : afin d'extraire le texte clair (message), l'intrus construit un récepteur avec des paramètres choisis arbitrairement et calcule l'erreur de synchronisation en ligne, ensuite l'erreur de synchronisation est multipliée par le signal du texte chiffré et enfin un filtrage passe bas de fréquence de coupure appropriée permet de restaurer le signal d'information transmis.

La première partie du premier chapitre a été dévolue au problème de synchronisation des systèmes chaotiques et ses applications dans les systèmes de transmission sécurisée d'informations. Nous avons mentionné que le problème de synchronisation maître-esclave peut être considéré comme étant un problème d'estimation d'état. Dans la seconde partie du chapitre, nous nous intéressons à la théorie des observateurs non linéaires et nous faisons un tour d'horizon de leurs méthodes de synthèse.

1.3 Observateurs non linéaires

Dans cette section, nous présentons le contexte et les motivations du problème d'estimation d'état, nous abordons ensuite la notion de l'observabilité, une propriété importante qui doit être vérifiée avant toute synthèse d'observateurs et enfin nous faisons un tour d'horizon des méthodes de synthèse d'observateurs pour différentes classes des systèmes non linéaires.

1.3.1 Position du problème

Dans l'étude des phénomènes physiques, tous les signaux ne sont pas accessibles aux mesures, pour de différentes raisons techniques et économiques. Le problème d'estimation d'état est motivé par le besoin d'accéder aux informations implicites du système, à partir des signaux mesurables. En effet, l'accès à l'état du système est nécessaire dans diverses applications telles que la détection de défauts, la commande des systèmes, l'identification (modélisation), la synchronisation des systèmes dynamiques, etc.
Si le modèle en considération est défini par une représentation d'espace d'état, le problème consiste à concevoir un système dynamique auxiliaire qui permet d'estimer les variables d'état à partir des variables d'entrée et de sortie. Un tel système est appelé *observateur*.
Le problème de synthèse d'observateurs peut être formulé comme suit :
On considère le système non linéaire suivant

$$\begin{aligned} \dot{x} &= f(x,u,t) \\ y &= h(x,u,t), \end{aligned} \tag{1.11}$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée et $y \in \mathbb{R}^p$ représente le vecteur de sortie mesurée. Les fonctions f et h sont supposées de classe C^∞ .
Afin de produire l'estimation de x, on a besoin de concevoir deux fonctions Ψ et Φ telles que le système dynamique défini par les équations suivantes

$$\begin{aligned} \dot{\xi} &= \Psi(\xi,u,y,t) \\ \hat{x} &= \Phi(\xi,u,t), \end{aligned} \tag{1.12}$$

avec $\xi \in \mathbb{R}^s$, $s \leq n$, $\hat{x} \in \mathbb{R}^n$, vérifie les deux conditions suivantes [35] :
(C1) Si $x(0) = \hat{x}(0)$ donc $x(t) = \hat{x}(t)$, $\forall t \geq 0$,
(C2) $\lim_{t\to\infty} |x(t) - \hat{x}(t)| = 0$.
La condition (C2) signifie que $\hat{x}(t)$ converge asymptotiquement vers $x(t)$. On dit que le système (1.12) est un observateur asymptotique pour le système (1.11).
Si la convergence est exponentielle, l'observateur est dit *exponentiel*.
Si la condition (C2) est satisfaite $\forall x(0), \hat{x}(0)$, l'observateur est dit *global*.

Ce problème a été largement étudié dans la littérature et différentes approches ont été développées. La technique souvent employée dans la littérature consiste à concevoir une copie du système original en ajoutant un terme correctif $K(\cdot)$ dans la dynamique de l'observateur afin de corriger l'intégration de l'état estimé $\hat{x}(t)$ à partir de l'état initial $\hat{x}(0)$. Ce terme correctif utilise principalement l'information disponible fournie par l'erreur d'observation $y - h(\hat{x},u,t)$. Ainsi, les équations de l'observateur sont décrites par

$$\begin{aligned} \dot{\hat{x}} &= f(\hat{x},u,t) + K(t, y - h(\hat{x},u,t)), \\ \hat{y} &= h(\hat{x},u,t). \end{aligned} \tag{1.13}$$

Le problème d'observation, dans sa phase d'analyse, se ramène à étudier la stabilité au sens de Lyapunov de la dynamique de l'erreur d'observation $x - \hat{x}$.

1.3.2 Observabilité des systèmes non linéaires

Avant d'entamer l'étape de synthèse de l'observateur, les questions suivantes doivent être posées : Est ce qu'on a suffisamment d'informations disponibles (variables d'entrée et de sortie) pour nous permettre de concevoir l'observateur ? Est ce que l'état du système peut être déterminé d'une façon unique ? Il s'agit du problème d'analyse de l'*observabilité* des systèmes dynamiques. Dans cette section, nous présentons le principe d'observabilité des systèmes non linéaires ainsi que les notions et les définitions annexes.

Définition 1.6. [35] (Indiscernabilité)
Soient x_0 et x_1 deux conditions initiales du système (1.11). Soient $X_u(t, x_0)$ et $X_u(t, x_1)$ les solutions de l'équation d'état du système (1.11) correspondant aux états initiaux x_0 et x_1 respectivement. La paire (x_0, x_1) est dite indiscernable si :
$\forall u \in \mathbb{R}^m$, $\forall t \geq 0$, $h(X_u(t, x_0)) = h(X_u(t, x_1))$.
Un état x est indiscernable de x_0 si la paire (x, x_0) est indiscernable.

Définition 1.7. [35] (observabilité)
Un système (1.11) est dit observable en x_0 s'il n'existe aucun état indiscernable de x_0.
(1.11) est dit observable s'il n'admet aucune paire indiscernable.

Cependant, il est également indispensable d'analyser le problème en tenant compte des entrées et de vérifier s'il existent parmi elles, des entrées qui pourraient affecter l'observabilité du système. Ainsi, des conditions supplémentaires sont nécessaires pour étudier la faisabilité de synthèse de l'observateur indépendamment des entrées. C'est la notion d'*observabilité uniforme*.

Définition 1.8. [35] (Entrées universelles)
Soient x_0 et x_1 deux conditions initiales du système (1.11). Soient $X_u(t, x_0)$ et $X_u(t, x_1)$ les solutions de l'équation d'état du système (1.11) correspondant aux états initiaux x_0 et x_1 respectivement. L'entrée u est dite universelle si :
$\forall x_0 \neq x_1$, $\exists \tau > 0$ tel que $h(X_u(\tau, x_0)) \neq h(X_u(\tau, x_1))$.
Une entrée est singulière si elle n'est pas universelle.

Définition 1.9. [36] (Observabilité uniforme) Un système est uniformément observable si toutes ses entrées sont universelles.

Dans [36], une liaison a été établie entre les systèmes uniformément observables et leur transformation sous la forme canonique d'observabilité.
Afin de mieux comprendre la problématique, on considère le système suivant

$$\begin{aligned} \dot{x} &= f_0(x) + u_1 f_1(x) + \cdots + u_m f_m(x), \\ y &= h(x), \end{aligned} \tag{1.14}$$

et la transformation

$$T(x) = \begin{bmatrix} h(x) \\ L^1_{f0}(h)(x) \\ \vdots \\ L^{n-1}_{f0}(h)(x) \end{bmatrix}$$

où

$$L^k_{f_0}(h)(x) = L_{f_0}[L^{k-1}_{f_0}(h)(x)], \quad k = 1, 2, \ldots, n, \tag{1.15}$$

où $L^k_{f_0}(h)$ est la ième-dérivée de Lie de h dans la direction de f_0, et $L^0_{f_0}(h) = h$.

Théorème 1.10. *[36] Si le système (1.14) est uniformément observable, alors il existe un sous-ensemble $M \subset \mathbb{R}^n$ ouvert et dense tel que, $\forall x^0 \in M$, il existe un voisinage V, tel que la transformation T est un difféomorphisme de V dans son domaine.*
En plus, T transforme le système (1.14), restreint dans V, en un système ayant la forme canonique suivante

$$\begin{aligned} \dot{z} &= Az + \eta_0(z) + \textstyle\sum_{i=1}^m \eta_i(z) u_i \\ y &= Cz, \end{aligned} \tag{1.16}$$

avec

$$A = \begin{pmatrix} 0 & 1 & \ldots & 0 \\ 0 & 0 & 1 & \vdots \\ \vdots & \vdots & \ldots & 1 \\ 0 & \ldots & \ldots & 0 \end{pmatrix}, \quad \eta_0(z) = \begin{pmatrix} 0 \\ \vdots \\ \eta_n(z) \end{pmatrix}, \quad \eta_k(z) = \begin{pmatrix} \eta_{k1}(z_1) \\ \eta_{k2}(z_1, z_2) \\ \vdots \\ \eta_{ki}(z_1, \ldots, z_i) \\ \vdots \\ \eta_{kn}(z) \end{pmatrix} \text{ et } \quad C = \begin{pmatrix} 1 & 0 & \ldots & 0 \end{pmatrix}.$$

Inversement, si le système (1.14) est transformable sous la forme canonique (1.16), donc le système est uniformément observable dans le domaine de définition du difféomorphisme.

Après l'analyse de l'observabilité, on passe à l'étape de conception de l'observateur. Dans la littérature, il existe diverses méthodes de synthèse d'observateurs pour plusieurs classes des systèmes non linéaires. Dans la section suivante, nous présentons une liste non exhaustive des méthodes spécifiques aux systèmes non linéaires continus parmi lesquelles les méthodes standards et celles qui sont en liaison directe avec ce travail de thèse.

1.3.3 Différentes approches de synthèse des observateurs non linéaires

Le problème d'estimation d'état a été étudié depuis les années soixante par Luenberger [37] et Kalman [38] pour une classe des systèmes linéaires continus déterministes et une classe des systèmes linéaires stochastiques, respectivement.

On considère le système linéaire ayant la forme suivante

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y &= Cx. \end{aligned} \tag{1.17}$$

Dans le cas où (1.17) est un système linéaire à temps invariant (A, B et C sont des matrices constantes), Luenberger propose l'observateur suivant

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + Bu + L(y - C\hat{x}) \\ \hat{y} &= C\hat{x}. \end{aligned} \tag{1.18}$$

Si le système (1.17) est observable, il suffit, pour que l'erreur d'observation $e = x - \hat{x}$ converge asymptotiquement vers 0, de choisir la matrice de gain L telle que les valeurs propres de la matrice $A - LC$ soient à partie réelle strictement négative [37], et qui peuvent être convenablement sélectionnées en utilisant la méthode de placement des pôles.
Cependant, dans le cas où le système (1.17) est un système linéaire à temps variant ($A := A(t)$, $B := B(t)$ et $C := C(t)$) sont des matrices qui dépendent du temps), l'observateur proposé par Kalman possède la même structure que celle de l'observateur de Luenberger (1.18) où $L := L(t)$ est à temps variant. Si (1.17) est observable et que les matrices $A(t)$, $C(t)$ sont bornées, alors il suffit de choisir $L(t)$ telle que [35]

$$\begin{aligned} \dot{\Upsilon}(t) &= \Upsilon(t)A^T(t) + A(t)\Upsilon(t) - \Upsilon C^T(t)W^{-1}(t)C(t)P(t) + V(t) + \lambda\Upsilon(t) \\ L(t) &= \Upsilon(t)C^T(t)W^{-1}(t) \\ \Upsilon(0) &= \Upsilon^T(0) > 0, \end{aligned} \tag{1.19}$$

où $V(t)$, $W(t)$ et $\Upsilon(t)$ sont des matrices symétriques définies positives. le paramètre λ est choisi tel que $\lambda > 2\,|A(t)|$, $\forall t$.

Les approches de synthèse d'observateurs linéaires ont fortement inspiré les chercheurs pour généraliser les méthodes déjà développées au cas non linéaire. En effet, on trouve que, dans des nombreuses références, la structure de base des observateurs non linéaires proposés est celle de l'observateur de Luenberger, ensuite la tâche la plus complexe consiste à faire face au termes non linéaires afin d'assurer la convergence de l'erreur d'observation. Les approches qui ont été développées sont étroitement liées à la nature et aux propriétés des termes non linéaires dont on associe des hypothèses supplémentaires telles que la *condition de Lipschitz* et la propriété de *restriction de pente*. Par exemple, les observateurs proposés dans [39] ainsi que les observateurs développés plus récemment dans les références [40] et [41] appartiennent à cette catégorie d'observateurs.

1.3.3.1 Synthèse d'observateur pour une classe de systèmes non linéaires satisfaisant la condition de Lipschitz

Une classe de systèmes non linéaires qui a attiré l'attention des chercheurs dans la littérature des observateurs non linéaires est représentée par les équations suivantes

$$\begin{aligned} \dot{x} &= Ax + f(x,u,t) + g(y,u,t) \\ y &= Cx, \end{aligned} \tag{1.20}$$

où $x \in \mathbb{R}^n$ représente le vecteur d'état, $u \in \mathbb{R}^m$ représente le vecteur d'entrée et $y \in \mathbb{R}^p$ est le vecteur de sortie mesurée. A et C sont des matrices constantes.

Hypothèse 1.11. *La fonction $f(x,u,t)$ est globalement Lipschitzienne en x uniformément en u et t, i.e : il existe une constante $c > 0$ telle que*

$$|f(\xi_1,u,t) - f(\xi_2,u,t)| \leq c\,|\xi_1 - \xi_2|\,, \quad \forall \xi_1,\xi_2 \in \mathbb{R}^n. \tag{1.21}$$

Ces systèmes peuvent contenir différents types des non-linéarités, notamment les fonctions trigonométriques utilisées dans plusieurs applications en robotique et les fonctions polynomiales (cubiques, carrés, etc.). La fonction $f(x,u,t)$ peut être également considérée comme étant une perturbation affectant le système. D'autre part, un système dont la fonction non linéaire est de classe $\mathcal{C}^1$ et dont la solution est globalement bornée, peut être transformé en utilisant les méthodes parfois nommées *techniques d'extension de Lipschitz*, afin d'appartenir à la classe des systèmes (1.20) satisfaisant la condition de Lipschitz. Ainsi, on remarque bien que cette classe des systèmes couvre plusieurs types des systèmes non linéaires et diverses applications. Un observateur pour le système de la forme (1.20) et satisfaisant l'hypothèse (1.11) a été développé pour la première fois par Thau qui a présenté, dans la référence [39], une condition suffisante pour garantir la convergence asymptotique de l'observateur. L'observateur proposé a la structure suivante :

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + f(\hat{x},u,t) + g(y,u,t) + L(y - C\hat{x}), \\ \hat{y} &= C\hat{x}. \end{aligned} \tag{1.22}$$

Le résultat de son travail est présenté dans le théorème suivant.

Théorème 1.12. *[39] L'erreur d'observation $e := x - \hat{x}$ converge asymptotiquement vers zéro si la matrice de gain L vérifie la condition :*

$$c \leq \frac{\lambda_{min}(Q)}{2\lambda_{max}(P)}, \tag{1.23}$$

où P et Q sont deux matrices définies positives telles que

$$(A - LC)^T P + P(A - LC) = -Q. \tag{1.24}$$

Le résultat de Thau a motivé par la suite plusieurs autres chercheurs qui ont essayé d'améliorer la méthode de conception de l'observateur et de relaxer les conditions utilisées. Dans la référence [42], les auteurs proposent un algorithme pour résoudre une équation algébrique de Riccatti décrite par l'équation

$$AP + PA^T + P(\gamma^2 I - \frac{1}{\varepsilon} C^T C)P + I + \varepsilon I = 0, \tag{1.25}$$

dont une solution $P = P^T > 0$ engendre un choix de la matrice de gain L telle que $L = \frac{1}{2\varepsilon} P C^T$. Ensuite, dans [43], ce problème a été traduit en un problème de minimisation H_∞ et un algorithme itératif a été développé pour la synthèse de l'observateur. Plus récemment, dans la référence [44], un nouveau problème d'optimisation LMI a été étudié pour la conception d'un observateur H_∞ dans le cas de présence des perturbations dans la dynamique du système en considération.

1.3.3.2 Méthode basée sur la transformation en systèmes linéaires à paramètres variants

Cette approche a été introduite par Zemouche et al dans [41]. L'approche est basée sur l'utilisation du théorème des accroissements finis pour la synthèse d'observateurs pour une classe de systèmes présentant des non-linéarités de classe C^1 et satisfaisant la condition de Lipschitz en partant de l'idée de transformer le système de l'erreur d'observation sous la forme d'un système linéaire à paramètres variants (LPV). Le système considéré est décrit par les équations suivantes

$$\begin{aligned} \dot{x} &= Ax + Bf(x, y, u) \\ y &= Cx, \end{aligned} \tag{1.26}$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée et $y \in \mathbb{R}^p$ est le vecteur de sortie. A, B et C sont des matrices constantes. La fonction $f : \mathbb{R}^n \times \mathbb{R}^p \times \mathbb{R}^m \to \mathbb{R}^q$ est supposée différentiable en x.

Hypothèse 1.13. *La matrice Jacobienne de f vérifie la condition suivante*

$$a_{ij} \leq \frac{\partial f_i}{\partial X_j}(X, y, u) \leq b_{ij}, \quad \forall X \in \mathbb{R}^n, \quad \forall y \in \mathbb{R}^p, \quad \forall u \in \mathbb{R}^m, \tag{1.27}$$

avec

$$a_{ij} = \min_{Z \in \mathbb{R}^n \times \mathbb{R}^p \times \mathbb{R}^m} \frac{\partial f_i}{\partial X_j}(Z), \qquad b_{ij} = \sup_{Z \in \mathbb{R}^n \times \mathbb{R}^p \times \mathbb{R}^m} \frac{\partial f_i}{\partial X_j}(Z). \tag{1.28}$$

L'observateur proposé a la forme standard suivante

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + Bf(\hat{x}, y, u) + L(y - C\hat{x}), \\ \hat{y} &= C\hat{x}, \end{aligned} \tag{1.29}$$

où $\hat{x}$ est l'estimation de x. Soit $e = x - \hat{x}$ l'erreur d'observation.
On définit un ensemble convexe $C_o(a, b) := \{\lambda a + (1 - \lambda)b, \quad 0 \leq \lambda \leq 1\}$.

En appliquant le théorème des accroissements finis [41], il existe $z_i \in Co(x, \hat{x})\,;\ i = 1..q$ tels que

$$f(x) - f(\hat{x}) = \sum_{i,j=1}^{q,n} e_q(i) e_n^T(j) h_{i,j} e, \tag{1.30}$$

où $e_k(i) := (0, \ldots, 0, 1, 0, \ldots, 0)^T \in \mathbb{R}^k$ est un vecteur de la base canonique de $\mathbb{R}^k$ et 1 est le i^{ieme} élément de $e_k(i)$. Soit $h := (h_{11}, \ldots, h_{1n}, \ldots, h_{qn})$, avec $h_{i,j} = \frac{\partial f_i}{\partial x_j}(z_i, y, u)$.
Par conséquent, la dynamique de l'erreur d'observation peut s'écrire sous la forme d'un système linéaire à paramètres variants (LPV) :

$$\dot{e} = [\mathcal{A}(h(t)) - LC]e, \tag{1.31}$$

avec $\mathcal{A}(h(t)) := A + B \sum_{i,j=1}^{q,n} e_q(i) e_n^T(j) h_{i,j}(t)$.

Ainsi, Le problème de conception de l'observateur pour le système (1.26) est transformé en un problème d'analyse de stabilité d'un système à paramètres variants (1.31). La démonstration de la stabilité asymptotique est effectuée en appliquant la théorie de Lyapunov, en choisissant une fonction de Lyapunov appropriée et en utilisant le principe de convexité. Le résultat est résumé dans le théorème suivant.

Théorème 1.14. *[41] L'erreur d'observation $e(t)$ converge asymptotiquement vers zéro s'il existe une matrice P définie positive et une matrice R de dimensions appropriées telles que les inégalités matricielles linéaires (LMIs) suivantes soient satisfaites*

$$\textit{Block-diag}(\Gamma(\alpha^1), \ldots, \Gamma(\alpha^{2^{qn}})) < 0 \tag{1.32}$$

$$\Gamma(\alpha^r) = \mathcal{A}^T(\alpha^r)P - C^T S + P\mathcal{A}(\alpha^r) - S^T C, \quad r = 1..2^{qn}. \tag{1.33}$$

La matrice de gain L est donnée par $L = P^{-1}S$.

Cette approche a été également appliquée pour les systèmes discrets et une extension du résultat a été réalisée pour tester la performance H_∞ en présence des bruits. L'avantage principal qui peut être tiré de l'approche basée sur la transformation en systèmes à paramètres variants est le fait qu'elle présente de bonnes performances dans le cas où la constante de Lipschitz prend de grandes valeurs. En plus, avec la méthode de conception de l'observateur basée sur la résolution des LMIs (1.33), on a plus de marge de manœuvre pour éviter les grands gains.

1.3.3.3 Méthode basée sur la propriété du secteur et sur le critère du cercle

Dans [40], Arcak et Kokotović proposent un observateur global pour une classe des systèmes avec des non-linéarités monotones. Leur méthode évite la condition de Lipschitz, cependant elle utilise une nouvelle restriction qui consiste à supposer que la non-linéarité est non décroissante. L'idée principale est de représenter le système de l'erreur d'observation sous la forme d'une interconnexion entre un

système linéaire et une non-linéarité variant dans le temps et satisfaisant la propriété du secteur. Ensuite, il faut résoudre une inégalité matricielle linéaire (LMI) afin de choisir les matrices de gain de l'observateur tel que le critère de cercle soit vérifié. Le système considéré possède la structure suivante

$$\begin{aligned} \dot{x} &= Ax + G\gamma(Hx) + \rho(y,u) \\ y &= Cx, \end{aligned} \tag{1.34}$$

où $x \in \mathbb{R}^n$ représente le vecteur d'état, $u \in \mathbb{R}^m$ représente le vecteur d'entrée et $y \in \mathbb{R}^p$ est le vecteur de sortie mesurée. La non-linéarité $\gamma(Hx) = [\gamma_1, \gamma_2, \ldots, \gamma_r]$ avec :

$$\gamma_i := \gamma_i(\sum_{j=1}^{n} H_{ij} xj), \quad i = 1, \ldots, r. \tag{1.35}$$

D'après [40], la non-linéarité $\gamma(Hx)$ doit satisfaire la condition du secteur suivante :

Hypothèse 1.15. *Pour $i = 1, \ldots, r$, $\gamma_i(\cdot)$ est non décroissante. Ainsi, $\forall \xi_1, \xi_2 \in \mathbb{R}$*

$$(\xi_1 - \xi_2)[\gamma_i(\xi_1) - \gamma_i(\xi_2)] \geq 0 \tag{1.36}$$

On considère l'observateur suivant pour le système (1.34) :

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + L(C\hat{x} - y) + G\gamma(H\hat{x} + K(C\hat{x} - y)) + \rho(y,u) \\ \hat{y} &= C\hat{x}. \end{aligned} \tag{1.37}$$

Les matrices de gain de l'observateur $K \in \mathbb{R}^{n\times p}$ et $L \in \mathbb{R}^{n\times p}$ sont à déterminer.
La dynamique de l'erreur d'observation $e = \hat{x} - x$ est décrite par l'équation

$$\dot{e} = (A + LC)e + G[\gamma(\xi_1) - \gamma(\xi_2)], \tag{1.38}$$

avec $\xi_1 := Hx$ et $\xi_2 := H\hat{x} + K(C\hat{x} - y)$.
Soient $z := \xi_1 - \xi_2$ et $\phi(t,z) := \gamma(v) - \gamma(w)$. Le système de l'erreur d'observation est réécrit sous la forme

$$\begin{aligned} \dot{e} &= (A + LC)e + G\phi(t,z) \\ z &= (H + KC)e. \end{aligned} \tag{1.39}$$

En utilisant l'hypothèse (1.15), on en déduit que chaque composante $\phi_i(t, z_i)$ de la non-linéarité $\phi(t,z)$ vérifie la condition de secteur suivante

$$z_i \phi_i(t, z_i) \geq 0, \quad \forall z_i \in \mathbb{R}. \tag{1.40}$$

On déduit que $\phi(t,z)^T \Lambda z$ est non négative $\forall \Lambda > 0$. En appliquant le critère de cercle, la stabilité asymptotique est garantie s'il existe une matrice définie positive P, une constante $\varepsilon > 0$ et une matrice diagonale $\Lambda > 0$ telles que

$$\begin{bmatrix} (A + LC)^T P + P(A + LC) + \varepsilon I & PG + (H + KC)^T \Lambda \\ G^T P + \Lambda(H + KC) & 0 \end{bmatrix} \leq 0 \tag{1.41}$$

Ce résultat a été étendu, dans [40], pour une classe de systèmes ayant la structure (1.34) sachant que le signal de sortie et la fonction $\gamma(\cdot)$ sont des scalaires, et que l'hypothèse (1.15) est remplacée par l'hypothèse suivante qui est moins contraignante :

Hypothèse 1.16. *Il existe $a, b \geq 0$ tels que $\gamma : \mathbb{R} \to \mathbb{R}$ vérifie :*

$$a \leq \frac{\gamma(\xi_1) - \gamma(\xi_2)}{\xi_1 - \xi_2} \leq b, \quad \forall \xi_1, \xi_2 \in \mathbb{R}, \quad \xi_1 \neq \xi_2. \tag{1.42}$$

D'après cette hypothèse, on peut déduire que $\gamma(\cdot)$ est globalement Lipschitzienne si $-a = b > 0$ et non décroissante si $a = 0$ et $b = +\infty$. D'autre part, si $\gamma(\cdot)$ est différentiable avec une pente vérifiant $a \leq \frac{\partial \gamma(\xi)}{\partial \xi} \leq b$, $\forall \xi \in \mathbb{R}$, alors elle vérifie la condition (1.16).

Théorème 1.17. *Considérons le système (1.34) et l'observateur (1.37). Supposons que l'hypothèse 1.16 est vérifiée. Si, en outre, il existe une matrice définie positive P et une constante $\varepsilon > 0$ telles que*

$$\begin{bmatrix} (A+LC)^T P + P(A+LC) + \varepsilon I & PG + (H+KC)^T \Lambda \\ G^T P + \Lambda(H+KC) & -\frac{2}{b} \end{bmatrix} \leq 0 \tag{1.43}$$

alors, l'erreur d'observation $e = x - \hat{x}$ converge exponentiellement vers zéro, c'est à dire qu'il existe deux constantes κ et β tels que $|e(t)| \leq \kappa |e(0)| e^{-\beta t}$, $\forall t \geq 0$

On remarque que l'inégalité (1.43) est moins restrictive que (1.41) grâce au terme $-\frac{2}{b}$ et si $b = +\infty$, on retrouve donc l'inégalité (1.41). La méthode d'Arcak a été appliquée pour la commande des systèmes (1.34) à base de l'observateur (1.37). Le problème a été également analysé dans le cas de présence de perturbations et d'erreurs de modélisation des non-linéarités [40]. Dans la référence [45], une extension de cette méthode a été effectuée dans le cas d'existence des paramètres inconnus (constants) en proposant un observateur adaptatif ayant la structure de base (1.37) associée à une loi d'adaptation. Plus récemment, dans [46], les auteurs proposent une méthode unifiée de synthèse d'un observateur H_∞ adaptatif pour une classe des systèmes présentant des non-linéarités monotones et Lipschitziennes. L'idée de base consiste à combiner la méthode d'Arcak avec l'approche présentée dans [41] basée sur le théorème d'accroissements finis et la transformation en un système à paramètres variants (LPV).

Remarque 1.18. Les conditions de "Lipschitz" et de "restriction de pente" sont particulièrement satisfaites pour plusieurs modèles des systèmes chaotiques. Comme nous allons le détailler dans les prochains chapitres, nous allons utiliser ces deux hypothèses dans les différentes méthodes de synchronisation élaborées, tout en essayant de relaxer le conservatisme sur les inégalités matricielles linéaires : par exemple, dans les chapitres 2 et 3, nous allons utiliser des techniques adaptatives afin de compenser l'effet des constantes de Lipschitz qui sont supposées inconnues et qui peuvent éventuellement prendre des larges valeurs.

1.3.3.4 Observateurs à grand gain

Dans cette section, nous reconsidérons la classe des systèmes uniformément observables étudiée dans la section 1.3.2. Nous avons expliqué que ces systèmes peuvent être transformés localement sous la forme canonique d'observabilité. Dans la référence [36], Gauthier et al. ont développé un algorithme garantissant la convergence exponentielle de l'erreur d'observation vers zéro et dont le réglage de la vitesse de convergence est effectué d'une façon arbitraire. Cet algorithme est bien connu sous le nom d'*observateur à grand gain*. Dans ce qui suit, nous rappelons les étapes de synthèse de cet observateur.
On considère le système ayant la forme canonique de l'observabilité :

$$\begin{aligned} \dot{x} &= Ax + \eta(x,u) \\ y &= Cx, \end{aligned} \tag{1.44}$$

avec

$$A = \begin{pmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & 1 & \vdots \\ \vdots & \vdots & \dots & 1 \\ 0 & \dots & \dots & 0 \end{pmatrix}, \quad \eta(x,u) = \begin{pmatrix} \eta_1(x_1,u) \\ \eta_2(x_1,x_2,u) \\ \vdots \\ \eta_n(x,u) \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix}.$$

La classe des systèmes (1.44) est plus générale que celle des systèmes (1.14) étudiée dans la section 1.3.2 puisque la non-linéarité $\eta(u,x)$ n'est pas nécessairement affine en u. Les deux hypothèses suivantes sont utilisées pour la synthèse de l'observateur à grand gain.

Hypothèse 1.19. *La fonction $\eta(u,x)$ est globalement Lipschitzienne en x uniformément en u, i.e : il existe $c > 0$ tel que*

$$|\eta(\xi_1,u) - \eta(\xi_2,u)| \leq c\,|\xi_1 - \xi_2|\,, \qquad \forall \xi_1, \xi_2 \in \mathbb{R}. \tag{1.45}$$

Un observateur pour le système (1.44) possède la forme :

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + \eta(\hat{x},u) + \Delta_\delta(C\hat{x} - y) \\ \hat{y} &= C\hat{x}, \end{aligned} \tag{1.46}$$

avec $\Delta_\delta = Diag(\delta, \delta^2, \dots, \delta^n)$ et $K = (k_1, k_2, \dots, k_n)^T$.

Théorème 1.20. *Le système (1.46) est un observateur exponentiel pour le système (1.44), i.e : il existe $\delta_0 > 0$ tel que $\forall \delta > \delta_0$, $\exists \alpha > 0$, $\exists \beta > 0$, $\forall \hat{x}(0)$,*

$$|\hat{x}(t) - x(t)| \leq \alpha e^{-\beta t}\,|\hat{x}(0) - x(0)|\,, \tag{1.47}$$

si l'hypothèse 1.19 est satisfaite et si la matrice $A + KC$ est Hurwitz.

La forme triangulaire et la condition de Lipschitz jouent un rôle capital dans la démonstration du théorème (Voir démonstration détaillée dans [35]). La vitesse de convergence de cet observateur peut être ajustée arbitrairement ; en effet, β dépend de δ et $\lim_{\delta\to+\infty}\beta(\delta)=0$.
Plusieurs extensions de ce résultat ont été réalisées. En particulier, le résultat a été généralisé dans la référence [47] pour le cas des systèmes uniformément observables multi-sorties. Plus récemment, dans [48], un observateur à grand gain a été développé pour une classe des systèmes multi-entrées, multi-sorties présentant des incertitudes. Le système considéré est composé d'une chaine de sous-systèmes tels que la dérivée de la dernière composante de chaque sous-système peut dépendre de tout l'état. La convergence de cet observateur est exponentielle en absence d'incertitudes ; et en cas de présence d'incertitudes, l'erreur d'observation peut être arbitrairement réduite en agissant sur le gain de l'observateur.

Par ailleurs, Praly propose, dans [49], un nouvel observateur à grand gain pour une classe des systèmes non linéaires sous la forme canonique de l'observabilité sachant que les termes non linéaires vérifient l'hypothèse suivante :

Hypothèse 1.21. *Pour $i=1..n$, pour tout $u\in\mathbb{R}^q$, pour tout $x\in\mathbb{R}^n$ et $\xi\in\mathbb{R}^n$,*

$$|\eta_i(x_1,x_2+\xi_2,\dots,x_i+\xi_i,u)-\eta_i(x_1,x_2,\dots,x_i,u))\leq\gamma(y_1)(|\xi_2|+\cdots+|\xi_i|)|\,. \tag{1.48}$$

Notons que la condition 1.48 est analogue à la condition de Lipschitz sauf que la "constante de Lipschitz" n'est pas constante mais dépend du signal de sortie y_1. Afin de compenser l'effet des termes non linéaires, une loi d'adaptation conçue sous la forme d'une équation de Riccatti est utilisée pour modifier le gain de l'observateur en ligne. L'observateur ainsi développé est le suivant :

$$\begin{aligned}
\dot{\hat{x}}_1 &= \eta_1(y_1)+\hat{x}_2+k_1r(y_1-\hat{x}_1)\\
\dot{\hat{x}}_2 &= \eta_2(y_1,\hat{x}_2,u)+\hat{x}_3+k_2r^2(y_1-\hat{x}_1)\\
&\vdots\\
\dot{\hat{x}}_n &= \eta_n(y_1,\hat{x}_2,\dots,\hat{x}_n,u)+\hat{x}_2+k_nr^n(y_1-\hat{x}_1)\\
\dot{r} &= -\frac{1}{b}r\Big(\frac{a}{3}(r-1)-\frac{2(p-1)}{\sqrt{q}}\gamma(y_1)\Big).
\end{aligned} \tag{1.49a}$$

L'observateur (1.49a) a été employé pour la stabilisation asymptotique à base d'une commande par retour de sortie. Plus récemment, dans [50], les auteurs proposent un nouvel observateur à grand gain avec un gain mis à jour en ligne et des termes correctionnels homogènes, permettant des meilleures performances sous des conditions moins restrictives.

Dans les méthodes présentées précédemment, les modèles des systèmes non linéaires considérés sont exactement connus. Nous nous intéressons maintenant aux cas où surgissent des perturbations, des bruits de mesures, des paramètres inconnues. Ces imperfections se produisent particulièrement dans les systèmes de communication basés sur la synchronisation maître-esclave avec transmission et restauration des informations transmises (problème d'estimation conjointe des états et des entrées

inconnues), en présence des perturbations et incertitudes au niveau du système émetteur, du bruit dans le canal de communication, etc. Dans le reste de ce chapitre, nous exposons des méthodes de synthèse d'observateurs utilisant des stratégies robustes et adaptatives tels que les observateurs adaptatifs, les observateurs à entrées inconnues, les observateurs singuliers et les observateurs par modes glissants.

1.3.4 Observateurs non linéaires adaptatifs

D'après ce qui précède, la structure et les paramètres des systèmes considérés sont exactement déterminés et les modèles étudiés ne présentent ni d'incertitudes, ni d'erreurs de modélisation. Néanmoins, dans les systèmes physiques paramétriques, on a souvent besoin d'estimer les paramètres inconnus : ce problème a été étudié dans le cadre d'*identification* des systèmes. Ce besoin s'impose également dans les applications où surgissent des incertitudes paramétriques, en particulier dans les applications de détection de défauts. Plus récemment, l'idée d'estimation des paramètres inconnus a été exploitée dans les applications des communications dans lesquelles on utilise la technique de modulation paramétrique qui consiste à moduler l'un des paramètres du système émetteur par l'information de type binaire à transmettre. En particulier, nous proposons dans les chapitres 2 et 4, des méthodes de synchronisation basées sur des observateurs adaptatifs et leur utilisation pour la transmission des informations en se basant sur la technique de modulation paramétrique.

Une alternative pour résoudre le problème de synthèse d'observateurs adaptatifs consiste à considérer les paramètres inconnus comme des variables d'état constants ; ainsi, le problème est ramené au cas des systèmes étudiés dans la section précédente et par conséquent, on peut appliquer l'une des méthodes présentées auparavant. L'inconvénient majeur de cette approche, qui réduit considérablement son applicabilité, consiste au fait qu'en augmentant le vecteur d'état par les paramètres inconnus, les propriétés structurelles du système telles que les propriétés détectabilité et l'observabilité peuvent se perdre. L'autre alternative consiste à associer aux observateurs des lois d'adaptation qui permettent de réaliser l'estimation conjointe des variables d'état et des paramètres inconnus du système ; ces observateurs sont désormais nommés *observateurs adaptatifs*. Dans cette section, nous nous intéressons à la deuxième alternative et nous présentons quelques exemples d'observateurs non linéaires adaptatifs.

1.3.4.1 Observateurs non linéaires adaptatifs utilisant la condition de Lipschitz et la propriété d'excitation persistante

On considère la classe des systèmes non linéaires présentant des paramètres inconnus et ayant la structure suivante

$$\begin{aligned} \dot{x} &= f(x,u,t) + g(x,u,t)\theta \\ y &= h(x), \end{aligned} \tag{1.50}$$

avec $x \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$, $y \in \mathbb{R}^p$, et $\theta \in \mathbb{R}^q$ représentent les vecteurs d'état, d'entrée, de sortie et de paramètres inconnus.
On considère l'observateur adaptatif suivant [51], pour le système (1.50) :

$$\begin{aligned} \dot{\hat{x}}(t) &= f(y,\hat{z},u,t) + g(y,\hat{z},u,t)\hat{\theta} + k(h(\hat{x}) - y, t) \\ \hat{x} &= [\hat{y},\hat{z}]^T, \end{aligned} \tag{1.51}$$

où $\hat{\theta}$ est mise à jour selon la loi d'adaptation

$$\dot{\hat{\theta}} = -\Lambda\phi^T(\hat{y} - y, y, \hat{z}, u, t), \qquad \Lambda = \Lambda^T > 0. \tag{1.52}$$

Afin de garantir la convergence paramétrique (estimation des paramètre inconnus), la fonction $g(\cdot)$ doit satisfaire une condition supplémentaire : la condition d'*excitation persistante*.

Définition 1.22. [51] Un signal $g : \mathbb{R}^+ \to \mathbb{R}^q$ satisfait la propriété d'excitation persistante s'il existe $T, k_1, k_2 > 0$ tels que $\forall t \geq 0$:

$$k_1 I_q \geq \int_t^{t+T} g(x(\tau), u(\tau), \tau) g^T(x(\tau), u(\tau), \tau) d\tau \geq k_2 I_q. \tag{1.53}$$

On définit $e_y := \hat{y} - y$, $e_z := \hat{z} - z$ et $e := \hat{x} - x$. La proposition suivante représente une formulation généralisée de la convergence des observateurs adaptatifs pour les systèmes de la forme (1.50).

Proposition 1.23. *[51] Le système (1.52)–(1.51) est un observateur asymptotique de (1.50) avec $\dot{\theta} = 0$, s'il existe une fonction $V(t,e)$ décroissante définie positive de classe C^1 avec $\left|(\frac{\partial V}{\partial e})(t,e)\right|$ décroissante et une fonction continue $(e_y, t) \to k$ bornée, avec $k(0,t) \equiv 0$ telles que*
$\forall u$, $\forall e = (e_y, e_z)^T$, $\forall y \in \mathbb{R}^p$, $\forall \sigma \in \mathbb{R}^{n-p}$, $\forall \alpha > 0$, $\forall t \geq 0$:

$$\begin{aligned} (i) \quad & \frac{\partial V}{\partial t} + \frac{\partial V}{\partial e}[f(y,\sigma,u,t) - f(y,\sigma - e_z,u,t) + \\ & (g(y,\sigma,u,t) - g(y,\sigma - e_z,u,t))\theta + k(e_y,t)] \leq -\alpha |e|^2 \end{aligned} \tag{1.54a}$$

$$(ii) \quad \frac{\partial V}{\partial e} g(y,\sigma,u,t) = \phi(e_y, y, \sigma, u, t) \tag{1.54b}$$

(iii) g est globalement bornée et f, g sont globalement Lipschitziennes en z uniformément en u, y et t.
Si, en plus, $g(x,u,t)$ satisfait la condition d'excitation persistante (1.53) et $\forall t \geq 0$ et $\dot{g}$ est bornée donc $\lim_{t\to\infty} \left|\hat{\theta}(t) - \theta\right| = 0$.

Considérons maintenant un cas particulier des systèmes (1.50) [52]

$$\begin{aligned} \dot{x} &= Ax + \psi_1(u,x) + B\psi_2(u,x)\theta \\ y &= Cx, \end{aligned} \tag{1.55}$$

où les fonctions ψ_1 et ψ_2 sont supposées globalement Lipschitziennes avec les constantes de Lipschitz respectives k_1 et k_2. On suppose également que le système (1.55) est *à minimum de phase* et qu'il

existe deux matrices définies positives P, Q et une matrice L telles que

$$P(A-LC)+(A-LC)^T P = -Q \tag{1.56a}$$

$$PB = C^T \tag{1.56b}$$

$$k_1 + k_{2\max}(\theta)\,|B| < \frac{\lambda_{min}(Q)}{2\lambda_{max}(P)} \tag{1.56c}$$

Ces conditions garantissent la faisabilité de synthèse d'un observateur adaptatif pour les systèmes (1.55) – voir [52].

1.3.4.2 Observateurs adaptatifs pour les systèmes MIMO à temps variant

Dans [53], Zhang propose une nouvelle approche de conception d'observateurs adaptatifs pour une classe des systèmes linéaires multi-entrées-multi-sorties (MIMO) à temps variant. Les systèmes en considération possèdent la forme suivante

$$\begin{aligned} \dot{x} &= A(t)x + B(t)u + \psi(t)\theta \\ y &= C(t)x, \end{aligned} \tag{1.57}$$

avec $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$, $y \in \mathbb{R}^p$ et $\theta \in \mathbb{R}^p$ représentent les vecteurs respectifs d'état, d'entrée, de sortie et des paramètre inconnus. Les fonctions A, B, C et ψ sont supposées continues par morceaux et uniformément bornées .
L'observateur adaptatif proposé est décrit par les équations suivantes

$$\dot{\hat{x}} = A(t)\hat{x} + B(t)u + \psi(t)\hat{\theta} + [K(t) + \Upsilon(t)\Gamma\Upsilon^T(t)C^T\Sigma(t)](y) - C(t)\hat{x}), \tag{1.58a}$$

$$\dot{\hat{\theta}} = \Gamma\Upsilon^T C^T(t)\Sigma(t)(y - C(t)\hat{x}), \tag{1.58b}$$

$$\dot{\Upsilon} = [A(t) - K(t)C(t)]\Upsilon + \psi(t), \tag{1.58c}$$

sous les deux hypothèses suivantes :

Hypothèse 1.24. *Il existe une fonction $t \to K$ bornée tel que le système : $\dot{\eta} = [A(t) - K(t)C(t)]\eta$ est globalement asymptotiquement stable.*

Hypothèse 1.25. *La matrice $\Upsilon(t)$ définie par le système (1.58c) satisfait la condition d'excitation persistante suivante : il existe deux constantes δ, T et une matrice symétrique définie positive bornée $\Sigma(t)$ tels que*

$$\int_t^{t+T} \Upsilon^T(\tau)C^T(\tau)\Sigma(\tau)C(\tau)\Upsilon(\tau)d\tau \geq \delta I \tag{1.59}$$

Théorème 1.26. *[53] Si les hypothèses (1.24) et (1.25) sont satisfaites, alors le système (1.58) est un observateur adaptatif exponentiel pour le système (1.57).*

Cette approche a été ensuite adoptée dans d'autres travaux et plusieurs extensions et généralisations ont été effectuées. Une première tentative d'étendre ce résultat pour une classe des systèmes non linéaires uniformément observables mono-sortie a été réalisé, dans [54], et une méthode constructive

d'observateurs adaptatifs à convergence exponentielle globale [53] a été développée. Plus récemment, dans [55], la technique de Zhang a été combinée avec les techniques de conception d'observateurs à grand gain pour construire un observateur adaptatif pour une classe de systèmes non linéaires multi-entrées-multi-sorties uniformément observables avec paramétrisation non linéaire. Dans la section suivante, nous nous intéressons à une autre famille d'observateurs : les observateurs à modes glissants.

1.3.5 Observateurs à modes glissants

La commande à structure variable a trouvé un grand succès dans diverses applications en théorie et en pratique grâce à sa robustesse vis-à-vis des incertitudes et des perturbations. Le principe de commande à structure variable a été exploité pour résoudre le problème d'estimation d'état des systèmes linéaires incertains et différentes approches de synthèse d'observateurs à modes glissants ont été développées. L'idée de base consiste à contraindre les trajectoires de l'observateur à évoluer, après un temps fini, dans une *surface de glissement* qui dépend généralement de l'erreur d'observation de la sortie mesurable. Une des propriétés des observateurs à modes glissants qui nous intéresse dans cette thèse est la possibilité de joindre l'estimation simultanée des états et des entrées inconnues, ce qui permet de réaliser à la fois la synchronisation maître-esclave (émetteur-récepteur) et la restauration des informations transmises dans un système de communication. La théorie des modes glissants a été particulièrement utilisée dans le chapitre 3 et une méthode des synchronisation des systèmes chaotiques à base d'observateurs adaptatifs à "modes glissants" a été développée et exploitée dans un nouveau schéma de communication.

On considère, maintenant, le système incertain :

$$\begin{aligned} \dot{x} &= Ax + Bu + Df(x,t), \\ y &= Cx, \end{aligned} \tag{1.60}$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée et $y \in \mathbb{R}^p$ est le vecteur de sortie mesurée.
$f(x,t)$ est une fonction inconnue satisfaisant :

$$|f(x,u,t)| \leq \rho, \quad \forall x \in \mathbb{R}^n,\ \forall u \in \mathbb{R}^m, \forall\ t \geq 0. \tag{1.61}$$

Le problème consiste à concevoir un observateur qui garantit l'estimation d'état et la reconstruction de l'entrée inconnue $f(x,t)$. Dans ce qui suit, nous explicitons trois types d'observateurs à modes glissants : l'*observateur de Walcott-Zak*, l'*observateur de Edwards-Spurgeon* et l'observateur à modes glissants d'ordre supérieur.

1.3.5.1 Observateur de Walcott-Zak

Dans l'approche de Walcott-Zak [56], une contrainte structurelle du système (1.60) est nécessaire pour garantir la faisabilité de l'observateur à modes glissants.

Hypothèse 1.27. *On suppose que la paire (A, C) est observable et qu'il existe deux matrices définies positives P et Q et deux matrices de dimensions appropriées L et F telles que*

$$\begin{aligned} &(A-LC)^T P + P(A-LC) = -Q, \\ &PD = C^T F^T. \end{aligned} \tag{1.62}$$

L'observateur de Walcott-Zak est décrit par les équations

$$\dot{\hat{x}} = A\hat{x} + Bu - L(C\hat{x} - y) + \mu(t), \tag{1.63}$$

où $t \to \mu$ est une fonction discontinue définie par

$$\mu = \begin{cases} -\rho \frac{P^{-1}C^T F^T FCe}{|FCe|}, & \text{si} \quad FCe \neq 0 \\ 0 & \text{si} \quad FCe = 0. \end{cases}$$

La démonstration de la convergence exponentielle de l'erreur d'observation $e = \hat{x} - x$ est obtenue en appliquant l'approche de Lyapunov en considérant une fonction de Lyapunov $V(e) = e^T Pe$ – voir la référence [57] pour plus des détails.
Notons que la discontinuité de μ engendre en pratique un phénomène oscillatoire à hautes fréquences qui apparaît dans la dynamique de l'erreur d'observation. C'est l'inconvénient principal d'utiliser les structures variables.

1.3.5.2 Observateur de Edwards-Spurgeon

L'objectif est d'estimer les vecteurs d'état $\hat{x}(t)$ et de sortie $\hat{y}(t) = C\hat{x}(t)$ tel que les trajectoires sont forcées d'atteindre la surface de glissement $\{e_y(t) = \hat{y}(t) - y(t) = 0\}$ en temps fini. Pour garantir la faisabilité de synthèse de l'observateur, le système considéré de la forme (1.60) doit satisfaire l'hypothèse que la matrice de la fonction de transfert entre l'entrée non mesurable et la sortie mesurée est à "minimum de phase" et du "degré relatif 1", $i.e$

Hypothèse 1.28. *Rang(CD)=Rang(D) et les zéros invariants de (A, D, C) doivent être dans $\mathbb{C}_-$.*

Il a été démontré dans [58] qu'il existe une transformation matricielle non singulière T qui transforme le système (1.60) en un système ayant la forme canonique suivante

$$\begin{aligned} \dot{x}_1 &= A_{11}x_1 + A_{12}x_2 + B_1 u \\ \dot{x}_2 &= A_{21}x_1 + A_{22}x_2 + B_2 u + D_2 f(x,t) \\ y &= x_2, \end{aligned} \tag{1.64}$$

avec $x_1 \in \mathbb{R}^{n-p}$, $x_2 \in \mathbb{R}^p$ et A_{11} Hurwitz. L'observateur de Edwards-Spurgeon possède la structure suivante

$$\begin{aligned} \dot{\hat{x}}_1 &= A_{11}\hat{x}_1 + A_{12}\hat{x}_2 + B_1 u \\ \dot{\hat{x}}_2 &= A_{21}\hat{x}_1 + A_{22}\hat{x}_2 A_{22} - A_{22}^s)e_y + B_2 u + \nu \\ \hat{y} &= \hat{x}_2, \end{aligned} \tag{1.65}$$

avec A_{22} Hurwitz et ν est une fonction discontinue donnée par

$$\nu = \begin{cases} -\rho\,|D_2|\,\frac{P_2 e_y}{|P_2 e_y|} & \text{si } e_y \neq 0 \\ 0 & \text{si } e_y = 0, \end{cases}$$

où $e_y = \hat{y} - y = \hat{x}_2 - x_2$ et P_2 la solution de l'équation $(A_{22}^s)^T P_2 + P_2 A_{22}^s = -Q_2$; avec Q_2 une matrice définie positive. L'estimation $\hat{x}$ du vecteur d'état original est donnée par $\hat{x} = T^{-1}[\hat{x}_1, \hat{x}_2]^T$.

1.3.5.3 Observateur à modes glissants d'ordre supérieur

Les inconvénients des observateurs par modes glissants conventionnels tels que l'observateur de Zak et l'observateur de Edwards-Spurgeon sont le phénomène oscillatoire de haute fréquences ainsi que l'hypothèse du "degré relatif 1" qui n'est pas toujours vérifiée. Les observateurs à modes glissants d'ordre supérieur [59–62] sont conçus essentiellement pour éviter ces limites tout en préservant les avantages des observateurs à modes glissants de premier ordre tels que la convergence en temps fini et la robustesse aux entrées inconnues et aux perturbations.

On considère le système non linéaire sous la forme triangulaire suivante :

$$\begin{aligned} \dot{x} &= A_n x + H_n V_n(x, w), \\ y &= C_n z, \end{aligned} \tag{1.66}$$

où

$$A_n = \begin{pmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & 1 & \vdots \\ \vdots & \vdots & \dots & 1 \\ 0 & \dots & \dots & 0 \end{pmatrix} \in \mathbb{R}^{n\times n}, \quad H_n = \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}, \quad C_n = \begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix},$$

$x = [x_1, \dots, x_n]^T \in \mathbb{R}^n$ est le vecteur d'état, $y \in \mathbb{R}$ est le vecteur de sortie et $w \in \mathbb{R}$ est l'entrée inconnue. On suppose que l'état du système est uniformément borné, $i.e\ |x_i(t)| < d_i$, pour $i = 1..n$. L'entrée inconnue et sa dérivée sont également supposées bornées.

Un observateur à modes glissants de dimension $2n$ a été proposé, dans [59], pour les systèmes ayant la forme canonique (1.66) :

$$\begin{aligned}
\dot{\hat{x}}_1 &= z_1 + \lambda_1 |x_1 - \hat{x}_1|^{1/2} \,\mathsf{sign}(x_1 - \hat{x}_1) \\
\dot{z}_1 &= \alpha_1 \mathsf{sign}(x_1 - \hat{x}_1) \\
\dot{\hat{x}}_2 &= z_2 + \lambda_2 |z_1 - \hat{x}_2|^{1/2} \,\mathsf{sign}(x_1 - \hat{x}_2) \\
\dot{z}_2 &= \alpha_2 \mathsf{sign}(z_1 - \hat{x}_2) \\
&\vdots \\
\dot{\hat{x}}_n &= z_n + \lambda_n |z_{n-1} - \hat{x}_n|^{1/2} \,\mathsf{sign}(z_{n-1} - \hat{x}_n) \\
\dot{z}_n &= \alpha_n \mathsf{sign}(z_{n-1} - \hat{x}_n).
\end{aligned} \tag{1.67}$$

On définit les erreurs d'observation $e_i = x_i - \hat{x}_i$ et $\xi_i = x_{i+1} - z_i$, pour $i = 1, \ldots, n$, avec $x_{n+1} = V_n(x, w)$. Les gains de l'observateur λ_i et α_i sont des scalaires positifs à déterminer. La dynamique de l'erreur d'observation est donnée par :

$$\dot{e}_1 = z_1 + \lambda_1 |e_1|^{1/2} \,\mathsf{sign}(e_1) \tag{1.68}$$

$$\dot{\xi}_1 = x_3 - \alpha_1 \mathsf{sign}(e_1) \tag{1.69}$$

$$\begin{aligned}
\dot{e}_2 &= \xi_2 - \lambda_2 |e_2 - \xi_1|^{1/2} \,\mathsf{sign}(e_2 - \xi_1) \\
\dot{\xi}_2 &= x_4 - \alpha_2 \mathsf{sign}(e_2 - \xi_1) \\
&\vdots \\
\dot{e}_n &= \xi_n - \lambda_n |e_n - \xi_{n-1}|^{1/2} \,\mathsf{sign}(e_n - \xi n - 1) \\
\xi_n &= \dot{x}_{n+1} - \alpha_n \mathsf{sign}(e_n - \xi n - 1).
\end{aligned} \tag{1.70}$$

On considère les deux premières équations (1.68)–(1.69) et on définit $\psi = \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} = \begin{pmatrix} |e_1|^{1/2} \,\mathsf{sign}(e_1) \\ \xi_1 \end{pmatrix}$. En définissant la fonction de Lyapunov $W = \psi^T P \psi$, où P est une matrice définie, positive. Le calcul et l'analyse de la dérivée de W le long des trajectoires de la dynamique de ψ donne :

$$\dot{W} \leq -k_p W^{1/2}, \tag{1.71}$$

où k_p est une constante positive dépendant de valeurs propres minimale et maximale de la matrice P. L'inégalité (1.71) implique que ψ converge vers zéro en temps fini, et par conséquent e_1 et ξ_1 convergent vers zéro en temps fini. D'une manière similaire, on peut démontrer la convergence des trajectoires en temps fini vers $\{e_2 = \xi_2 = 0\}$. En appliquant la même démarche récursivement, on obtient : $e_i = x_i - \hat{x}_i = 0$ et $\xi_i = x_{i+1} - z_i = 0$, en temps fini. L'étape finale ($i = n$) permet de générer une estimation en temps fini de $V(x, w) = z_n$. Cette procédure a été également généralisée dans [59] pour le cas des systèmes à entrées multiples et sorties multiples (MIMO).

Dans la section suivante, nous nous intéressons à une autre famille des observateurs considérant le problème d'estimation d'état en présence d'incertitudes et de perturbations (entrées inconnues) :

c'est la famille des *observateurs à entrées inconnues*.

1.3.6 Observateurs à entrées inconnus

Les *observateurs à entrées inconnus* ont été développés dans le but d'estimer l'état d'un système en dépit des entrées inconnues non mesurables. Ces entrées inconnues apparaissent dans les processus physiques sous la forme des erreurs de modélisation, des incertitudes, des perturbations, des défauts, etc. Les premières approches qui ont été élaborées dans les années soixante-dix partent du principe d'utiliser une transformation linéaire. Ainsi, le vecteur d'état est divisé en une partie influencée par les entrées inconnues et une autre partie non influencée. Cette méthode permet de concevoir un observateur d'ordre réduit [63].
Plus récemment, les méthodes algébriques nécessitant la résolution d'équations matricielles linéaires ont été également développées [64]. Ces méthodes considèrent les systèmes linéaires de la forme

$$\begin{aligned} \dot{x} &= Ax + Bu + Fw \\ y &= Cx, \end{aligned} \tag{1.72}$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée connue, $w \in \mathbb{R}^q$ représente le vecteur d'entrée inconnue et $y \in \mathbb{R}^p$ est le vecteur de sortie mesurée. La matrice F est de plein rang et la paire (A, C) est supposée observable. La structure de l'observateur à entrées inconnues d'ordre plein est décrite par [65], [64]

$$\begin{aligned} \dot{z} &= Nz + Gu + Ly \\ \hat{x} &= z - Ey. \end{aligned} \tag{1.73}$$

La dynamique de l'erreur d'observation $e = x - \hat{x}$ est donnée par

$$\begin{aligned} \dot{e} &= \dot{x} - \dot{z} + EC\dot{x} \\ &= Ne + (PB - G)u + (PA - NP - LC)x, \quad \text{où} \quad P = I + EC. \end{aligned}$$

L'erreur d'observation converge asymptotiquement vers zéro si et seulement si

$$N \text{ est stable} \tag{1.74a}$$
$$P = I + EC \tag{1.74b}$$
$$LC = PA - NP \tag{1.74c}$$
$$G = PB \tag{1.74d}$$
$$PF = 0. \tag{1.74e}$$

Les conditions nécessaires et suffisantes d'existence des solutions pour ces équations matricielles sont [64] :

$$\begin{aligned} &(i)\ \text{rang}(CF) = \text{rang}(F) \\ &(ii)\ \text{rang}\begin{bmatrix} sP - PA \\ C \end{bmatrix} = n, \quad \forall s \in \mathbb{C},\ \mathcal{R}e(s) \geq 0 \end{aligned} \tag{1.75}$$

Ces conditions signifient que le système (1.72) est *à minimum de phase* et de *degré relatif 1*, ainsi, on retrouve les mêmes conditions utilisées pour la conception d'observateurs à modes glissants de premier ordre. La résolution des équations matricielles (1.74) est basée sur le calcul de la pseudo-inverse de la matrice (CF) afin d'obtenir les différentes matrices de l'observateur. Ces résultats ont été étendus dans [66] au cas où les entrées inconnues apparaissent à la fois dans la dynamique du système et dans les équations de la sortie. Le système en considération est décrit par

$$\begin{aligned} \dot{x} &= Ax + Bu + F_1 w \\ y &= Cx + F_2 w, \end{aligned} \tag{1.76}$$

et (1.76) vérifie les contraintes structurelles suivantes

$$\text{rang}\begin{bmatrix} CF_1 & F_2 \\ F_2 & 0 \end{bmatrix} = \text{rang}(G) + \text{rang}\begin{bmatrix} F_1 \\ F_2 \end{bmatrix} \tag{1.77}$$

$$\text{rang}\begin{bmatrix} sI - A & -F_1 \\ C & F_2 \end{bmatrix} = n + \text{rang}\begin{bmatrix} F_1 \\ F_2 \end{bmatrix}, \quad \forall s \in \mathbb{C},\ \mathcal{R}e(s) \geq 0 \tag{1.78}$$

L'observateur proposé dans [66] possède la structure suivante

$$\begin{aligned} \dot{z} &= Nz + Hu + Jy \\ \hat{x} &= z - Ey. \end{aligned} \tag{1.79}$$

Proposition 1.29. *L'erreur d'observation $e = x - \hat{x}$ converge vers zéro asymptotiquement si les conditions suivantes sont satisfaites*

$$N \text{ est stable} \tag{1.80a}$$

$$P = I + EC \tag{1.80b}$$

$$PA - NP - JC = 0 \tag{1.80c}$$

$$PF_1 - NEG - JG = 0 \tag{1.80d}$$

$$EF_2 = 0 \tag{1.80e}$$

$$H = PB. \tag{1.80f}$$

La résolution des différentes équations matricielles linéaires est basée sur le calcul de l'inverse généralisée de la matrice $\Sigma = \begin{bmatrix} CF_1 & F_2 \\ F_2 & 0 \end{bmatrix}$. Un algorithme a été proposé pour décrire les étapes de calcul de matrices de l'observateur.

D'autre part, les systèmes singuliers ont fait l'objet de diverses approches de synthèse d'observateurs à entrées inconnus. Un système singulier possède la structure suivante

$$\begin{aligned} E\dot{x} &= Ax + Bu + Fw \\ y &= Cx \end{aligned} \tag{1.81}$$

avec $x \in \mathbb{R}^n$ le vecteur d'état et $w \in \mathbb{R}^q$ le vecteur d'entrées inconnues. La plupart des méthodes élaborées s'appuient sur l'idée de transformer le système (1.81) en un système augmenté en considérant le nouveau vecteur d'état $\bar{x} = \begin{bmatrix} x \\ w \end{bmatrix}$:

$$\bar{E}\dot{\bar{x}} = \bar{A}\bar{x} + \bar{B}u \tag{1.82a}$$

$$y = \bar{C}\bar{x}, \tag{1.82b}$$

avec $\bar{E} = \begin{bmatrix} E & 0 \\ 0 & I \end{bmatrix}$, $\bar{A} = \begin{bmatrix} A & N \\ 0 & 0 \end{bmatrix}$, $\bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}$ et $\bar{C} = \begin{bmatrix} C & 0 \end{bmatrix}$.

D'après [67], [68], un observateur pour le système (1.82) est donné par [64]

$$\begin{aligned} \dot{z} &= Rz + Hu + Ly \\ \hat{x} &= Mz - Ny \end{aligned} \tag{1.83}$$

Théorème 1.30. *[68] Considérons le système singulier (1.82) vérifiant les conditions structurelles :*

$$\mathit{rang} \begin{bmatrix} s\bar{E} - \bar{A} \\ \bar{C} \end{bmatrix} = n, \quad \forall s \in \mathbb{C} \tag{1.84}$$

$$\mathit{rang} \begin{bmatrix} sI - R \\ M \end{bmatrix} = n, \quad \forall s \in \mathbb{C}. \tag{1.85}$$

Il existe une matrice K de dimensions appropriées telle que $\lim_{t\to+\infty} Kx - \hat{x} = 0$, $\forall x(0), z(0)$ si et seulement s'il existe une matrice P sachant que les équations matricielles linéaires suivantes sont vérifiées :

$$R \text{ est stable}, \tag{1.86a}$$

$$P\bar{A} - RP\bar{E} - L\bar{C} = 0, \tag{1.86b}$$

$$K = MP\bar{E} + N\bar{C}, \tag{1.86c}$$

$$H = P\bar{B}. \tag{1.86d}$$

Dans la référence [69], un autre observateur pour l'estimation conjointe de l'état et des entrées inconnues du système (1.81) a été développé

$$\begin{aligned} \dot{z} &= Fz + L_1 y + L_2 y + Ju + T_1 N \hat{w}, \\ \dot{\hat{w}} &= L_3(y - \hat{y}), \\ \hat{x} &= M_1 z + T_2 y, \\ \hat{y} &= C\hat{x}. \end{aligned} \tag{1.87}$$

Pour garantir la faisabilité de cet observateur, le système augmenté (1.82) doit satisfaire les conditions structurelles suivantes :

$$\text{rang} \begin{bmatrix} E \\ \bar{C} \end{bmatrix} = n, \tag{1.88}$$

$$\text{rang} \begin{bmatrix} sI - A & -N \\ 0 & sI \\ C & 0 \end{bmatrix} = n + q, \quad \forall s \in \mathbb{C}, \quad \mathcal{R}e(s) \geq 0. \tag{1.89}$$

La condition (1.89) est équivalente à l'équation (1.84) utilisée dans [68] ; ceci peut être facilement vérifié en remplaçant $\bar{E}$, $\bar{A}$, $\bar{B}$ et $\bar{C}$ par leurs expressions. Si ces propriétés structurelles sont satisfaites, alors le système (1.87) est un observateur asymptotique pour (1.82).

Les propriétés des observateurs à entrées inconnues et des observateurs singuliers ont été particulièrement bien exploitées dans les chapitres 2 et 3 pour le développement des méthodes de synchronisation plus robustes aux perturbations et au bruit présent dans le canal de communication, dans les applications de transmission d'informations à base des systèmes chaotiques.

1.4 Conclusion

La première partie de ce chapitre a été dévolue aux systèmes de communications analogiques qui sont basés sur la synchronisation des systèmes chaotiques. Ensuite, et après avoir expliqué l'utilité de la théorie des observateurs non linéaires dans les applications de synchronisation et de transmission d'informations à base des systèmes chaotiques, une liste non exhaustive des observateurs non linéaires a été présentée tout en étudiant et analysant leurs méthodes de synthèse. En particulier, nous avons exposé les approches de synthèse des observateurs qui sont en liaison étroite avec les méthodes développées dans cette thèse telles que les observateurs adaptatifs, les observateurs à entrées inconnues et les observateurs à modes glissants. Ce travail de thèse est principalement basée sur la connexion entre le problème d'estimation d'état et le phénomène de synchronisation. Nous verrons dans les prochains chapitres plus clairement l'utilité de la théorie d'observateurs non linéaires dans les applications de transmission de données à base du chaos. Dans ce contexte, nous présentons, dans le chapitre 2, une méthode de synchronisation des systèmes chaotiques à base d'un observateur adaptatif à entrées inconnues et son application dans un système de transmission d'informations

dans un scénario évoquant la présence des perturbations, des incertitudes paramétriques et du bruit dans le canal public.

Chapitre 2

Synchronisation à base d'observateurs adaptatifs à entrées inconnues

2.1 Introduction

Dans les systèmes de communications basés sur la synchronisation maître-esclave des systèmes chaotiques, les imperfections tels que les perturbations, le bruit dans le canal et les incertitudes paramétriques sont inévitables. Dans ce chapitre, nous présentons une méthode de synchronisation robuste basée sur un observateur adaptatif à entrées inconnues et son application dans un système de communication. Le système maître considéré est un système chaotique présentant, dans sa dynamique, une fonction non linéaire de classe $\mathcal{C}^1$ pour laquelle on peut appliquer la technique de *transformation de Lipschitz* sous l'hypothèse de bornitude des solutions du système maître. La constante de Lipschitz est supposée inconnue et peut prendre des grandes valeurs. L'équation d'état présente également des paramètres inconnus ainsi que des perturbations et les signaux de sortie sont corrompus par un bruit. Pour la transmission de l'information, nous utilisons la technique de modulation paramétrique : le message à transmettre (supposé constant par morceaux) module l'un des paramètres du système maître. Le système esclave proposé est un observateur adaptatif à entrées inconnues pour le système maître. Il assure le rejet du bruit dans le canal de transmission et des perturbations présentes dans la dynamique du système maître et la restauration de l'information transmise. Nous présentons également une analyse des conditions nécessaires et suffisantes pour la synchronisation maître-esclave et la convergence paramétrique. Deux applications de transmission d'informations sont présentées pour vérifier l'efficacité de la méthode de synchronisation proposée.

2.2 Contexte et position du problème

On considère la classe des systèmes non linéaires vérifiant les équations :

$$\dot{x} = Ax + Bf_0(x) + Bg_0(x)m(t) + Fd(t) \tag{2.1a}$$
$$y = Cx + Gd(t), \tag{2.1b}$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, $y \in \mathbb{R}^p$ est la sortie mesurable, $f_0 : \mathbb{R}^n \to \mathbb{R}^s$ et $g_0 : \mathbb{R}^n \to \mathbb{R}^{s\times q}$ sont de classe $\mathcal{C}^1$; $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times s}$, $C \in \mathbb{R}^{p\times n}$, $F \in \mathbb{R}^{n\times r}$ et $G \in \mathbb{R}^{p\times r}$ sont des matrices constantes.

La fonction $m : \mathbb{R}_{\geq 0} \to \mathbb{R}^q$ est supposée constante par morceaux et $d : \mathbb{R}_{\geq 0} \to \mathbb{R}^r$ est une fonction mesurable au sens de Lebesgue. On suppose également qu'il existe une constante $K_m > 0$ telle que

$$\sup_{t\geq 0} |m(t)| \leq K_M. \tag{2.2}$$

La fonction m représente un vecteur composé des paramètres inconnus représentant les erreurs de modélisation et/ou des messages à transmettre, dans le contexte de synchronisation pour la transmission des données. Le signal transmis $y(t)$ est affecté par un bruit représenté par le terme $Gd(t)$.

La classe des systèmes (2.1) couvre plusieurs modèles des systèmes chaotiques. En effet, les systèmes de *Duffing*, de *Van der Pol*, de *Lorenz*, de *Lü* de troisième et quatrième ordre, de *Rössler* et de *Chua*, parmi tant d'autres, peuvent s'écrire sous la forme

$$\dot{x} = Ax + Bf_0(x). \tag{2.3}$$

En particulier, le système de Rössler :

$$\dot{x}_1 = -(x_2 + x_3) \tag{2.4a}$$
$$\dot{x}_2 = x_1 + ax_2 \tag{2.4b}$$
$$\dot{x}_3 = b + x_3(x_1 - c) \tag{2.4c}$$

est de la forme (2.3) avec $A = \begin{bmatrix} 0 & -1 & -1 \\ 1 & a & 0 \\ 0 & 0 & -c \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$, $f_0(x) = b + x_1x_3$.

Par ailleurs, le *système de Lorenz :*

$$\dot{x}_1 = \sigma(x_2 - x_1) \tag{2.5a}$$
$$\dot{x}_2 = rx_1 - x_2 - x_1x_3 \tag{2.5b}$$
$$\dot{x}_3 = x_1x_2 - bx_3 \tag{2.5c}$$

est de la forme (2.3) avec $A = \begin{bmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$, $f_0(x) = \begin{bmatrix} -x_1 x_3 \\ x_1 x_2, \end{bmatrix}$.

D'une manière similaire, le système de *Chua*

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1 - \phi(x)) \\ \dot{x}_2 &= x_1 - x_2 + x_3 \\ \dot{x}_3 &= -\beta x_2 \end{aligned}$$

avec

$$\phi(x) = \begin{cases} bx + a - b & \text{if} \quad x > 1 \\ ax & \text{if} \quad |x| \leq 1 \\ bx - a + b & \text{if} \quad x < -1 \end{cases}$$

appartient également à la classe des systèmes (2.3).

Le problème de synchronisation maître-esclave consiste à concevoir un système dynamique

$$\dot{z} = \Phi(t, y, z, \hat{m}) \tag{2.7a}$$
$$\hat{x} = h(y, z) \tag{2.7b}$$
$$\dot{\hat{m}} = \Psi(t, y, z) \tag{2.7c}$$

tel que pour tout $r > 0$

$$\lim_{t \to \infty} |x(t) - \hat{x}(t)| = 0, \quad \forall\, x(0), \hat{x}(0) \in B_r \times \mathbb{R}^n \tag{2.8}$$

avec $B_r := \{x \in \mathbb{R}^n : |x| < r\}$. En particulier, on a besoin de rejeter la perturbation $d(t)$ qui affecte à la fois la dynamique du système et la sortie mesurée.

Pour résoudre ce problème, on a besoin de la propriété suivante.

Propriété de bornitude. Les solutions $x(\cdot)$ de (2.1) sont globalement, uniformément bornées.

La propriété de bornitude est une hypothèse commune dans la littérature de synthèse d'observateurs : plusieurs systèmes physiques tels que les oscillateurs[1] vérifient cette propriété, et plus particulièrement les oscillateurs chaotiques. La propriété de bornitude permet d'utiliser la méthode de transformation, souvent appelée "technique d'extension de Lipschitz" :
Soit $\omega_i > 0$, $\forall i \in \{1, \dots n\}$. On définit le compact $\Omega \subset \mathbb{R}^n$

$$\Omega := \{x \in \mathbb{R}^n : |x_i| \leq \omega_i\}$$

1. Le lecteur est invité à consulter la référence [70] pour voir les différentes définitions d'oscillateurs.

et la fonction saturation $\sigma : \mathbb{R}^n \to \Omega$ telle que chaque composante σ_i de σ est donnée par

$$\begin{array}{l} i \in \{1, \dots n\}, \\ \omega_i > 0 \end{array} \Rightarrow \sigma_i(x) := \begin{cases} x_i & \text{, if } |x_i| \leq \omega_i \\ \text{sgn}(\omega_i)\,|\omega_i| & \text{, sinon} \end{cases}$$

On définit les fonctions $f : \mathbb{R}^n \to \mathbb{R}^s$ et $g : \mathbb{R}^n \to \mathbb{R}^{s\times q}$ pour tout $x \in \mathbb{R}^n$ telles que $f(x) := f_0 \circ \sigma(x)$ et $g(x) := g_0 \circ \sigma(x)$.

En appliquant le théorème d'accroissement finis pour les fonctions vectoriels ([Théorème A.3],[71]), on déduit que pour tout $w \in \mathbb{R}^s$, σ_1 et $\sigma_2 \in \Omega$, il existe $\alpha \in (0,1)$ et $\xi := \sigma_2 + \alpha[\sigma_1 - \sigma_2]$ tels que

$$w^\top [\, f_0(\sigma_1) - f_0(\sigma_2)] = [\sigma_1 - \sigma_2]^\top \underbrace{\begin{bmatrix} \dfrac{\partial f_0}{\partial s_1}\Big|_{s=\xi} & \cdots & \dfrac{\partial f_0}{\partial s_n}\Big|_{s=\xi} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial f_0}{\partial s_1}\Big|_{s=\xi} & \cdots & \dfrac{\partial f_0}{\partial s_n}\Big|_{s=\xi} \end{bmatrix}}_{=:\,\Gamma(\xi)} w.$$

Puisque $\frac{\partial f_0}{\partial s_i}$ est continue pour tout i et que $\xi \in \Omega$, il s'ensuit que chaque élément dans cette matrice est borné. Ainsi, il existe $K_f > 0$ tel que $|\Gamma(\xi)| \leq K_f$ pour tout $\xi \in \Omega$. Ceci est vrai pour tout σ_1, $\sigma_2 \in \Omega$, par conséquent pour $\sigma_1 := \sigma(a)$ et $\sigma_2 := \sigma(b)$, pour tout a et $b \in \mathbb{R}^n$. En utilisant la définition de σ , il s'en suit que

$$|\sigma(a) - \sigma(b)| \leq |a - b|, \qquad \forall\, a, b \in \mathbb{R}^n\,.$$

Ainsi, on retient les deux observations suivantes :

1. pour tout $x \in \Omega$, on a $f(x) = f_0(x)$ et $g(x) = g_0(x)$;
2. pour tout Ω, il existe deux réels positifs K_f et K_g tels que pour tout $a \in \mathbb{R}^n$, $b \in \mathbb{R}^n$ et $w \in \mathbb{R}^s$,

$$\begin{aligned} \left|w^\top [f(a) - f(b)]\right| &\leq K_f\,|a-b|\,|w|\,, \\ \left|w^\top [g(a) - g(b)]\right| &\leq K_g\,|a-b|\,|w|\,. \end{aligned}$$

Il s'en suit que pour tout t tel que $x(t) \in \Omega$, les trajectoires du système (2.1) coïncident avec celles du système :

$$\dot{x} = Ax + Bf(x) + Bg(x)m(t) + Fd(t), \tag{2.9a}$$
$$y = Cx + Gd(t). \tag{2.9b}$$

Le problème de synchronisation sous les hypothèses précédentes peut être considéré comme étant un problème de synthèse d'observateurs adaptatifs à entrées inconnues pour le système maître (2.9) de telle manière que l'équation (2.8) soit vérifiée.

2.3 Observateur adaptatif à entrées inconnues

2.3.1 Estimation d'état et rejet des perturbations

Nous présentons un observateur adaptatif à entrées inconnues qui accomplit l'objectif de synchronisation (2.8) en présence des perturbations externes, incertitudes paramétriques et bruit de canal dans le contexte des communications à base du chaos. L'observateur est donné par les équations

$$\dot{z} = Nz + Jy + Hf(\hat{x}) + Hg(\hat{x})\hat{m} + \frac{1}{2}\hat{\beta}HM(Ty - C_1\hat{x}), \tag{2.10a}$$

$$\hat{x} = z - Ey, \tag{2.10b}$$

et les lois d'adaptation

$$\dot{\hat{m}} = \delta g(\hat{x})^T M(Ty - C_1\hat{x}), \tag{2.11}$$

$$\dot{\hat{\beta}} = \gamma \left| M(Ty - C_1\hat{x}) \right|^2 . \tag{2.12}$$

Les constantes δ et γ sont deux nombres réels positifs. Les matrices N, E, J, H, T, M et C_1 sont constantes et de dimensions appropriées à déterminer. Elles doivent satisfaire les équations matricielles suivantes

$$EG = 0 \tag{2.13}$$

$$PA - NP - JC = 0 \tag{2.14}$$

$$PF - NEG - JG = 0 \tag{2.15}$$

$$H = PB \tag{2.16}$$

$$P = I + EC \tag{2.17}$$

$$TG = 0 \tag{2.18}$$

$$TC = C_1 . \tag{2.19}$$

En plus, le triple (N, H, C_1) doit satisfaire les conditions suivantes

$$N^T Q + QN < 0 \tag{2.20}$$

$$H^T Q = MC_1. \tag{2.21}$$

Proposition 2.1. *Sous les conditions (2.13)–(2.21), l'expression (2.8) est satisfaite pour les solutions $x(\cdot)$ du système maître (2.1) et les trajectoires $\hat{x}(\cdot)$ de l'observateur (2.10), pour tous les états initiaux tels que les solutions $x(\cdot)$ sont bornées et pour tous les états initiaux $\hat{x}(0) \in \mathbb{R}^n$.*

Démonstration :

Nous commençons tout d'abord par écrire la dynamique de l'erreur d'observation sous une forme appropriée, ensuite, nous utilisons des arguments standards de la théorie de Lyapunov afin de prouver la convergence des erreurs d'estimation vers zéro. Pour ce faire, nous définissons les variables d'erreurs

$e := x - \hat{x}$, $\tilde{m} := m - \hat{m}$ et $\tilde{\beta} := \beta - \hat{\beta}$. Donc, on a

$$\begin{aligned} e &= x - z + Ey && \Leftarrow (2.10b) \\ &= x - z + ECx + EGd && \Leftarrow (2.1b) \\ &= Px - z. && \Leftarrow (2.13),\ (2.17) \end{aligned}$$

On applique la dérivée à cette dernière pour obtenir

$$\begin{aligned} \dot{e} &= PAx + PBf(x) + PBg(x)m(t) + PFd(t) - Nz - Jy \\ &\quad -Hf(\hat{x}) - Hg(\hat{x})\hat{m}(t) - \frac{1}{2}\hat{\beta}HM(Ty - C_1\hat{x}). \end{aligned}$$

Compte tenu des équations (2.18) et (2.19), on a $Ty - C_1\hat{x} = C_1 e$. En plus, en utilisant l'équation(2.9b) ainsi que $z = x - e + E(Cx + Gd)$, on obtient

$$\begin{aligned} \dot{e} &= (PA - JC)x - JGd(t) - Nx + Ne - NECx - NEGd(t) + PBf(x) + PBg(x)m(t) \\ &\quad + PFd(t) - Hf(\hat{x}) - Hg(\hat{x})\hat{m} - \frac{1}{2}\hat{\beta}HMC_1 e\,. \end{aligned}$$

Ensuite, on regroupe les termes et on utilise l'équation (2.15) pour obtenir

$$\dot{e} = (PA - JC - NEC)x - N\hat{x} - \frac{1}{2}\hat{\beta}HMC_1 e + PB[f(x) + g(x)m(t)] - H[f(\hat{x}) + g(\hat{x})\hat{m}]\,.$$

À partir de (2.17), il s'en suit que l'équation (2.14) est équivalente à $PA - NEC - JC = N$. Par conséquent, en utilisant l'équation (2.16), on obtient

$$\dot{e} = Ne + H[f(x) - f(\hat{x})] + H[g(x)m(t) - g(\hat{x})\hat{m}] - \frac{1}{2}\hat{\beta}HMC_1 e\,. \tag{2.23}$$

Soit $\beta > 0$ une constante à déterminer et $\tilde{\beta} := \beta - \hat{\beta}$. En additionnant $Hg(\hat{x})m(t)$ de chaque côté de l'équation (2.23), il en résulte que

$$\begin{aligned} \dot{e} &= Ne + H[f(x) - f(\hat{x})] + H[g(x) - g(\hat{x})]m(t) \\ &\quad - \frac{1}{2}\beta HMC_1 e + \left[Hg(\hat{x})\ \frac{1}{2}HMC_1 e\right]\begin{bmatrix}\tilde{m}\\ \tilde{\beta}\end{bmatrix}. \end{aligned} \tag{2.24}$$

En utilisant les expressions des lois d'adaptation (2.11) et (2.12), $\tilde{m}$ et $\tilde{\beta}$ sont les solutions du système [2]

$$\dot{\tilde{m}} = -\delta g(\hat{x})^T MC_1 e - \dot{m} \quad \text{p.p,} \tag{2.25}$$

$$\dot{\tilde{\beta}} = -\gamma\,|MC_1 e|^2\,. \tag{2.26}$$

2. Noter que $\dot{m}(t) = 0$ pour presque pour tout t puisque m est constant par morceaux.

On considère maintenant la fonction positive définie et radialement non bornée

$$V_1(e,\tilde{\beta},\tilde{m}) := e^\top Qe + \frac{1}{\delta}\tilde{m}^2 + \frac{1}{2\gamma}\tilde{\beta}^2\,. \tag{2.27}$$

La dérivée totale le long des trajectoires de (2.24)–(2.26) est donnée par [3]

$$\begin{aligned}\dot{V}_1 = {} & e^\top[N^\top Q + QN]e + 2e^\top QH[f(x) - f(\hat{x})] - e^\top Q[HMC_1e]\beta + 2e^\top QH[g(x) - g(\hat{x})]m(t) \\ & + 2e^\top QH\tilde{m}g(\hat{x}) - \frac{2}{\delta}\tilde{m}^\top[\delta g(\hat{x})^\top MC_1e - \dot{m}(t)],\end{aligned}$$

où nous avons utilisé (2.21). Ensuite, si la condition (2.20) génère un nombre réel positif constant η tel que $N^\top Q + QN \leq -2\eta$. En posant $w^\top = e^\top QH$ et en utilisant (2.21) et (2.2), on obtient

$$\dot{V}_1 \quad \leq \quad -2\eta\,|e|^2 + 2\,|MC_1e|\,[K_f + K_gK_m]\,|e| - \beta\,|MC_1e|^2 - \frac{2}{\delta}\tilde{m}^\top\dot{m}(t)\,.$$

Soit $\beta := [K_f + K_gK_m]^2/\eta$. En appliquant l'inégalité de "Young" au terme $2\,|MC_1e|\,[K_f + K_gK_m]\,|e|$, il en résulte finalement que

$$\dot{V}_1(e,\tilde{m},\tilde{\beta}) \leq -\eta\,|e|^2 - \frac{2}{\delta}\tilde{m}^\top\dot{m}(t)$$

qui est satisfaite pour tout e telle que $x \in \Omega$ et pour tout $t \geq 0$ presque partout. Ainsi, pour tout compact Ω et pour toutes les conditions initiales $x_\circ \in \mathbb{R}^n$ telles que les solutions $x(\cdot)$ restent dans l'ensemble Ω et pour presque tout t , nous avons

$$\dot{V}_1(e(t),\tilde{m}(t),\tilde{\beta}(t)) \leq -\eta\,|e(t)|^2 - \frac{2}{\delta}\tilde{m}(t)^\top\dot{m}(t).$$

D'après l'hypothèse $\dot{m}(t) = 0$ presque partout, il en résulte que

$$\dot{V}_1(e(t),\tilde{m}(t),\tilde{\beta}(t)) \leq -\eta\,|e(t)|^2\,, \qquad \text{p.p.} \tag{2.28}$$

En intégrant de chaque côté de cette dernière de 0 à ∞, on déduit que $e(t)$, $\tilde{m}(t)$ et $\tilde{\beta}(t)$ sont bornés pour tout t et en plus, $e(t) \in L_2$. Ensuite, nous appliquons les substitutions suivantes dans l'équation (2.24) :

$$\begin{gathered}x = x(t) \quad \hat{x} = x(t) - e(t) \quad \dot{e} = \dot{e}(t) \\ \tilde{m} = \tilde{m}(t) \quad \tilde{\beta} = \tilde{\beta}(t),\end{gathered}$$

pour conclure que $\dot{e}(t)$ est aussi uniformément borné pour tout t puisque $m(t)$ est borné. En faisant appel au lemme de Barbălat, nous déduisons que

$$\lim_{t\to+\infty} |e(t)| = 0,$$

ainsi, l'équation(2.8) est bien satisfaite. ■

3. Ceci est valide, à l'exception où $\dot{m}$ n'existe pas, ce qui correspond à un nombre compté des points

2.3.2 Convergence paramétrique

Dans les articles [14, 72], l'analyse de la convergence paramétrique a été traitée à travers deux différentes approches : la commande par suivi de trajectoires et l'approche de synthèse d'observateurs, respectivement. Dans cette section, nous discutons brièvement la théorie fondamentale utilisée pour démontrer la convergence paramétrique pour les systèmes non linéaires non autonomes, qui couvrent notamment les systèmes chaotiques.
La proposition 2.1 établit la convergence de l'erreur d'observation vers zéro. Cependant, il s'agit en général d'une propriété faible qui n'implique pas la robustesse. Dans cette section, nous montrons que sous les conditions de la proposition 2.1 et une hypothèse supplémentaire d'*excitation persistante*, il est possible d'établir la stabilité globale, uniforme et asymptotique de l'origine du système d'erreur *i.e.*, $(e, \tilde{m}, \tilde{\beta}) = (0, 0, 0)$. Une définition de l'excitation persistante est présentée ci-après.

Définition 2.2. [14] Une fonction continue $\phi : \mathbb{R}_+ \to \mathbb{R}^{m\times n}$ est à excitation persistante s'il existe deux nombres positifs μ et T tels que

$$\int_t^{t+T} \phi(s)\phi(s)^T ds \geq \mu I, \qquad \forall t \geq 0. \tag{2.29}$$

Remarque 2.3. La propriété d'excitation persistante a été définie à l'origine pour les fonctions utilisées dans les théorèmes de stabilité des systèmes linéaires. Les notions générales qui concernent les systèmes non linéaires à temps variant (que nous allons détailler dans la suite du chapitre) sont utilisées pour la démonstration de notre résultat principal. Le lecteur est invité à consulter la référence [14] pour des discussions supplémentaires et plus d'illustrations sur l'utilisation de la propriété d'excitation persistante des systèmes chaotiques. □

Avant de présenter notre résultat principal, nous introduisons les conditions nécessaires et suffisantes pour la convergence uniforme, globale et asymptotique (UGAS), sous la condition d'excitation persistante et qui ont été bien établies dans [73] :
On considère les systèmes non linéaires à temps variant $\dot{z} = F(t, z)$ avec

$$F(t, z) := \begin{bmatrix} A(t, z) + B(t, z) \\ C(t, z) \end{bmatrix}, \tag{2.30}$$

On suppose que $A(\cdot, 0) \equiv 0$, $B(\cdot, 0) \equiv 0$ et $C(\cdot, 0) \equiv 0$. En outre, on définit

$$B_\circ(t, z_2) := B(t, z)\big|_{z_1=0}, \tag{2.31}$$

Supposons que les hypothèses suivantes sont satisfaites.

Hypothèse 2.4. *Il existe une fonction localement Lipschitzienne $V : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$, des fonctions α_1, α_2 de classe $\mathcal{K}_\infty$ et une fonction continue, positive et définie α_3 telles que*

$$\alpha_1(|z|) \leq V(t, z) \leq \alpha_2(|z|) \tag{2.32}$$

$$\dot{V}(t, z) \leq -\alpha_3(z_1). \tag{2.33}$$

Hypothèse 2.5. *Les fonctions A, B et C sont localement Lipschitziennes en z uniformément en t. De plus, pour tout $\Delta \geq 0$, il existe $b_M > 0$ et des fonctions continues non décroissantes $\rho_i : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ telles que $\rho_i(0) = 0$ et pour presque tout $t \in \mathbb{R}$ et $z \in \mathbb{R}^n$*

$$\max_{|z_2| \leq \Delta} \left\{ |B_\circ(t, z_2)| \,, \left| \frac{\partial B_\circ}{\partial t} \right| , \left| \frac{\partial B_\circ}{\partial z_2} \right| \right\} \leq b_M \,, \tag{2.34}$$

$$|B(t,z) - B_\circ(t, z_2)| \leq \rho_1(|z_1|) \tag{2.35}$$

$$\max_{|z_2| \leq \Delta} \{ |A(t,z)| \,, |C(t,z)| \} \leq \rho_2(|z_1|) \tag{2.36}$$

Théorème 2.6. *[73] Le système (2.30) sous les hypothèses 2.4-2.5 est uniformément, globalement, asymptotiquement stable si et seulement si $B_\circ(\cdot, \cdot)$ vérifie la condition de δ-excitation persistante uniforme*[4].

Nous sommes maintenant prêts à présenter notre principal résultat (2.10).

Théorème 2.7. *On considère le système (2.1) et l'observateur (2.10) avec les lois d'adaptation (2.11), (2.12). Supposons que les conditions (2.13)–(2.21) soient vérifiées. Donc, l'origine $(e, \tilde{m}, \tilde{\beta}) = (0, 0, 0)$ du système d'erreur (2.24)–(2.26) est uniformément, globalement, asymptotiquement stable* si et seulement s'*il existe μ, $T > 0$ tels que*

$$\int_t^{t+T} g(x(s))^\top H^\top H g(x(s)) ds \;\geq \mu, \qquad \forall\, t \geq 0 \,. \tag{2.37}$$

Remarque 2.8. Signalons que la propriété d'excitation persistante est supposée vérifiée pour la fonction g le long des trajectoires du système maître et non pas le long les trajectoires de l'erreur d'estimation destinée à converger vers zéro. Ceci est crucial puisque le système maître doit rester en régime chaotique.

Démonstration du théorème 2.7 :

La démonstration est basée sur le théorème 2.6 conjointement avec les définitions suivantes : $z_1 = e$, $z_2 = \text{col}[\tilde{m} \,, \tilde{\beta}]$, donc en utilisant $\hat{x}(t) = x(t) - z_1$,

$$\begin{aligned}
A(t,z) &:= Ne + H[f(x(t)) - f(x(t) - z_1)] + H[g(x(t)) - g(x(t) - z_1)]m(t) - \frac{1}{2}\beta H M C_1 z_1 \\
B(t,z) &:= \begin{bmatrix} Hg(x(t) - z_1) & \frac{1}{2} H M C_1 z_1 \end{bmatrix} \begin{bmatrix} \tilde{m} \\ \tilde{\beta} \end{bmatrix} \\
C(t,z) &:= \begin{bmatrix} -\delta g(x(t) - z_1)^\top M C_1 z_1 - \dot{m} \\ -\gamma \, |M C_1 z_1|^2 \end{bmatrix} .
\end{aligned}$$

4. Une fonction $\phi(\cdot, \cdot) : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^m$ vérifie la condition de δ-excitation persistante si pour tout $x = \text{col}[x_1, x_2] \in \mathcal{D}_1 := \mathbb{R}^{n_1}/\{0\} \times \mathbb{R}^{n_2}$ (où $x_1 \in \mathbb{R}^{n_1}$ et $x_2 \in \mathbb{R}^{n_2}$), il existe $\delta > 0$, $T > 0$ et $\mu > 0$ tels que $\forall t \in \mathbb{R}$, $|z - x| \leq \delta \Longrightarrow \int_t^{t+T} |\phi(s, z)| \, ds \geq \mu$. ([74], Définition 3)
Pour plus de détails, le lecteur est invité à consulter la référence [74].

Clairement, l'hypothèse 2.5 du théorème 2.6 est vérifiée. La condition nécessaire et suffisante d'excitation persistante est équivalente à (2.37) puisque[5] $B_\circ(t, z_2) = Hg(x(t))\tilde{m}$. Le fait que l'hypothèse 2.4 soit vérifiée résulte de la démonstration de la proposition 2.1. ■

2.3.3 Procédure de synthèse de l'observateur

Nous avons montré que le système esclave (2.10) accomplit l'objectif de synchronisation si les conditions (2.13)–(2.21) sont vérifiées. Dans cette section, nous montrons en détail comment ces conditions peuvent être satisfaites. En particulier, nous présentons une procédure pour déterminer les matrices utilisées dans les équations (2.13)–(2.21). Tout d'abord, nous considérons les équations (2.18) et (2.19). Elles peuvent s'écrire sous la forme

$$T \begin{bmatrix} C & G \end{bmatrix} = \begin{bmatrix} C_1 & 0 \end{bmatrix}, \tag{2.38}$$

qui est de la forme

$$XR_1 = R_2, \tag{2.39}$$

pour laquelle, étant données les matrices R_1 et R_2, le but est de trouver X. D'après [66], l'équation (2.39) est solvable si et seulement si

$$\text{Rang} \begin{bmatrix} R_1 \\ R_2 \end{bmatrix} = \text{Rang}[R_1] \tag{2.40}$$

et pour toute matrice Z de dimensions appropriées, la solution est donnée par

$$X = R_2 R_1^+ - Z(I - R_1 R_1^+), \tag{2.41}$$

où R^+ représente la pseudo-inverse de R *i.e.*, telle que[6] $RR^+R = R$. Par conséquent, T peut être obtenue à partir de l'équation (2.41) avec

$$X = T, \quad R_1 = \begin{bmatrix} C & G \end{bmatrix}, \quad R_2 = \begin{bmatrix} C_1 & 0 \end{bmatrix} \tag{2.42}$$

Considérons ensuite les équations (2.14) et (2.15). Étant donnée une matrice arbitraire K telle que $J = -NE - K$, les équations (2.14) et (2.15) deviennent respectivement,

$$PA + KC = N \tag{2.43}$$

$$KG = -PF\,. \tag{2.44}$$

5. D'après la propriété [[74], Propriété 3, p191], la condition d'excitation persistante au sens usuel (2.37) est équivalente à l'hypothèse de δ-excitation persistante uniforme.

6. Une méthode pratique pour calculer R^+, consiste à trouver une décomposition en valeurs singulières de R telle que $R = USV^\top$ avec U et V sont des matrices unitaires et *e.g.*, $S := [S_1\, 0]$ est non-négative et de même dimension que R, avec S_1 carrée et diagonale. Donc, $R^+ = V\tilde{S}U^\top$ avec $\tilde{S} := [S_1^{-1}\, 0]^\top$. Par définition, $R^+ = 0$ if $R = 0$.

La condition nécessaire et suffisante pour la solvabilité de (2.44) est

$$\text{Rang}\begin{bmatrix} G \\ -PF \end{bmatrix} = \text{Rang}[G] \tag{2.45}$$

et, selon (2.41), sa solution générale est

$$K = -PFG^{+} - L(I - GG^{+}) \tag{2.46}$$

où G^{+} est l'inverse généralisée de G et L une matrice arbitraire de dimensions appropriées. Utilisant (2.43) dans (2.46), on déduit que

$$N = A_1 - LC_1 \tag{2.47}$$

avec

$$A_1 = PA - PFG^{+}C \tag{2.48}$$

$$C_1 = (I - GG^{+})C. \tag{2.49}$$

D'après [75], Les conditions nécessaires et suffisantes de solvabilité des équations (2.20) et (2.21) sont

$$\text{Rang}[C_1 H] = \text{Rang}[H] \tag{2.50}$$

$$\text{Rang}\begin{bmatrix} A_1 - \lambda I & H \\ C_1 & 0 \end{bmatrix} = n + \text{Rang}[H] \tag{2.51}$$

pour tout nombre complexe λ tel que $Re(\lambda) \geq 0$. Pour résoudre (2.20), (2.21) avec $N = A_1 - LC_1$, on considère le problème convexe d'optimisation suivant [75] : Minimiser ρ tel que

$$Q > 0 \tag{2.52}$$

$$QA_1 + A_1^{\top}Q + WC_1 + C_1^{\top}W^{\top} < 0 \tag{2.53}$$

$$\begin{bmatrix} \rho I & H^{\top}Q - MC_1 \\ QH - C_1^{\top}M^{\top} & \rho I \end{bmatrix} \leq 0\,. \tag{2.54}$$

La solution à ce problème implique un minimum $\rho = 0$, Q et M tels que $L = -Q^{-1}W$ satisfassent (2.20), (2.21) avec $N = A_1 - LC_1$. ■

Nous avons démontré que l'observateur adaptatif (2.10) – (2.12) garantit la convergence de l'erreur d'estimation pour une classe générale des systèmes non linéaires (chaotiques). Les conditions nécessaires et suffisantes sont données par (2.40), (2.45), (2.50) et (2.51) qui imposent des propriétés structurelles au système maître.

Pour conclure, un algorithme pour calculer les matrices de l'observateur se présente comme suit.

Étape 1 : calculer C_1 en utilisant l'équation (2.49) ;

Étape 2 : calculer T en utilisant les équations (2.41) and (2.42) ;

Étape 3 : si $p = n$, choisir $E = T$. Sinon, si $p < n$, choisir $E = \begin{bmatrix} T \\ 0 \end{bmatrix}$;

Étape 4 : calculer H et P en utilisant respectivement les équations (2.16) et (2.17) ;

Étape 5 : calculer A_1 en utilisant l'équation (2.48) ;

Étape 6 : trouver les matrices M, L et Q après la résolution du problème convexe d'optimisation présenté dans l'analyse précédente. Nous pouvons également appliquer la méthode détaillée dans [75], pour déterminer les matrices M, L et Q.

Étape 7 : calculer K et N en utilisant respectivement les équations (2.46) et (2.47) ;

Étape 8 : calculer $J = -NE - K$.

2.4 Applications : synchronisation des systèmes chaotiques pour la transmission d'informations

Nous présentons maintenant deux exemples d'application de notre méthode de synchronisation pour la transmission d'informations en utilisant des porteuses chaotiques. La technique que nous utilisons pour la transmission d'informations est la technique de modulation paramétrique. Notons que cette méthode doit être utilisée avec précaution dans le cas des transmissions sécurisées. En effet, cette méthode s'est avérée sensible à quelques techniques d'attaques et d'interception des informations transmises. Par exemple, dans [31], les auteurs présentent des cas pour lesquels la technique de modulation paramétrique échoue dans la sécurisation l'information ; en effet, l'information transmise peut être restaurée en utilisant des technologies simples tels que les filtres passe-bas – voir également la référence [76]. Néanmoins, la technique de modulation paramétrique est efficace dans les applications qui n'exigent pas un niveau élevé de confidentialité telles que les schémas de transmission CDMA (code-division-multiple-access, en Anglais).

2.4.1 Exemple 1 : Émetteur à base du système de Rössler

On considère un émetteur à base du système de Rössler avec les paramètres $a = 0.398$, $b = 2$ et $c = 4$. On suppose que la même perturbation $d(t)$ agit dans les trois dynamiques ainsi que dans les équations de sortie. Pour la transmission d'informations, on utilise la technique de modulation paramétrique en injectant un message binaire $m(t)$ dans la dynamique du système maître. Ainsi

l'émetteur est représenté par le système suivant

$$\dot{x}_1 = -(x_2 + x_3) + d(t) \tag{2.55a}$$
$$\dot{x}_2 = x_1 + ax_2 + d(t) \tag{2.55b}$$
$$\dot{x}_3 = b + x_3(x_1 - c) + m(t)x_3 + d(t) \tag{2.55c}$$
$$y_1 = x_1 + 2d(t) \tag{2.55d}$$
$$y_2 = x_3 + d(t) \tag{2.55e}$$

qui possède la forme (2.1) avec $g_0(x) = x_3$,

$$C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad G = \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \quad F = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

Sous ces conditions, l'émetteur (2.55) fonctionne en régime chaotique malgré la présence des perturbations additives et l'injection du signal d'information. La figure 2.1 représente les attracteurs des systèmes (2.55) et (2.4) sous les conditions initiales fixées à $x_0 = [0.2, -0.4, -0.2]^\top$ pour les deux systèmes (avec et sans perturbations).

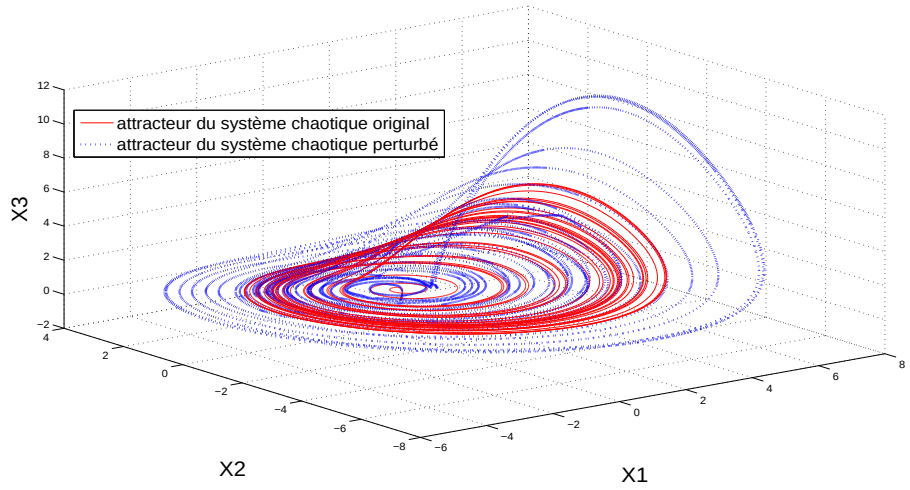

FIGURE 2.1: Attracteurs du système de Rössler (2.4) et de l'émetteur à base du système de Rössler-perturbé (2.55)

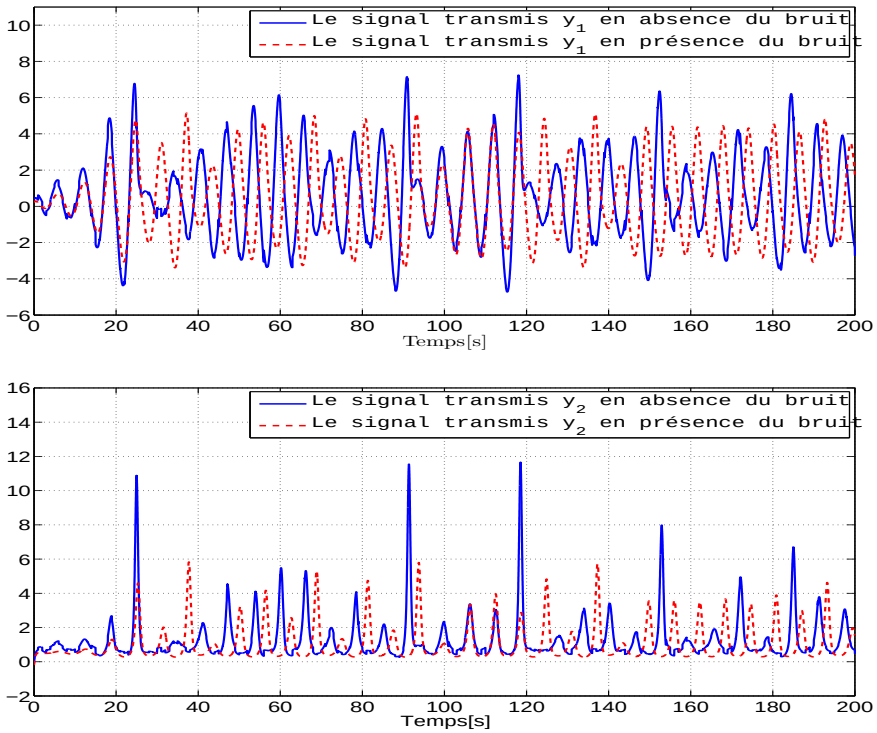

FIGURE 2.2: Graphe des signaux de sortie $y_1(t)$ et $y_2(t)$

Soit $\Omega := \{x \in \mathbb{R}^3 : |x_i| \leq \omega_i \ \forall\, i \in \{1 \dots 3\}\}$. Observons à partir de la figure 2.1 que Ω contient strictement l'attracteur du système.

On fixe les niveaux de saturation à $\omega_1 = \omega_2 = \omega_3 = 12$ et on définit $f(x) := f_0(\sigma(x))$ et $g(x) := g_0(\sigma(x))$. Clairement, $f(x) = f_0(x)$ et $g(x) = g_0(x)$ pour tout $x \in \Omega$. Ainsi, l'émetteur (2.55) prend la forme (2.9) avec $f(x) = 2 + \sigma_1(x)\sigma_3(x)$ et $g(x) = \sigma_3(x)$.

Remarque 2.9. Notons que la condition d'excitation persistante est généralement satisfaite dans le cas des systèmes chaotiques qui présentent des dynamiques suffisamment riches, elle est notamment satisfaite dans le cas du système de Rössler étudié dans cet exemple et le cas du système de Genesio Tsei qui sera présenté, par la suite, dans le deuxième exemple. La propriété d'excitation persistante peut être vérifiée numériquement à l'aide des simulations sous Matlab en calculant une approximation du terme $N(t) = \int_t^{t+T} g(x(s))^\top H^\top H g(x(s)) ds$, sur un temps de simulation arbitraire : par exemple $t \in [0, 1000]$, sachant que la valeur de T est fixée arbitrairement.

Le système récepteur est décrit par les équations (2.10) et les lois d'adaptation (2.11) et (2.12). Pour trouver les valeurs des matrices de l'observateur, nous utilisons la procédure de calcul décrite précédemment dans la section 2.3.3. On obtient :

$$T = \begin{bmatrix} 0.2 & -0.4 \\ -0.4 & 0.8 \end{bmatrix}, \quad E = \begin{bmatrix} 0.2 & -0.4 \\ -0.4 & 0.8 \\ 0 & 0 \end{bmatrix}, H = \begin{bmatrix} -0.4 \\ 0.8 \\ 1 \end{bmatrix}, \quad P = \begin{bmatrix} 1.2 & 0 & -0.4 \\ -0.4 & 1 & 0.8 \\ 0 & 0 & 1 \end{bmatrix},$$

$$A_1 = \begin{bmatrix} -0.32 & -1.2 & 0.24 \\ 0.44 & 0.798 & -3.08 \\ -0.4 & 0 & -4.2 \end{bmatrix}, C_1 = \begin{bmatrix} 0.2 & 0 & -0.4 \\ -0.4 & 0 & 0.8 \end{bmatrix}, Q = \begin{bmatrix} 5.1283 & 4.9395 & -2.6505 \\ 4.9395 & 6.5315 & -3.2496 \\ -2.6505 & -3.2496 & 3.0395 \end{bmatrix},$$

$$L = \begin{bmatrix} ccc19.9972 & -39.9943 \\ -40.0010 & 80.0020 \\ -50.0030 & 100.0059 \end{bmatrix}, M^\top = \begin{bmatrix} -0.75 \\ 1.5 \end{bmatrix}, K = \begin{bmatrix} -20.3172 & 39.8343 \\ 39.441 & -80.282 \\ 49.603 & -100.2059 \end{bmatrix}$$

$$N = \begin{bmatrix} -20.3172 & -1.2 & 40.2343 \\ 40.4410 & 0.798 & -83.082 \\ 49.603 & 0 & -104.2059 \end{bmatrix}, J = \begin{bmatrix} 23.9006 & -47.0012 \\ -47.21 & 95.82 \\ -59.5235 & 120.0471 \end{bmatrix}$$

Les gains d'adaptation sont $\delta = 200$ et $\gamma = 5000$.

Pour mettre notre contribution en perspective, nous avons réalisé des simulations avec l'observateur adaptatif (2.10) ainsi que l'observateur adaptatif classique de type 'Luenberger'

$$\dot{\hat{x}} = Ax + f(\hat{x}) + Bg(\hat{x})\hat{m} + L_2(y - C\hat{x}) \tag{2.56a}$$
$$\hat{m} = kg(\hat{x})^\top M_2(y - C\hat{x}) \tag{2.56b}$$

où k est un nombre positif. D'après les références [22, 75], on obtient

$$L_2 = \begin{bmatrix} 0.8424 & 0 \\ -0.6459 & 0 \\ 0 & 20 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 0 & 1 \end{bmatrix}$$

et $k = 200$. Supposons que le message transmis est un signal binaire tel que $m(t) = 0.5\text{sign}(\sin(0.2t))$ Les conditions initiales de deux récepteurs (2.10) et (2.56) sont fixées à $\hat{x}_0 = [-0.12,\ 0.24,\ 0]^\top$ et le message estimé $\hat{m}$ est initialisé à $\hat{m}_0 = 0$. Ainsi, les deux systèmes esclaves (2.10) et (2.56) qui doivent synchroniser avec le même système maître (2.4) sont soumis aux même conditions initiales et dont l'objectif est de restaurer le signal $m(\cdot)$.

Les résultats de simulation se présentent comme suit. Tout d'abord, des tests sont réalisés sans bruit (*i.e.*, avec $d = 0$) ; les résultats obtenus sont représentés dans les figures 2.4, 2.5, 2.6 et 2.7. Remarquons que les deux récepteurs possèdent des performances acceptables en termes de synchronisation et restauration de l'information transmise.

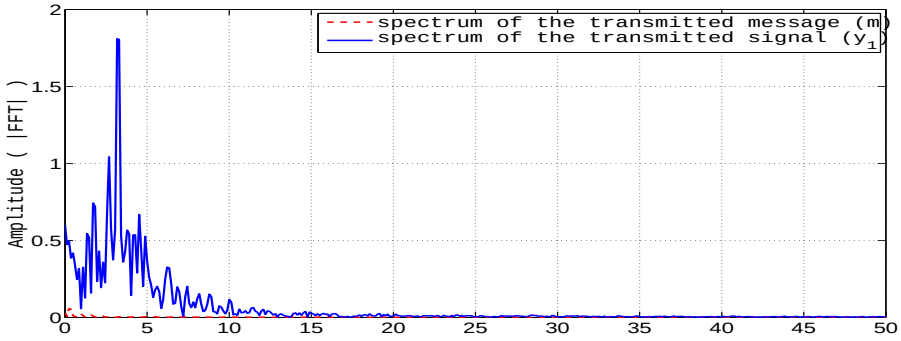

FIGURE 2.3: Diagramme de spectre du signal chaotique porteur et de l'information

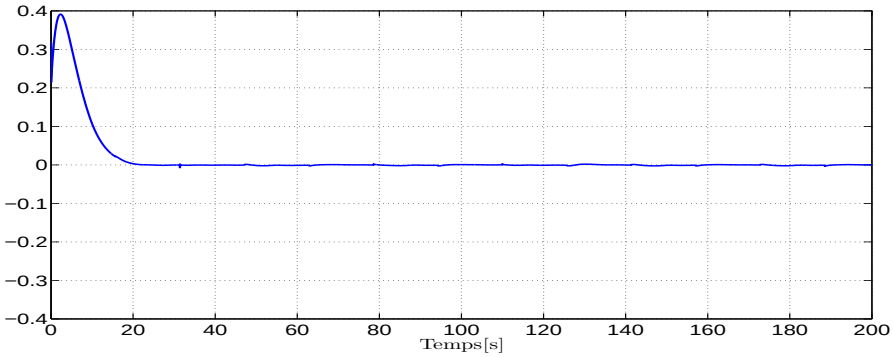

FIGURE 2.4: Erreur de synchronisation $e_1 = x_1 - \hat{x}_1$ pour l'observateur adaptatif (2.10) en absence du bruit et perturbations

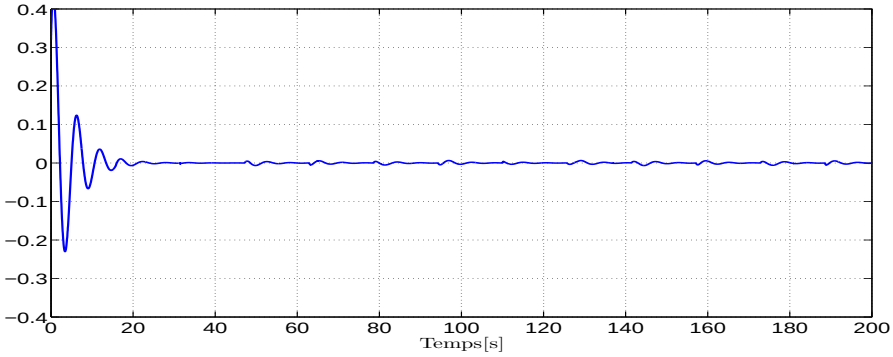

FIGURE 2.5: Erreur de synchronisation $e_1 = x_1 - \hat{x}_1$ en appliquant l'observateur (2.56) en absence du bruit et perturbations

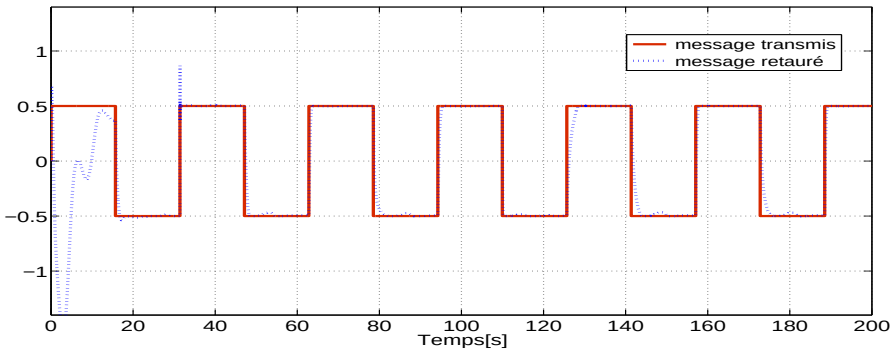

FIGURE 2.6: Le message transmis m et le message restauré $\hat{m}$ par l'observateur adaptatif classique (2.10) en présence du bruit et perturbations

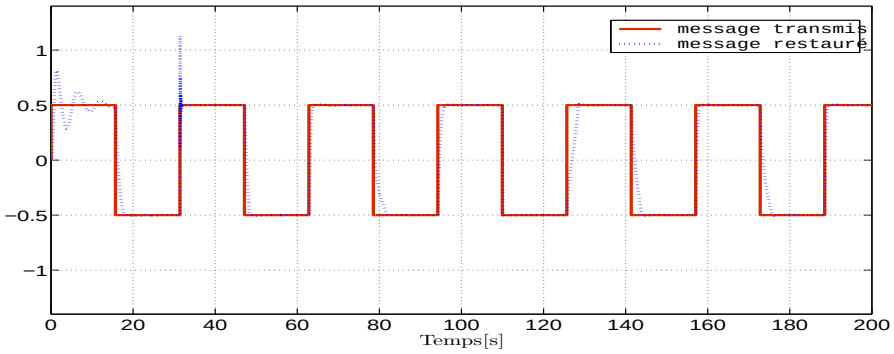

FIGURE 2.7: Le message transmis $m$et le message restauré $\hat{m}$ en appliquant notre observateur (2.56) en présence du bruit et perturbations

Ensuite, les simulations sont réalisées dans le cas où l'émetteur (2.55) est perturbé. La perturbation $d(t)$ est un bruit aléatoire uniformément distribué généré entre les bornes inférieure et supérieure respectivement égales à 0 et 0.4. Ce qui corresponds à un rapport signal/bruit (SNR) égal à $-17.5dB$.

Les résultats de simulation sont montrés dans les figures 2.8 et 2.9. Notons que l'effet du bruit et des perturbations est parfaitement annulé. En effet, l'erreur de synchronisation n'est pas affectée comme illustré dans la figure 2.8. Afin de comparer entre les deux observateurs, nous montrons dans la figure 2.9 les performances du récepteur (2.56).

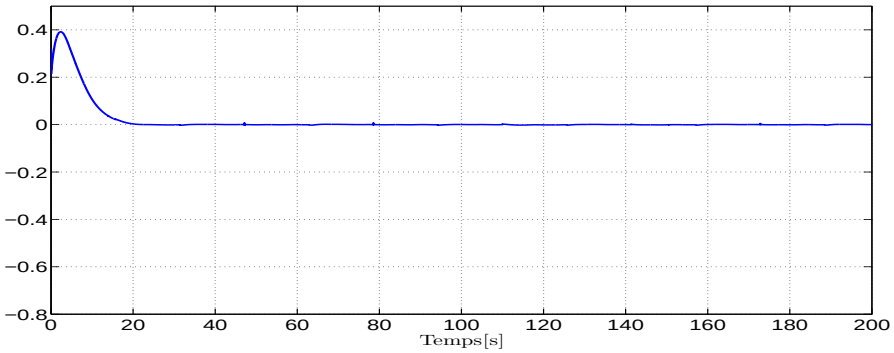

FIGURE 2.8: Erreur de synchronisation $e_1 = x_1 - \hat{x}_1$ en utilisant l'observateur (2.10) en présence du bruit et perturbations

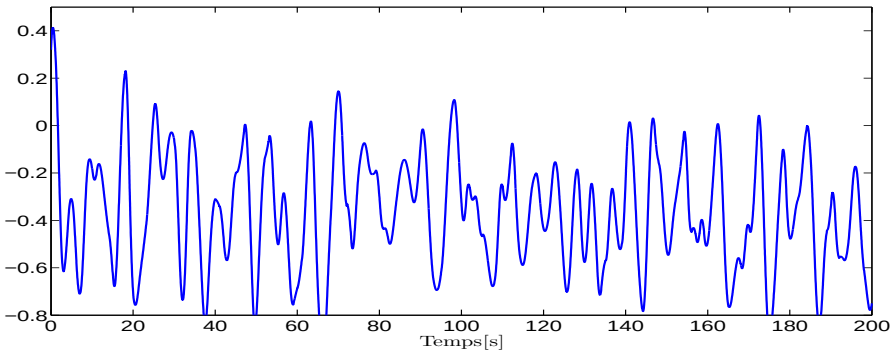

FIGURE 2.9: Erreur de synchronisation $e_1 = x_1 - \hat{x}_1$ en utilisant l'observateur (2.56) en présence du bruit et perturbations

L'amélioration des performances en présence du bruit et des perturbations est clairement illustrée dans les figures 2.10 et 2.11 qui représentent les informations transmises et restaurées pour les deux observateurs (2.10) et (2.56), respectivement.

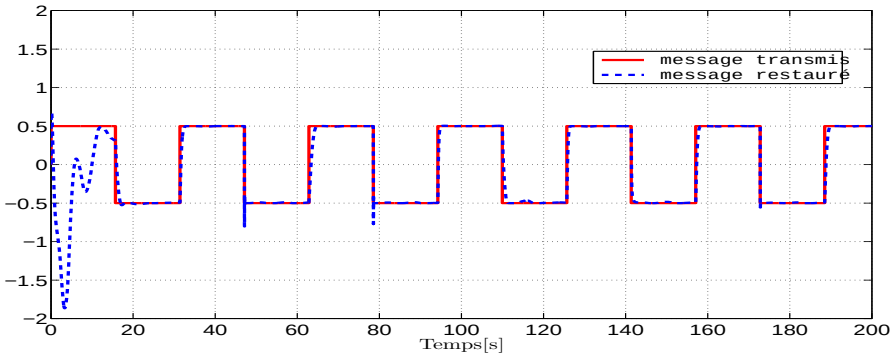

FIGURE 2.10: Le message transmis m et le message restauré $\hat{m}$ en appliquant l'observateur (2.10) en présence du bruit et perturbations

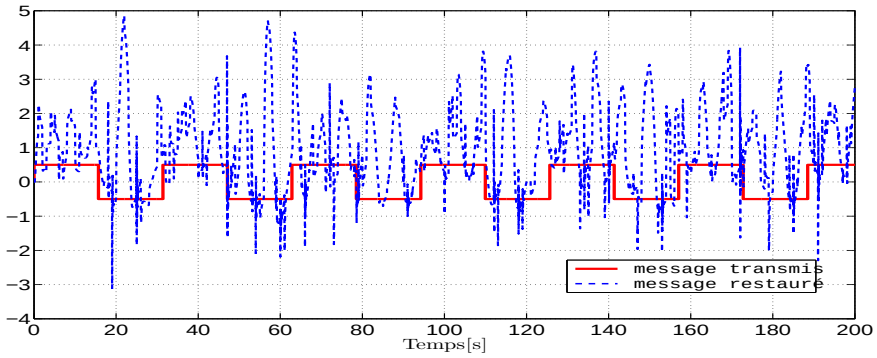

FIGURE 2.11: Le message transmis m et le message restauré $\hat{m}$ en appliquant l'observateur (2.56) en présence du bruit et perturbations

Dans les simulations précédentes, le signal d'information utilisé est de faible fréquence. Autres tests sont également réalisés dans le cas de fréquences plus élevées de la fonction $m(t)$. Les figures 2.12 et 2.13 représentent l'estimation du message avec des fréquences relativement élevées et en appliquant deux gains d'adaptation différents $\delta_1 = 20000$ et $\delta_2 = 5000$, respectivement. Comme illustré dans les deux figures, dans le cas des fréquences élevées, nous devons augmenter suffisamment les gains d'adaptation pour améliorer la qualité de restauration du message transmis. Nous observons également qu'en augmentant le gain adaptatif, on diminue le temps de convergence paramétrique.

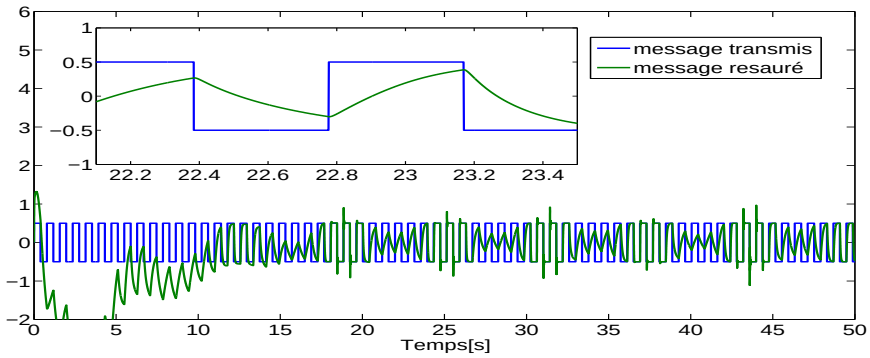

FIGURE 2.12: Le message de haute fréquence m et le message restauré $\hat{m}$ en appliquant l'observateur (2.10) en présence du bruit et perturbations ; gain d'adaptation $\delta = 5000$

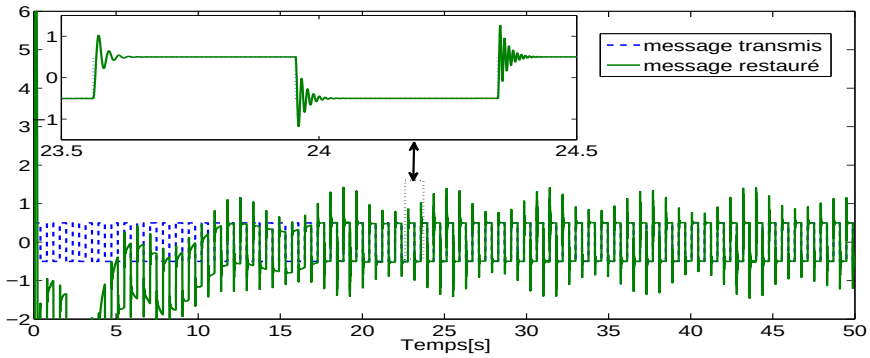

FIGURE 2.13: Le message de haute fréquence m et le message restauré $\hat{m}$ en appliquant l'observateur (2.10) en présence du bruit et perturbations ; gain d'adaptation $\delta = 20000$

2.4.2 Exemple 2 : Émetteur à base du système Genesio-Tesi avec incertitudes

Dans cette section, nous présentons un autre cas d'étude où le système émetteur est un système chaotique de Genesio-Tesi présentant des incertitudes paramétriques. En plus, la dynamique du système maître et les équations de sortie sont affectées par des perturbations. Le signal d'information de type binaire est injecté dans la dynamique de l'émetteur en modulant l'un de ses paramètres. Ainsi, le système maître se présente comme suit

$$\dot{x}_1 = x_2 + d(t) \tag{2.57a}$$
$$\dot{x}_2 = x_3 + d(t) \tag{2.57b}$$
$$\dot{x}_3 = -[c + m_1(t)]x_1 - bx_2 - ax_3 + x_1^2 + d(t) \tag{2.57c}$$

avec d une perturbation bornée. les sorties mesurées sont

$$y_1 = x_1 + 2d(t), \qquad y_2 = x_1 + x_3 + d(t)\,. \tag{2.58}$$

Selon les développements précédents, nous réécrivons le système sous la forme :

$$\begin{cases} \dot{x} = Ax + Bf_0(x) + Bg_0(x)m + Fd, \\ y = Cx + Gd \end{cases} \tag{2.59}$$

avec $x = [x_1, x_2, x_3]^T$, $y = [y_1, y_2]^T$,

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{bmatrix},\ B = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix},\ C = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$G = \begin{bmatrix} 2 \\ 1 \end{bmatrix},\ F = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix},\ m = \begin{bmatrix} a \\ b \\ m_1 \end{bmatrix},$$

$f_0(x) = x_1^2$ et $g_0(x) = [-x_3, -x_2, -x_1]$. Les paramètres a et b sont supposés inconnus. Le signal d'information est le signal binaire $m_1(t) = 0.05\text{sgn}(\sin(0.05t))$. Nous initialisons l'état du système (2.57) à $x_0 = [0.2, -0.4, -0.2]^T$. La figure 2.14 représente l'attracteur du système (2.57) sans bruit ($d = 0$) et en présence d'un bruit uniformément distribué généré entre les bornes inférieure et supérieure respectivement égales à 0 et 0.1 (2.15). On remarque qu'en présence des perturbations, l'attracteur est rétracté. La figure 2.16 illustre l'effet du bruit additif sur le signal transmis $y_1 = x_1 + 2d$. Le rapport signal/bruit (SNR) est égal à $= -14$db.

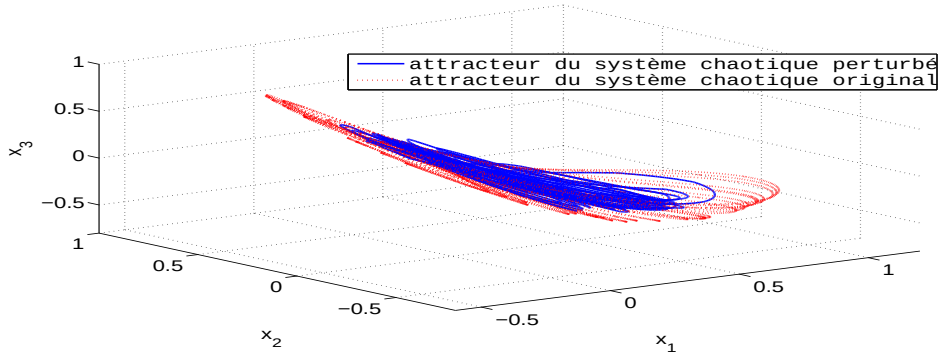

FIGURE 2.14: Attracteurs du système chaotique (2.57) avec et sans perturbations

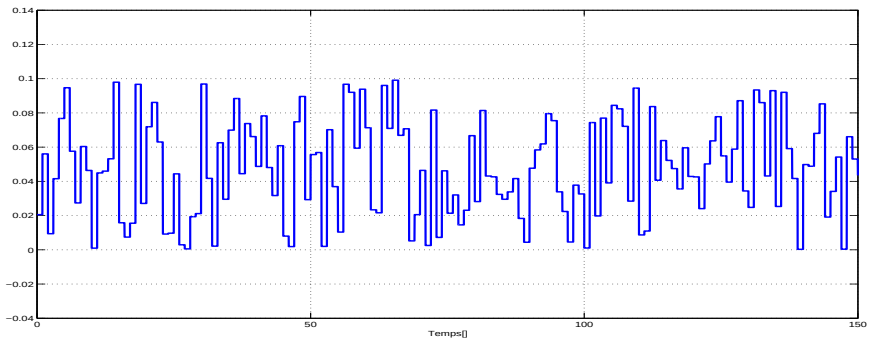

FIGURE 2.15: Le bruit uniformément distribué

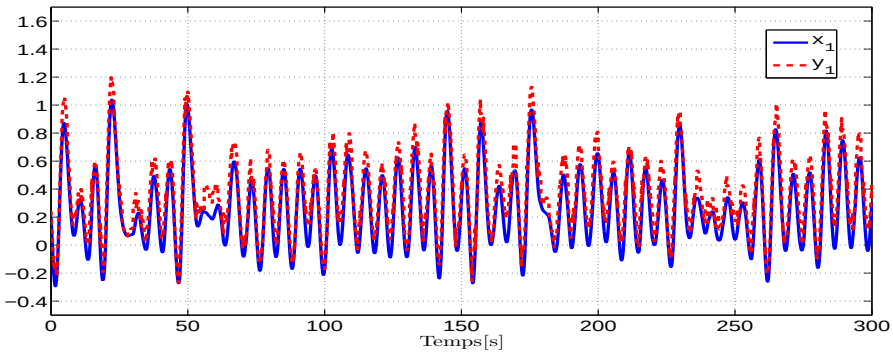

FIGURE 2.16: Effet du bruit additif sur le signal transmis y_1

On considère l'ensemble compact $\Omega = \{x \in \mathbb{R}^n \ : \ |x_i| \leq \omega_i, \ 1 \leq i \leq 3\}$ avec $\omega_1 = \omega_2 = \omega_3 = 2$. Nous déduisons à partir de la figure 2.14, que Ω contient strictement l'attracteur du système (2.57). Soit $\sigma(x)$ une fonction de saturation définie par : $\sigma(x) = [\sigma_1(x), \sigma_2(x), \sigma_3(x)]^\top$, et pour $1 \leq i \leq 3$,

$$\sigma_i(x) = \begin{cases} \omega_i & \text{if } x_i > \omega_i \\ x_i & \text{if } -\omega_i \leq x_i \leq \omega_i \\ -\omega_i & \text{if } x_i < -\omega_i. \end{cases} \tag{2.60}$$

Dans ce cas, pour tout $x \in \Omega$, $f(x) = f_0(\sigma(x)) = f_0(x)$ et $g(x) = g_0(\sigma(x)) = g_0(x)$. En plus, $f(x)$ et $g(x)$ sont globalement Lipschitziennes en x avec les constantes de Lipschitz respectives K_f et K_g. Donc, le système peut être réécrit sous la forme

$$\begin{cases} \dot{x} = Ax + Bf(x) + Bg(x)m + Fd \\ y = Cx + Gd \end{cases} \tag{2.61}$$

avec $f(x) = \sigma_1(x)^2$ et $g(x) = [-\sigma_3(x), -\sigma_2(x), -\sigma_1(x)]$. Signalons que $[Hg(x(t))]^T$ est à excitation persistante (puisque le système émetteur (2.61) possède un comportement chaotique). Le signal de sortie y est transmis vers le récepteur conçu à base de l'observateur adaptatif à entrées inconnues (2.10). Les gains d'adaptation sont $\delta = 150$ et $\gamma = 5000$. Les matrices de l'observateur sont calculées à partir de l'algorithme donné dans la section 2.3.3 :

$$T = \begin{bmatrix} 0.2 & -0.4 \\ -0.4 & 0.8 \end{bmatrix}, \quad E = \begin{bmatrix} 0.2 & -0.4 \\ -0.4 & 0.8 \\ 0 & 0 \end{bmatrix}, H = \begin{bmatrix} -0.4 \\ 0.8 \\ 1 \end{bmatrix}, \; P = \begin{bmatrix} 1.2 & 0 & -0.4 \\ -0.4 & 1 & 0.8 \\ 0 & 0 & 1 \end{bmatrix},$$

$$A_1 = \begin{bmatrix} -0.24 & 0.8 & -0.08 \\ -1.32 & 0.4 & 0.56 \\ -0.6 & 0 & -0.2 \end{bmatrix}, C_1 = \begin{bmatrix} -0.2 & 0 & -0.4 \\ 0.4 & 0 & 0.8 \end{bmatrix}, Q = \begin{bmatrix} 9.7684 & -3.4037 & 7.7542 \\ -3.4037 & 4.5589 & -5.0082 \\ 7.7542 & -5.0082 & 9.3571 \end{bmatrix},$$

$$L = \begin{bmatrix} 4.9987 & -9.9973 \\ -9.999 & 19.998 \\ -12.4992 & 24.9984 \end{bmatrix}, \; M^\top = \begin{matrix} -1.0629 \\ 2.1258 \end{matrix}, K = \begin{bmatrix} -5.1587 & 9.9173 \\ 9.119 & -20.438 \\ 12.0992 & -25.1984 \end{bmatrix},$$

$$N = \begin{bmatrix} 1.3763 & 0.8 & 9.9173 \\ -4.2530 & 0.4 & -19.438 \\ -3.4198 & 0 & -25.1984 \end{bmatrix}, J = \begin{bmatrix} 1.4210 & -2.4420 \\ -0.2424 & 2.6848 \\ -0.7359 & 2.4717 \end{bmatrix}.$$

L'état de l'observateur est initialisé à $\hat{x}_0 = [-0.12, 0.24, 0]^T$ et le vecteur $\hat{m}$ constitué par les paramètres inconnus et le message estimé est initialisé à $\hat{m}_0 = 0$.

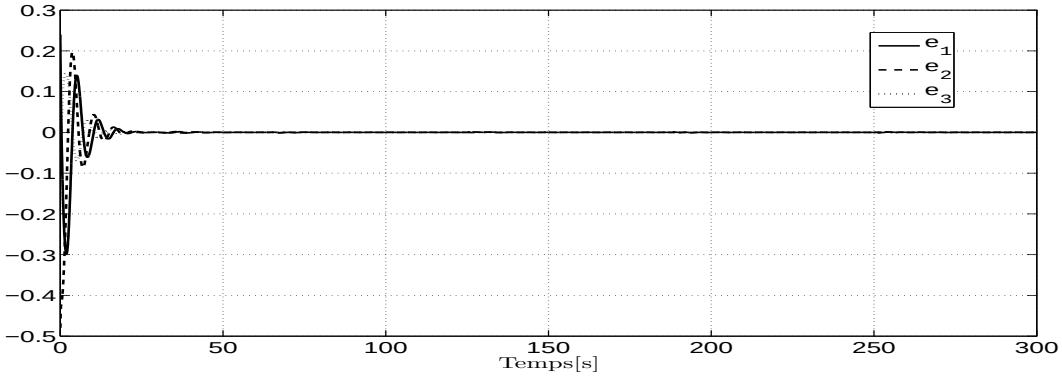

FIGURE 2.17: Erreurs de synchronisation $e_1 = x_1 - \hat{x}_1$, $e_2 = x_2 - \hat{x}_2$ et $e_3 = x_3 - \hat{x}_3$

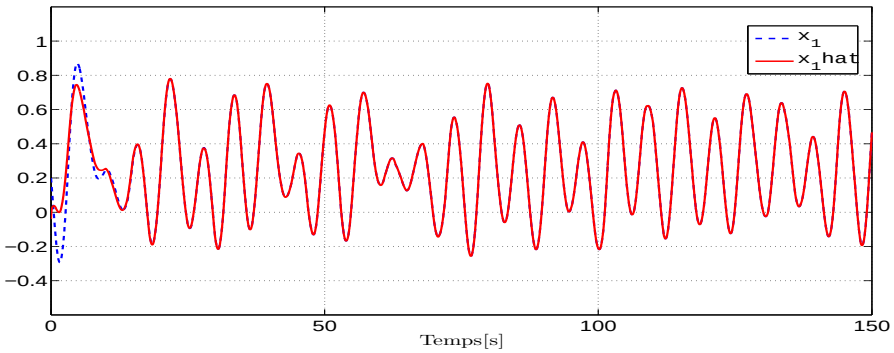

FIGURE 2.18: Comparaison entre l'état x_1 et son estimation $\hat{x}_1$

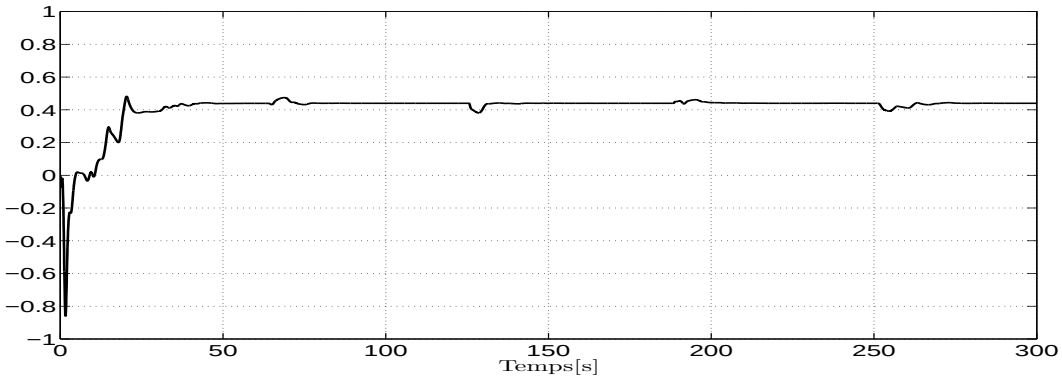

FIGURE 2.19: Estimation du paramètre a

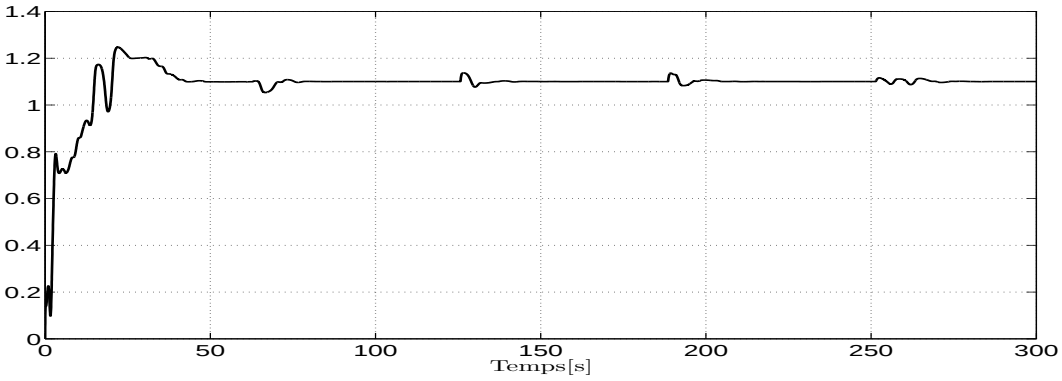

FIGURE 2.20: Estimation du paramètre b

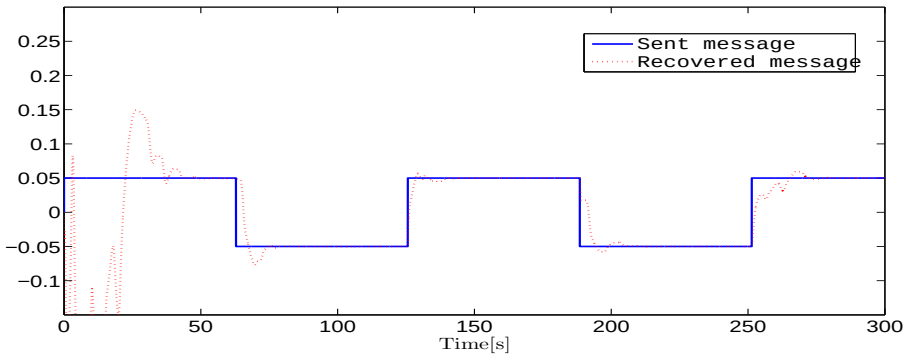

FIGURE 2.21: Le signal d'information transmis $m(t)$ et le signal restauré $\hat{m}(t)$

Les résultats de simulation représentés dans les figures 2.17 et 2.18 montrent que le bruit est parfaitement annulé par l'observateur et l'erreur de synchronisation n'est pas affectée. De plus, en présence des perturbations, les paramètres inconnus a et b ainsi que le signal d'information $m(t)$ sont bien restaurés comme illustré dans les figures 2.19, 2.20 et 2.21.

2.5 Conclusion

Nous avons présenté une méthode de synchronisation maître-esclave basée sur l'estimation robuste et adaptative pour une classe des systèmes non linéaires affectés par des perturbations additives et des incertitudes paramétriques et telle que les signaux mesurés sont soumis à un bruit (affectant le canal de transmission). L'approche est appliquée à des modèles des systèmes chaotiques utilisés pour la transmission d'informations modélisées par des fonctions constantes par morceaux. Nous avons établi les conditions nécessaires et suffisantes pour l'estimation des paramètres inconnus, la restauration des informations transmises et le rejet des perturbations. En particulier, nous avons présenté deux exemples de systèmes chaotiques utilisés dans un schéma de synchronisation maître-esclave classique pour la transmission des informations. Nous avons démontré que la méthodologie proposée possède des bonnes performances et une robustesse face aux bruits. En effet, ni la stabilité, ni la qualité de restauration de l'information sont compromises par les perturbations et le bruit présent dans le canal public. Notons, en revanche, que la méthode de transmission par modulation paramétrique est spécifique seulement aux messages binaires lentement variants. Dans le chapitre suivant, nous proposons une méthode de synchronisation adaptative à base d'observateurs à modes glissants et son application dans un nouveau schéma de communication.

Chapitre 3

Synchronisation à base d'observateurs adaptatifs à " modes glissants"

3.1 Introduction

Dans ce chapitre, nous proposons une méthodologie de synchronisation à base d'un *observateur adaptatif par modes glissants* et son application dans un schéma de communication sécurisée. La méthode de synthèse de l'observateur repose essentiellement sur les techniques de conception d'observateurs singuliers, la théorie des modes glissants et la commande adaptative. En utilisant des arguments à partir de la théorie de Lyapunov, nous démontrons la stabilité pratique et la convergence de l'erreur d'estimation vers un ensemble compact centré autour de l'origine.
Dans la deuxième partie de ce chapitre, les observateurs adaptatifs par modes glissants sont utilisés dans un nouveau schéma de communication sécurisée basé sur la synchronisation maître-esclave des systèmes chaotiques. Les performances du schéma en termes de sécurité, de robustesse aux attaques et de qualité de transmission, sont testées à travers deux cas d'étude utilisant différents modèles des systèmes chaotiques et à travers une application de cryptage des images binaires.

3.2 Synthèse d'observateurs adaptatifs à "modes glissants"

Dans cette section, nous développons un observateur adaptatif à "modes glissants" pour une classe de systèmes non linéaires présentant des non-linéarités "Lipschitziennes" [1], des entrées inconnues dans sa dynamique et du bruit dans les signaux de sortie. On suppose que les états, les entrées inconnues et le bruit dans l'équation de sortie sont bornés tel que les valeurs exactes des bornes supérieures sont inconnues ; la constante de Lipschitz est également supposée inconnue. L'objectif de l'observateur est d'estimer conjointement les états et les entrées inconnues malgré la présence du bruit dans l'équation de sortie. En particulier, le problème de synthèse d'observateurs à modes glissants pour les systèmes

1. On suppose que les non-linéarités sont de classe $\mathcal{C}^1$, néanmoins on utilise la bornitude des trajectoires et on applique la technique de transformation de Lipschitz. Voir p. 72.

présentant des entrées inconnues et dont les signaux de sortie sont affectés par du bruit reste un problème ouvert. Notons néanmoins que dans la référence [58], les auteurs considèrent un système linéaire en présence des entrées inconnues ou du bruit de mesure, mais pas simultanément. Dans le même contexte, dans [77], les auteurs proposent un observateur par modes glissants d'ordre supérieur pour une classe des systèmes linéaires où la même perturbation affecte la dynamique et la sortie mesurée. Notre approche repose sur la combinaison entre les techniques de synthèse d'observateurs singuliers, la théorie des observateurs par modes glissants et la commande adaptative.
Dans une première étape et après avoir formulé le problème, nous faisons une étude préliminaire dans la section 3.2.2 dans laquelle nous analysons le problème et nous expliquons les étapes de construction de notre observateur. Suite à cette analyse, nous constaterons que l'utilisation des lois d'adaptation, dont l'objectif est de compenser l'effet des non-linéarités et des incertitudes sur les bornes de différents signaux, ne permet pas d'atteindre le mode glissant idéal, ni la convergence en temps fini de l'erreur d'estimation. Dans la section 3.2.3, nous apportons des modifications appropriées sur la structure de l'observateur afin d'établir la stabilité pratique et nous prouvons que l'erreur d'estimation converge vers un ensemble compact centré autour de l'origine et qu'on peut réduire arbitrairement en agissant convenablement sur les paramètres de l'observateur : ainsi, les états du système ainsi que les entrées inconnues peuvent être reconstruits avec une faible tolérance malgré la présence du bruit dans l'équation de sortie. Dans la section 3.2.5, nous présentons un exemple numérique d'un robot flexible afin d'illustrer nos résultats théoriques.

3.2.1 Contexte et position du problème

On considère les systèmes non linéaires

$$\dot{x}_* = A_0 x_* + B f_0(x_*) + F\eta_1(t) \tag{3.1a}$$
$$y = C_0 x_* + G_0 \eta_2(t), \tag{3.1b}$$

où $x_* \in \mathbb{R}^n$ représente le vecteur d'état et $\eta_1 \in \mathbb{R}^{q_1}$ représente les vecteur des entrées inconnues. La sortie mesurée $y \in \mathbb{R}^p$ est contaminée par un bruit additif $\eta_2 \in \mathbb{R}^{q_2}$ et la fonction $f_0 : \mathbb{R}^n \to \mathbb{R}^s$ est de classe $\mathcal{C}^1$.

Dans les méthodes conventionnelles de synthèse d'observateurs à modes glissants de premier ordre [58, 78–80] en absence du bruit dans l'équation de sortie , on utilise souvent l'hypothèse que le nombre d'entrées inconnues ne doit pas dépasser celui des sorties mesurées, c'est à dire que $q_1 \leq p$ (voir par exemple [79, 80]) et que la condition du "degré relatif égal à1" soit vérifiée. En particulier, cette condition est utilisée dans les méthodes de conception d'observateurs par modes glissants conventionnels (du premier ordre) qui sont basées sur l'approche de Lyapunov – voir [78] et les méthodes basées sur la transformation du système sous une forme canonique (Observateur de Edwards-Supergeon) comme dans les références [79] et [58]. En contre partie, il faut bien noter que les observateurs à modes glissants d'ordre supérieur [59–62] ont l'avantage d'éviter l'hypothèse du "degré relatif égal à 1" : par exemple, dans la référence [60], les auteurs proposent une méthode de transformation sous une nouvelle forme canonique en évitant la condition du "degré relatif égal à1" ; sachant que

la sortie mesurée n'est pas affectée par un bruit, *i.e.* $y = C_0 x_*$. Ce travail a été ensuite étendu, dans [59], au cas des systèmes non linéaires localement transformables sous une forme triangulaire spécifique d'observabilité pour laquelle est proposé un nouvel observateur à modes glissants d'ordre supérieur.

Remarque 3.1. Dans le problème étudié dans ce chapitre, il est question d'estimer conjointement les états et les entrées inconnues du système. Ce problème peut être vu comme étant un problème d'inversion à gauche. En effet, le vecteur de sortie du système considéré (3.1) est un vecteur d'entrée pour l'observateur et le vecteur de sortie de ce dernier est constitué des estimées des entrées inconnues. Pour plus de détails sur les problèmes d'inversions, le lecteur est invité à consulter la référence [81] où Respondek présentait les conditions nécessaires et suffisantes pour la résolution du problème d'inversion à gauche ainsi que le problème d'inversion à droite pour les cas linéaire et non linéaire.

Dans le présent scénario, en présence du bruit dans l'équation de sortie, nous avons besoin d'imposer $q_2 \leq p$ afin que G_0 soit de plein rang : cette condition sera utilisée dans la procédure de synthèse de l'observateur comme nous allons le détailler dans la prochaine section. Par ailleurs, nous avons besoin de l'hypothèse suivante :

Hypothèse 3.2.

a) η_1, η_2 *et* y *sont tels que* $q_1 + q_2 \leq p$ *;*
b) F *et* G_0 *sont de plein rang et* $\text{rang}(C_0 F) = \text{rang}(F)$ *;*
c) L'entrée inconnue $\eta_1(t)$ *et le bruit* $\eta_2(t)$ *dans l'équation de sortie sont bornés et leurs dérivées premières sont bornées ;*
d) les solutions $x_*(t)$ *de (3.1) sont globalement uniformément bornées.*

Le critère $q_1 + q_2 \leq p$ considéré dans la condition 3.2a) est imposé comme étant une condition suffisante pour que $q_1 \leq p$ et $q_2 \leq p$ soient vérifiées simultanément. En pratique, cette hypothèse est achevée si tous les signaux de sortie ne sont pas corrompues par du bruit ou bien si tous les signaux de sortie sont affectées par le même bruit ; ce qui restreint clairement la classe des systèmes en considération.

La condition 3.2c) est une condition technique récurrente dans la littérature de la commande par modes glissants.

La condition 3.2d) est utilisée afin de permettre l'application de la technique de *transformation de Lipschitz* sur la non-linéarité f_0. Soit $x_* = [x_{*1}, \ldots, x_{*n}]^\top$, $\Omega = \{x_* \in \mathbb{R}^n, |x_{*i}| \leq \omega_i, 1 \leq i \leq n\}$ pour un ensemble de n nombres donnés $\omega_i > 0$. Soit $\varsigma : \mathbb{R}^n \to \Omega$ une fonction de saturation linéaire telle que $\varsigma(x_*) = x_*$ pour tout $x_* \in \Omega$ et $|\varsigma(x_{*i})| = 1$ ailleurs, pour toute composante x_*. On définit $f_1 : \mathbb{R}^n \to \mathbb{R}^s$ telle que $f_1(x_*) = f_0(\varsigma(x_*))$; et par conséquent $f_1(x_*) = f_0(x_*)$ pour tout $x_* \in \Omega$. En procédant comme dans le chapitre 1, en appliquant le théorème d'accroissement finis pour les fonctions vectoriels ([Théorème A.3],[71]), on peut démontrer que f_1 est globalement Lipschitzienne avec une constante de Lipschitz K_f *i.e.*,

$$|f_1(x_1) - f_1(x_2)| \leq K_f |x_1 - x_2|, \quad \forall\, x_1,\, x_2 \in \mathbb{R}^n. \tag{3.2}$$

Il s'en suit que pour tout t tel que $x_*(t) \in \Omega$, les trajectoires du système (3.1) coïncident avec celles du système :

$$\dot{x}_* = A_0 x_* + B f_1(x_*) + F\eta_1(t) \tag{3.3a}$$
$$y = C_0 x_* + G_0 \eta_2(t). \tag{3.3b}$$

Ainsi, sans perte de généralité, on suppose que le point (d) de l'hypothèse 3.2 est vérifié pour l'ensemble compact Ω. Le problème de conception d'un observateur pour le système (3.1) est donc adressé maintenant au système (3.3).

Ensuite, nous introduisons l'état augmenté $x = [x_*^\top,\ \eta_2^\top]^\top$, les matrices

$$A = \begin{bmatrix} A_0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} C_0 & G_0 \end{bmatrix}, \quad T = \begin{bmatrix} I_n & 0 \end{bmatrix}$$

et $f : \mathbb{R}^{n+q_2} \to \mathbb{R}^s$ telle que $f(x) = f_1(x_*)$. Par conséquent, le système (3.3) peut s'écrire sous la forme singulière suivante :

$$T\dot{x} = Ax + Bf(x) + F\eta_1(t), \tag{3.4a}$$
$$y = Cx. \tag{3.4b}$$

Le problème revient donc à concevoir un observateur pour le système (3.4a) ayant comme objectif d'estimer conjointement le vecteur d'état et le vecteur d'entrées inconnues malgré la présence du bruit dans la sortie mesurée.

3.2.2 Observateur adaptatif à modes glissants : analyse du problème

Notre approche d'estimation consiste en trois parties principales : tout d'abord, après avoir transformé le système original sous la forme singulière (3.3) comme déjà expliqué dans la section précédente, nous commençons par développer un observateur pour la partie linéaire de ce système. Ensuite, nous utilisons des termes inspirés de la théorie des modes glissants et du concept de commande équivalente pour reconstruire les entrées inconnues. Enfin, en se basant sur la théorie de Lyapunov, nous introduisons une loi d'adaptation afin de compenser l'effet d'une constante dépendant des bornes inconnues des états, des entrées inconnues et du bruit affectant l'équation de sortie. D'une manière similaire, l'adaptation est employée afin de compenser l'effet de la constante de Lipschitz.

3.2.2.1 Un observateur pour le système $T\dot{x} = Ax$

Soit $P : \mathbb{R}^{n+q_2 \times n}$ et $E : \mathbb{R}^{n+q_2 \times p}$ deux matrices telles que

$$PT = I + EC \tag{3.5}$$

pour les matrices C et T. Afin d'étudier la solvabilité de l'équation matricielle linéaire (3.5), nous commençons par la réécrire sous la forme

$$\begin{bmatrix} P & E \end{bmatrix} \begin{bmatrix} T \\ -C \end{bmatrix} = I_{n+q_2} \tag{3.6}$$

avec I_{n+q_2} la matrice identité de dimension $n+q_2$. L'équation (3.6) est de la forme $XR_1 = R_2$ avec $R_1 = \begin{bmatrix} T \\ -C \end{bmatrix}$, $R_2 = I_{n+q_2}$ et $X = \begin{bmatrix} P & E \end{bmatrix}$. Cette équation est solvable en X si et seulement si

$$\text{Rang} \begin{bmatrix} R_1 \\ R_2 \end{bmatrix} = \text{Rang} \begin{bmatrix} R_1 \end{bmatrix}. \tag{3.7}$$

De plus, pour toute matrice arbitraire Z_a, la solution de (3.7) est

$$X = R_2 R_1^+ - Z_a(I - R_1 R_1^+) \tag{3.8}$$

où R_1^+ représente l'inverse généralisée de R_1. La condition (3.7) est équivalente à

$$\text{Rang} \begin{bmatrix} I_n & 0 \\ -C_0 & -G_0 \\ I_n & 0 \\ 0 & I_{q_2} \end{bmatrix} = \text{Rang} \begin{bmatrix} I_n & 0 \\ -C_0 & -G_0 \end{bmatrix}.$$

Cette dernière est satisfaite si et seulement si G_0 est de plein rang – voir Hypothèse 1.1b) et [85, 86].

Maintenant, nous faisons ce choix naturel d'un observateur pour le système singulier "nominal" $T\dot{x} = Ax$:

$$PT\dot{\hat{x}} = PA\hat{x} - v_1, \tag{3.9}$$

où v_1 représente un terme correctif additionnel tel que la dynamique de l'erreur d'observation $e = x - \hat{x}$ devient :

$$\dot{e} = Ke \tag{3.10}$$

avec K est *Hurwitz*.

$$PT(\dot{x} - \dot{\hat{x}}) = PA(x - \hat{x}) + v_1. \tag{3.11}$$

En utilisant les équations (3.5) dans (3.11), on obtient :

$$\begin{aligned} \dot{e} + EC\dot{e} &= PAe + v_1 \\ \dot{e} + E\dot{y} - EC\dot{\hat{x}} &= PAe + v_1 - \dot{\hat{x}} + \dot{\hat{x}} \\ \dot{e} &= PAe + v_1 - E\dot{y} + (EC + I)\dot{\hat{x}} - \dot{\hat{x}} \\ &= PAe + v_1 + PT\dot{\hat{x}} - (E\dot{y} + \dot{\hat{x}}). \end{aligned}$$

Ensuite, soit $z := Ey + \hat{x}$, ainsi on obtient :

$$\dot{e} = PAe + v_1 + PT\dot{\hat{x}} - \dot{z},$$

et en introduisant la matrice L telle que

$$K = PA - LC \tag{3.12}$$

soit Hurwitz et si on impose

$$v_1 = -LCe + \dot{z} - PT\dot{\hat{x}}, \tag{3.13}$$

le système de l'erreur d'observation (3.10) est exponentiellement stable à l'origine.

Maintenant, on remplace v_1 par son expression dans (3.9) pour obtenir :

$$\begin{aligned}
\dot{z} &= PAz - PAEy + LCe \\
&= PAz - PAEy - LC\hat{x} + LCx \\
&= PAz - PAEy - LC(z - Ey) + LCx \\
&= Kz - KEy + Ly \\
&= Kz + (L - KE)y.
\end{aligned}$$

En résumé, l'observateur ayant la structure suivante :

$$\dot{z} = Kz + Jy, \tag{3.14a}$$
$$\hat{x} = z - Ey \tag{3.14b}$$

avec L telle que $PA - LC = K$ et $J = L - KE$, est un observateur exponentiel pour le système $T\dot{x} = Ax$ – voir également [86].

3.2.2.2 Compensation adaptative des non-linéarités

Dans cette section, nous apportons des modifications sur la structure de l'observateur (3.9) en introduisant les termes de compensation $H_1 f(\hat{x})$, $H_2 u$ et $\frac{1}{2}\hat{\beta} H_1 M(y - C\hat{x})$, avec $H_1 := PB$ et $H_2 = PF$. À la place de (3.9), nous introduisons

$$PT\dot{\hat{x}} = PA\hat{x} - v_1 + \frac{1}{2}\hat{\beta} H_1 M(y - C\hat{x}) + H_1 f(\hat{x}) + H_2 u \tag{3.15}$$

et nous remplaçons v_1 par son expression (3.13) dans l'équation (3.15) pour enfin obtenir la nouvelle structure de l'observateur :

$$\dot{z} = Kz + Jy + H_1 f(\hat{x}) + \frac{1}{2}\hat{\beta} H_1 M(y - C\hat{x}) + H_2 u \tag{3.16a}$$
$$\hat{x} = z - Ey \tag{3.16b}$$

où l'entrée u a pour but d'estimer η_1. Comme nous allons détailler dans la section suivante, la conception de u est basée sur la notion de commande équivalente : c'est à dire $u \equiv \eta_1$ si le mode glissant idéal est atteint – voir les références [87, 88]. Notons que les termes correctifs $H_1 f(\hat{x})$ et $\frac{1}{2}\hat{\beta} H_1 M(y - C\hat{x})$ sont utilisés pour compenser l'effet des non-linéarités. Cependant, puisque la constante de Lipschitz K_f est inconnue, nous utilisons la loi d'adaptation :

$$\dot{\hat{\beta}} = \gamma_1 \left| M(y - C\hat{x}) \right|^2 - \sigma_2 \hat{\beta} \tag{3.17}$$

avec γ_1 et $\sigma_2 > 0$, $\hat{\beta}$ est l'estimation d'une constante β qui dépend de K_f et de M est une matrice à déterminer. Soit $G = NC \in \mathbb{R}^{q_1 \times (n+q_2)}$ avec $N \in \mathbb{R}^{q_1 \times p}$ est telle que GH_2 est inversible. On définit les matrices :

$$A_G = \Big[I - H_2 (GH_2)^{-1} G \Big] PA \tag{3.18}$$

$$B_G = \Big[I - H_2 (GH_2)^{-1} G \Big] H_1. \tag{3.19}$$

D'après [75], pour toute matrice définie positive Q, il existe $P_G = P_G^\top$, L et M telles que

$$[A_G - LC]^\top P_G + P_G [A_G - LC] = -Q \tag{3.20}$$

$$P_G B_G = (MC)^\top, \tag{3.21}$$

si (et seulement si) pour tout nombre complexe λ tel que $Re(\lambda) \geq 0$,

$$\text{rang}(CB_G) = \text{rang}(B_G) \tag{3.22}$$

$$\text{rang} \begin{pmatrix} A_G - \lambda I & B_G \\ C & 0 \end{pmatrix} = n + \text{rang}(B_G) \tag{3.23}$$

Afin de résoudre (3.20), (3.21), nous considérons le problème d'optimisation suivant :
Minimiser ρ_* tel que

$$P_G \; > \; 0 \tag{3.24}$$

$$P_G A_G + A_G^\top P_G + RC + C^\top R^\top \; < \; 0 \tag{3.25}$$

$$\begin{bmatrix} \rho_* I & B_G^\top P_G - MC \\ P_G B_G - C^\top M^\top & \rho_* I \end{bmatrix} \geq \; 0\,. \tag{3.26}$$

Une solution pour ce dernier donne le minimum $\rho_* = 0$ tel que P_G, M, R et $L = -P_G^{-1} R$ vérifient (3.20) et (3.21).

L'entrée u dans (3.16) est un signal discontinu qui a pour objectif d'atteindre une surface invariante $\{S \equiv 0\}$ dans laquelle l'erreur d'observation $e(t)$ converge vers zéro. La variable de glissement S est définie par

$$S(t) := NCe(t) + \int_0^t GLCe(\tau) d\tau, \tag{3.27}$$

qui est équivalente à

$$\dot{S} = G\dot{e} + GLCe\,. \tag{3.28}$$

On multiplie (3.4a) par P et on soustrait (3.15). Ensuite, en procédant comme dans la section 3.2.2.1, on obtient :

$$\dot{e} \;=\; PAe - LCe - \frac{1}{2}\hat{\beta}H_1M(y - C\hat{x}) + H_1\Big[f(x) - f(\hat{x})\Big] + H_2(\eta_1 - u) \tag{3.29}$$

où nous avons utilisé l'équation (3.13). Remplaçant (3.29) dans (3.28), on obtient

$$\dot{S} \;=\; G(PA - LC)e + GH_1\Big[f(x) - f(\hat{x})\Big] + GH_2(\eta_1 - u) - \frac{1}{2}\hat{\beta}GH_1M(y - C\hat{x}) + GLCe. \tag{3.30}$$

Soit

$$u \;=\; (GH_2)^{-1}\left[(\delta + \hat{\rho})\frac{S}{|S|} - GPA\hat{x} - GH_1f(\hat{x}) - \frac{1}{2}GH_1\hat{\beta}M(y - C\hat{x})\right], \tag{3.31}$$

où $\hat{\rho}$ est un paramètre adaptatif mis à jour suivant la loi d'adaptation

$$\dot{\hat{\rho}} = \gamma_2\,|S| - \sigma\hat{\rho}. \tag{3.32}$$

Ensuite, on remplace u par son expression (3.31) dans l'équation (3.30) pour obtenir :

$$\dot{S} \;=\; -(\hat{\rho} + \delta)\frac{S}{|S|} + \Phi(\eta_1, x), \tag{3.33a}$$

$$\Phi(\eta_1, x) \;:=\; GH_2\eta_1 + GPAx + GH_1f(x). \tag{3.33b}$$

Compte tenu de l'hypothèse 3.2, $\varphi(t) := \Phi(\eta_1(t), x(t))$ est majorée par un nombre ρ défini par :

$$\rho := \sup_{t\geq 0}|\varphi(t)|\,. \tag{3.34}$$

Définissons également l'erreur d'adaptation $\tilde{\rho} = \rho - \hat{\rho}$ et considérons la fonction définie positive et radialement bornée

$$V_1(S, \tilde{\rho}) = \frac{1}{2}\,|S|^2 + \frac{1}{2\gamma_2}\tilde{\rho}^2. \tag{3.35}$$

La dérivée totale de V_1 le long des trajectoires de (3.33a) et (3.32) est donnée par

$$\begin{aligned}\dot{V}_1 \;&\leq\; |\varphi(t)|\,|S| - (\hat{\rho} + \delta)\,|S| + \tilde{\rho}\Big[-|S| + \frac{\sigma}{\gamma_2}(\rho - \tilde{\rho})\Big]\\ &\leq\; -\delta\,|S| - \frac{\sigma}{\gamma_2}\tilde{\rho}^2 + \frac{\sigma}{\gamma_2}\rho\tilde{\rho}\end{aligned} \tag{3.36}$$

En utilisant l'inégalité de Young $2\rho\tilde{\rho} \leq \rho^2 + \tilde{\rho}^2$, on obtient $\dot{V} \leq -\delta\,|S| - \frac{\sigma}{2\gamma_2}\tilde{\rho}^2 + \frac{\sigma}{2\gamma_2}\rho^2$, ce qui implique que les trajectoires de (3.33a)–(3.32) sont bornées.

Corollaire 3.3. *Soit Ω un ensemble compact tel que $x(t) \in \Omega$ pour tout t. On considère l'observateur donné par les équations (3.16), (3.31) et (3.17). Si $\hat{\rho} \equiv \rho$, donc le mode glissant $\{S = 0\}$ est atteint en temps fini.*

La démonstration s'en suit directement de l'observation que $V_1(S)$ est une fonction quadratique de S et que sa dérivée est négative définie et vérifie $\dot{V}_1 \leq -2\delta V_1^{1/2}$.

3.2.2.3 Convergence de l'erreur d'estimation

Nous nous intéressons maintenant à l'étude du comportement dynamique des trajectoires de l'erreur d'observation lorsque les trajectoires sont proches de la surface de glissement. D'après (3.30), on obtient

$$(\eta_1 - u) = (GH_2)^{-1}\Big[\frac{1}{2}\hat{\beta}GH_1MCe - GLCe - GH_1\left[f(x) - f(\hat{x})\right] - GKe + \dot{S}\Big] \tag{3.37}$$

où nous avons utilisé $K = PA - LC$. Nous remplaçons $(\eta_1 - u)$ par son expression (3.37) dans (3.29) pour obtenir

$$\dot{e} = [A_G - LC]e + B_G\Big[f(x) - f(\hat{x}) - \frac{1}{2}\hat{\beta}MCe\Big] + H_2(GH_2)^{-1}\dot{S}. \tag{3.38}$$

Soient β une constante définie par

$$\det\begin{vmatrix} \frac{\lambda_m(Q)}{2} & K_f \\ K_f & \beta \end{vmatrix} \geq 0, \tag{3.39}$$

et $\tilde{\beta} = \beta - \hat{\beta}$. La dérivée totale de la fonction définie, positive et radialement bornée

$$V_2(e, \tilde{\beta}) = e^\top P_G e + \frac{1}{2\gamma_1}\tilde{\beta}^2, \tag{3.40}$$

le long des trajectoires de l'erreur d'observation (3.38) et

$$\dot{\hat{\beta}} = -\gamma_1 \left|M(y - C\hat{x})\right|^2 + \sigma_2\hat{\beta},$$

donne

$$\dot{V}_2 \;\leq\; -e^\top Qe + 2e^\top P_G B_G\Big[f(x) - f(\hat{x}) - \frac{1}{2}\beta MCe\Big] - 2e^\top P_G H_2(GH_2)^{-1}\dot{S} + \frac{1}{\gamma_1}\tilde{\beta}\Big[\sigma_2(\beta - \tilde{\beta})\Big],$$

pour laquelle nous avons utilisé les équations (3.20) et (3.21). De plus, en utilisant encore une fois (3.21) ainsi que (3.2), nous obtenons

$$\dot{V}_2 \;\leq\; -\lambda_m(Q)\left|e\right|^2 - \beta\left|MCe\right|^2 + 2K_f\left|e\right|\left|MCe\right| + 2\left|P_G H_2(GH_2)^{-1}\right|\left|e\right|\left|\dot{S}\right| - \frac{\sigma_2}{\gamma_1}\tilde{\beta}^2 + \frac{\sigma_2}{\gamma_1}\beta\tilde{\beta}.$$

D'où,

$$\begin{aligned} \dot{V}_2 \;&\leq\; -\frac{\lambda_m(Q)}{2}\left|e\right|^2 - \begin{pmatrix} |e| \\ |MCe| \end{pmatrix}^\top \begin{pmatrix} \frac{\lambda_m(Q)}{2} & -K_f \\ -K_f & \beta \end{pmatrix}\begin{pmatrix} |e| \\ |MCe| \end{pmatrix} \\ &+\; 2\left|P_G H_2(GH_2)^{-1}\right|\left|e\right|\left|\dot{S}\right| - \frac{\sigma_2}{\gamma_1}\tilde{\beta}^2 + \frac{\sigma_2}{\gamma_1}\beta\tilde{\beta}\,. \end{aligned} \tag{3.41}$$

Ensuite, nous utilisons la définition de la constante inconnue β introduite ci-dessus dans l'équation (3.39) pour déduire que

$$\dot{V}_2 \leq -\frac{\lambda_m(Q)}{2}|e|^2 + 2\left|P_G H_2 (GH_2)^{-1}\right||e|\left|\dot{S}\right| - \frac{\sigma_2}{\gamma_1}\tilde{\beta}^2 + \frac{\sigma_2}{\gamma_1}\beta\tilde{\beta}\,. \tag{3.42}$$

Soit la constante c_b telle que $\left|P_G H_2 (GH_2)^{-1}\right| \leq c_b$. En utilisant l'inégalité de Young $2c_b|e|\left|\dot{S}\right| \leq c_b^2\left|\dot{S}\right|^2 + |e|^2$, on obtient

$$\dot{V}_2 \leq -\left[\frac{\lambda_m(Q)}{2} - 1\right]|e|^2 + c_b^2\left|\dot{S}\right|^2 - \frac{\sigma_2}{2\gamma_1}\tilde{\beta}^2 + \frac{\sigma_2}{2\gamma_1}\beta^2. \tag{3.43}$$

Nous concluons que si le mode glissant est établi ($\{S \equiv 0\}$), les trajectoires $e(t)$ convergent vers un petit voisinage de l'origine de rayon dépendant de β, σ_2 et γ_1 pourvu que $\lambda_m(Q) > 2$ – voir [89].

Notons que dans le cas particulier où le gain $\sigma_2 = 0$ ou si la constante β est connue, (3.42) devient

$$\dot{V}_2 \leq -\left[\frac{\lambda_m(Q)}{2} - 1\right]|e|^2\,.$$

Dans ce cas, on peut conclure en faisant appel au lemme de Barbălat que $e(t)$ converge vers zéro asymptotiquement à condition que les trajectoires soient dans sur la surface de glissement. Malgré que ceci n'est pas faisable puisqu'en effet, β est inconnu compte tenu des incertitudes sur les bornes supérieures des différents signaux (états, entrées inconnues, bruit), cette analyse nous a permis de fixer les modifications nécessaires pour établir notre résultat principal que nous détaillons dans la section suivante.

3.2.3 Observateur adaptatif à "modes glissants" modifié

Dans ce qui précède, nous avons démontré que dans le cas où les paramètres ρ et β sont exactement connus, le mode glissant est atteint en temps fini et que l'erreur d'estimation converge asymptotiquement vers zéro. Néanmoins, dans le scénario étudié dans notre cas, les constantes ρ et β sont supposées inconnues. Dans cette partie, nous apportons des modifications sur la structure de l'entrée u et nous démontrons que les trajectoires de l'erreur d'observation convergent vers la surface de glissement et que par conséquent, elles tendent arbitrairement vers un petit ensemble compact arbitraire centré autour de l'origine.

Théorème 3.4. *Considérons le système (3.1) vérifiant l'hypothèse 3.2 et l'observateur défini par les équations (3.16), (3.17), (3.27), (3.32) et la version modifiée de l'entrée u dans (3.31),*

$$u = (GH_2)^{-1}\left[\delta S + \hat{\rho}\frac{S}{\varepsilon + |S|} - GPA\hat{x} - GH_1 f(\hat{x}) - \frac{1}{2}GH_1\hat{\beta}M(y - C\hat{x})\right], \quad \varepsilon > 0. \tag{3.44}$$

Supposons que les conditions (3.22) et (3.23) sont vérifiées et que

$$I + EC - PT = 0, \tag{3.45a}$$
$$H_1 = PB, \tag{3.45b}$$
$$H_2 = PF, \tag{3.45c}$$
$$K = PA - LC, \quad \textit{est Hurwitz} \tag{3.45d}$$
$$J = L - KE. \tag{3.45e}$$

Donc, les trajectoires de l'erreur d'estimation convergent vers un ensemble compact centré autour de $\{e = 0\}$ *et qui peut être diminué arbitrairement pour des larges valeurs de* γ_1 *et* δ.

Remarque 3.5. Les conditions du théorème restreignent clairement la classe de systèmes pour la quelle l'observateur que nous proposons est applicable. Il s'agit des conditions structurelles que doit satisfaire le système en considération pour que les équations matricielles linéaires ainsi que le problème d'optimisation convexe soient solubles. A cet égard et afin de satisfaire toutes les conditions, les matrices de l'observateur sont calculées dans l'ordre suivant :

(1) P et E sont générées par l'équation (3.8) avec $X = [P\ E]$, $R_1 = [T^\top\ -C^\top]^\top$, et $R_2 = I_{n+q_2}$;
(2) H_1 et H_2 sont définies par les équations (3.45b) et (3.45c) ;
(3) N et G sont sélectionnées telles que $GH_2 = NCH_2$ est inversible ;
(4) Les matrices A_G et B_G sont obtenues via les équations (3.18) et (3.19) et sous les conditions (3.22)–(3.23) ;
(5) $L = -P_G^{-1}R$ avec P_G et M générées par la solution le problème d'optimisation définie dans la section précédente par les équations (3.24)–(4.17) ;
(6) K est définie par (3.45d) ;
(7) J est définie par (3.45e).

Démonstration du Théorème 3.4

La preuve est étroitement liée à l'analyse développée dans la section précédente. Nous démontrons tout d'abord que $S(t)$ et $\tilde{\rho}(t)$ convergent vers un voisinage de l'origine. Ensuite, nous prouvons la convergence de $\dot{S}(t)$ vers un voisinage de zéro et enfin nous déduisons la stabilité asymptotique pratique de l'origine du système de l'erreur d'observation. En outre, pour démontrer la convergence de $\dot{S}$, nous utilisons le lemme suivant obtenu comme corollaire du [90, Théorème 2].

Lemme 3.6. *On considère l'équation différentielle ordinaire*

$$\dot{\zeta}(t) = -\delta\zeta(t) + \nu(t), \quad t_0 \in \mathbb{R}_{\geq 0},\ \zeta(t_0) = \zeta_o \in \mathbb{R}^n,\ \delta > 0 \tag{3.46}$$

où ν *est uniformément continuellement borné dans son domaine* $\mathbb{R}^p$. *Donc,*

$$\lim_{\delta \to +\infty} \dot{\zeta}(t, \delta) = 0, \tag{3.47}$$

uniformément pour tout $t > t_0$.

1.– *Convergence de $S(t)$ et $\tilde{\rho}(t)$.*

D'après les développements dans la section 3.2.2.3, les trajectoires de l'erreur d'observation vérifient l'équation (3.38). D'autre part, la dynamique de la surface de glissement est définie par (3.30). En remplaçant dans cette dernière l'expression de u donnée par (3.44), on obtient

$$\dot{S} \;=\; -\delta S + \Phi(\eta_1, x) - \hat{\rho}\frac{S}{\varepsilon + |S|}. \tag{3.48}$$

En utilisant l'équation (3.48) et $\hat{\rho} = \rho - \tilde{\rho}$, la dérivée totale de V_1 définie dans (3.35) satisfait

$$\begin{aligned}\dot{V}_1 \;&\leq\; S^\top\Big[-\delta S + \varphi(t)\Big] + \frac{\tilde{\rho}}{\gamma_2}\left[-\gamma_2\,|S| + \sigma(\rho - \tilde{\rho})\right] + \Big(\rho - \tilde{\rho}\Big)\left[|S| - \frac{|S|^2}{|S| + \varepsilon}\right] \\ &\leq\; -\delta\,|S|^2 - \frac{\sigma}{\gamma_2}\tilde{\rho}^2 + \frac{\sigma}{\gamma_2}\rho\tilde{\rho} + (\rho - \tilde{\rho})\frac{\varepsilon\,|S|}{|S| + \varepsilon},\end{aligned} \tag{3.49}$$

et compte tenu des inégalités

$$\begin{aligned}\frac{|S|}{|S| + \varepsilon} \;&\leq\; 1 \\ \rho\tilde{\rho} \leq \frac{1}{2}\left(\rho^2 + \tilde{\rho}^2\right)& \\ \tilde{\rho}\varepsilon = \left(\tilde{\rho}\Big[\frac{\sigma}{2\gamma_2}\Big]^{1/2}\right)\left(\varepsilon\Big[\frac{2\gamma_2}{\sigma}\Big]^{1/2}\right) \;&\leq\; \frac{1}{2}\left[\frac{\tilde{\rho}^2\sigma}{2\gamma_2} + \frac{2\varepsilon^2\gamma_2}{\sigma}\right],\end{aligned}$$

on observe que

$$\dot{V}_1 \;\leq\; -\delta\,|S|^2 - \frac{\sigma}{4\gamma_2}\tilde{\rho}^2 + \frac{\sigma}{2\gamma_2}\rho^2 + \rho\varepsilon + \varepsilon^2\frac{\gamma_2}{\sigma}. \tag{3.50}$$

Ensuite, on définit

$$c_2(\rho, \varepsilon, \gamma_2, \sigma) := \frac{\sigma}{2\gamma_2}\rho^2 + \rho\varepsilon + \varepsilon^2\frac{\gamma_2}{\sigma}, \tag{3.51}$$

donc

$$\dot{V}_1 \;\leq\; -\min\Big\{2\delta,\; \frac{\sigma}{2}\Big\}\left[\frac{|S|^2}{2} + \frac{\tilde{\rho}^2}{2\gamma_2}\right] + c_2. \tag{3.52}$$

Soit $K_0 := \min\big\{2\delta,\; \frac{\sigma}{2}\big\}$. On déduit que

$$\dot{V}_1(S(t), \tilde{\rho}(t)) \;\leq\; -K_0 V_1(S(t), \tilde{\rho}(t)) + c_2.$$

En intégrant de deux côtés et en invoquant le théorème de comparaison, il s'en suit que

$$\lim_{t\to\infty} V_1(S(t), \tilde{\rho}(t)) \leq \frac{c_2(\rho, \varepsilon, \gamma_2, \sigma)}{K_0(\sigma, \delta)}.$$

Soit $\varepsilon \propto (1/\gamma_2)$, donc le quotient c_2/K_0 peut être arbitrairement réduit en élargissant γ_2 et δ. Par conséquent, $S(t)$ et $\tilde{\rho}(t)$ tendent asymptotiquement vers un ensemble compact arbitraire centré autour de l'origine $\{S = 0, \tilde{\rho} = 0\}$.

2.– *Convergence de $\dot{S}(t)$*

Pour démontrer la convergence de $\dot{S}(t)$, nous faisons appel au lemme 3.6 avec $\zeta = S$ et $\nu(t) = \tilde{\nu}(t, \hat{\rho}(t), S(t))$ avec

$$\tilde{\nu}(t, \hat{\rho}, S) := \varphi(t) - \hat{\rho}\frac{S}{|S| + \varepsilon}, \qquad \text{avec} \varphi(t) := \Phi(\eta_1(t), x(t)). \tag{3.53}$$

Pour ce faire, nous commençons par démontrer que $\nu(t)$ est borné et uniformément continu en t. La bornitude uniforme de $\nu(t)$ est déduite de la bornitude de $\tilde{\rho}(t)$ (donc de $\hat{\rho}(t) = \rho - \tilde{\rho}(t)$), de $S(t)$ et de $\varphi(t)$ – voir (3.34). La continuité uniforme résulte du fait que $\dot{\nu}(t)$ est également borné. En effet, on a

$$\dot{\tilde{\nu}} = \dot{\varphi}(t) - \dot{\hat{\rho}}\frac{S}{|S| + \varepsilon} - \hat{\rho}F(S)\dot{S}$$

avec

$$F(S) = \frac{\varepsilon}{(|S| + \varepsilon)^2} \leq \frac{1}{\varepsilon},$$

donc

$$\dot{\nu}(t) \leq |\dot{\varphi}(t)| + \left|\dot{\tilde{\rho}}(t)\right| + \frac{1}{\varepsilon}\Big[\rho + |\tilde{\rho}(t)|\Big]\left|\dot{S}(t)\right|. \tag{3.54}$$

Afin d'étudier la bornitude de $\dot{\nu}(t)$, nous analysons l'équation (3.54) terme par terme. À partir de l'équation (3.48), il en résulte que

$$\dot{S}(t) = -\delta S(t) + \varphi(t) - \Big[\rho - \tilde{\rho}(t)\Big]\frac{S(t)}{|S(t)| + \varepsilon}.$$

Puisque $S(t)$, $\tilde{\rho}(t)$ et $\varphi(t)$ sont bornés, $\dot{S}(t)$ est donc borné. De plus, la norme de

$$\dot{\varphi}(t) = GH_2\dot{\eta}_1(t) + GPA\dot{x}(t) + GH_1\frac{\partial f}{\partial x}(x(t))\dot{x}(t)$$

est bornée compte tenu de l'hypothèse 3.2. Finalement, on observe à partir de l'équation (3.32) que

$$\left|\dot{\tilde{\rho}}(t)\right| \leq \sigma\rho + \gamma_2\left|S(t)\right| + \sigma\left|\tilde{\rho}(t)\right|,$$

qui est borné pour tout $t \geq 0$. Nous concluons que $\dot{\nu}(t)$ est bornée et par conséquent, $\nu(t)$ est uniformément continu.

Ainsi, en appliquant le lemme 3.6 à l'équation (3.48), on déduit que

$$\lim_{\delta \to \infty} \dot{S}(t, \delta) = 0,$$

uniformément pour tout $t > t_0 \geq 0$. Ainsi, pour toute constante $\Delta_c > 0$, il existe une constante $\delta_c > 0$ telle que pour tout $\delta \geq \delta_c \Longrightarrow$

$$\left|\dot{S}(t)\right| \leq \Delta_c, \qquad \forall t > t_0. \tag{3.55}$$

3.– *Convergence de* $e(t)$

Nous rappelons que la fonction V_2 est définie dans l'équation (3.40). Sa dérivée totale vérifie l'inégalité (3.43) indépendamment de u et que le mode glissant soit atteint ou non. Soit $p_m > 0$ tel que $e^\top P_G e \geq p_m |e|^2$. Soit $\Delta_c > 0$: d'après ce qui précède, il existe δ_c telle que pour tout $\delta \geq \delta_c$, l'inégalité (3.55) est satisfaite, et par conséquent, la dérivée de V_2 vérifie :

$$\begin{aligned}\dot{V}_2 &\leq -\sigma_2 \left(\frac{1}{2\gamma_1}\tilde{\beta}^2\right) - \frac{\lambda_m(Q)-2}{p_m}\left(\frac{1}{2}p_m |e|^2\right) + \underbrace{\frac{\sigma_2}{2\gamma_1}\beta^2 + \Delta_c^2 c_b^2}_{c_3} \\ &\leq -\min\left\{\sigma_2,\ \frac{\lambda_m(Q)-2}{p_m}\right\} V_2 + c_3.\end{aligned}$$

En intégrant de deux côtés de cette inégalité le long des trajectoires, de t_0 à t, nous déduisons que $V_2(e(t), \tilde{\beta}(t))$ tend asymptotiquement vers l'ensemble compact suivant

$$\left\{(e,\tilde{\beta}) \in \mathbb{R}^{n+q_2} \times \mathbb{R} \,:\, V_2(e,\tilde{\beta}) \leq \frac{c_3}{\min\left\{\sigma_2,\ \frac{\lambda_m(Q)-2}{p_m}\right\}}\right\}.$$

Notons que la borne précédente majorant $V_2(e,\tilde{\beta})$ peut être réduite pour toute constante fixe σ_2, en élargissant γ_1 et δ. L'énoncé du théorème s'en suit. ■

3.2.4 Reconstruction de l'entrée inconnue η_1

L'estimation de l'entrée inconnues η_1 découle des résultats établis précédemment à partir desquels le corollaire suivant est obtenu.

Corollaire 3.7. *Pour tout réel $\varepsilon_\eta > 0$, il existe des paramètres δ, γ_1, γ_2, σ_2 et $0 < T_\eta < \infty$ tels que*

$$|u(t) - \eta_1(t)| \leq \varepsilon_\eta, \qquad \forall t \geq t_0 + T_\eta.$$

Démonstration :

A partir de (3.37), on obtient

$$|u(t) - \eta_1(t)| \ \leq\ \left|(GH_2)^{-1}\right| \left[\frac{1}{2}\left|\hat{\beta}(t)\right| |GH_1|\,|MCe(t)| + |GLCe(t)| + (|GH_1K_f| + |GK|)\,|e(t)| + \left|\dot{S}(t)\right|\right].$$

Nous avons démontré que $\hat{\beta}(t) = \beta - \tilde{\beta}(t)$ est borné et que tous les termes de l'expression ci-dessus sont facteurs de $e(t)$ et $\dot{S}(t)$ qui convergent vers un petit ensemble compact arbitraire centré autour de l'origine. L'énoncé du corollaire s'en suit. ■

Avant de présenter notre principale application qui consiste en un système de communication sécurisée à base de l'approche de synchronisation proposée (voir la section 3.3), nous illustrons, tout d'abord, les résultats théoriques à l'aide d'une application d'estimation conjointe de l'état et d'une entrée inconnue d'un robot flexible en présence d'un bruit de mesure.

3.2.5 Exemple numérique : robot flexible

Afin d'illustrer les résultats théoriques, nous présentons un exemple d'estimation d'état d'un robot flexible avec des mesures bruitées et sous l'influence d'un signal de friction inconnu.
On considère le modèle d'un robot flexible à un bras, excité par une entrée sinusoïdale *i.e.*,

$$J_2\ddot{\theta}_2 + F_2\dot{\theta}_1 + K(\theta_2 - \theta_1) + mgl\cos(\theta_2) = 0 \quad (3.56a)$$

$$J_1\ddot{\theta}_1 + F_1\dot{\theta}_1 + K(\theta_1 - \theta_2) = K_t\sin(t) \quad (3.56b)$$

où θ_1 et θ_2 représentent la rotation angulaire du moteur et du bras, respectivement. Les paramètres du robot se présentent comme suit : $J_1 = 3.7 \times 10^{-3}\ kgm^2$ et $J_2 = 3.7 \times 10^{-3}\ kgm^2$ sont les inerties du moteur et du bras ; $m = 2.1 \times 10^{-1}$kg est la masse du bras, $l = 0.15$m est la position du centre de gravité du bras, $K = 0.18$Nms/rad est un paramètre constant, $F_1 = 4.6 \times 10^{-3}$Nms/rad et $F_2 = 6.4 \times 10^{-3}$Nms/rad représentent les coefficients du friction du moteur et du bras et $K_t = 32 \times 10^{-3}$Nms/rad est un gain d'entrée.

On définit l'état $x_* = [x_{*1}, x_{*2}, x_{*3}, x_{4*}]^\top$ avec $x_{1*} = \theta_1$, $x_{2*} = \theta_2$, $x_{3*} = \dot{\theta}_1$ et $x_{4*} = \dot{\theta}_2$. Soit $y = [y_1 = x_{*1} + \eta_2, y_2 = x_{*2} + x_{4*}]^\top$ le vecteur de sortie mesurée où $\eta_2(t)$ représente le bruit de mesure (bruit Gaussien de moyenne égale à zéro). Nous supposons, comme dans la référence [79], que la rotation angulaire du moteur ainsi que la somme de la rotation angulaire et de la vélocité du bras sont mesurées. Nous rappelons également que $x = [x_*,\ \eta_2]^\top$ représente l'état augmenté. Supposons que que le paramètre de friction F_2 est inconnu et qu'il génère un signal inconnu $\eta_1(t) = \frac{F_2}{J_2}\dot{\theta}_2$. Donc, le système (3.56) peut s'écrire sous la forme (3.1) avec

$$A_0 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -48.6486 & 48.6486 & -12.4324 & 0 \\ 19.3548 & 619.3548 & 0 & 0 \end{bmatrix},\ B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ -33.1935 \end{bmatrix},\ F = \begin{bmatrix} 0 \\ 0 \\ 0 \\ -1 \end{bmatrix},$$

$$C_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix},\ G_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ f_0(x_*) = cos(x_{*2}).$$

Les matrices de l'observateur sont obtenues en appliquant la procédure décrite dans la remarque 3.5 :

$$E = \begin{bmatrix} 0 & 0 \\ 0 & -0.33 \\ 0 & 0 \\ 0 & -0.33 \\ -1 & 0 \end{bmatrix},\ P = \begin{bmatrix} 1.0000 & 0 & 0 & 0 \\ 0 & 0.66 & 0 & -0.33 \\ 0 & 0 & 1 & 0 \\ 0 & -0.33 & 0 & 0.66 \\ -1 & 0 & 0 & 0 \end{bmatrix},\ L = \begin{bmatrix} 0.4955 & -0.0013 \\ 0.0002 & 0.9969 \\ -24.3170 & 24.3251 \\ 0.0001 & -0.0001 \\ 0.4954 & 0.0011 \end{bmatrix},$$

$$K = \begin{bmatrix} -0.4955 & 0.0013 & 1 & 0.0013 & -0.4955 \\ -6.4512 & 5.4541 & 0 & -0.3302 & -0.0002 \\ -24.3316 & 24.3235 & -12.4324 & -24.3251 & 24.3170 \\ 12.9037 & -12.9038 & 0 & -0.3332 & -0.0001 \\ -0.4954 & -0.0011 & -1 & -0.0011 & -0.4954 \end{bmatrix}, \; N = \begin{bmatrix} 0 & 3 \end{bmatrix}.$$

Les paramètres de l'observateur sont choisis comme suit : $\varepsilon = 0.001$, $\delta = 100$, $\sigma = 100$ et $\gamma_2 = 1000$. Les conditions initiales sont : $x(0) = [3,\ 1,\ 1,\ 2,\ -0.8]^\top$, $\hat{x}(0) = [-2,\ 0,\ 2,\ 4,\ 2.17]^\top$ et $\hat{\rho} = 0$.

Les résultats de simulations se présentent comme suit. La figure 3.1 illustre que les états et le bruit η_2 sont effectivement estimés, donc l'effet du bruit est parfaitement annulé (nous rappelons que $e_5 = x_5 - \hat{x}_5$ représente l'erreur d'estimation du bruit affectant l'équation de sortie). La figure 3.2 montre que l'entrée inconnue η_1 est bien reconstruite.

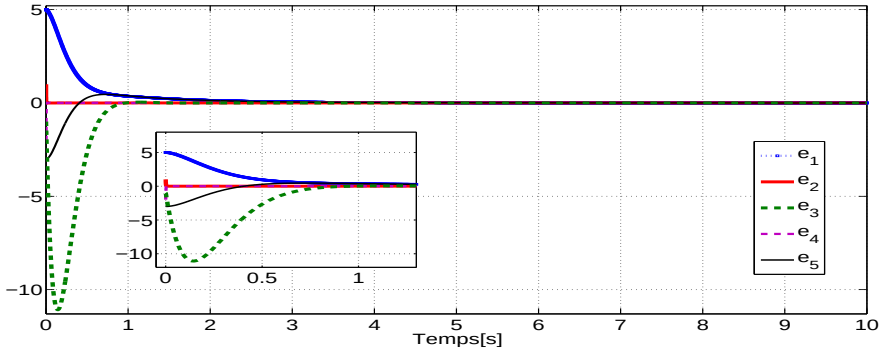

FIGURE 3.1: Les erreurs d'estimation $e_1 = x_1 - \hat{x}_1$, $e_2 = x_2 - \hat{x}_2$, $e_3 = x_3 - \hat{x}_3$, $e_4 = x_4 - \hat{x}_4$ and $e_5 = x_5 - \hat{x}_5$

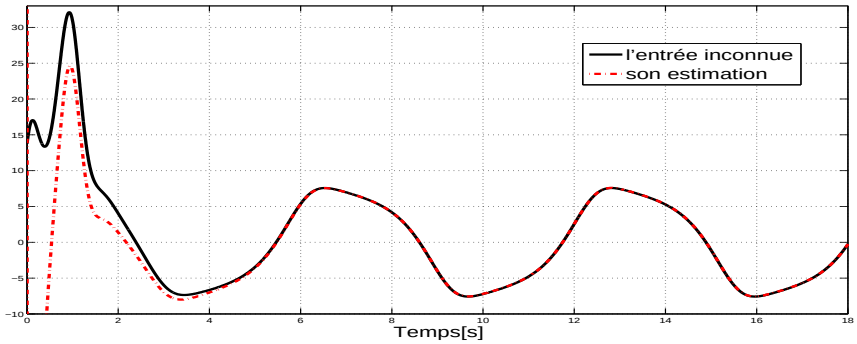

FIGURE 3.2: L'entrée inconnue η_1 et son estimée

3.3 Un système de communication sécurisée basé sur la synchronisation de systèmes chaotiques utilisant les observateurs adaptatifs à "modes glissants"

Dans cette section, nous exploitons les propriétés de l'observateur adaptatif à "modes glissants" dans un nouveau schéma de communication sécurisée basée sur la synchronisation des systèmes chaotiques. Le système de communication que nous proposons est dédié pour le cryptage et la transmission des informations de type analogiques/numériques et de grandes amplitudes. L'architecture du système repose sur la séparation entre les opérations de cryptage et de synchronisation en utilisant deux systèmes chaotiques en cascade au niveau de l'émetteur. Le système de transmission proposé est robuste aux différents types d'attaques, notamment les attaques basées sur l'analyse des caractéristiques du signal de texte chiffré et les attaques basées sur l'identification de la structure et des paramètres du système émetteur. Une analyse de la clé secrète est effectuée pour évaluer sa robustesse aux attaques à force brute.
Les bruits dans le canal de communication sont souvent négligés dans la littérature, cependant ces bruits sont inévitables en pratique et influencent considérablement les performances des systèmes de transmissions puisqu'ils changent le comportement des systèmes dynamiques et détériorent l'opération de synchronisation. Le schéma que nous proposons est robuste aux bruits de canal. La performance du système de communication proposé est illustrée à travers des simulations numériques dans une application pour la transmission des signaux harmoniques et une application de cryptage des images binaires.

3.3.1 Description du système de communication

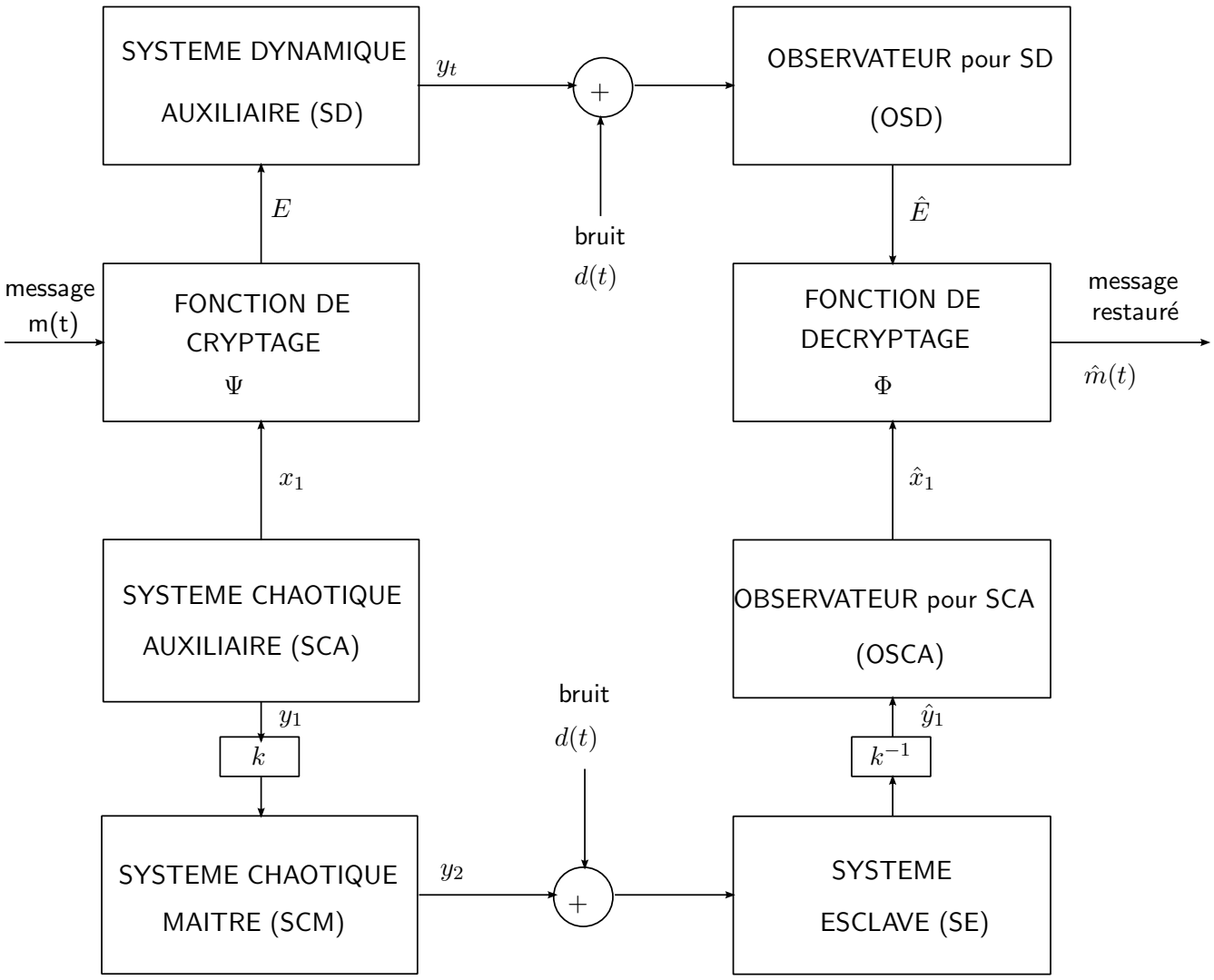

FIGURE 3.3: Schéma de communication sécurisée

Les méthodes classiques de communications sécurisées telles que la technique de masquage chaotique, la modulation paramétrique, le cryptage par injection et la commutation chaotique sont condamnées par leur faible niveau de sécurité, le nombre relativement faible des messages à transmettre, les restrictions sur l'amplitude du signal information qui sont imposées pour ne pas compromettre le comportement chaotique de l'émetteur ainsi que les restrictions sur la nature du message à transmettre. Par exemple, la technique de modulation paramétrique basée sur les techniques adaptatives utilisant l'hypothèse que les messages soient lentement variants en fonction du temps ou constants par morceaux et la technique de commutation chaotique est spécifique aux messages binaires. Par ailleurs, la plupart des techniques de communications traditionnelles ne tiennent pas compte du bruit présent dans le canal public. Dans ce qui suit, nous proposons une méthode qui ne présente aucun de ces inconvénients.

Le schéma de communication que nous proposons est représenté dans la figure 3.3. L'émetteur consiste en trois systèmes dynamiques : un système chaotique auxiliaire (SCA) employé pour crypter le message à transmettre, $m(t)$; le système chaotique maître (SCM) qui produit un signal de sortie y_2 pour entraîner la synchronisation avec le système récepteur, et un système dynamique auxiliaire (SD) qui produit l'information cryptée y_t envoyée à travers le canal public présentant du bruit additif.

Le processus est comme suit. Un message numérique ou analogique $m(t)$ est crypté par l'intermédiaire d'une fonction de cryptage $\Psi(\cdot,\cdot)$ qui dépend d'un signal chaotique x_1 généré par le SCA. Ensuite, afin d'améliorer d'avantage la sécurité contre les attaques externes, le signal de sortie y_1 du SCA n'est pas directement envoyé à travers le canal public mais inséré dans un autre système dynamique modulo un facteur d'atténuation k de manière que le comportement chaotique du système SCM soit préservé. Le signal de sortie y_2 de ce dernier est transmis à travers le canal de communication bruité.

Une fonction de cryptage $\Psi(\cdot,\cdot)$ qui dépend du signal chaotique x_1 (généré par le SCA) et du message $m(t)$ génère le signal crypté $E(t) = \Psi(x_1(t), m(t))$. Notons que $\Psi(x_1(t), m(t))$ doit être inversible par rapport à $m(t)$, *i.e.*, $m(t)$ peut être exprimé en termes de $E(t)$ et de $x_1(t)$ dans le but de résoudre le problème d'inversibilité au niveau du récepteur. Le niveau de sécurité dépend étroitement de la complexité de la fonction $\Psi(\cdot,\cdot)$.

Contrairement aux schémas de transmission classiques, le message à transmettre n'est pas inséré dans la dynamique du système chaotique émetteur, ni additionné au signal de sortie, cependant le signal $E(t)$ dans lequel le message est masqué, est injecté dans la dynamique d'un système dynamique auxiliaire (SD). De cette manière, les opérations de synchronisation et de cryptage sont séparées, ce qui permet d'augmenter la taille et l'amplitude du message $m(t)$, éviter l'affectation du comportement chaotique du système (SCA) ainsi que la détérioration de la synchronisation entre les systèmes maître et esclave. Le signal de sortie y_t du système SD est transmis à travers le canal de communication bruité.

D'une autre part, le récepteur est constitué de trois systèmes dynamiques : le système esclave (SE) dont l'objectif est de synchroniser avec le système SCM et de reconstruire l'entrée inconnue $ky_1(t)$ malgré le bruit du canal, le système auxiliaire (OSCA) excité par le signal reconstruit $\hat{y}_1$ dont le but est de synchroniser avec le système SCA et finalement, l'observateur auxiliaire (OSD) doit synchroniser avec le système SD en utilisant le signal y_t et estimer le signal crypté $E(t)$. Les signaux reconstruits $\hat{E}(t)$ et $\hat{x}_1$ sont employés par la fonction de décryptage $\Phi(\cdot,\cdot)$ afin de restaurer le message transmis $\hat{m}(t)$.

Si la capacité du canal de communication est limitée à un seul signal alors que plusieurs signaux sont à transmettre, il est convenable d'utiliser un multiplexeur. Au niveau du récepteur, nous ajoutons un démultiplexeur qui récupère tous les signaux transmis. Une méthode pratique de réalisation du multiplexeur et du démultiplexeur dans un tel système de transmission (capacité limitée du canal) est détaillée dans [17].

3.3.2 Description des différents systèmes dynamiques

L'émetteur : Le système SCA est un système chaotique décrit par l'équation

$$\text{SCA} : \begin{cases} \dot{x}_1 = A_1 x_1 + B_1 f_1(x_1), \\ y_1 = C_1 x_1, \end{cases} \tag{3.57}$$

où f_1 est de classe $\mathcal{C}^1$. Un grand nombre d'oscillateurs chaotiques sont de la forme (3.57) comme par exemple les systèmes de Rössler, de Lü, de Chua, de Van der Pol, *etc.* Le système SCM est un système chaotique de structure similaire telle que le signal $ky_1(t)$ est injecté dans sa dynamique. De plus, le canal de communication est corrompu par le bruit $d(t)$. Donc, on a

$$\text{SCM} : \begin{cases} \dot{x}_2 = A_2 x_2 + B_2 f_2(x_2) + kF_2 y_1 \\ y_2 = C_2 x_2 + G_2 d(t). \end{cases} \tag{3.58}$$

Le système SD est un système linéaire stable,

$$\begin{cases} \dot{x}_t = A_t x_t, \\ y_t = C_t x_t. \end{cases} \tag{3.59}$$

où A_t est Hurwitz. Ensuite, l'information cryptée $E(t) = \Phi(x_1(t), m(t))$ est injectée dans la dynamique du système SD et puisque le signal de sortie y_t est corrompu par le bruit de canal $d(t)$, le système SD devient

$$\text{SD} : \begin{cases} \dot{x}_t = A_t x_t + F_t E(t) \\ y_t = C_t x_t + G_t d(t), \end{cases} \tag{3.60}$$

où x_1, x_2 et x_t sont des vecteurs d'état ; y_1, y_2 et y_t représentent les signaux de sortie ; A_1, A_2, A_t, B_1, B_2, C_1, C_2, C_t,G_2, G_t, F_2 et F_t sont des matrices constantes à déterminer.

Les systèmes SCM et SD vérifient l'hypothèse 3.2 – Voir section 3.2.1

Le récepteur : Les systèmes (SE) et (OSD) au niveau récepteur sont respectivement deux observateurs adaptatifs à "modes glissants" pour les systèmes SCM (3.58) et SD (3.59) synthétisés selon l'approche détaillée dans la section (3.2). Ils sont décrits par les équations (3.17), (3.27) et (3.32).

Le signal de sortie $y_1(t)$ du système SCA n'est pas directement envoyé à travers le canal public mais injecté dans la dynamique du système SCM ; ky_1 est reconstruit par le système esclave RS. Le signal $\hat{y}_1(t)$ ainsi obtenu est reçu par le système OSCA dont l'objectif est de synchroniser avec le système SCA. Il est clair que la relation entre $y_1(t)$ et son estimation $\hat{y}_1(t)$ peut être définie par $\hat{y}_1(t) = y_1(t) + \bar{\varepsilon}(t)$ sachant que $\bar{\varepsilon}(t)$ représente une fonction dépendant de l'erreur d'estimation. Puisque $\bar{\varepsilon}(t)$ est de faible amplitude, nous pouvons utiliser un simple observateur de Luenberger (voir [19]). Une autre alternative consiste à utiliser l'observateur intégral proposé dans la référence [18]. L'avantage de cette alternative est la réduction de l'effet de $\bar{\varepsilon}(t)$.

3.3.3 Simulations numériques

Afin de tester le schéma de communication proposé, nous présentons deux applications de communication sécurisée : dans la première application, nous utilisons les systèmes de Rössler et de Lorenz pour la transmission des signaux harmoniques et la deuxième application est dédiée au cryptage et à la transmission des images binaires. Une analyse de sécurité et de la clé secrète sont effectuées pour vérifier les propriétés cryptographiques du système.

3.3.3.1 Transmission des signaux harmoniques

Dans le premier cas d'étude, le message à transmette $m(t) = [m_1(t), m_2(t)]^T$ est de type analogique représenté par des signaux sinusoïdaux d'amplitudes respectives : $m_{1max} = 5$, $m_{2max} = 4$ et des fréquences : $f_1 = 0.796Hz$ et $f_2 = 0.557Hz$.

Pour réaliser le système émetteur, nous utilisons le système de Rössler

$$\begin{cases} \dot{x}_{11} = -(x_{12} + x_{13}) \\ \dot{x}_{12} = x_{11} + ax_{12} \\ \dot{x}_{13} = b + x_{13}(x_{11} - c) \end{cases} \tag{3.61}$$

avec les signaux de sortie

$$\begin{cases} y_{11} = x_{11} \\ y_{12} = x_{13} \end{cases} \tag{3.62}$$

à la place du système (SCA). Les paramètres sont fixés comme suit : $a = 0.398$, $b = 2$ et $c = 4$, tels que le système (3.61) possède un comportement chaotique. Le système (SCM) est un système de Lorenz pour lequel on injecte dans sa dynamique le signal de sortie y_1 du système SCA *i.e.*,

$$\begin{cases} \dot{x}_{21} = -a_1 x_{21} + a_2 x_{22} \\ \dot{x}_{22} = r x_{21} - x_{22} - x_{21} x_{23} + k y_{11} \\ \dot{x}_{23} = x_{21} x_{22} - b_2 x_{23} + k y_{12} \end{cases} \tag{3.63}$$

Les signaux de sortie sont :

$$\begin{cases} y_{21} = x_{21} + d(t) \\ y_{22} = 2x_{22} + d(t) \\ y_{23} = x_{23} + d(t). \end{cases} \tag{3.64}$$

Nous fixons les paramètres comme suit : $a_1 = a_2 = 10$, $b_2 = 8/3$ et $r = 28$ tels que le système (3.63) fonctionne en régime chaotique. Notons que le système (3.63) peut être réécrit sous la forme (3.3) avec $x = x_2 = [x_{21}, x_{22}, x_{23}]^T$ le vecteur d'état, $y = y_2 = [y_{21}, y_{22}, y_{23}]^T$ le vecteur de sortie

et $\eta_1(t) = y_1(t)$ l'entrée inconnue. Ainsi, on a

$$A_0 = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -8/3 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, F = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, C_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, G_0 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix},$$

$$k = 1, \quad f(x) = \begin{bmatrix} -x_{21}x_{23} \\ x_{21}x_{22} \end{bmatrix}, \quad \eta_2(t) = d(t).$$

Supposons que le bruit dans le canal de communication $d(t)$ est un bruit Gaussien de moyenne égale à zéro, de fréquence égale à $10Hz$ et de variance 1, généré entre les bornes inférieure et supérieure respectivement égales à -3 et 3. On initialise les états du système SCA et SCM respectivement à $x_1(0) = [0.2, -0.4, -0.2]^T$ et $x_2(0) = [0.3 - 0.2 - 0.4]^T$. Les attracteurs respectifs des systèmes SCA et SCM sont illustrés dans la figure 3.4.

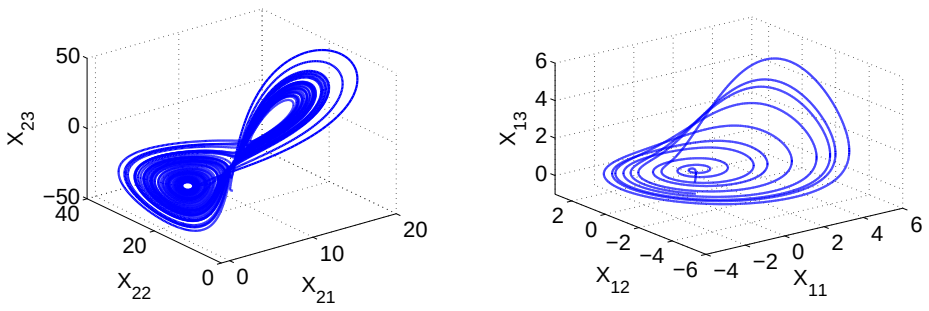

FIGURE 3.4: Attracteurs des systèmes chaotiques SCA-Rössler (droite) et SCM-Lorenz (gauche)

Le signal crypté $E = [E_1, E_2]^T$ est généré par la fonction de cryptage Ψ, le signal chaotique $x_1(t)$ et l'information $m(t)$:

$$E(t) = \Psi(x_1, m(t)) = \begin{bmatrix} 30.5x_{11} + 30.3x_{12} + (7.5x_{12}^2 + 1.25x_{13}^2 + 2)m_1(t) \\ 55x_{11} + 44x_{13} + (2x_{12}^2 + 5x_{11}^2 + 1)m_2(t) \end{bmatrix}.$$

Le système dynamique auxiliaire (SD) est donné par

$$\begin{cases} \dot{x}_t = -x_t + F_t E(t) \\ y_t = x_t + G_0 d(t), \end{cases} \tag{3.65}$$

qui représente un cas particulier de (3.3) avec $x = x_t = [x_{t1}, x_{t2}, x_{t3}]^T$ le vecteur d'état, $y_t = [y_{t1}, y_{t2}, y_{t3}]^T$ le vecteur de sortie et $\eta_1(t) = E(t)$ l'entrée inconnue, $A = -I_3$, $B = 0$,

$$F = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, G_0 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, C_0 = I_3, f(x) = 0 \text{ et } \eta_2(t) = d(t).$$

Le système SD est initialisé à $x_t(0) = [0.3, -0.2, -0.4]^T$. Les systèmes SE et OSD sont des observateurs adaptatifs à "modes glissants" décrits par les équations (3.17), (3.27) et (3.32).

Synthèse de l'observateur RS :

L'observateur SE est synthétisé suivant l'algorithme proposé dans la remarque (3.5). On obtient les valeurs numériques des matrices de l'observateur

$$E = \begin{bmatrix} -0.2917 & 0.0833 & 0.2083 \\ 0.1667 & -0.3333 & 0.1667 \\ 0.2083 & 0.0833 & -0.2917 \\ -0.4167 & -0.1667 & -0.4167 \end{bmatrix}, H_1 = H_2 = \begin{bmatrix} 0.1667 & 0.2083 \\ 0.3333 & 0.1667 \\ 0.1667 & 0.7083 \\ -0.3333 & -0.4167 \end{bmatrix}, G = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

$$K = \begin{bmatrix} 12.5547 & -14.9125 & -0.6923 & 3.9188 \\ 23.3386 & -22.5158 & -0.8919 & 3.3011 \\ 25.5741 & -25.4770 & -5.8261 & 5.3555 \\ -31.6960 & 30.7092 & 2.3883 & -7.9821 \end{bmatrix} \text{ et } J = \begin{bmatrix} -7.0448 & 5.6092 & 1.4386 \\ -3.5506 & 3.1007 & 0.4547 \\ -7.8373 & 4.4529 & 3.3894 \\ 8.3421 & -5.9254 & -2.4235 \end{bmatrix}.$$

Les paramètres de l'observateur sont choisis comme suit : $\varepsilon = 0.0001$, $\delta = 1000$, $\sigma = 1000$ et $\gamma_1 = 10000$. Les états du système SE sont initialisés à$\hat{x}(0) = [-0.11, -0.14, 0.2, -0.38]^T$ et le paramètre adaptatif $\hat{\rho}$ est initialisé à $\hat{\rho}(0) = 0$.

Synthèse de l'observateur ARS :

Puisque la dynamique du système SCA ne présente pas des entrées inconnues et que le signal de sortie n'est pas affecté par un bruit, l'observateur OSCA est un simple observateur de "Luenberger" dont la matrice de gain est donnée par :

$$L = \begin{bmatrix} 0.8424 & 0 \\ -0.6459 & 0 \\ 0 & 20 \end{bmatrix}.$$

Synthèse de l'observateur AO :

De manière similaire, nous appliquons l'algorithme proposé dans la remarque (3.5) afin d'obtenir les matrices de l'observateur (OSD) :

$$E = \begin{bmatrix} -0.3333 & 0.1667 & 0.1667 \\ 0.1667 & -0.3333 & 0.1667 \\ 0.1667 & 0.1667 & -0.3333 \\ -0.3333 & -0.3333 & -0.3333 \end{bmatrix} \quad H_1 = 0, \quad H_2 = \begin{bmatrix} 0.1667 & 0.1667 \\ 0.6667 & 0.1667 \\ 0.1667 & 0.6667 \\ -0.3333 & -0.3333 \end{bmatrix}, \quad G = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$K = \begin{bmatrix} -0.4172 & -0.2796 & -0.2796 & 0.0237 \\ 0.6924 & -1.2927 & -0.2365 & 0.1632 \\ 0.6924 & -0.2365 & -1.2927 & 0.1632 \\ -0.4048 & 0.3502 & 0.3502 & -0.7043 \end{bmatrix} \quad \text{and} \quad J = \begin{bmatrix} -0.2874 & 0.1438 & 0.1438 \\ -0.3190 & 0.1736 & 0.1455 \\ -0.3190 & 0.1455 & 0.1736 \\ 0.2517 & -0.1258 & -0.1258 \end{bmatrix}.$$

Finalement, les paramètres de l'observateur sont sélectionnés comme suit : $\varepsilon = 0.0001$, $\delta = 1000$, $\sigma = 1000$ et $\gamma_1 = 10000$. La condition initiale de l'état de l'observateur OSD est donnée par $\hat{x}(0) = [-0.11, -0.14, 0.2, -0.38]^T$ et le paramètre adaptatif est initialisé à $\hat{\rho}$ à $\hat{\rho}(0) = 0$. Le message reçu $\hat{m}(t)$ est extrait à partir de la fonction de décryptage $\Phi(\cdot,\cdot)$ après avoir résolu le problème d'inversibilité :

$$\hat{m}(t) = \Phi(E(t), \hat{x}_1(t)) = \begin{bmatrix} \dfrac{E_1(t) - 30.5\hat{x}_{11} - 30.3\hat{x}_{12}}{75\hat{x}_{12}^2 + 1.25\hat{x}_{13}^2 + 2} \\ \\ \dfrac{E_2(t) - 55\hat{x}_{11} - 44\hat{x}_{13}}{2\hat{x}_{12}^2 + 5\hat{x}_{11}^2 + 1} \end{bmatrix}.$$

Les résultats de simulation se présentent comme suit. La figure 3.5 représente les erreurs de synchronisation du système OSCA avec le système SCA, et du système SE avec le système SCM, respectivement. La figure 3.6 illustre le bruit Gaussien du canal et son estimation via le système RS.

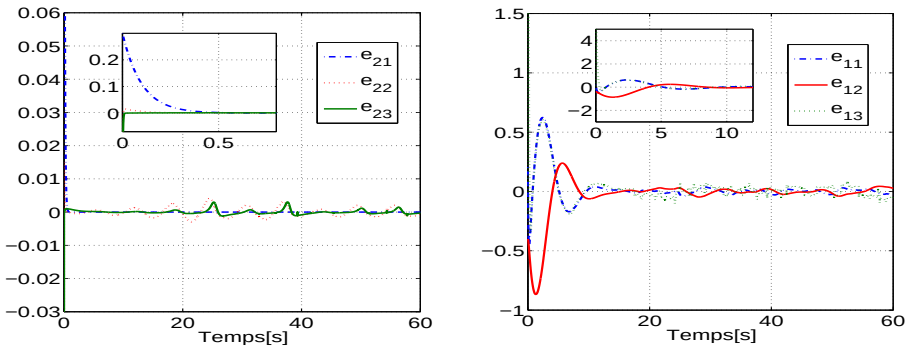

FIGURE 3.5: Erreurs de synchronisation (SCA)-(OSCA) (droite) et (SCM)-(SE) (gauche)

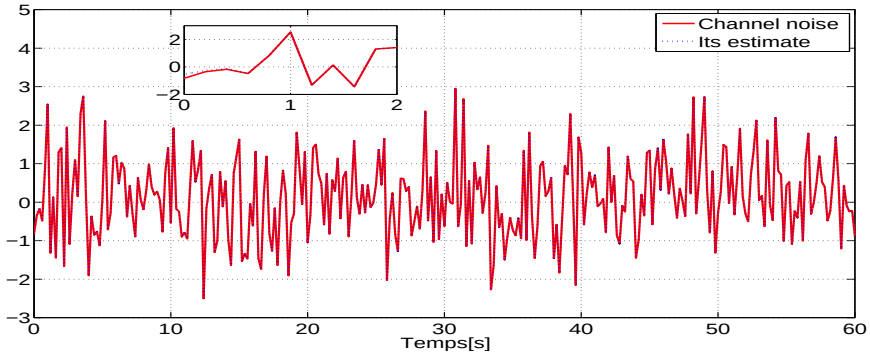

FIGURE 3.6: Le bruit de canal et son estimation par l'observateur (SE)

Dans la figure 3.7, il est illustré que les signaux de cryptage E_1 et E_2 sont bien reconstruits par l'observateur OSD et la figure 3.8 représente les messages transmis et leurs estimations respectives. Notons que la reconstruction de l'information m_2 est effectuée après une période de temps égale à $8s$, ceci peut être justifié par le régime transitoire relativement long de l'erreur de synchronisation correspondant au système de Rössler – voir la figure 3.5. Dans ce qui suit, nous remplaçons les système de Rössler par le système de Chua et nous montrons l'utilité de ce dernier dans une application de transmission des images binaires.

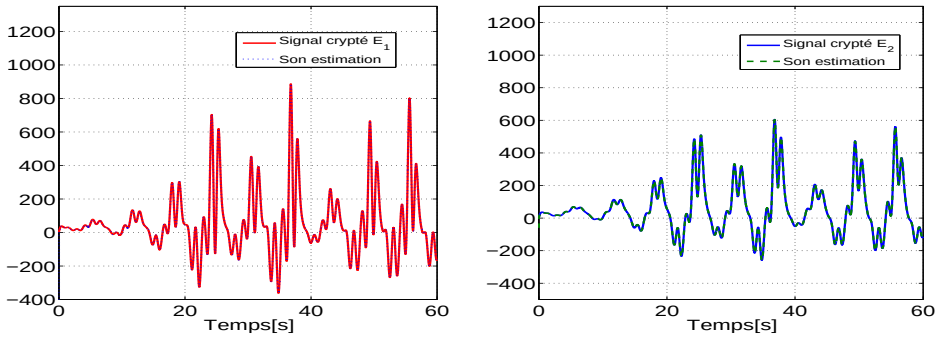

FIGURE 3.7: Reconstruction des signaux de cryptage E_1 (gauche) et E_2 (droite)

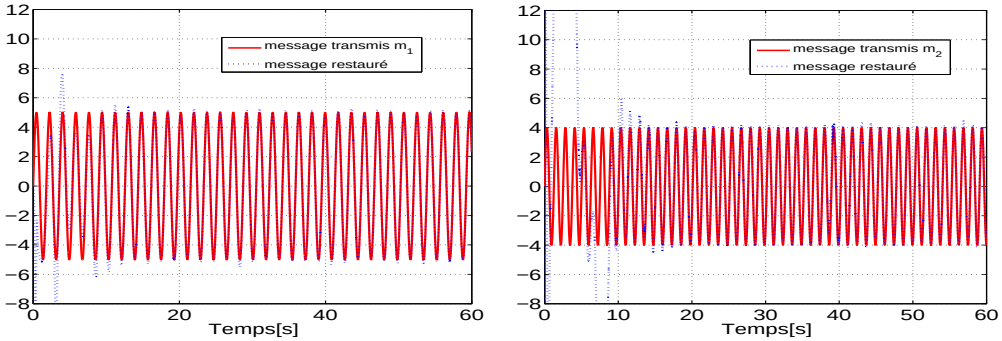

FIGURE 3.8: Les informations analogiques m_1 et son estimation $\hat{m}_1$ (gauche) & m_2 est son estimation $\hat{m}_2$ (droite)

3.3.3.2 Cryptage d'images binaires

Dans cette application, nous gardons le même système chaotique (SCM) maître en utilisant l'oscillateur de Lorenz. Cependant, le système SCA que nous utilisons pour crypter une image de type binaire est le système de Chua modifié proposé dans [91]. Le circuit de Chua modifié permet d'ajuster arbitrairement les régions de distribution des spectres de fréquences des signaux chaotiques en sélectionnant convenablement une résistance et une capacité qui déterminent le facteur de transformation de l'échelle du temps. Par conséquent, nous pouvons étendre la bande de fréquences des signaux chaotiques afin d'obtenir des signaux de hautes fréquences. Ce degré de liberté est très utile pour le cryptage de l'image à transmettre puisque nous pouvons ajuster la largeur des spectres des signaux chaotiques en fonction de la fréquence du signal correspondant à l'image binaire.

La dynamique du circuit de Chua modifié est donnée par

$$\begin{cases} T_s^{-1}\dot{x}_{31} = -\alpha(x_{32} - \bar{a}x_{31} + \bar{b}x_{31}\,|x_{31}| + \bar{c}x_{31}^3) \\ T_s^{-1}\dot{x}_{32} = x_{31} - x_{32} + x_{33} \\ T_s^{-1}\dot{x}_{33} = -\bar{\beta}x_{32} \end{cases} \tag{3.66}$$

Le signal de sortie est $y_3 = x_{31}$. Nous fixons le facteur de transformation de l'échelle de temps à $T_s = 100$. Le vecteur d'état $x_3 = [x_{31}; x_{32}; x_{33}]$ est initialisé à [0.7 ;0.2 ;-0.5]. En choisissant $\alpha = 12.8$, $\bar{\beta} = 19.1$, $\bar{a} = 0.472$, $\bar{b} = -1$ et $\bar{c} = 0.47$, le système (4.75) est caractérisé par un attracteur à triple spirale comme montré dans la figure 3.9.

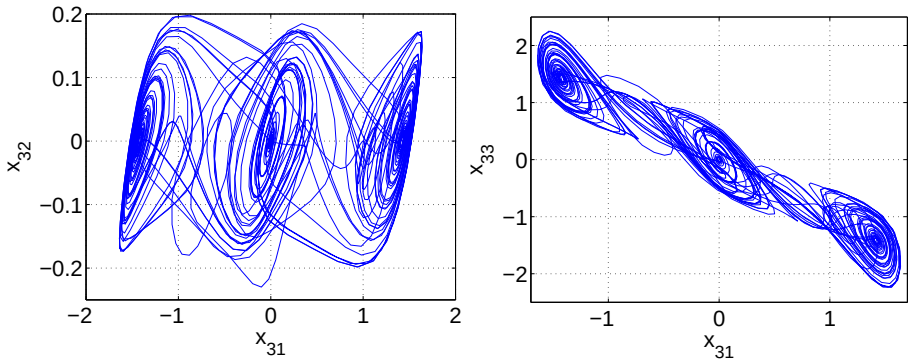

FIGURE 3.9: Plan de phase du système chaotique de Chua : $x_{31}\%x_{32}$ (gauche) et $x_{31}\%x_{33}$ (droite)

L'information à crypter est une image binaire (voir Figure 3.10a). Nous concaténons les lignes de la matrice carrée de dimension (256×256) correspondant à l'image afin d'obtenir un vecteur de taille 65536. Nous utilisons les coefficients de ce dernier pour générer un signal discret $m_3(t)$ en choisissant convenablement la période d'échantillonnage ($T = 10^{-3}s$) et nous envoyons le signal crypté $E_3(t) = 55x_{31} + 44x_{33} + (0.5x_{31}^2 + 1)m_3(t)$ via le système SD à travers le canal de communication bruité. Pour le récepteur, nous utilisons la fonction de décryptage afin de récupérer le message $\hat{m}_3(t) = \frac{\hat{E}_3 - 55\hat{x}_{31} + 44\hat{x}_{33}}{0.5\hat{x}_{31}^2 + 1}$ à partir duquel nous obtenons les coefficients de la matrice correspondant à l'image décryptée grâce au processus inverse. Les figures 3.10a, 3.10b et 3.10c illustrent respectivement les images (originale, cryptée et décryptée). La reconstruction du signal discret généré à partir de l'image originale est illustrée dans la figure 3.11.

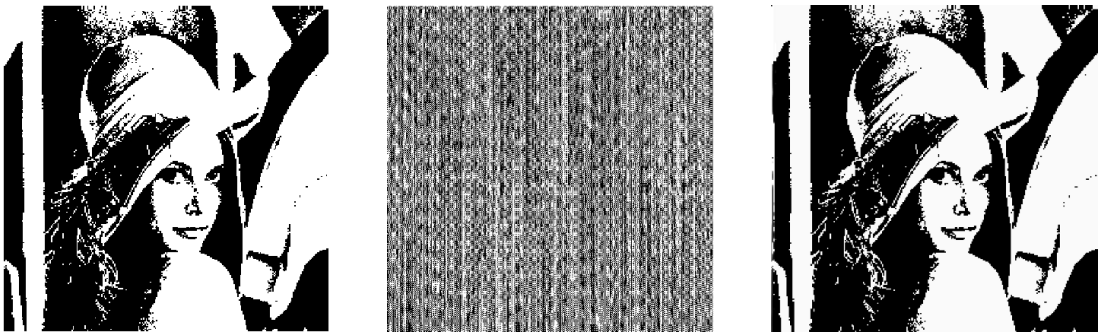

FIGURE 3.10: a) Image originale b) Image cryptée c) Image décryptée

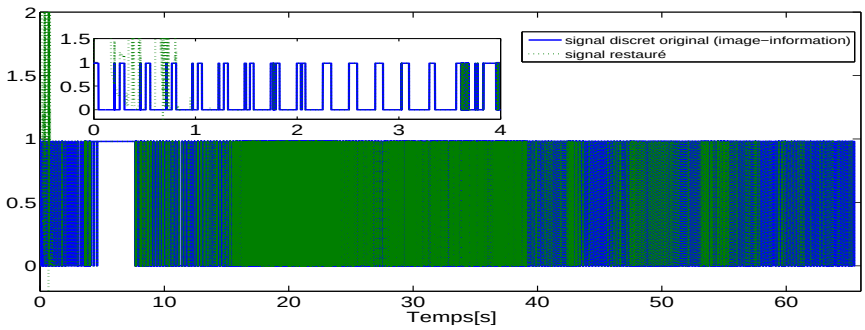

FIGURE 3.11: Reconstruction du signal discret généré à partir de l'image originale

3.3.3.3 Analyse de sécurité

Comme il est montré dans la figure 3.3, les signaux disponibles dans le canal public sont y_t émettant le signal de cryptage $E(t)$ et y_2 généré par le système SCM ; ces signaux sont totalement indépendants. De plus, le signal de sortie y_1 du système SCA est masqué à l'intérieur de la dynamique du système SCM et non directement transmis à travers le canal public. Donc, un espion ne peut pas utiliser les attaques basées sur l'identification de la structure et des paramètres du système émetteur – pour plus de détails, voir le chapitre 1.

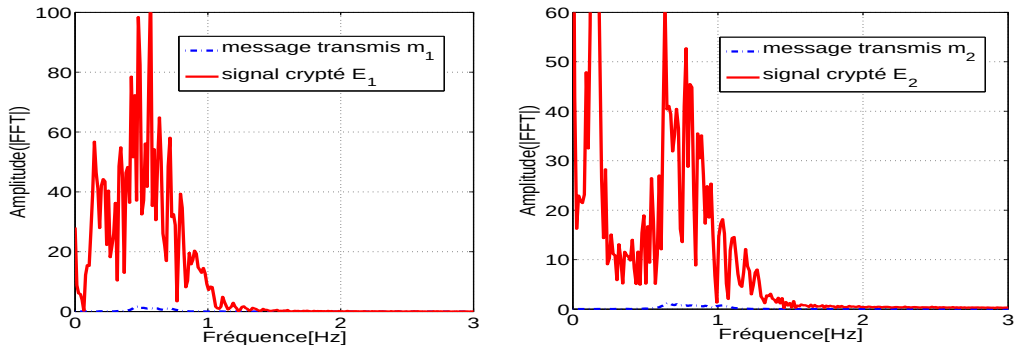

FIGURE 3.12: Cryptage des informations sinusoïdales analogiques dans les domaines temporel et fréquentiel

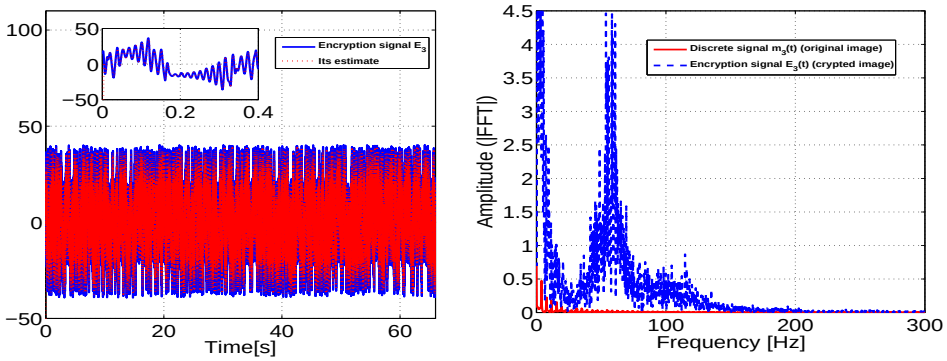

FIGURE 3.13: Cryptage de l'image binaire dans les domaines temporel et fréquentiel

La séparation entre les opérations de synchronisation et de cryptage permet de compliquer d'avantage le signal de cryptage $E(t)$ en combinant les opérations de multiplication et d'addition entre les différents signaux chaotiques et les messages sans affecter le comportement chaotique du système SCA ni compromettre la synchronisation entre les systèmes maître et esclave. Grâce à la fonction de cryptage $\Psi(\cdot,\cdot)$ qui peut être convenablement conçue, on obtient un signal crypté $E(t)$ qui assure un niveau élevé de sécurité. Cependant, notons qu'il y a un compromis entre la qualité du message décrypté et le niveau désiré de confidentialité.

En observant la figure 3.7, nous déduisons que les messages m_1 et m_2 sont bien cryptés. La figure 3.12 illustre les spectres des messages transmis et celui des signaux cryptés. Finalement, la figure 3.13 illustre le processus de cryptage de l'image dans les domaines temporels et fréquentiels. On constate que le spectre du message transmis est bien masqué à l'intérieur de celui du signal crypté correspondant et qu'il est effectivement caché dans le domaine temporel. Donc, un espion ne peut pas utiliser les méthodes des attaques basées sur l'analyse des caractéristiques du signal du texte chiffré (Voir le chapitre 1).

3.3.3.4 Analyse de la clé secrète

Dans l'application de cryptage d'images binaires pour laquelle on a utilisé deux systèmes chaotiques en cascade au niveau de l'émetteur (un système de Lorenz et un système de Chua modifié), on suppose que les conditions initiales sont exactement connues par un espion. Nous considérons les paramètres du système de Lorenz et de Chua afin de construire la clé secrète. Tout d'abord, on suppose qu'un espion connait la structure de deux systèmes chaotiques en cascade sans connaitre exactement les valeurs réelles de ces paramètres. Soit $P_i := (p_1 = \bar{\beta}, p_2 = \alpha, p_3 = \bar{a}, p_4 = \bar{b}, p_5 = \bar{c}, p_6 = r, p_7 = b_2, p_8 = a_1)$ la clé secrète. Notre objectif est de déterminer la taille r de l'espace clé $K_s = \{P_1, P_2, ..., P_r\}$ qui représente un ensemble fini de toutes les clés secrètes afin d'évaluer le niveau de sécurité produit par la clé secrète. Pour ce faire, on définit la marge de variation et la sensibilité de chaque paramètre p_i ; pour $i = 1..8$.

On suppose que la taille s de l'intervalle de variation de chaque paramètre p_i correspondant à un comportement chaotique du système de Lorenz et du système de Chua modifié est égale à 10^{-1}. Les simulations sont réalisées afin d'évaluer la sensibilité S_i de chaque paramètre p_i en déterminant la plus petite variation paramétrique qui génère deux comportements chaotiques différents (*i.e.*, deux attracteurs différents) alors que le reste des paramètres p_j ; pour $j \in \{1, 2..8\}/\{i\}$ sont fixés. La figure 3.14 illustre la sensibilité des systèmes de Lorenz et de Chua aux petites variations paramétriques $\bar{\beta}$ et r. La sensibilité aux paramètres est illustrée dans le tableau 4.1.

Système chaotique	**Paramètres**	**Sensibilité**	**Nb. de possibilités :** $(N_i = s \times {S_i}^{-1})$
Système de Chua	$p_1 = \bar{\beta} = 19.1$ $p_2 = \alpha = 12.8$ $p_3 = \bar{a} = 0.47$ $p_4 = \bar{b} = -1$ $p_5 = \bar{c} = 0.472$	$S_1 = 10^{-14}$ $S_2 = 10^{-15}$ $S_3 = 10^{-15}$ $S_4 = 10^{-16}$ $S_5 = 10^{-16}$	$N_1 = 10^{13}$ $N_2 = 10^{14}$ $N_3 = 10^{14}$ $N_4 = 10^{15}$ $N_5 = 10^{15}$
Système de Lorenz	$p_6 = r = 28$ $p_7 = b_2 = \frac{8}{3}$ $p_8 = a_1 = 10$	$S_6 = 10^{-14}$ $S_7 = 10^{-15}$ $S_8 = 10^{-15}$	$N_6 = 10^{13}$ $N_7 = 10^{14}$ $N_8 = 10^{14}$

TABLE 3.1: Sensibilité des paramètres

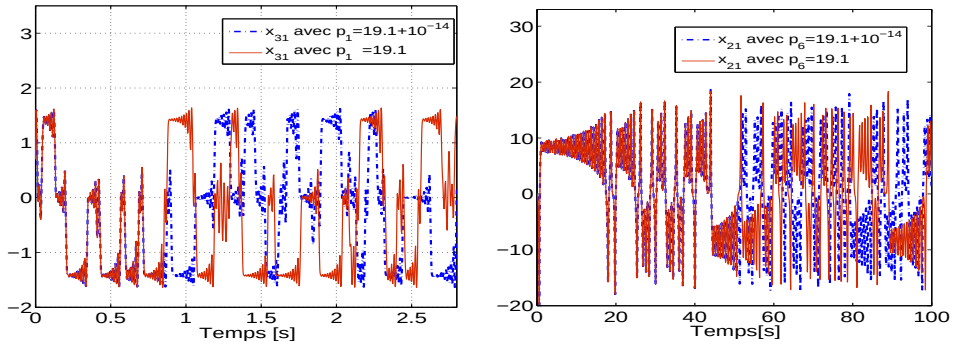

FIGURE 3.14: Les états du système de Lorenz (droite) et du système de Chua modifié (gauche) sous l'influence des petites variations (10^{-14}) des paramètres r et $\bar{\beta}$

La taille de l'espace clé est : $r = \prod_{i=1}^{8}(N_i) = 10^{(13\times2+14\times4+15\times2)} = 10^{112}$. Il a été évoqué dans la récente littérature des systèmes cryptographiques qu'un espace clé de taille $O(2^{100})$ est exigé pour résister aux attaques à force brute. Dans notre cas, $r = 10^{112} \gg 2^{100}$, ce qui implique que l'espace clé possède un niveau de sécurité satisfaisant d'un point de vue cryptographique. Le même raisonnement est applicable pour définir et caractériser une clé secrète pour l'application de transmission des signaux harmoniques.

3.4 Conclusion

Dans ce chapitre, nous avons présenté une méthode de synchronisation à base d'un *observateur adaptatif à modes glissants*. La méthode de synthèse de l'observateur repose sur des techniques adaptatives pour compenser l'effet des termes résiduels incertains tels que les bornes supérieures des états du système, des entrées inconnues et du bruit présent dans les signaux de sortie, ainsi que la "constante de Lipschitz" pouvant éventuellement prendre des grandes valeurs. La méthode proposée s'appuie également sur les techniques de conception d'observateurs singuliers et sur la théorie des

modes glissants (concept du commande équivalente) afin de reconstruire les entrées inconnues en présence du bruit dans les signaux de sortie. En se basant sur la théorie de Lyapunov, la stabilité pratique a été prouvé en démontrant que les états du système et les entrées inconnues peuvent être estimés avec une faible tolérance malgré la présence du bruit présent dans les équations de sortie.

Ensuite, nous avons appliqué l'observateur élaboré dans un nouveau schéma de communication chaotique sécurisée pour la transmission des données cryptées et représentées par des signaux de grande amplitude. L'architecture du système de communication proposé est basée sur l'utilisation de deux systèmes chaotiques en cascade au niveau de l'émetteur pour améliorer la sécurité. Par ailleurs, le système proposé est également robuste au bruit affectant le canal de communication. Les résultats théoriques ont été testés à travers des simulations numériques et une application de transmission des images binaires. Afin de vérifier l'efficacité du système développé, une analyse de robustesse aux différentes méthodes d'attaques connues et une étude de la clé secrète ont été effectuées et ont prouvé que le schéma de communication proposé possède des bonnes performances en terme de sécurité.
Dans le chapitre 4, nous nous intéressons à un autre cas de figure qui se présente en pratique où les systèmes de communications sont soumis à des retards de transmission et nous développons une méthode de synchronisation à base d'observateurs adaptatifs pour une classe des systèmes chaotiques de Lur'e.

Chapitre 4

Synchronisation à base d'observateurs adaptatifs en présence des retards de transmission

4.1 Introduction

Dans les schémas de communications basés sur la synchronisation des systèmes chaotiques, les retards de transmission se produisent fréquemment dans les configurations de synchronisation maître-esclave. Dans ce chapitre, nous proposons une méthode de synchronisation à base d'observateurs adaptatifs pour une classe des systèmes de Lur'e avec des non-linéarités à pente limitée en présence d'un retard de transmission. La méthode de synchronisation élaborée est utilisée dans un système de communication chaotique présentant un retard dans le canal public. Le retard est supposé à temps variant et borné, et l'information à transmettre est un signal constant par morceaux. En se basant sur l'approche de Lyapunov-Krasovskii, nous montrons que pour des valeurs de la borne supérieure du retard suffisamment petites, les objectifs de synchronisation et de reconstruction des messages transmis sont accomplis sous une condition d'excitation persistante et après la résolution d'un problème d'optimisation convexe. Ensuite, l'approche ainsi développée a été étendue pour le cas des longs retards de transmission et un schéma de synchronisation basé sur les observateurs en cascade a été proposé. Les résultats théoriques sont illustrés à travers des exemples numériques des systèmes de communication présentant des retards de transmission. La méthode de synchronisation proposée est également exploitée dans un système de communication sécurisée, basée sur la combinaison de notre approche avec des techniques de cryptage garantissant un niveau élevé de confidentialité. Une analyse détaillée de la sécurité du système de communication ainsi proposé est présentée à la fin du chapitre.

4.2 Contexte et motivations

Dans la dernière décennie, une attention particulière a été accordée au problème de synchronisation des systèmes chaotiques de Lur'e avec propagation du retard. L'approche de communication adoptée dans la littérature est basée sur les commandes par retour d'état/sortie et l'exploitation des propriétés du secteur et de restriction de pente des systèmes de Lur'e – voir les références [92], [93], [94], [95], [96].

Le premier travail traitant ce problème a été réalisé dans la référence [92] dans laquelle un critère de synchronisation dépendant du retard a été développé en se basant sur la théorie de Lyapunov-Krasovskii. Ce résultat a motivé plusieurs travaux de recherche abordant le problème de synchronisation des systèmes chaotiques de Lur'e. Dans la référence [93], deux critères de synchronisation ont été proposés : le premier critère est dépendant du retard et le deuxième est indépendant du retard. Dans [94], les auteurs proposent une méthode de synchronisation utilisant une commande qui comprend à la fois un retour de l'erreur de l'état actuel et un retour de l'erreur de sortie statique, et en considérant une fonctionnelle de Lur'e-Postnikov-Lyapunov de forme plus générale, des nouveaux critères dépendant du retard sont présentés sous la forme des inégalités matricielles linéaires (LMIs). Plus récemment, ce résultat a été étendu dans [95] pour le cas des retards à temps variant uniformément bornés et le cas des retards à temps variant uniformément bornés et différentiables avec des dérivées bornées.

Dans ce chapitre, le problème de synchronisation des systèmes de Lur'e est considéré comme étant un problème d'estimation d'état où le système esclave est un observateur pour le système maître. Plusieurs approches de synchronisation à base d'observateurs ont été développées exclusivement dans le cas d'absence des retards de transmission (les retards sont souvent supposés négligeables). Cependant, le cas des sorties retardées dans les problèmes de synthèse d'observateurs a été récemment traité dans la littérature de *la théorie des commandes et systèmes*.

Par exemple, dans la référence [97], les auteurs proposent une chaîne d'algorithmes d'observation pour une classe des systèmes observables avec des sorties retardées et qui assurent la convergence globale exponentielle de l'erreur d'estimation. Une conception similaire a été adoptée dans [98], néanmoins l'observateur non linéaire proposé possède un gain dépendant de l'état qui calcule à partir de la solution du système des équations différentielles partielles du premier ordre et les conditions garantissant la convergence de l'erreur d'observation ont été présentées.

D'autre part, dans la référence [99], les auteurs proposent un observateur pour une classe des systèmes non linéaires observables en présence d'un retard d'observation à temps variant borné. La convergence asymptotique et la convergence exponentielle de l'erreur d'estimation ont été démontrées en se basant sur l'approche de Lyapunov-Razumikhiin.
Plus récemment, dans les références [100],[101], une approche élégante basée sur la méthode de synthèse d'observateurs à grand gain a été introduite pour une classe des systèmes non linéaires triangulaires avec respectivement des retards de mesure constants et à temps variant. La convergence

asymptotique a été démontrée grâce à une fonctionnelle de Lyapunov-Krasovskii appropriée et sous une certaine condition reliant le gain de l'observateur et la borne supérieure du retard de mesure.

Dans ce chapitre, nous proposons une méthode de synchronisation à base d'observateurs pour une classe des systèmes chaotiques de Lur'e avec des non-linéarités à pente limitée, en présence des retards de transmission. La méthode de synchronisation proposée est également appliquée dans un système de communication chaotique, et par conséquent se pose également la question de restauration des messages transmis. Pour résoudre ce problème, la méthode de synchronisation que nous proposons est adaptative et permet l'estimation conjointe des états et des messages envoyés malgré la présence du retard de transmission (dans le cas d'un message binaire, la durée d'un bit est supposée plus longue que le retard de transmission). D'après notre connaissance, le problème de synchronisation à base d'observateurs adaptatifs dans un tel scénario complet n'est pas encore résolu. En se basant sur l'approche de Lyapunov-Krasovskii, nous montrons que pour des valeurs suffisamment petites des retards, l'estimation des états et la reconstruction des messages transmis sont assurées sous une condition d'excitation persistante et après la résolution d'un problème convexe d'optimisation.

4.3 Position du problème

Considérons le système de communication composé d'un système *émetteur* et d'un système *récepteur*. La technique de transmission que nous utilisons consiste à injecter d'une manière appropriée les messages (constants par morceaux) dans la dynamique de l'émetteur chaotique. On suppose que le canal public de communication présente un retard de transmission $h(t)$. L'émetteur est basé sur une classe des systèmes chaotiques de Lur'e et représenté par les équations :

$$\dot{x} = Ax + Ff(Hx,u) + B\sum_{k=1}^{q}\Psi^k(R_kx,u)m_k \tag{4.1a}$$

$$y = Cx(t-h(t)) \tag{4.1b}$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, $y \in \mathbb{R}^p$ représente le vecteur de sortie affectée par le retard de transmission h et $u \in \mathbb{R}^l$ représente un signal d'entrée d'excitation. On suppose que $h(t)$ est une fonction à temps variant satisfaisant $0 \leq h(t) \leq h_m$, $\forall t \geq 0$. $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times s}$, $F \in \mathbb{R}^{n\times m}$, $C \in \mathbb{R}^{p\times n}$ et $H = (H_1, H_2, \ldots, H_m)^T \in \mathbb{R}^{m\times n}$ et $R_k = (R_{k1}, \ldots, R_{ks})^T \in \mathbb{R}^{s\times n}$ sont des matrices constantes ; où H_i est la i-ème ligne de H ; pour $i = 1..m$ et R_{k_i} est la i-ème ligne de R_k ; pour $i = 1..s$. Soit $m := (m_1, \ldots, m_q)^T$ le vecteur du signal information, avec $m_k \in \mathbb{R}$ supposé constant par morceaux (la durée de chaque morceau constant du message est supposée supérieure à la valeur de la borne supérieure h_m du retard de transmission), $f : \mathbb{R}^m \times \mathbb{R}^l \to \mathbb{R}^m$ est une fonction non linéaire telle que $f(Hx,u) = (f_1(H_1x,u), \ldots, f_m(H_mx,u))$ et $\Psi^k : \mathbb{R}^s \times \mathbb{R}^l \to \mathbb{R}^s$ représentent des fonctions à excitation persistante telles que $\Psi^k(R_kx,u) = (\Psi_1^k(R_{k1}x,u), \ldots, \Psi_s^k(R_{ks}x,u))$.

On suppose que $\forall i \in 1..m$, $f_i(\cdot)$ satisfait la condition de restriction de pente :

$\forall u \in \mathbb{R}^l$, $\forall \xi_1, \xi_2 \in \mathbb{R}$ telles que $\xi_1 \neq \xi_2$, on a

$$0 \leq \frac{f_i(\xi_1, u) - f_i(\xi_2, u)}{\xi_1 - \xi_2} \leq b \tag{4.2}$$

D'une manière similaire, on suppose que $\Psi^k(R_k x, u)$ satisfait les mêmes propriétés que $f(Hx, u)$ tel que la pente est limitée dans l'intervalle $[0, \bar{b}_k]$, avec $\bar{b}_k$ est une constante positive avec $k = 1..q$.

Remarque 4.1. Si f_i est continuellement différentiable et que $a_i \leq \frac{\partial f_i(w)}{\partial w} \leq b_i$, $\forall w \in \mathbb{R}$, ce qui est le cas des systèmes chaotiques (puisque les solutions sont globalement bornées), donc en appliquant le théorème d'accroissements finis, f_i vérifie la condition de restriction de pente (4.2). De cette manière, la classe des systèmes considérés dans ce chapitre est élargie.

Notons qu'à l'origine, le système émetteur (4.1) est conçu à base des systèmes de Lur'e sous la forme *nominale* suivante :

$$\dot{x}(t) = A_0 x(t) + F_0 f(Hx(t), u(t)). \tag{4.3}$$

La classe des systèmes (4.3) couvrent particulièrement les systèmes chaotiques non autonomes (à temps variant) sous la forme de Lur'e où le chaos est généré en appliquant un signal d'excitation harmonique. Un exemple typique de ces systèmes est l'oscillateur de Duffing :

$$\begin{aligned} \dot{x}_1 &= x_2, \\ \dot{x}_2 &= -a_2 x_2 - 1.1\theta x_1^3 + b_2 cos(\omega_2 t), \end{aligned} \tag{4.4}$$

qui est sous la forme nominale (4.3). Dans ce cas, le signal d'excitation est $u(t) = cos(\omega_2 t)$, le terme non linéaire $f_0(x) = \theta x_1^3$ est continuellement différentiable et les trajectoires du système (4.4) sont globalement bornées dans le régime chaotique, donc, conformément à la remarque 4.1, la fonction f_0 vérifie la propriété de restriction de pente (4.2).
La classe des systèmes considérés dans ce chapitre couvre également les systèmes chaotiques autonomes (à temps invariant) sous la forme de Lur'e tels que les systèmes de Chua, les systèmes de Chua couplés, l'oscillateur de Van der Pol, etc. Puisqu'à la origine, ces derniers ne sont pas excités par des signaux d'excitation (à temps variant) et afin d'obtenir la forme finale (4.1) du système émetteur, leur structure peut être soigneusement modifiée en injectant convenablement le signal d'information $m(t)$ et le signal d'excitation $u(t)$ de telle manière que leurs amplitudes soient suffisamment petites pour préserver le comportement chaotique. Comme nous allons détailler plus loin, nous avons besoin que le signal $u(t)$ vérifie la condition d'excitation persistante afin de pouvoir reconstruire l'information transmise.

En particulier, le *système de Chua généralisé*

$$\dot{x}_1 = a(x_2 - g_1(x_1)) \tag{4.5a}$$

$$\dot{x}_2 = x_1 - x_2 + x_3 \tag{4.5b}$$

$$\dot{x}_3 = -bx_2 \tag{4.5c}$$

avec

$$g_1(x_1) = m_{2q-1}x_1 + \frac{1}{2}\sum_{i=1}^{2q-1}(m_{i-1} - m_i)(|x_1 + 1| - |x_1 - 1|), \tag{4.6}$$

est sous la forme (4.3) ; les paramètres a, b et m_i pour$i \in \{1, \ldots, 2q-1\}$ sont sélectionnés tels que le système (4.5) fonctionne en régime chaotique.

Notre objectif consiste à concevoir un système esclave (le récepteur) qui synchronise avec le système maître (4.1) et reconstruit le signal d'information $m(t)$ malgré la présence du retard de transmission $h(t)$. Le problème de synchronisation est formulé comme suit : il s'agit de synthétiser un système dynamique :

$$\dot{z}(t) = \Phi(t, y(t), z(t), z(t-h(t)), \hat{m}(t)) \tag{4.7a}$$

$$\dot{\hat{m}}(t) = \Psi(t, y(t), z(t), z(t-h(t))) \tag{4.7b}$$

tel que

$$\lim_{t\to\infty} |x(t) - z(t)| = 0. \tag{4.8}$$

et

$$\lim_{t\to\infty} |m(t) - \hat{m}(t)| = 0. \tag{4.9}$$

4.4 Synthèse du système esclave

Le problème de synthèse d'observateurs pour les systèmes non linéaires avec des non-linéarités à pente limitée a été particulièrement étudié dans la référence [40] par Arcak et Kokotović qui ont présenté une approche utilisant les bornes de la pente du terme non linéaire pour prouver la convergence de l'erreur d'estimation. Cette méthode a été étendue dans [46] dans lequel les auteurs présentent un observateur H_∞ adaptatif pour une classe des systèmes avec des non-linéarités Lipschitziennes et monotones. En particulier, les propriétés de restriction de pente ont été utilisées pour résoudre le problème de synchronisation des systèmes de Lur'e à base des commandes à retour d'état [102] en présence des retards [103], [92].

D'un autre côté, le problème d'estimation conjointe des états et des paramètres inconnus à base d'observateurs adaptatifs dans le scénario *sans retard dans l'équation de sortie* a été étudié dans la littérature – voir [51], [53], [54]. La référence [14] traite ce problème dans le contexte de synchronisation des systèmes chaotiques avec des incertitudes paramétriques.

Motivés par les méthodes de synthèse des observateurs pour les systèmes avec des non-linéarités à pente limitée et les approches de synthèse d'observateurs adaptatifs, nous proposons un observateur (le système esclave) pour le système (4.1) qui assure la synchronisation entre les systèmes maître et esclave ainsi que l'estimation de l'information transmise malgré la présence des retards de

transmission :

$$\dot{z} = Az + Ff(Hz,u) + B\sum_{k=1}^{q}\Psi^k(R_kz,u)\hat{m}_k + K(\hat{y} - Cz(t-h(t))) \quad (4.10a)$$

$$\dot{\hat{m}}_k = \rho\Upsilon_k^{-1}\Psi^k(R_kz,u)^T M(y(t) - Cz(t-h(t))) \quad (4.10b)$$

$$\dot{\Upsilon}_k = -\alpha\Upsilon_k + \Psi^k(R_kz,u)^T B^T B\Psi^k(R_kz,u) \quad (4.10c)$$

$$\Upsilon_k(0) > 0, \quad k = 1..q, \quad (4.10d)$$

où $z(t)$ est l'état estimé et $\hat{m}_k(t)$ représente les informations restaurées ; ρ et α sont deux constantes positives.

On définit l'erreur de synchronisation $e(t) := x(t) - z(t)$ et l'erreur d'adaptation $\tilde{m}(t) := (\tilde{m}_1(t), \ldots, \tilde{m}_q(t))$, avec $\tilde{m}_k(t) := m_k(t) - \hat{m}_k(t)$, pour $k = 1..q$. En utilisant le fait que $\dot{m}_k(t) = 0$ presque partout, le système d'erreurs est décrit par les équations :

$$\begin{aligned}\dot{e} &= Ae - KCe(t-h) + F\eta(He,x,u) \\ &\quad + B\sum_{k=1}^{s}(\bar{\eta}^k(R_ke,x,u)m_k + \Psi^k(R_kz,u)\tilde{m}_k) \quad (4.11a)\\ \dot{\tilde{m}}_k &= -\rho\Upsilon_k^{-1}\Psi^k(R_kz,u)^T MCe(t-h), \quad (4.11b)\end{aligned}$$

avec $\eta(He,x,u) = (\eta_1(H_1e,x,u), \ldots, \eta_m(H_me,x,u))$, tel que pour $i = 1..m$:
$\eta_i(H_ie,x,u) = f_i(H_ix,u) - f_i(H_ix - H_ie,u)$; et $\bar{\eta}^k(R_ke,x,u) = (\bar{\eta}_1^k(R_1e,x,u), \ldots, \bar{\eta}_s^k(R_se,x,u)$ tel que pour $i = 1..s$,
$\bar{\eta}_i^k(R_{ki}e,x,u) = \Psi^k(R_{ki}x,u) - \Psi^k(R_{ki}x - R_{ki}e,u)$.

Le système d'erreurs (4.11) est initialisé comme suit :

$$e(\vartheta) = \phi_s(\vartheta), \quad (4.12a)$$

$$\tilde{m}(\vartheta) = \phi_a(\vartheta), \quad \forall\vartheta \in [-h_m, 0]. \quad (4.12b)$$

où $\phi_s(\cdot)$ et $\phi_s(\cdot)$ sont des fonctions continues définies dans l'intervalle $[-h_m, 0]$.
Maintenant, compte tenu la propriété de restriction de pente (4.2) avec $\xi_1 = H_ix$ et $\xi_2 = H_ix - H_ie$, on suppose que $\forall e \neq 0, \forall x, \forall u$

$$0 \leq \frac{\eta_i(H_ie,x,u)}{H_ie} \leq b. \quad (4.13)$$

En multipliant de deux côtés de (4.13) par $\eta_i(H_ie,x,u)H_ie$, on obtient :
pour $i = 1..m$, $\forall t \geq 0$, $\forall e, \forall x, \forall u$

$$\eta_i(H_ie,x,u)[\eta_i(H_ie,x,u) - bH_ie] \leq 0 \quad (4.14)$$

qui signifie que $\eta(He, x, u)$ appartient au secteur $[0, b]$. Soit $D = diag(d_1, d_2, \ldots, d_m)$ avec $d_i > 0$, $\forall i = 1..m,$. Ensuite, on obtient facilement la relation suivante :

$$-\eta^T(He, x, u)D\eta(He, x, u) + b\eta(He, x, u)DHe \geq 0. \tag{4.15}$$

On procède avec le même raisonnement dans le cas de $\Psi^k(R_k x, u)$, on obtient :

$\forall k = 1..q$ et $\bar{D}_k = diag(\bar{d}_{k1}, \ldots, \bar{d}_{ks})$ avec $\bar{d}_{ki} > 0$, $\forall i = 1..s$.

$$-\bar{\eta}^{kT}(R_k e, x, u)\bar{D}_k\bar{\eta}(R_k e, x, u) + \bar{b}^k\bar{\eta}^k(R_k e, x, u)\bar{D}_k R_k e \geq 0. \tag{4.16}$$

Hypothèse 4.2. *On suppose qu'il existe une matrice définie positive P, des matrices diagonales positives D, $\bar{D}_1, \ldots, \bar{D}_q$; des matrices M et K de dimensions appropriées et une constante positive ε telles que*

$$\mathcal{S} = \begin{bmatrix} -Q + \varepsilon I & PF + bH^T D & \Lambda \\ F^T P + bDH & -2D & 0 \\ \Lambda^T & 0 & -2\bar{D} \end{bmatrix} \leq 0 \tag{4.17a}$$

$$B^T P = MC \tag{4.17b}$$

avec $Q = -[(A - KC)^T P + P(A - KC)]$, $\Lambda = (PB + \bar{b}_1 R_1^T \bar{D}_1, \cdots, PB + \bar{b}_q R_q^T \bar{D}_q)$ *et* $\bar{D} = block - diag(\bar{D}_1, \ldots, \bar{D}_q)$

Des inégalités matricielles similaires à (4.17) peuvent être retrouvées dans la littérature de la synchronisation maître-esclave des systèmes de Lur'e en présence des retards de transmission, et particulièrement les méthodes basées sur la commande par retour d'état/sortie et l'exploitation des propriétés du secteur et de restriction de pente des systèmes de Lur'e – voir les références [92], [93], [94], [95], [96]. D'autre part, notons qu'une condition nécessaire pour la solvabilité de l'équation matricielle (4.17b) est l'hypothèse du "degré relatif 1" ($i.e$ si Rang(CB)=Rang(B)). Cette dernière est souvent utilisée pour la conception des observateurs à entrées inconnues, des observateurs à modes glissants de premier ordre et des observateurs adaptatifs.

Afin de trouver les matrices P, D, $\bar{D}_1, \ldots, \bar{D}_q$, M et K utilisées dans l'hypothèse 4.2, on considère le problème convexe d'optimisation suivant :

Minimiser ς tel que

$$P > 0 \tag{4.18}$$

$$D > 0 \tag{4.19}$$

$$\varepsilon > 0 \tag{4.20}$$

$$\begin{bmatrix} \Xi & PF + bH^T D & \Lambda \\ F^T P + bDH & -2D & 0 \\ \Lambda^T & 0 & -2\bar{D} \end{bmatrix} \leq 0 \tag{4.21}$$

$$\begin{bmatrix} \varsigma I & B^\top P - MC \\ PB - C^\top M^\top & \varsigma I \end{bmatrix} \leq 0\,, \tag{4.22}$$

avec $\Xi = PA + A^\top P + WC_1 + C^\top W^\top + \varepsilon I$.
La solution correspondant à ce problème donne un minimum $\varsigma = 0$, ε, P, D, $\bar{D}_1, \ldots, \bar{D}_q$, M et W tels que $K = -P^{-1}W$ vérifient (4.17a). Ce problème peut être résolu en utilisant des algorithmes d'optimisation convexes bien développés dans LMI toolbox de Matlab. Une autre alternative consiste à utiliser le paquet *cvx* spécifique aux problèmes LMIs et compatible avec Matlab.

Hypothèse 4.3. *On suppose que pour tout u bornée, pour tout $\zeta \in \mathbb{R}^s$, $\Psi^k(.,u)$ et $k \in \{1 \ldots q\}$, il existe $\mu_\psi > 0$ tel que :*

$$\left|\Psi^k(\zeta, u)\right| \leq \mu_\psi. \tag{4.23}$$

On suppose également que $m_k(t)$ est bornée et qu'il existe $\mu_m > 0$ tel que

$$\sup_{t \geq 0} |m_k(t)| \leq \mu_m. \tag{4.24}$$

Notons que dans le cas où $\Psi^k(\cdot)$ ne vérifie pas la propriété de bornitude et si les solutions $x(t)$ du système maître (4.1) appartiennent à un ensemble compact X, on peut utiliser une fonction de saturation $\sigma : \mathbb{R}^n \to X$, $x \to \sigma(x)$ bornée, pour tout $x \in \mathbb{R}^n$. La bornitude des solutions est une hypothèse commune dans la littérature de synthèse d'observateurs, elle est satisfaite dans le cas de plusieurs systèmes physiques tels que les oscillateurs chaotiques et en particulier les systèmes chaotiques de Lur'e. Ainsi, cette hypothèse n'est pas contraignante dans le présent contexte.

Hypothèse 4.4. *On suppose que le signal d'excitation u est tel que pour toute trajectoire $z(t)$ du système (4.10), $\forall k = 1..q$, il existe $\mu_k, T_k > 0$, tels que $\forall\, t \geq 0$*

$$\int_t^{t+T_k} \Psi^k(R_k z(s), u(s))^T B^T B \Psi^k(R_k z(s), u(s)) ds \;\geq \mu_k. \tag{4.25}$$

La dernière hypothèse signifie que les signaux $B\Psi^k(R_k z(t), u(t))$ doivent être à excitation persistante. Ceci est possible si le signal d'excitation $u(t)$ est choisi suffisamment riche. Une hypothèse similaire a été utilisée dans la référence [55] pour la synthèse des observateurs adaptatifs pour une classe des systèmes non linéaires MIMO uniformément observables.

La condition d'excitation persistante est nécessaire pour garantir la positivité des solutions $\Upsilon_k(t),\ k = 1..q$ de l'équation (4.10c). Ceci est également indispensable pour la restauration des informations transmises comme nous allons détailler plus loin.

Lemme 4.5. *Soit $\Upsilon_k(t)$ la solution de l'équation (4.10c), $\forall k = 1..q$. Si $B\Psi^k(R_k z(t), u(t))$ vérifie l'hypothèse 4.4, donc $\Upsilon_k(t)$ est une fonction positive telle que*

$$\forall t \geq max\{T_k, k = 1..q\}, \quad \Upsilon_k(t) \geq \upsilon_m, \tag{4.26}$$

avec $\upsilon_m = \min\{\mu_k e^{-\alpha T_k}, k = 1..q\}$.

Démonstration :

Soit $\Upsilon_k(t)$ la solution de l'équation (4.10c), $\forall k = 1..q$.
Soit $\Omega^k(t) := \Psi^k(R_k z(t), u(t))^T B^T B \Psi^k(R_k z(t), u(t))$.

On a

$$\begin{aligned} \frac{d}{dt}(e^{\alpha t}\Upsilon_k(t)) &= e^{\alpha t}(\dot{\Upsilon}_k(t) + \alpha\Upsilon_k(t)) \\ &= e^{\alpha t}\Omega^k(t). \end{aligned}$$

Intégrant l'équation précédente de 0 à $t + T_k$,

$$\begin{aligned} e^{\alpha(t+T_k)}\Upsilon_k(t+T_k) &= \Upsilon_k(0) + \int_0^{t+T_k} e^{\alpha s}\Omega^k(s)ds \\ &\geq \int_0^{t+T_k} e^{\alpha s}\Omega^k(s)ds. \end{aligned}$$

Multipliant de deux côtés de $e^{-\alpha(t+T_k)}$, on obtient

$$\begin{aligned} \Upsilon_k(t+T_k) &\geq \int_0^{t+T_k} e^{\alpha(s-t-T_k)}\Omega^k(s)ds. \\ &\geq \int_t^{t+T_k} e^{\alpha(s-t-T_k)}\Omega^k(s)ds. \end{aligned}$$

Pour $t \leq s \leq t + T_k$, $e^{-\alpha T_k} \leq e^{\alpha(s-t-T_k)} \leq 1$, donc

$$\Upsilon_k(t+T_k) \geq e^{-\alpha T_k}\int_t^{t+T_k} \Omega^k(s)ds.$$

Par conséquent, en utilisant l'équation (4.25), $\forall t \geq T_k$, on obtient

$$\Upsilon_k(t) \geq \mu_k e^{-\alpha T_k}.$$

Finalement, il s'en suit que

$$\forall t \geq \max\{T_k, k = 1..q\}, \quad \Upsilon_k(t) \geq \upsilon_m, \tag{4.31}$$

avec $\upsilon_m = \min\{\mu_k e^{-\alpha T_k}, k = 1..q\} > 0$. ■

Dans la section suivante, nous discutons les conditions garantissant la synchronisation entre les systèmes maître et esclave ainsi que la reconstruction du message en se basant sur la théorie de *Stabilité de Lyapunov-Krasovskii*.

4.5 Analyse de stabilité

4.5.1 Stabilité des systèmes à retard

On considère l'équation fonctionnelle différentielle retardée

$$\dot{x}(t) = f(x_t), \qquad x_0 = \phi \in \mathcal{C}; \qquad x_t \in \mathcal{C} \tag{4.32}$$

où $\mathcal{C} = C([-r, 0], \mathbb{R}^n)$ représente l'ensemble des fonctions continues dans l'intervalle $[-r, 0]$, $x \in \mathbb{R}^n$, $f : \mathbb{R} \times \mathcal{C} \to \mathbb{R}^n$ est continue, $f(t, 0) = 0$ pour tout $t \in \mathbb{R}$ et x_t la fonction définie par

$$x_t(\vartheta) = x(t + \vartheta), \qquad -r \leq \vartheta \leq 0. \tag{4.33}$$

Pour une fonction $\psi \in \mathcal{C}$, on définit $|\psi|_c := \max_{-r \leq \theta \leq 0} |\psi(\theta)|$.

Définition 4.6. (Stabilité asymptotique) Pour un système retardé décrit par (4.32), la solution triviale $x(t) \equiv 0$ est stable si pour tout $\tau \in \mathbb{R}$ et $\varepsilon > 0$, il existe $\delta > 0$ tel que $|x_\tau|_c \leq \delta$ implique $|x_\tau|_c \leq \varepsilon$ pour tout $t \geq \tau$. Il est dit asymptotiquement stable s'il est stable et pour tout $\tau \in \mathbb{R}$ et $\varepsilon > 0$, il existe, en plus, $\delta_a > 0$ tel que $|x_\tau|_c \leq \delta_a$ implique $\lim_{t \to \infty} x(t) = 0$. Il est globalement asymptotiquement stable s'il est asymptotiquement stable et δ_a peut être choisi arbitrairement large.

Définition 4.7. (Stabilité exponentielle)
La solution triviale du système (4.32) est exponentiellement stable s'il existe $\alpha > 0$ et $\gamma > 0$ tels que pour toute solution $x(\cdot, t_0, \phi)$, $\phi \in \mathcal{C}$:

$$|x(t, t_0, \phi)| \leq \gamma |\phi|_c \exp(-\alpha(t - t_0)), \forall t \geq t_0. \tag{4.34}$$

Théorème 4.8. *(Théorème de Lyapunov-Krasovskii)*
On suppose que $f : \mathbb{R} \times \mathcal{C} \to \mathbb{R}^n$ dans l'équation (4.32) et que u, v, $w : \mathbb{R}^+ \to \mathbb{R}^+$ sont des fonctions continues non décroissantes. En plus, $u(s)$ et $v(s)$ sont positives pour $s > 0$ et $u(0) = v(0) = 0$. S'il existe une fonctionnelle continuellement différentiable $V : \mathbb{R} \times \mathcal{C} \to \mathbb{R}$ telle que

$$u(|x(t)|) \leq V(t, x_t) \leq v(\max_{-r \leq \theta \leq 0} |x(t + \theta)|) \tag{4.35}$$

et

$$\dot{V}(t, x_t) \leq -w(|x(t)|), \tag{4.36}$$

et que la solution d'équilibre du système (4.32) est uniformément stable. Si $w(s) > 0$ *pour* $s > 0$, *donc elle est uniformément asymptotiquement stable. Si en plus,* $\lim_{|s|\to+\infty} \mu(s) = +\infty$, *elle est globalement uniformément asymptotiquement stable.*

Pour la définition 4.6 et le théorème 4.8, voir [Théorème 4.1, [104]] et pour la définition 4.7, voir [105].

4.5.2 Synchronisation maître-esclave et restauration des messages transmis

Le théorème suivant présente les conditions garantissant la synchronisation maître-esclave et la reconstruction des messages transmis en se basant sur le théorème de Lyapunov-Krasovskii .

Théorème 4.9. *On considère le système maître (4.1) et le système esclave (4.10). Supposons que les hypothèses 4.2, 4.3 et 4.4 sont satisfaites. Donc, la solution d'équilibre du système d'erreurs (4.11) est globalement asymptotiquement stable pour une valeur suffisamment petite de la borne supérieurs* h_m *du retard de transmission.*

Démonstration :

Tout d'abord, on applique la formule de Leibniz-Newton à l'erreur de synchronisation $e(t)$:

$$\begin{aligned} e(t) - e(t-h) &= \int_{t-h}^{t} \dot{e}(s)ds \\ &= \int_{-h}^{0} \dot{e}(t+\vartheta)d\vartheta. \end{aligned} \tag{4.37}$$

La dynamique de $e(t)$ peut donc être réécrite comme suit :

$$\begin{aligned} \dot{e} = (A-KC)e + F\eta(He,x,u) + KC\int_{-h}^{0} \dot{e}(t+\vartheta)d\vartheta \\ + B(\sum_{k=1}^{q} \bar{\eta}^k(R_k e,x,u)m_k + \sum_{k=1}^{q} \Psi^k(R_k z,u)\tilde{m}_k). \end{aligned} \tag{4.38}$$

Soit $\omega(t) = (e(t), \tilde{m}(t))^T$ et ω_t la fonction définie par :

$$\omega_t(\vartheta) = \omega(t+\vartheta), \qquad -h_m \leq \vartheta \leq 0. \tag{4.39}$$

On considère la fonctionnelle de Lyapunov-Krasovskii :

$$V(t,\omega_t) = V_1(e(t)) + V_2(\omega_t) + V_3(t,\tilde{m}(t)) \tag{4.40}$$

où

$$V_1(e(t)) = e(t)^T P e(t), \tag{4.41a}$$
$$V_2(\omega_t) = \int_{-h_m}^{0} (\vartheta + h_m)|\dot{e}(t+\vartheta)|^2 \, d\vartheta, \tag{4.41b}$$
$$V_3(t, \tilde{m}(t)) = \sum_{k=1}^{q} \rho^{-1} \Upsilon_k(t) \tilde{m}_k(t)^2, \tag{4.41c}$$

et $\Upsilon_k(t)$ est une solution de l'équation (4.10c). Pour simplifier la présentation, on introduit les notations suivantes

$$\Gamma(t) := \int_{-h(t)}^{0} \dot{e}(t+\vartheta)d\vartheta \quad ; \quad \beta_a := |A| \, ;$$
$$\beta_b := |B| \quad ; \quad \beta_c := |KC| \, .$$

La dérivée de V_1 le long des trajectoires du système (4.11) est donnée par

$$\dot{V}_1 = e^T[(A-KC)^T P + P(A-KC)]e + 2e^T PF\eta(He,x,u) + 2e^T PB \sum_{k=1}^{q} \bar{\eta}^k(R_k e, x, u) m_k$$
$$+ 2e^T PKC \int_{-h(t)}^{0} \dot{e}(t+\vartheta)d\vartheta + 2e^T PB \sum_{k=1}^{q} \Psi^k(R_k z, u)\tilde{m}_k.$$

En utilisant (4.15) et (4.16), on obtient

$$\begin{aligned}\dot{V}_1 \leq\ & e^T[(A-KC)^T P + P(A-KC)]e + 2b\eta(He,x,u)DHe + 2e^T PKC \int_{-h(t)}^{0} \dot{e}(t+\vartheta)d\vartheta \\ & -2\sum_{k=1}^{q} \bar{\eta}^{kT}(R_k e, x, u) m_k \bar{D}_k \bar{\eta}(R_k e, x, u) + \sum_{k=1}^{q} \bar{b}_k \bar{\eta}^k(R_k e, x, u) m_k \bar{D}_k R_k e \\ & +2e^T PB \sum_{k=1}^{q} \Psi^k(R_k z, u)\tilde{m}_k + 2e^T PF\eta(He,x,u) - 2\eta^T(He,x,u)D\eta(He,x,u).\end{aligned}$$

On définit
$\zeta := [e, \eta(He,x,u), \bar{\eta}^1(R_1 e, x, u)m_1, \ldots, \bar{\eta}^q(R_q e, x, u)m_q]^T$, donc on a

$$\dot{V}_1 \leq \zeta^T \mathcal{S} \zeta + 2e^T PKC \textstyle\int_{-h(t)}^{0} \dot{e}(t+\vartheta)d\vartheta - \varepsilon |e|^2 + 2e^T C^T M^T \sum_{k=1}^{q} \Psi^k(R_k z, u)\tilde{m}_k,$$

oú nous avons utilisé également l'équation (4.17b). $\mathcal{S} \leq 0$ est la matrice définie dans l'hypothèse 4.2. En appliquant l'inégalité de Young $\left|2c^T d\right| \leq \gamma c^T c + \frac{1}{\gamma} d^T d$ au terme "$2e(t)^T PKC\dot{e}(t+\vartheta)$" avec $c^T = e(t)^T PKC$, $d = \dot{e}(t+\vartheta)$ et $\gamma = 2$, et en intégrant entre $\vartheta = -h(t)$ et $\vartheta = 0$, on obtient

$$\begin{aligned}2e(t)^T PKC \int_{-h(t)}^{0} \dot{e}(t+\vartheta)d\vartheta &\leq 2he(t)^T C^T K^T P^2 KCe(t) + \frac{1}{2}\int_{-h}^{0} |\dot{e}(t+\vartheta)|^2 \, d\vartheta \\ &\leq 2h_m \beta_c^2 p_M^2 \, |e(t)|^2 + \frac{1}{2}\int_{-h_m}^{0} |\dot{e}(t+\vartheta)|^2 \, d\vartheta.\end{aligned}$$

donc,

$$\dot{V}_1 \leq -(\frac{\varepsilon}{p_M} + 2h_m\beta_c^2 p_M^2 P_m^{-1})V_1 + \frac{1}{2}\int_{-h}^{0} |\dot{e}(t+\vartheta)|^2 \, d\vartheta + 2e^T C^T M^T \sum_{k=1}^{q} \Psi^k(R_k z, u)\tilde{m}_k.$$

La dérivée de V_3 le long des trajectoires du système (4.11) est donnée par

$$\dot{V}_3 = \rho^{-1} \sum_{k=1}^{q} (\dot{\tilde{m}}_k^T \Upsilon_k \tilde{m}_k + \tilde{m}_k^T \Upsilon_k \dot{\tilde{m}}_k + \tilde{m}_k^T \dot{\Upsilon}_k \tilde{m}_k).$$

D'après (4.10c) et (4.11b), on obtient

$$\begin{aligned} \dot{V}_3 &= -2e(t-h)^T C^T M^T \sum_{k=1}^{q} \Psi^k(R_k z, u)\tilde{m}_k - \alpha V_3 \\ &\quad + \rho^{-1} \sum_{k=1}^{q} \Psi^k(R_k z, u)^T B^T B \Psi^k(R_k z, u)\tilde{m}_k^2. \end{aligned} \tag{4.42}$$

Ensuite, en appliquant l'inégalité de Young et en utilisant l'équation (4.17b), on obtient

$$2\Gamma^T C^T M^T \sum_{k=1}^{q} \Psi^k(R_k z, u)\tilde{m}_k \leq q\,|\Gamma|^2 + (\mu_\psi \beta_b p_M)^2 \sum_{k=1}^{q} \tilde{m}_k^2,$$

et en utilisant l'inégalité précédente et l'équation (4.37), il s'en suit que

$$\dot{V}_3 \leq \upsilon_m^{-1}((\rho^{-1} + p_M^2)(\beta_b \mu_\psi)^2 - \alpha)V_3 - 2e^T C^T M^T \sum_{k=1}^{q} \Psi^k(R_k z, u)\tilde{m}_k + q\,|\Gamma|^2 \tag{4.43}$$

où nous avons également utilisé la positivité de $\Upsilon_k(t)$ (4.5). Par ailleurs, la dérivée de V_2 est donnée par :

$$\dot{V}_2 = h_m\,|\dot{e}|^2 - \int_{-h_m}^{0} |\dot{e}(t+\vartheta)|^2 \, d\vartheta. \tag{4.44}$$

En utilisant l'équation (4.64) et la propriété de secteur à $\eta(\cdot)$ et $\bar{\eta}^k(\cdot)$, on obtient

$$h_m\,|\dot{e}|^2 \leq h_m(\beta_a + \beta_c + b + \sum_{k=1}^{q} \bar{b}_k \mu_m)^2 P_m^{-1} V_1 + h_m \upsilon_m^{-1}(\mu_\psi \beta_b)^2 V_3 + h_m \beta_c^2\,|\Gamma|^2\,. \tag{4.45}$$

Ensuite, en utilisant l'équation de Jensen ([106], Lemma 1), il s'en suit que

$$h_m \int_{-h_m}^{0} |\dot{e}(t+\vartheta)|^2 \, d\vartheta \geq \left| \int_{-h(t)}^{0} \dot{e}(t+\vartheta) d\vartheta \right|^2 = |\Gamma|^2\,. \tag{4.46}$$

D'après les inégalités (4.42)–(4.46) et en arrangeant les termes, la dérivée totale de $V(t, \omega_t)$ le long des trajectoires du système (4.11) est donnée par

$$\dot{V} \leq [-\frac{\varepsilon}{p_M} + h_m C_e]V_1 + (q - \frac{N}{2h_m} + h_m\beta_c^2)\,|\Gamma|^2 + (C_m + h_m \upsilon_m^{-1}(\mu_\psi \beta_b)^2 - \alpha)V_3,$$

où

$$\begin{aligned} C_e &= p_m^{-1}((\beta_a+\beta_c+b+\sum_{k=1}^{q}\bar{b}_k\mu_m)^2+2\beta_c^2p_M^2), \\ C_m &= \upsilon_m{}^{-1}(\beta_b\mu_\psi)^2(\rho^{-1}+p_M^2). \end{aligned}$$

Donc, si h_m vérifie le système d'équations suivant

$$\begin{cases} h_mC_e-\frac{\varepsilon}{2p_M}\leq 0 \\ C_m+h_m\upsilon_m^{-1}(\mu_\psi\beta_b)^2\frac{\alpha}{2}\leq 0 \\ q-\frac{1}{2h}+h_m\beta_c^2\leq 0, \end{cases} \tag{4.47}$$

on a

$$\dot{V}(t,\omega_t)\leq -\frac{\varepsilon}{2p_M}V_1(e(t))-\frac{\alpha}{2}V_3(t,\tilde{m}(t)),\qquad p.p. \tag{4.48}$$

Après la résolution du système d'inéquations (4.47), on déduit que (4.48) est vérifiée pour

$$h_m\leq \min\{\pi_a,\pi_b,\pi_c\} \tag{4.49}$$

avec $\pi_a=C_e^{-1}(\frac{\varepsilon}{2p_M})$, $\pi_c=\frac{-q+\sqrt{q^2+2\beta_c^2}}{2\beta_c^2}$ et $\pi_b=\upsilon_m(\mu_\psi\beta_b)^{-2}(\frac{\alpha}{2}-C_m)$.

Ainsi, en appliquant le théorème de Lyapunov-Krasovskii 4.8 ([104], Théorème 4.1), on déduit que la solution d'équilibre du système d'erreurs (4.11) est globalement asymptotiquement stable. ■

La convergence exponentielle du système esclave découle des résultats précédents.

Corollaire 4.10. *Considérons le système maître (4.1) et le système esclave (4.10). Supposons que les hypothèses 4.2, 4.3 et 4.4 soient satisfaites. Donc, la solution d'équilibre du système d'erreurs (4.11) est exponentiellement stable pour des valeurs suffisamment petites de la borne supérieure h_m.*

Démonstration : Soit θ une constante positive dépendant de $\beta_c=|KC|$ et α. En procédant comme dans la preuve du théorème 4.9 et en utilisant le fait que

$$V_2\leq h_m\int_{-h_m}^{0}|\dot{e}(t+\vartheta)|^2\,d\vartheta, \tag{4.50}$$

nous obtenons :

$$\begin{aligned} \dot{V}+\theta V &\leq (\theta-\frac{\varepsilon}{p_M}+h_mC_e)V_1+(q+h_m\beta_c^2)\,|\Gamma|^2 \\ &+ (-\frac{1}{2}+\theta h_m)\int_{-h_m}^{0}|\dot{e}(t+\vartheta)|^2\,d\vartheta \\ &+ (C_m+h_m\upsilon_m^{-1}(\mu_\psi\beta_b)^2-\alpha)V_3\quad p.p. \end{aligned} \tag{4.51}$$

Supposons que h_m vérifie le système d'inéquations suivant :

$$\theta + h_m C_e - \frac{\varepsilon}{2p_M} \leq 0 \tag{4.52a}$$

$$\theta + C_m + h_m \upsilon_m^{-1}(\mu_\psi \beta_b)^2 - \frac{\alpha}{2} \leq 0 \tag{4.52b}$$

$$\theta + q - \frac{1}{2h_m} + h_m \beta_c^2 \leq 0, \tag{4.52c}$$

donc, on a

$$h_m \leq \min\{\bar{\pi}_a, \bar{\pi}_b, \bar{\pi}_c\} \tag{4.53}$$

avec $\bar{\pi}_a = C_e^{-1}(\frac{\varepsilon}{2p_M} - \theta)$, $\bar{\pi}_c = \frac{-q-\theta+\sqrt{(q+\theta)^2+2\beta_c^2}}{2\beta_c^2}$ et $\pi_b = \upsilon_m(\mu_\psi\beta_b)^{-2}(\frac{\alpha}{2} - C_m - \theta)$.
Ainsi, en utilisant les inégalités (4.46), (4.52a) et (4.52b), il en résulte que

$$\dot{V} + \theta V \quad \leq \quad -\frac{\varepsilon}{2p_M} V_1 - \frac{\alpha}{2} V_3 + (-\frac{1}{2h_m} + \theta + q + h_m\beta_c^2)\,|\Gamma|^2 \quad p.p, \tag{4.54}$$

et, d'après l'équation (4.52c), nous obtenons :

$$\dot{V}(t, \omega_t) \leq -\theta V(t, \omega_t) \quad p.p. \tag{4.55}$$

En multipliant de deux cotés de cette dernière par $1/V(t, \omega_t)$ et en intégrant entre t_0 et t, nous obtenons :

$$V(t, \omega_t) \leq V(t_0, \omega_{t_0}) \exp(-\theta(t - t_0)) \quad p.p. \tag{4.56}$$

où $\omega_{t_0} = (\phi_s, \phi_a)^T$ est la condition initiale du système d'erreurs.
D'après les équations (4.40), (4.41a), (4.41c) et (4.26), il s'en suit que

$$\min\{p_m, \rho^{-1}\upsilon_m\}\,|\omega(t)|^2 \leq V(t, \omega_t). \tag{4.57}$$

donc

$$\left|(e(t), \tilde{m}(t))^T\right| \leq \sqrt{\frac{V(t_0, \omega_{t_0})}{\min\{p_m, \rho^{-1}\upsilon_m\}}} \exp\Big(-\frac{\theta}{2}(t - t_0)\Big). \tag{4.58}$$

Nous concluons que la solution d'équilibre du système d'erreurs (4.11) est exponentiellement stable.

■

4.6 Synchronisation à base d'observateurs en cascade dans le cas des longs retards de transmission

L'inégalité (4.53) implique une limitation sur les valeurs admissibles de la borne supérieure du retard de transmission et clairement restreint la classe des systèmes pour lesquels notre approche s'applique.

Ceci est une restriction technique classique rencontrée dans la littérature, cependant, les retards ne sont pas souvent négligeables et peuvent prendre des valeurs élevées. Afin de surmonter cette restriction, la conception des observateurs en cascade pour les systèmes présentant des long retards a été adoptée dans quelques articles récents – voir les articles [100],[98]. L'idée consiste à diviser le long retard en des retards suffisamment courts qui sont admissibles par chacun des observateurs de la configuration en cascade, et ainsi il est possible d'estimer l'état pour des retards relativement longs.

4.6.1 Conception du système esclave en configuration cascade

Motivés par les références [98] et [100], nous considérons le système émetteur décrit par l'équation (4.1) et les états retardés $x_j = x(t - \bar{h} + j\frac{\bar{h}}{N})$ correspondant aux instants $t_j = t - \bar{h} + j\frac{\bar{h}}{N}$, avec $j = 1, \ldots, N$, où $\bar{h}$ représente un retard constant et pouvant éventuellement prendre des larges valeurs..

Nous obtenons les dynamiques des états retardés x_j et les systèmes virtuels V_j suivants :

$$\dot{x_j} = Ax_j + Ff(Hx_j, u_j) + B\sum_{k=1}^{q}\Psi^k(R_k x_j, u_j)m_{kj} \tag{4.59a}$$

$$y_1 = Cx_1(t - \frac{\bar{h}}{N}) = y(t) = Cx(t - \bar{h}) \tag{4.59b}$$

$$y_j = Cx_{j-1} = Cx_j(t - \frac{\bar{h}}{N}), \quad j = 2..N \tag{4.59c}$$

où $u_j := u(t - h + j\frac{\bar{h}}{N})$, $y_j := y(t - \bar{h} + j\frac{\bar{h}}{N})$, $m_{kj} := m_k(t - \bar{h} + j\frac{\bar{h}}{N})$ sont respectivement les entrées retardées , les sorties retardées et les messages retardés correspondant aux instants t_j, pour $j = 1..N$. Nous pouvons facilement vérifier que la dynamique de l'état retardé x_N du dernier système virtuel V_N correspond exactement à la dynamique de l'état actuel $x(t)$ du système maître (4.1) ($x(t) = x_N(t)$) et le signal de sortie $y_1(t)$ du premier système virtuel est identique au signal de sortie $y(t)$ du système maître (4.1) ($y_1(t) = y(t)$). Le schéma de synchronisation basé sur la configuration des observateurs en cascade est représenté dans la figure 4.1.

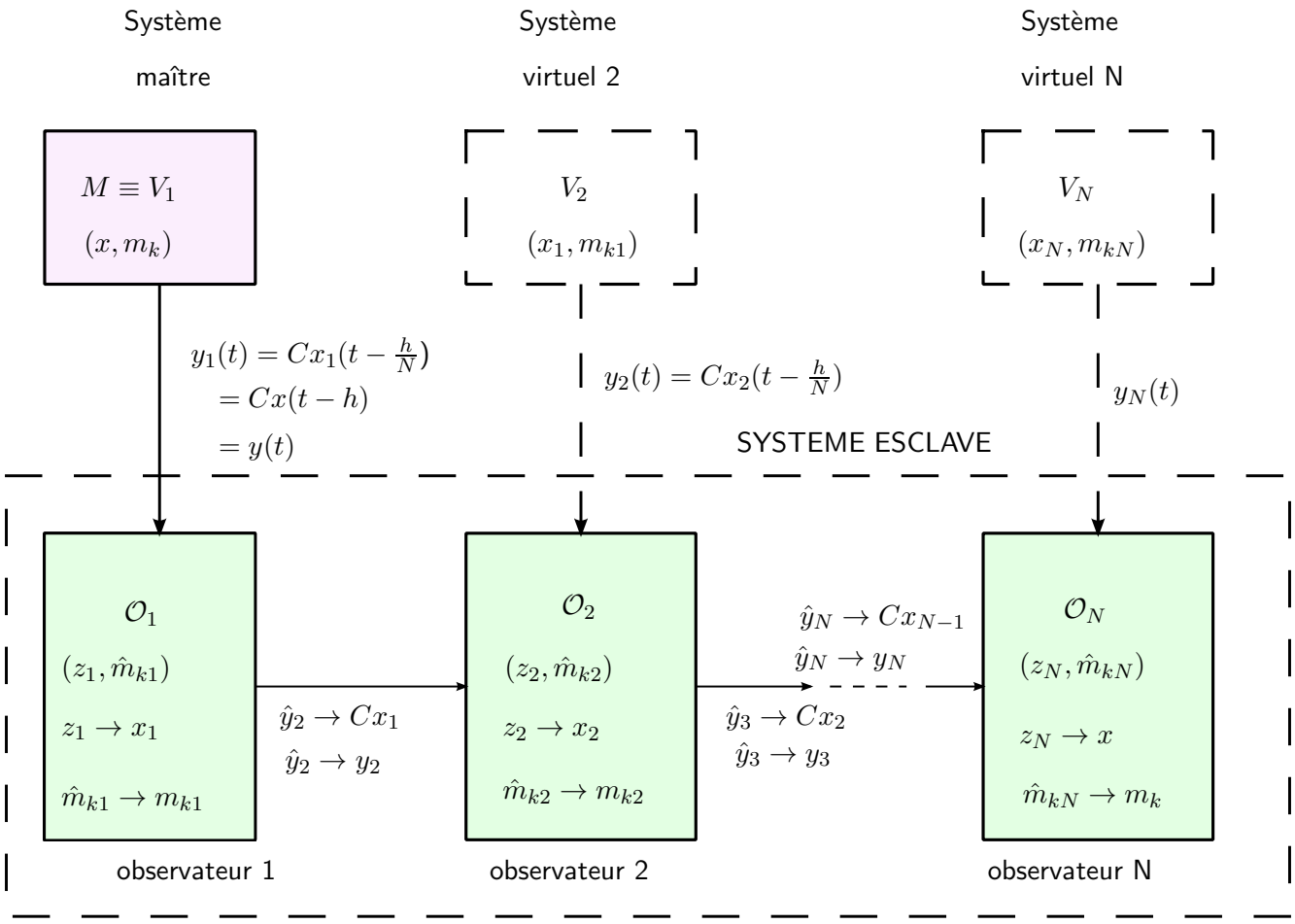

FIGURE 4.1: Schéma de synchronisation basé sur la configuration des observateurs en cascade

Afin d'estimer l'état actuel $x(t)$, nous concevons une chaîne de N observateurs tels que $\forall j = 1, \ldots, N$, chaque observateur $\mathcal{O}_j$ reproduit l'état retardé x_j du système virtuel V_j en présence du retard $\frac{\bar{h}}{N}$ qui peut être réduit arbitrairement pour un nombre suffisamment large N ; l'objectif du N-ième observateur est d'assurer l'estimation de l'état actuel $x(t)$ et de reconstruire les messages transmis malgré la présence des longs retards de transmission. L'observateur en cascade que nous proposons possède la structure suivante : $\forall j = 1..N$,

$$\dot{z}_j = Az_j + Ff(Hz_j, u_j) + B\sum_{k=1}^{q} \Psi^k(R_k z_j, u_j)\hat{m}_{kj} + K(\hat{y}_j - Cz_j(t - \frac{\bar{h}}{N})) \tag{4.60a}$$

$$\dot{\hat{m}}_{kj} = \rho \Upsilon_{kj}^{-1} \Psi^k(R_k z_j, u_j)^T M(\hat{y}_j - Cz_j(t - \frac{\bar{h}}{N})) \tag{4.60b}$$

$$\dot{\Upsilon}_{kj} = -\alpha \Upsilon_{kj} + \Psi^k(R_k z_j, u_j)^T B^T B \Psi^k(R_k z_j, u_j) \tag{4.60c}$$

$$\Upsilon_{kj}(0) > 0, \quad k = 1..q \tag{4.60d}$$

où

$$\hat{y}_1(t) = y_1(t) = y(t) = Cx(t - \bar{h}) \tag{4.61a}$$

$$\hat{y}_j(t) = Cz_{j-1}(t), \quad j = 2..N, \tag{4.61b}$$

$z_j(t)$ et $\hat{m}_{kj}(t)$ représentent respectivement les estimés de x_j et m_{kj} aux instants t_j, pour $j = 1..N$.

Théorème 4.11. *Considérons le système (4.1) et l'observateur en cascade (4.60–4.61). Supposons que les hypothèses 4.2, 4.3 et 4.4 soient satisfaites. Donc, pour tout retard de transmission constant $\bar{h}$, il existe un entier N tel que l'état estimé $\hat{x}_N(t)$ et les messages estimés $\hat{m}_{kN}(t)$ $(k = 1..s)$ du N-ième observateur (4.60) convergent exponentiellement vers l'état actuel $x(t)$ et les messages transmis $m_k(t)$ du système maître (4.1).*

Démonstration : Nous définissons les erreurs de synchronisation par $e_j(t) := x_j(t) - z_j(t)$ et les erreurs d'estimation du message $\tilde{m}_{kj}(t) := m_{kj}(t) - \hat{m}_{kj}(t)$.
En utilisant le fait que $\dot{m}_{kj}(t) = 0$ presque partout, où le système des erreurs est décrit par :

$$\begin{aligned} \dot{e}_j &= Ae_j - KCe_j(t - \tfrac{\bar{h}}{N}) + F\eta(He_j, x_j, u_j) - K\bar{e}_{j-1} \\ &\quad + B\textstyle\sum_{k=1}^{s}(\bar{\eta}^k(R_k e_j, x_j, u_j)m_{kj} + \Psi^k(R_k z_j, u_j)\tilde{m}_{kj}) \end{aligned} \tag{4.62a}$$

$$\dot{\tilde{m}}_{kj} = -\rho\Upsilon_{kj}^{-1}\Psi^k(R_k z_j, u_j)^T MC(e_j(t - \tfrac{\bar{h}}{N}) - \bar{e}_{j-1}), \tag{4.62b}$$

où $\bar{e}_0 = y_1 - \hat{y}_1 = 0$; $\bar{e}_{j-1} = Ce_{j-1} = y_j - \hat{y}_j = Cx_{j-1} - Cz_{j-1}$, $j = 2..N$.
$\eta(He_j, x_j, u_j) = (\eta_1(H_1 e_j, x_j, u_j), \ldots, \eta_m(\bar{h}e_j, x_j, u_j))$ tel que pour tout $i = 1..m$,
$\eta_i(H_i e, x_j, u_j) = f_i(H_i x_j, u_j) - f_i(H_i x - H_i e, u_j)$;
et $\bar{\eta}^k(R_k e_j, x_j, u_j) = (\bar{\eta}_1^k(R_1 e_j, x_j, u_j), \ldots, \bar{\eta}_s^k(R_s e, x_j, u_j)$ tel que pour $i = 1..s$,
$\bar{\eta}_i^k(R_{ki} e_j, x_j, u_j) = \Psi^k(R_{ki} x_j, u_j) - \Psi^k(R_{ki} x_j - R_{ki} e_j, u_j)$.
Nous appliquons la formule de Leibniz-Newton à l'erreur d'observation $e_j(t)$. Ainsi,

$$e_j(t) - e_j(t - \frac{\bar{h}}{N}) = \int_{t-\frac{\bar{h}}{N}}^{t} \dot{e}_j(s)ds. \tag{4.63}$$

Dans ce qui suit, $k = 1..s$ et $j = 1..N$. La dynamique de l'erreur de synchronisation $e(t)$ est réécrite comme

$$\begin{aligned} \dot{e}_j &= (A - KC)e_j + F\eta(He_j, x_j, u_j) + KC\int_{t-\frac{\bar{h}}{N}}^{t} \dot{e}_j(s)ds \\ &\quad + B(\sum_{k=1}^{q}\bar{\eta}^k(R_k e_j, x_j, u_j)\theta_{kj} + \sum_{k=1}^{q}\Psi^k(R_k z_j, u_j)\tilde{\theta}_{kj}) - K\bar{e}_{j-1}. \end{aligned} \tag{4.64}$$

Soit $\omega_j(t) = (e_j(t), \tilde{m}_j(t))^T$ et

$$\omega_{jt}(\vartheta) = \omega_j(t + \vartheta), \qquad -\bar{h} \le \vartheta \le 0. \tag{4.65}$$

Afin de prouver l'estimation d'état et la restauration des messages, nous considérons la fonctionnelle de Lyapunov-Krasovskii suivante : $\forall j = 1..N$,

$$V_j(t, \omega_{jt}) = V_{1j}(e_j) + V_{2j}(\omega_{jt}) + V_{3j}(t, \tilde{m}_{kj}) \tag{4.66}$$

où

$$V_{1j}(e_j) = e_j^T P e_j, \tag{4.67}$$

$$V_{2j}(t) = \int_{-\frac{\bar{h}}{N}}^{0} (\vartheta + \frac{\bar{h}}{N}) |\dot{e}_j(t+\vartheta)|^2 \, d\vartheta, \tag{4.68}$$

$$V_{3j}(t, \tilde{m}_{kj}) = \sum_{k=1}^{q} \rho^{-1} \Upsilon_{kj}(t) \tilde{m}_{kj}^2, \tag{4.69}$$

où $\Upsilon_{kj}(t)$ est une solution de l'équation (4.60c).
À chaque étape j, nous procédons comme dans la preuve du théorème 4.9 et du corollaire 4.10 et nous appliquons l'inégalité de Young au terme $2e_j^T PK\bar{e}_{j-1}$:

$$\begin{aligned} 2e_j^T PK\bar{e}_{j-1} &\leq \bar{e}_{j-1}^T K^T P^2 K \bar{e}_{j-1} + e_j^T e_j \\ &\leq (|K|\, p_M)^2 \, |\bar{e}_{j-1}|^2 + p_m^{-1} V_{1j}. \end{aligned}$$

Donc, en réarrangeant les termes, nous déduisons que la dérivée totale de V_j le long des trajectoires de (4.62) satisfait :

$$\begin{aligned} &\dot{V}_j + \gamma V_j \leq (\gamma - \frac{\varepsilon}{p_M} + p_m^{-1} + \frac{\bar{h}}{N} C_e) V_{1j} + (\gamma + C'_m + \frac{\bar{h}}{N} \upsilon_m^{-1} (\mu_\psi \beta_b)^2 - \alpha) V_{3j} \\ &+(\gamma + q - \frac{N}{2\bar{h}} + \frac{\bar{h}}{N}(1+\beta_c^2)) \, |\Gamma_j|^2 + ((|K|\, p_M)^2 + \frac{\bar{h}}{N} |K|^2 + q(\mu_\psi |M|)^2) \, |\bar{e}_{j-1}|^2 \quad p.p. \end{aligned}$$

où

$$C'_m = \upsilon_m{}^{-1}(1 + (\beta_b \mu_\psi)^2 (\rho^{-1} + p_M^2)).$$

Par conséquent, si $\bar{h}$ vérifie :

$$\begin{cases} \gamma + \frac{\bar{h}}{N} C_e + p_m^{-1} - \frac{\varepsilon}{2p_M} \leq 0 \\ \gamma + C'_m + \frac{\bar{h}}{N} \upsilon_m^{-1} (\mu_\psi \beta_b)^2 \leq \frac{\alpha}{2} \\ \gamma + q - \frac{N}{2\bar{h}} + \frac{\bar{h}}{N}(1+\beta_c^2) \leq 0, \end{cases} \tag{4.70}$$

nous obtenons :

$$\dot{V}_j(t, \omega_{jt}) \leq -\gamma V_j(t, \omega_{jt}) + ((|K|\, p_M)^2 + \frac{\bar{h}}{N} |K|^2 + q(\mu_\psi |M|)^2) \, |\bar{e}_{j-1}|^2 \tag{4.71}$$

et en résolvant en $\bar{h}$ le système des inéquations (4.70), nous déduisons que (4.71) est vérifiée pour

$$\bar{h} \leq N \min\{\pi'_a, \pi'_b, \pi'_c\} \tag{4.72}$$

où $\pi'_a = C_e^{-1}(\frac{\varepsilon}{2p_M} - \gamma - p_m^{-1})$, $\pi'_c = \frac{-(q+\gamma) + \sqrt{(q+\gamma)^2 + 2(1+\beta_c^2)}}{2(1+\beta_c^2)}$ et $\pi'_b = \upsilon_m (\mu_\psi \beta_b)^{-2} (\frac{\alpha}{2} - C'_m - \gamma)$.

Remarquons que pour toute borne $\bar{h}$ du retard, il existe un entier N tel que la relation (4.72) est satisfaite. Pour $j = 1$, nous avons $\bar{e}_{j-1} = \bar{e}_0 = y_1 - \hat{y}_1 = 0$, puisque $y_1(t) = \hat{y}_1(t) = y(t) = Cx(t - \bar{h})$. Il s'en suit que

$$\dot{V}_1(t, \omega_{1t}) \quad \leq \quad -\gamma V_1(t, \omega_{1t}),$$

qui implique que $\hat{x}_1(t)$ et $\hat{m}_{k1}(t)$ convergent exponentiellement vers $x_1(t)$ et $m_{k1}(t)$ respectivement ; ainsi, $\bar{e}_1(t)$ converge exponentiellement vers zéro. En utilisant le lemme de comparaison [89], nous déduisons à partir de (4.71), que pour $j = 2, \ldots, N$, si $\bar{e}_{j-1} \to 0$ exponentiellement, donc $e_j \to 0$ et $\tilde{m}_{kj} \to 0$ exponentiellement. Par conséquent, en se basant sur une induction mathématique, nous concluons que $\forall j = 1, \ldots, N$, $e_j \to 0$ et $\tilde{m}_{kj} \to 0$ exponentiellement. Nous rappelons que $e_N(t) = x_N(t) - \hat{x}_N(t) = x(t) - \hat{x}_N(t)$ et $\tilde{m}_{kN}(t) = m_{kN}(t) - \hat{m}_{kN}(t) = m_k(t) - \hat{m}_{kN}(t)$ pour conclure que $\hat{x}_N$ et $\hat{m}_{kN}$ convergent exponentiellement vers l'état actuel $x(t)$ et les messages transmis $m_k(t)$, avec $k = 1..s$. ■

Remarque 4.12. Notons que la rapidité de convergence de l'observateur dans la configuration en cascade dépend étroitement du nombre N d'observateurs utilisés. En effet, le temps nécessaire pour la convergence de l'observateur final ordre N est égal à la somme des temps de convergence de tous les observateurs de la configuration en cascade. En d'autres termes, plus le retard de transmission est long, plus le nombre d'observateurs utilisés est grand, et donc plus le temps de convergence de l'observateur final est long.

4.7 Exemples numériques

Nous illustrons la performance de l'approche de synchronisation décrite dans les sections précédentes en présentant trois cas d'étude. Dans le premier cas d'étude, nous testons les résultats théoriques à travers la transmission d'un message binaire en utilisant l'oscillateur de Duffing au niveau de l'émetteur sachant que le canal public est soumis à un retard constant. Dans le second cas d'étude, l'approche est appliquée pour transmettre un message (constant par morceaux) via un système de communication chaotique sous l'influence d'un retard de transmission à temps variant en utilisant des circuits de Chua couplés. Dans le troisième cas, nous testons l'efficacité de l'observateur dans la configuration en cascade (avec $N = 2$) en reprenons le système de Duffing traité dans le premier exemple, tout en augmentant la valeur du retard.

4.7.1 Un système de communication chaotique utilisant l'oscillateur de "Duffing" sous l'influence d'un retard de transmission constant

On considère l'oscillateur chaotique de "Duffing" pour lequel on injecte une information binaire $m(t)$ dans sa dynamique. Le signal de sortie $y(t)$ est corrompu par un retard de transmission constant

$h = 0.04s$. Donc, la dynamique de l'émetteur chaotique est donnée par

$$\begin{aligned} \dot{X}_1 &= X_2, \\ \dot{X}_2 &= -0.4X_2 - 1.1X_1 - (1 + m(t))X_1^3 + cos(1.8t) \\ y(t) &= X_1(t-h) + X_2(t-h). \end{aligned} \tag{4.73}$$

qui est clairement de la forme (4.1) avec

$$x = \begin{bmatrix} X_1 \\ X_2 \end{bmatrix}, \ A = \begin{bmatrix} 0 & 1 \\ 0.4 & -1.1 \end{bmatrix}, \ B = \begin{bmatrix} 0 \\ -1 \end{bmatrix},$$

$$F = \begin{bmatrix} 0 \\ -1 \end{bmatrix}, \ C = \begin{bmatrix} 1 & 1 \end{bmatrix}, \ H = \begin{bmatrix} 1 & 0 \end{bmatrix},$$

$$f(Hx, u) = X_1^3 + u, \ u(t) = cos(1.8t), \ k = 1,$$
$$R_1 = \begin{bmatrix} 1 & 0 \end{bmatrix}, \Psi^1(R_1 x, u) = X_1^3.$$

Le récepteur est donné par l'équation (4.10). En résolvant le problème d'optimisation (4.17), on obtient :

$$D = \bar{D}_1 = 2.6464, \ P = \begin{bmatrix} 12.1437 & 1.5679 \\ 1.5679 & 1.5679 \end{bmatrix}, \ \varepsilon = 5.9542.$$

Ainsi, les valeurs numériques des matrices de l'observateur sont :

$$K = \begin{bmatrix} 0.0596 \\ 3.4896 \end{bmatrix}, \ M = -1.5679, \ \rho = 10, \ \alpha = 0.5.$$

L'état $x(t)$ du système (4.76) est initialisé à $x_0 = [0, 0]^T$, $\forall s \in [-0.04, 0]$. Les conditions initiales de l'observateur sont $z(s) = [1, 2]^T$, $\forall s \in [-0.04, 0]$, $\hat{m} = 0.6$, $\Upsilon = 0.2$.

Les résultats de simulation se présentent comme suit. La figure 4.2 illustre la synchronisation entre l'émetteur et le récepteur, la figure 4.3 montre que l'information transmise est bien restaurée. Notons, que pour réconstruire parfaitement le message transmis et ne pas produire des erreurs des bits, le temps de convergence de l'erreur d'estimation du message doit être inférieur à la durée d'un bit dans l'information binaire.

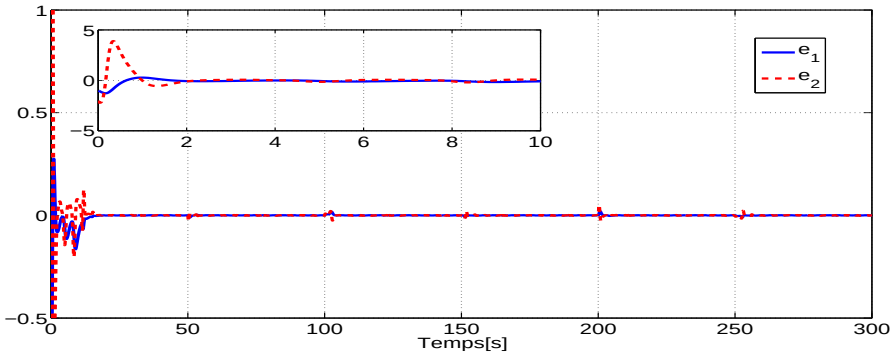

FIGURE 4.2: L'état X_1 et son estimé en présence du retard d transmission

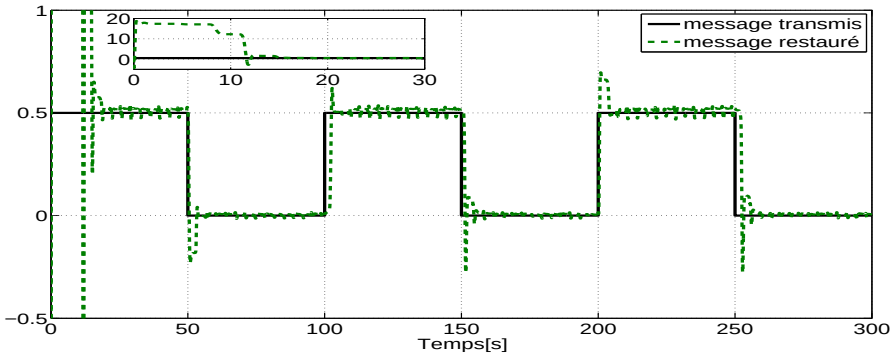

FIGURE 4.3: L'information transmise $m(t)$ et son estimé en présence du retard de transmission

4.7.2 Exemple 2 : Un système de communication chaotique à base des circuits de Chua couplés sous l'influence d'un retard de transmission à temps variant

On considère le système chaotique composé de deux circuits de "Chua" couplés – voir [92]. Un message $m(t)$ (constant par morceaux) est injecté dans sa dynamique. Le signal de sortie $y = [y_1, y_2]^\top$ est affecté par un retard de transmission $h(t)$ qui correspond à une fonction uniformément distribuée entre les bornes inférieure et supérieure respectivement égales à 0 et $h_m = 0.09s$. Ainsi, la dynamique de l'émetteur chaotique est donnée par

$$\dot{x}_1 = 9(x_2 - g(x_1)) + \Psi(t)m(t) \quad (4.74a)$$
$$\dot{x}_2 = x_1 - x_2 + x_3 \quad (4.74b)$$
$$\dot{x}_3 = -14.28x_2 \quad (4.74c)$$
$$\dot{x}_4 = 9(x_2 - g(x_4)) \quad (4.74d)$$
$$\dot{x}_5 = x_4 - x_5 + x_6 + 0.01(x_5 - x_2) \quad (4.74e)$$
$$\dot{x}_6 = -14.28x_5 \quad (4.74f)$$
$$y_1 = x_1(t - h(t)) \quad (4.74g)$$
$$y_2 = x_4(t - h(t)), \quad (4.74h)$$

où $g(x_i) = \frac{1}{2}(|x_i - 1| - |x_i + 1|)$, $i \in \{1, 4\}$. Notons que $g(\cdot)$ vérifie la propriété de restriction de pente (4.2) avec $b = 1$. Le système (4.74) est de la forme (4.1), avec

$$A = \begin{bmatrix} -2.5714 & 9 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & 0 & 0 & 0 \\ 0 & -14.28 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2.5714 & 9 & 0 \\ 0 & -0.01 & 0 & 1 & -0.09 & 1 \\ 0 & 0 & 0 & 0 & -14.28 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T,$$

$$F = \begin{bmatrix} -3.8571 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & -3.8571 \\ 0 & 0 \\ 0 & 0 \end{bmatrix},$$

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

$f(x) = [g(x_1); g(x_4)]$, $\Psi(t) = sin(3t) + cos(27t)$.

L'état initial du système (4.74) est donné par $x(s) = [-0.2, -0.2, -0.33, 0.2, 0.9, 0.33]^T$, $\forall s \in [-0.09, 0]$. Sous ces conditions, l'émetteur (4.74) fonctionne en régime chaotique (Voir Figure 4.4).

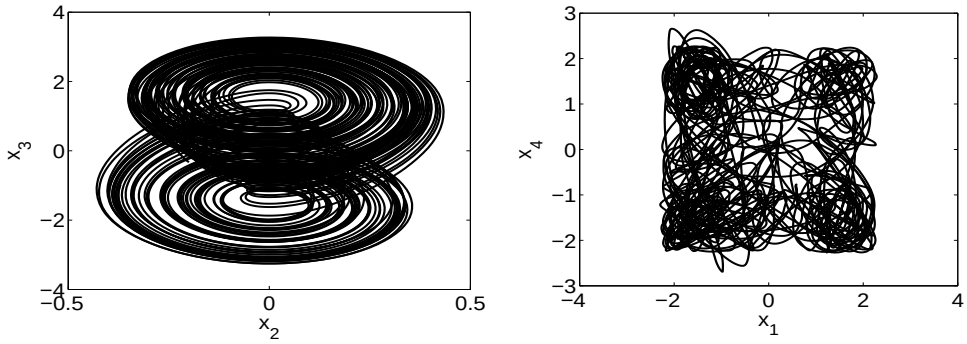

FIGURE 4.4: Les attracteurs dans le plan (x_1, x_4) (droite) et le plan (x_2, x_3) (gauche)

Le système récepteur est donné par (4.10). La solution au problème d'optimisation présenté dans la section 4.4 est donnée par

$$D = \begin{bmatrix} 29.8972 & 0 \\ 0 & 33.4389 \end{bmatrix},$$

$$P = \begin{bmatrix} 10.43 & 0 & 0 & 0 & 0 & 0 \\ 0 & 122.58 & -6.91 & 0 & 0 & 0 \\ 0 & -6.91 & 9.11 & 0 & 0 & 0 \\ 0 & 0 & 0 & 10.96 & -7.01 & 0.89 \\ 0 & 0 & 0 & -7.01 & 74.57 & -7.63 \\ 0 & 0 & 0 & 0.89 & -7.63 & 6.32 \end{bmatrix},$$

$\varepsilon = 8.9250$ and $\varsigma = 0$. On obtient également les valeurs numériques des matrices de l'observateur :

$$K = \begin{bmatrix} 0.1992 & -0.0053 \\ 1.8141 & 0 \\ 0.5965 & 0 \\ -0.0047 & 1.0278 \\ 0.0005 & 2.5823 \\ -0.0002 & 0.3639 \end{bmatrix}, \quad M = \begin{bmatrix} 10.4397 & 0 \end{bmatrix}$$

$\rho = 0.25$ et $\alpha = 8$.

L'état estimé est initialisé par $z(s) = [0, 0, 0, 0, 0, 0]^\top$, $\forall s \in [-0.09, 0]$. L'équation (4.10c) est initialisée $\Upsilon(0) = 1$ et le message estimé $\hat{m}$ est initialisé à $\hat{m}_0 = 1$. Les résultats de simulation se présentent comme suit. La figure 4.5 représente l'évolution de la fonction du retard en fonction du temps. Les figures 4.6 et 4.7 illustrent la convergence des erreurs de synchronisation et finalement la figure 4.8 illustre que l'information transmise est bien reconstruite par l'observateur proposé.

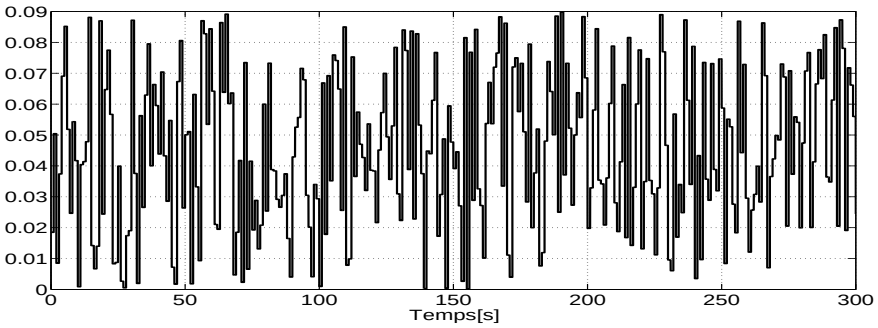

FIGURE 4.5: Évolution de la fonction du retard $h(t)$ en fonction du temps

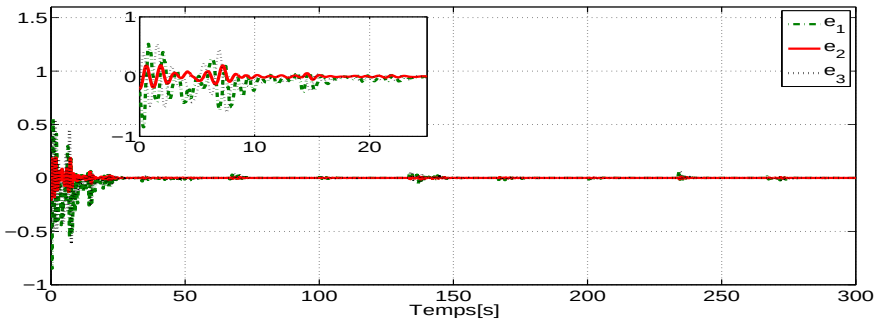

FIGURE 4.6: Erreurs d'estimation $e_1 = x_1 - z_1$, $e_2 = x_2 - z_2$ et $e_3 = x_3 - z_3$ en présence du retard de transmission

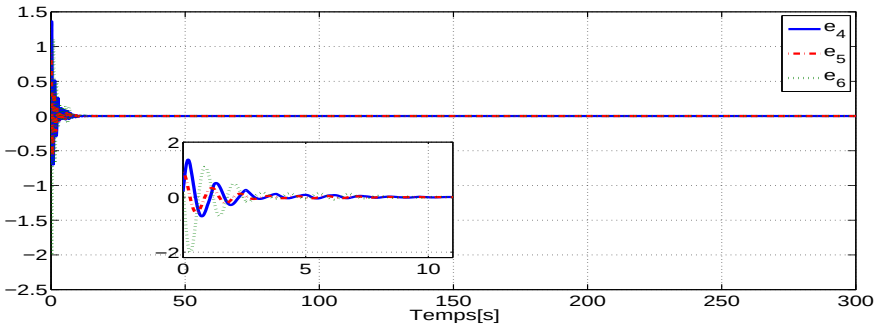

FIGURE 4.7: $h(t)$ $e_4 = x_4 - z_4$, $e_5 = x_5 - z_5$ et $e_6 = x_6 - z_6$ en présence du retard de transmission

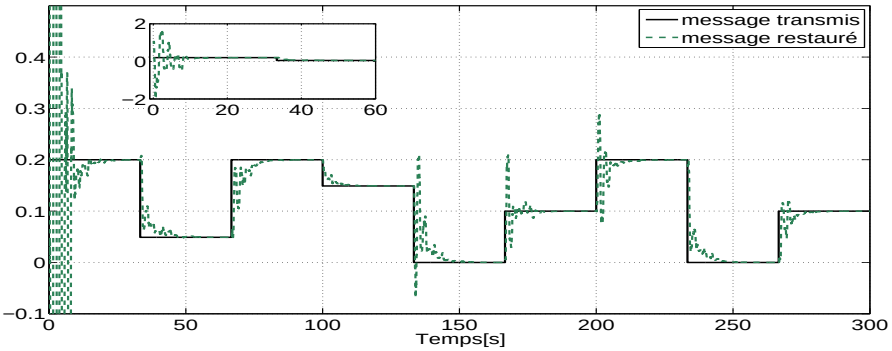

FIGURE 4.8: Le message transmis m et le message reçu $\hat{m}$ en présence du retard de transmission

4.7.3 Un système de communication utilisant l'oscillateur de "Duffing" et la configuration en cascade des observateurs en présence d'une valeur de retard plus élevée

Dans cet exemple, nous reconsidérons l'émetteur chaotique donné par l'équation (4.76) ; cependant, le signal de sortie est affecté par un retard d'une valeur plus élevée ($\bar{h} = 0.08s$) comparé avec le premier exemple. Dans des simulations préliminaires, en utilisant seulement un seul observateur

(Système (4.60) with N=1), nous constatons que l'observateur échoue à converger vers le système maître. Dans des simulations supplémentaires, le système récepteur est conçu à base de deux observateurs en cascade donné par (4.60) (N=2). L'état $x(t)$ du système (4.76) est initialisé à $x_0 = [0, 0]^T$, $\forall s \in [-0.08, 0]$. Les deux observateurs en cascade (N=2) sont initialisés à $z_1(s) = z_2(s) = [1, 2]^T$, $\forall s \in [-0.04, 0]$, $\hat{m}_{10} = \hat{m}_{20} = 0.6$, $\Upsilon_1(0) = \Upsilon_2(0) = 0.2$. Les résultats de simulation sont comme suit. La figure 4.9 illustre la synchronisation entre les systèmes émetteur et récepteur et la figure 4.10 montre que l'information transmise est bien reconstruite par le système récepteur à base des observateurs en cascade.

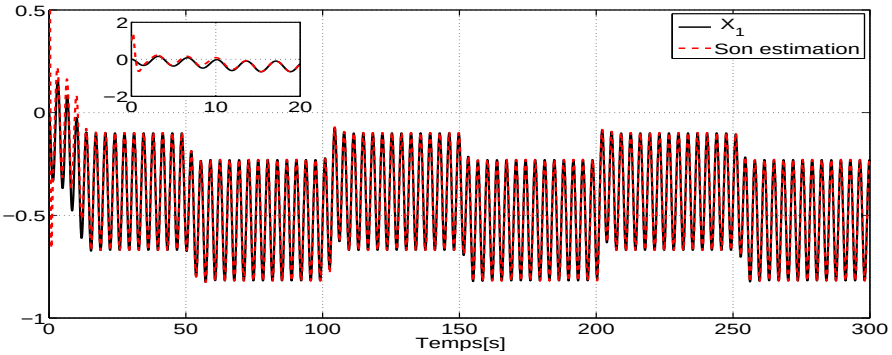

FIGURE 4.9: L'état X_1 et son estimé en présence d'un retard de transmission $h = 0.08s$

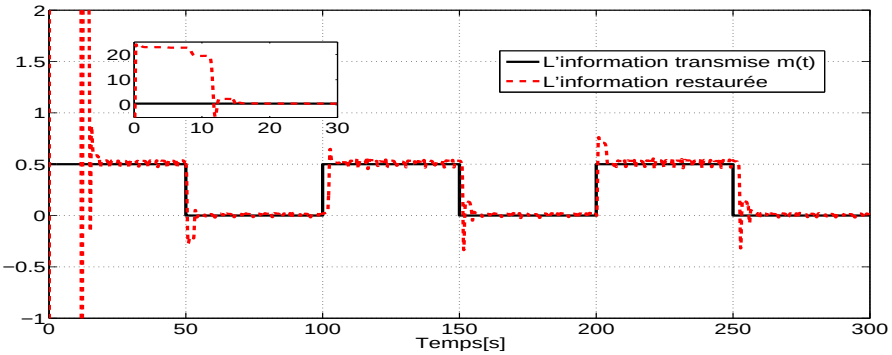

FIGURE 4.10: L'information transmise $m(t)$ et son estimée en présence d'un retard de transmission $h = 0.08s$

4.8 Application : Un système de communication sécurisée en présence des retards de transmissions

Afin d'améliorer la sécurité dans les systèmes de transmission de données à base de la méthode de synchronisation maître-esclave développée dans ce chapitre (en présence d'un retard dans le canal public), nous proposons un nouveau schéma de communication exploitant les avantages de notre méthode de synchronisation, notamment la robustesse aux retards de transmission et garantissant un bon niveau de sécurité et de confidentialité. L'idée consiste à faire passer l'information à transmettre par une étape de cryptage pour la sécuriser avant de l'injecter dans le système maître en

utilisant la technique de modulation paramétrique. De cette manière, l'opération de cryptage est effectuée indépendamment de la configuration maître-esclave, ce qui nous permet d'éviter le compromis sécurité/synchronisation qui représente la faiblesse des quelques systèmes de communications traditionnels tels que la technique de masquage chaotique ou la technique de modulation paramétrique où les opérations de cryptage et de synchronisation dépendent l'une de l'autre puisque le même système chaotique (système maître) est utilisé dans la réalisation de deux tâches. La description schématique du système de communication proposé est représentée dans la figure 4.11.

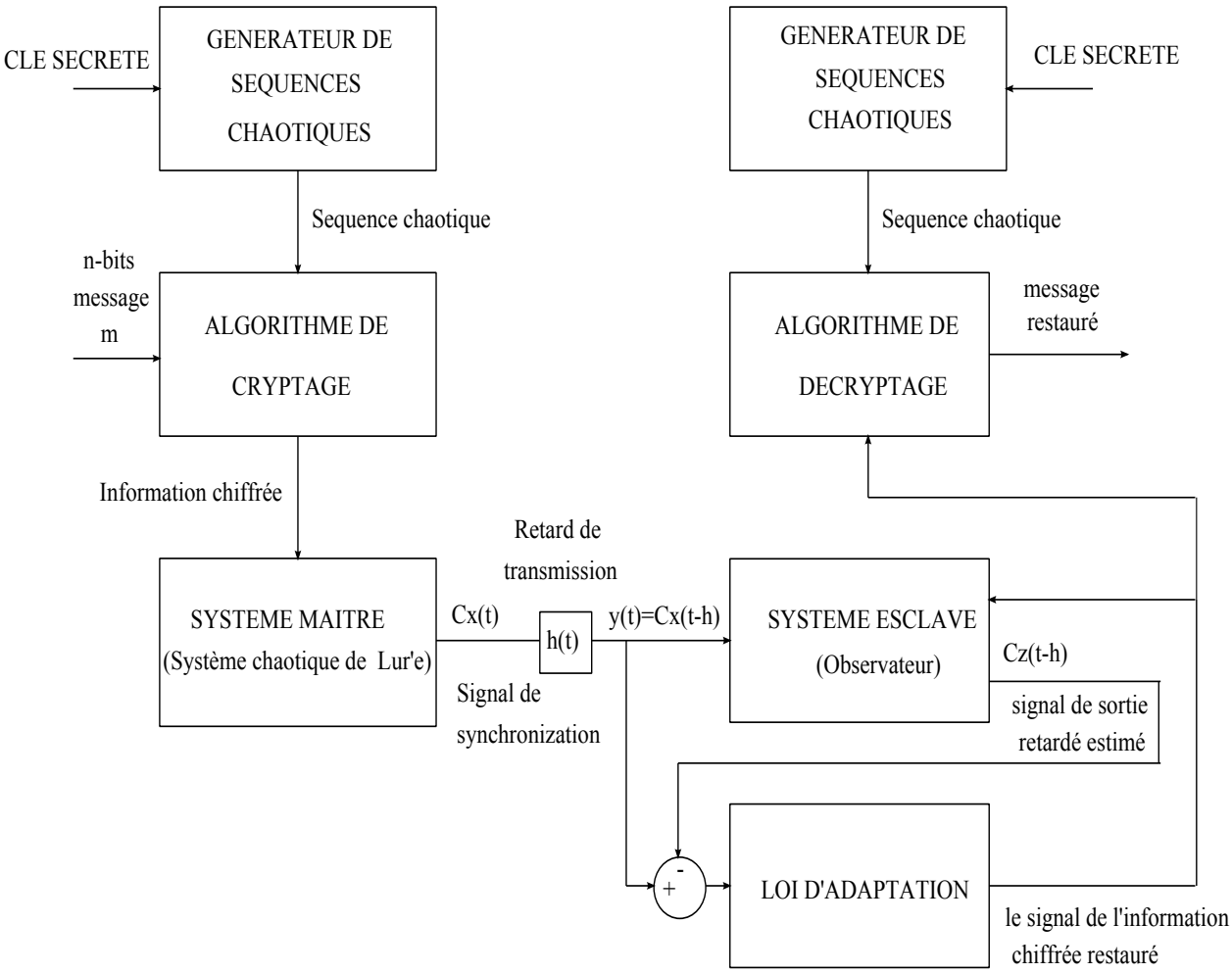

FIGURE 4.11: Le système de communication proposé

Le schéma est inspiré de la technique de cryptage combinée utilisant un algorithme de cryptage pour lequel l'information doit être traitée avant son injection dans le système maître (Voir Chapitre 1), cependant avec cette méthode, l'algorithme de cryptage utilise une séquence chaotique générée à partir du système maître dont les paramètres et/ou les conditions initiales sont utilisées pour produire une clé secrète, or des techniques d'attaque telles que la technique de synchronisation généralisée ou la technique d'identification des paramètres ont dévoilé les limites de ces systèmes de communication basées conjointement sur la synchronisation du chaos et l'exploitation des paramètres et des conditions initiales pour la construction de la clé secrète. Afin de surmonter ce problème, nous avons choisi d'utiliser deux systèmes chaotiques indépendants : un premier système génère une

séquence chaotique utilisée par l'algorithme de cryptage et un deuxième système jouant le rôle du système maître assurant seulement la transmission du signal chiffré obtenu à la fin de l'opération de cryptage grâce à la technique de modulation paramétrique. Ainsi, les tâches de cryptage et de synchronisation sont totalement indépendantes et donc on peut utiliser, sans soucis, les paramètres et les conditions initiales du premier système chaotique afin de produire un espace clé suffisamment large pour résister aux attaques à force brute. Notons que le système maître est conçu à base des systèmes chaotiques de Lur'e ayant la forme (4.1). Au niveau du récepteur, on dispose d'un système esclave à base de l'observateur (4.10) qui synchronise avec le système maître malgré l'existence du retard h dans le canal public grâce à notre méthode de synchronisation. La loi d'adaptation décrite par l'équation (4.10b) permet de restaurer le signal chiffré envoyé vers un algorithme de décryptage utilisant une séquence chaotique identique à celle utilisée par l'algorithme de décryptage, et finalement on peut restaurer l'information originale transmise. On déduit que l'avantage principal du schéma proposé consiste à la possibilité de transmission des informations dans un canal présentant des retards de transmission tout en offrant des marges de manœuvres pour garantir un niveau élevé de sécurité.

4.8.1 Illustrations et simulations numériques : cryptage et transmission d'une image

Récemment, dans [107], une nouvelle méthode de cryptage d'images a été élaborée en utilisant le système chaotique de Chen. L'algorithme de cryptage est construit à base de deux opérations de diffusion présentant une forte sensibilité à la clé secrète et au texte clair. Bien que le système de Chen utilisé pour la génération des séquences chaotiques possède des propriétés cryptographiques meilleures que plusieurs autres systèmes chaotiques, il présente tout de même des limites et ses caractéristiques statistiques (histogramme, corrélation, auto-corrélation) ne sont pas tout à fait appropriés pour le cryptage d'images, ce qui justifie l'opération supplémentaire de pré-traitement de la séquence chaotique produite à partir du système de Chen, qui a été effectuée, dans [107], dans le but d'avoir des séquences pseudo-aléatoires. Dans notre application, nous avons choisi, pour la génération des séquences chaotiques, le système de Chua modifié introduit dans le chapitre 3 et qui a prouvé son utilité pour le cryptage d'images, ce qui nous dispense d'effectuer une étape supplémentaire de pré-traitement de la séquence chaotique.

4.8.1.1 Génération de la séquence chaotique

Le choix du système de Chua modifié est justifié, comme expliqué dans le chapitre 3, par la capacité d'étendre arbitrairement la bande de fréquences jusqu'aux hautes fréquences ce qui permet de générer des séquences chaotiques de plus en plus complexes et présentant des bonnes propriétés statistiques

pour le cryptage de l'information. Nous rappelons ici les équations du système de Chua modifié :

$$\begin{cases} T_s^{-1}\dot{x}_1 = -\alpha(x_2 - \bar{a}x_1 + \bar{b}x_1\,|x_1| + \bar{c}x_1^3) \\ T_s^{-1}\dot{x}_2 = x_1 - x_2 + x_3 \\ T_s^{-1}\dot{x}_3 = -\bar{\beta}x_2 \\ y = x_1 \end{cases} \tag{4.75}$$

On ajuste le facteur de transformation de l'échelle du temps à $T_s = 100$.

La figure 4.12 représente les attracteurs dans les plans de phase (x_1, x_2) et (x_2, x_3). L'évolution dans le temps des états x_1 et x_2 est illustrée dans la figure 4.13. Les bonnes propriétés statistiques du système de Chua modifié sont montrées dans la figure (4.14) qui illustre bien que les corrélations sont proches de zéro ce qui permet d'obtenir des séquences chaotiques pseudo-aléatoires.

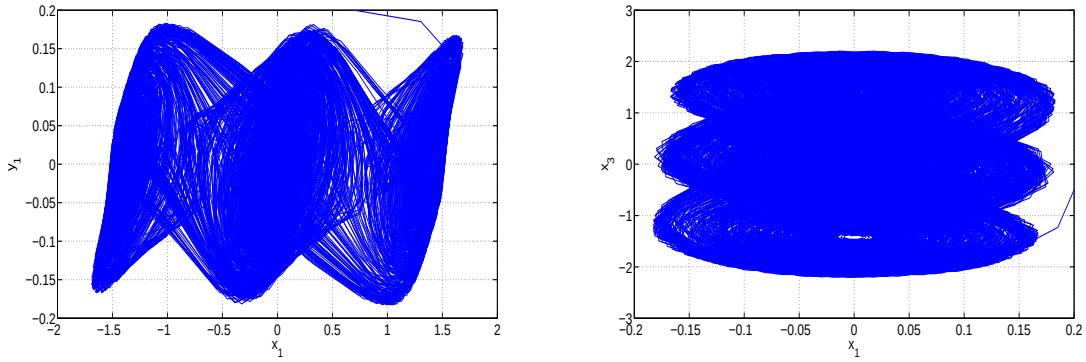

FIGURE 4.12: Attracteurs dans les plan de phase (x_1, x_2) (gauche) et (x_2, x_3) (droite) du système de Chua modifié

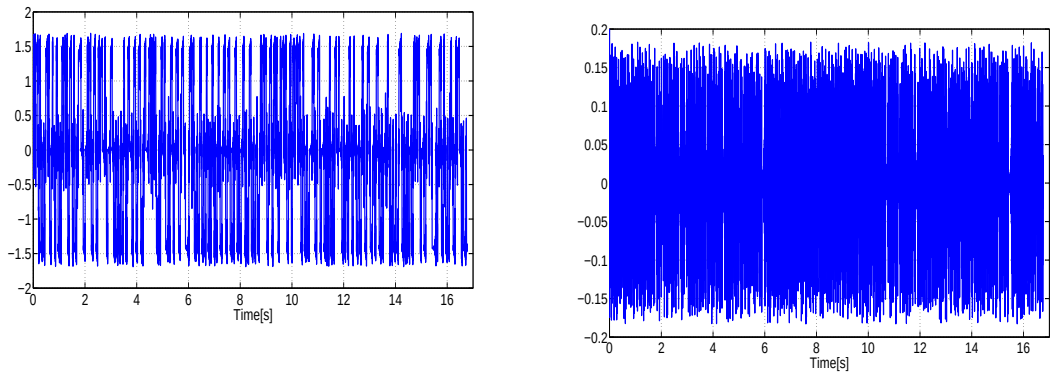

FIGURE 4.13: L'évolution dans le temps des états x_1 (gauche) et x_2 (droite) du système de Chua modifié

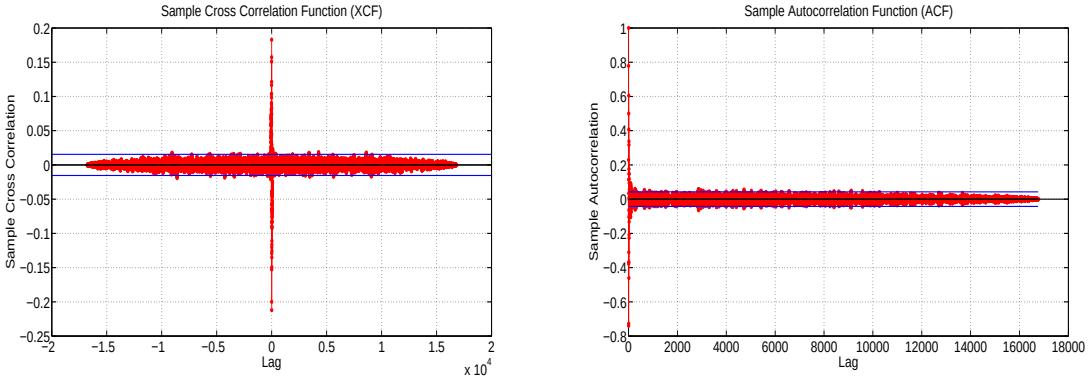

FIGURE 4.14: Cross-correlation entre les séquences chaotiques x_1 et x_2 (gauche) et l'autocorrélation dans la séquence chaotique x_2 (droite) du système de Chua modifié

Afin d'obtenir une séquence d'entiers naturels entre 0 et 256, nous effectuons les traitement suivants :

for $i = 1 : 16766$

$K_{s1}(i) = mod(abs(fix(x_1(i) - fix(x_1(i))) \times 10^{14}, 256);$

$K_{s2}(i) = mod(abs(fix(x_2(i) - fix(x_2(i))) \times 10^{14}, 256);$

$K_{s3}(i) = mod(abs(fix(x_3(i) - fix(x_3(i))) \times 10^{14}, 256);$

end

Nous obtenons enfin la nouvelle séquence d'entiers $K_s = [K_{s1}, K_{s2}, K_{s3}]$ qui sera utilisée par l'algorithme de cryptage.

4.8.1.2 Algorithme de cryptage

L'information à crypter est une image (voir Figure 4.17) (166×303) . Nous concaténons les lignes de cette dernière pour obtenir le vecteur $P_m = \{P_m(1), P_m(2), \ldots, P_m(L)\}$ de dimension $L = 166 \times 303$. Soit $C_m = \{C_m(1), C_m(2), \ldots, C_m(L)\}$ la séquence de l'image chiffrée. L'algorithme de cryptage proposé dans [107] consiste en deux routines de diffusion (programme écrit sous Matlab) :

1-première routine de diffusion :

$C_m(0) = 1$;

$C_m(1) = bitxor(P_m(1), bitxor(uint8(mod(single(C_m(0)) + single(K_s(1)), 256)), K_s(1)))$;

for i=2 :L

$C_m(i) = bitxor(P_m(i), bitxor(uint8(mod((single(C_m(i-1)) + single(K_s(i))), 256)), K_s(i-1)))$;

end

2-Deuxième routine de diffusion :

$C_m(1) = bitxor(C_m(1), bitxor(uint8(mod(single(C_m(L)) + single(K_s(1)), 256)), K_s(1)))$;

for i=2 :L

$C_m(i) = bitxor(C_m(i), bitxor(uint8(mod((single(C_m(i-1)) + single(K_s(i))), 256)), K_s(i-1)))$;

end

4.8.1.3 Conception des systèmes maître et esclave

Pour la conception du système maître, nous reprenons le modèle de "Duffing" qui appartient à la famille des systèmes de Lur'e (4.1) et on injecte le signal d'information chiffrée $C_m(t)$ dans sa dynamique. Le signal de sortie $y(t)$ est corrompu par un retard de transmission constant $h = 0.04s$. Donc, la dynamique de l'émetteur chaotique est donnée par

$$\begin{aligned} \dot{X}_1 &= X_2, \\ \dot{X}_2 &= -0.4X_2 - 1.1X_1 - (1 + m(t))X_1^3 + cos(1.8t) \\ y(t) &= X_1(t-h) + X_2(t-h). \end{aligned} \tag{4.76}$$

Le récepteur est donné par l'équation (4.10). La solution au problème d'optimisation (4.17) est donnée par :

$$D = \bar{D}_1 = 2.6464,\ P = \begin{bmatrix} 12.1437 & 1.5679 \\ 1.5679 & 1.5679 \end{bmatrix},\ \varepsilon = 5.9542.$$

$$K = \begin{bmatrix} 0.0596 \\ 3.4896 \end{bmatrix},\ M = -1.5679,\ \rho = 10,\ \alpha = 0.5.$$

L'état $x(t)$ du système (4.76) est initialisé à $x_0 = [0, 0]^T$, $\forall s \in [-0.04, 0]$. Les conditions initiales de l'observateur sont $z(s) = [1, 2]^T$, $\forall s \in [-0.04, 0]$, $\hat{m} = 0.6$, $\Upsilon = 0.2$.

Les résultats de simulation se présentent comme suit. La figure 4.15 illustre la synchronisation entre les systèmes maître et esclave, la figure 4.16 montre que l'image chiffrée est bien restaurée.

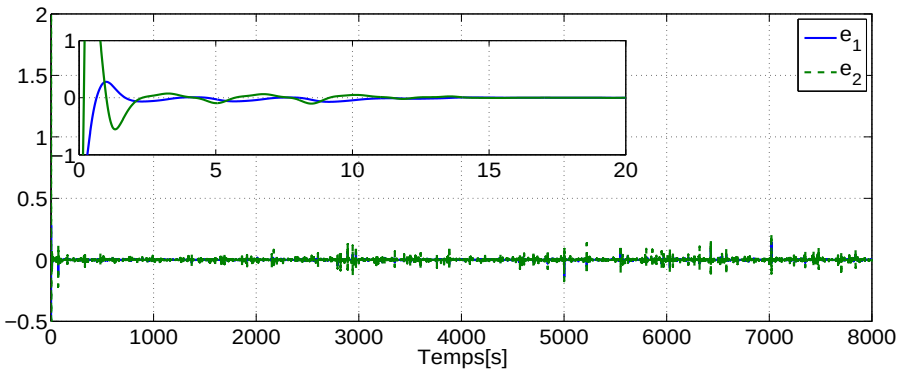

FIGURE 4.15: Erreurs de synchronisation $e_1 = X_1 - \hat{X}_1$ et $e_2 = X_2 - \hat{X}_2$ en présence d'un retard de transmission $h = 0.04s$

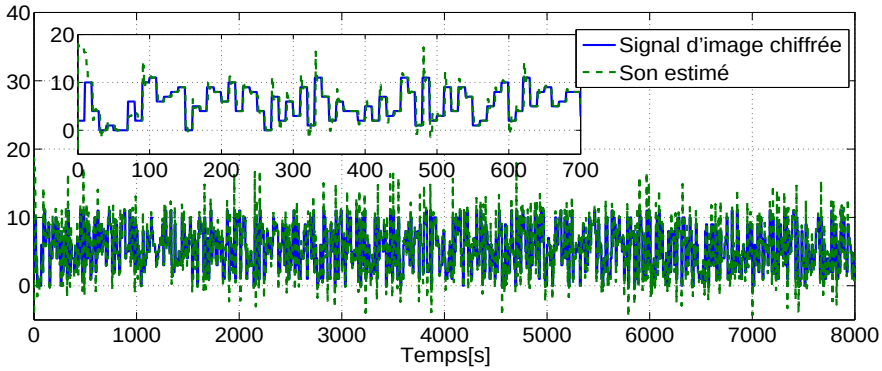

FIGURE 4.16: L'information chiffrée $C_m(t)$ et son estimée en présence du retard de transmission

4.8.1.4 Algorithme de décryptage

L'algorithme de décryptage ci-dessus (écrit sous matlab) est développé pour effectuer le processus inverse de l'algorithme de cryptage.

$i = L.$
while $i \geq 2$
$C_m(i) = bitxor(C_m(i), bitxor(uint8(mod((single(C_m(i-1)) + single(K_s(i))), 256)), K_s(i-1)))$;
$i = i - 1;$
end
$C_m(1) = bitxor(C_m(1), bitxor(mod((C_m(L) + K_s(1)), 256), K_s(1)));$
$i = L$;
while $i \geq 2$
$D_m(i) = bitxor(C_m(i), bitxor(uint8(mod((single(C_m(i-1)) + single(K_s(i))), 256)), K_s(i-1)));$
$i = i - 1;$
end
$D_m(1) = bitxor(C_m(1), bitxor(uint8(mod((single(C_m(0)) + single(K_s(1))), 256)), K_s(1))).$

Ainsi, on obtient la séquence de l'image décryptée $D_m = \{D_m(1), D_m(2), \ldots, D_m(L)\}$, et par conséquent, on peut déduire l'image décryptée.

Système chaotique	**Paramètres**	**Sensibilité**	**Nb. de possibilités :** $(N_i = s \times {S_i}^{-1})$
Système de Chua modifié	$p_1 = \bar{\beta} = 19.1$ $\alpha = 12.8$ $\bar{a} = 0.47$ $\bar{b} = -1$ $\bar{c} = 0.472$	$S_1 = 10^{-14}$ $S_2 = 10^{-15}$ $S_3 = 10^{-15}$ $S_4 = 10^{-16}$ $S_5 = 10^{-16}$	$N_1 = 10^{13}$ $N_2 = 10^{14}$ $N_3 = 10^{14}$ $N_4 = 10^{15}$ $N_5 = 10^{15}$

TABLE 4.1: Sensibilité des paramètres

4.8.2 Analyse de sécurité

4.8.2.1 Analyse de la clé secrète

Soit $R = (\alpha, a, b, c)$ la clé secrète. Le tableau 4.1 représente la sensibilité de chacun des paramètres. Il s'agit de la plus petite variation paramétrique engendrant deux attracteurs différents. On suppose que la marge de variation de chacun des paramètres impliquant un régime chaotique est égale à 10^{-1}. La taille de l'espace clé est : $T_l = \prod_{i=1}^{8}(N_i) = 10^{(13+14\times2+15\times2)} = 10^{71}$. Un espace clé de taille $O(2^{100})$ est exigé pour résister aux attaques à force brute. Dans notre cas, $T_l = 10^{71} \geq 2^{100}$, ce qui implique que l'espace clé possède un niveau de sécurité largement satisfaisant.

4.8.2.2 Analyse statistique

Afin de vérifier la robustesse du cryptosystème aux attaques statistiques [108], nous avons réalisé un test des histogrammes de l'image originale et de l'image chiffrée (Voir Figure 4.18). Le résultat obtenu montre que la distribution de l'image chiffrée est presque uniforme contrairement à la distribution de l'image originale. Ceci peut être interprété par l'efficacité de deux opérations de diffusion dans l'algorithme de cryptage.
Nous avons également réalisé un test des propriétés de corrélations entre les pixels de l'image chiffrée. La figure 4.19 représente une comparaison entre les corrélations des pixels horizontalement adjacents dans l'image originale et l'image chiffrée. On déduit que la corrélation entre les pixels est très faible dans l'image chiffrée contrairement à l'image originale. En outre, nous avons calculé le coefficient de corrélation entre les pixels horizontalement adjacents. Pour ce faire, on choisit N paires de pixels horizontalement adjacents (x_i, y_i) et on utilise la formule suivante :

$$C_r = \frac{N\sum_{i=1}^{N}(x_i y_i) - \sum_{i=1}^{N} x_i \sum_{i=1}^{N} y_i}{\sqrt{(N\sum_{i=1}^{N} x_i^2 - (\sum_{i=1}^{N} x_i)^2)(N\sum_{i=1}^{N} y_i^2 - (\sum_{i}^{N} y_i)^2)}}. \tag{4.77}$$

Nous obtenons un coefficient de corrélation égal à 0.002301 dans le cas de l'image chiffrée et 0.910381 dans le cas de l'image originale, ce qui confirme bien le résultat de la figure 4.19.

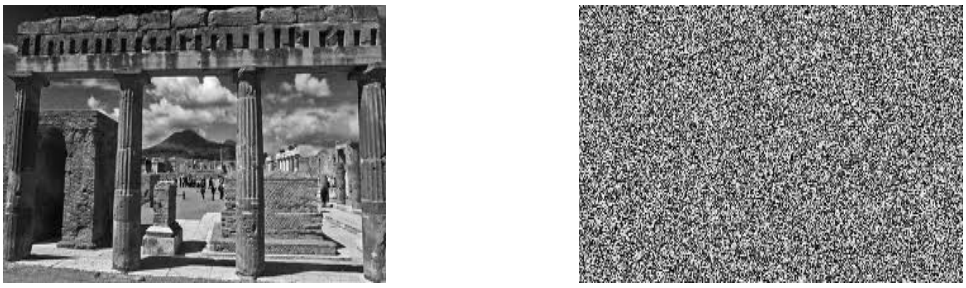

FIGURE 4.17: a) Image originale b)Image chiffrée

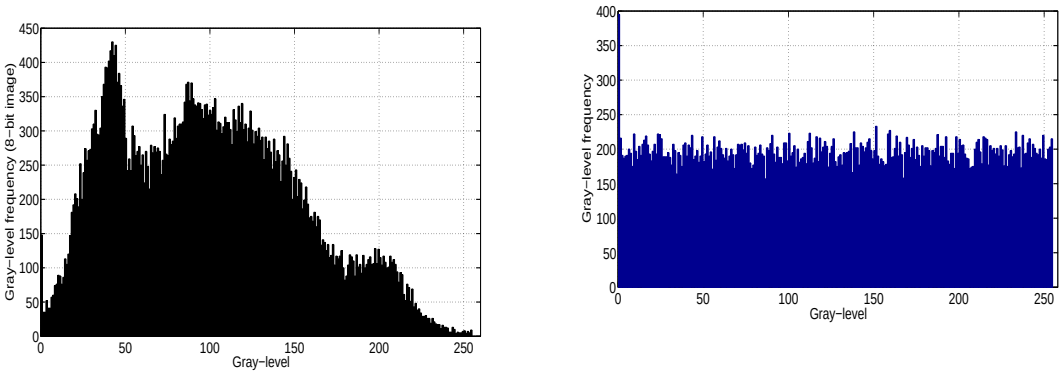

FIGURE 4.18: a) Histogramme de l'image originale b) Histogramme de l'image chiffrée

Nous nous intéressons maintenant à la corrélation entre l'image originale et l'image chiffré. Pour ce faire, nous utilisons la corrélation 2D dont le coefficient CC est donné par la formule :

$$CC = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}(A_{ij}-\bar{A})(B_{ij}-\bar{B})}{\sqrt{(\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}((A_{ij}-\bar{A})^2)(\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}(B_{ij}-\bar{B})^2)}}, \tag{4.78}$$

avec $\bar{A} = \frac{1}{M_1 M_2}\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} A_{ij}$ et $\bar{B} = \frac{1}{M_1 M_2}\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} B_{ij}$. Dans notre cas, A représente l'image originale et B représente l'image chiffrée. M_1 et M_2 représentent les dimensions des images. La valeur calculée est égale à $CC = -6.284 \times 10^{-4}$ (qui est très proche de zéro), ce qui montre que la corrélation entre les deux images originale et chiffrée est très faible et qui confirme les bonnes propriétés de diffusion du cryptosystème.

Tous ces tests montrent que le cryptosystème possède une robustesse aux attaques statistiques [108].

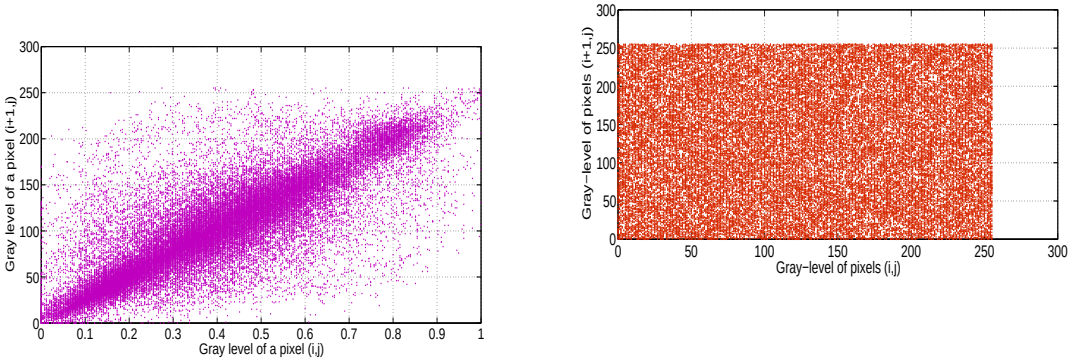

FIGURE 4.19: Corrélations entre les pixels horizontalement adjacents dans l'image originale (gauche) et dans l'image chiffrée (droite)

Nous testons maintenons la sensibilité par rapport au texte clair en modifiant un seul pixel dans l'image originale et en analysant l'effet sur l'image chiffrée. Le coefficient $NPCR$ permet d'évaluer le taux de changement des pixels dans l'image, il est donnée par la formule suivante :

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M_1 M_2} \times 100\%, \tag{4.79}$$

où $D_{ij} = 0$, si $c_1(i,j) = c_2(i,j)$ et $D_{ij} = 1$, sinon. $c_1(i,j)$ et$c_2(i,j)$ représentent deux images chiffrées correspondant à deux images originales légèrement modifiées (un pixel changé).
Le deuxième coefficient qui permet de quantifier la sensibilité par rapport au texte clair est le coefficient d'intensité du changement moyen unifié ($UACI$) donné par l'expression :

$$NPCR = \frac{1}{M_1 M_2} \sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \times 100\%. \tag{4.80}$$

On effectue trois changements différents des pixels (au début, au centre et à la fin), on obtient les résultats suivants :
-Changement du pixel N°1 : $NPCR = 99.99\%$ et $UACI = 33.4636\%$.
-Changement du pixel N°25000 : $NPCR = 99.5\%$ et $UACI = 33.37\%$.
-Changement du pixel N°50000 : $NPCR = 99.18\%$ et $UACI = 33.37\%$.

Dans [109], les auteurs suggèrent un critère pour juger si le cryptosystème est bon de point de vue la sensibilité par rapport au texte clair. Les valeurs "références" proposées sont calculées comme suit :

$$NPCR_{ref} = (1 - 2^{-n}) \times 100\%. \tag{4.81}$$

$$UACI_{ref} = \frac{1}{2^n} \frac{\sum_{i=1}^{2^{-n}-1} i(i+1)}{2^{-n} - 1}, \tag{4.82}$$

où n représente le nombre des bits utilisés dans la représentation d'un pixel. Dans notre cas (image 8-bits), $n = 8$, donc les valeurs références obtenues sont $NPCR_{ref} = 99.6094\%$ et $UACI_{ref} = 33.4635\%$.
On remarque bien que les valeurs de $NPCR$ et de $UACI$ correspondant au cryptosystème sont très proches des valeurs références $NPCR_{ref}$ et $UACI_{ref}$, donc le cryptosystème possède une sensibilité au texte clair. Notons que les mêmes coefficients peuvent être utilisés pour tester la sensibilité à la clé secrète, mais au lieu de changer un pixel dans l'image originale, on change légèrement la clé secrète. Nous avons changé le paramètre $a = 0.47$ de 10^{-14}, les valeurs obtenues sont $NPCR = 99.54\%$ et $UACI = 33.26\%$.

4.9 Conclusion

Dans ce chapitre, nous avons proposé une méthode de synchronisation basée sur les observateurs adaptatifs pour une classe des systèmes de Lur'e avec des non-linéarités à pente limitée et tels que le canal de transmission est soumis à un retard à temps variant et connu. La synchronisation maître-esclave et la reconstruction du signal d'information sont réalisées pour des valeurs suffisamment petites de la borne supérieure du retard et si une condition d'excitation persistante est satisfaite. Les matrices de l'observateur sont obtenues après la résolution d'un problème convexe d'optimisation. Le cas de longs retards de transmission a été également étudié en développant un système esclave construit à base des observateurs en cascade. L'approche a été évaluée à travers des exemples numériques et exploitée dans un système de communication sécurisé présentant un retard de transmission.

Conclusion générale

Dans ce travail de thèse, nous avons développé des méthodes de synchronisation des systèmes non linéaires tels que les systèmes chaotiques et les systèmes de Lur'e à base d'observateurs non linéaires et leur application pour la transmission d'informations. Les stratégies qui ont été employées tiennent compte de différents scénarios pouvant se produire en pratique : la présence de perturbations, d'incertitudes paramétriques, de bruits dans le canal public, de retards de transmission, etc. La première approche de synchronisation présentée dans le chapitre 2 est basée sur un observateur adaptatif à entrées inconnues. Ce dernier possède l'avantage de joindre l'estimation de l'état, des paramètres inconnus et des informations transmises et le rejet des perturbations dans la dynamique du système maître et du bruit dans le canal de transmission. La convergence paramétrique et la restauration des messages envoyés sont accomplies grâce à l'utilisation des lois d'adaptations et sous la condition d'excitation persistante.

Le chapitre 3 a été dédié à la deuxième méthode de synchronisation proposée dans cette thèse. Il s'agit d'une méthode de synchronisation à base d'un observateur adaptatif à "modes glissants" qui repose sur la combinaison de la théorie des modes glissants, les techniques de synthèse d'observateurs singuliers et la commande adaptative. la méthode élaborée permet l'estimation simultanée de l'état et des entrées inconnues (les informations à transmettre dans contexte de communication chaotique) malgré la présence d'un bruit additif dans le signal de sortie (bruit dans le canal). Deux lois d'adaptation et une commande à "modes glissants" modifiée sont associées à l'observateur et garantissent la compensation des non-linéarités et des termes résiduels et la stabilité pratique des erreurs d'estimation et d'adaptation.

Ensuite, l'observateur adaptatif à modes glissants a été employé dans un nouveau schéma de communication basé sur la synchronisation maitre-esclave des systèmes chaotiques. L'idée de base consiste à séparer les tâches de cryptage et de synchronisation en utilisant deux systèmes chaotiques en cascade au niveau de l'émetteur afin d'améliorer le niveau de sécurité et augmenter l'amplitude des messages transmis. Le schéma proposé permet également la transmission des données analogiques et numériques et possède une robustesse aux bruits affectant le canal de communication. Une analyse de sécurité et de la clé secrète ont démontré les bonnes performances du schéma proposé en termes de confidentialité et de robustesse aux techniques d'attaques spécifiques aux systèmes de communications chaotiques et cryptographiques. Les simulations numériques ont également confirmé l'efficacité du système dans une application de cryptage d'images binaires.

Dans le chapitre 4, nous avons présenté une approche de synchronisation à base d'observateurs adaptatifs pour une classe des systèmes chaotiques de Lur'e avec des non-linéarités à pente restreinte en présence d'un retard de transmission à temps variant. Nous avons montré que pour des valeurs de la borne supérieure du retard de transmission suffisamment petites et sous l'hypothèse d'excitation persistante, les objectifs de synchronisation et de restauration des messages sont accomplis. La démonstration de stabilité est basée sur la théorie de Lyapunov-Krasovskii et la résolution d'un problème convexe d'optimisation. Une extension des résultats obtenus a été effectuée pour le cas des longs retards de transmission en présentant un schéma de synchronisation à base des observateurs en cascade. Les résultats théoriques ont été confirmés à l'aide des exemples numériques de simulation. Enfin, une application de communication sécurisée en présence des retards de transmission a été présentée tout en étudiant les aspects reliés à la sécurité des informations transmises.

Ce travail de thèse ouvre la voie à des diverses perspectives, extensions et généralisations :
Tout d'abord, l'adaptation des méthodes de synchronisation qui ont été élaborées dans cette thèse pour des systèmes chaotiques continus aux cas des systèmes chaotiques discrets.

Nous avant étudié dans cette thèse différents scénarios où les systèmes de transmissions d'informations sont soumis à des contraintes de communication telles que la présence du bruit dans le canal de communication et l'existence des retards de transmission. Dans ce contexte, d'autres contraintes de communications sont envisageables, notamment le cas d'utilisation des sorties quantifiées et le cas où le signal de sortie est envoyé à des instants discrets en utilisant du régime de synchronisation impulsive. En outre, des scénarios plus sophistiqués évoquant la présence simultanée des plusieurs contraintes peuvent être traités : par exemple, l'étude du cas de présence simultanée du bruit et du retard de transmission dans le canal de communication.

Par ailleurs, dans ce travail de thèse, nous avons essayé de montrer que les systèmes de communications basés sur la synchronisation des systèmes chaotiques continus peuvent garantir un niveau satisfaisant de sécurité, néanmoins il reste à entrevoir d'autres schémas de communications garantissant un niveau plus élevé de confidentialité et mener des études plus approfondies de cryptanalyse en tenant compte des différentes techniques d'attaques spécifiques aux systèmes cryptographiques.

Bibliographie

[1] B. R. Andrievskii et A. L. Fradkov. Control of chaos : Methods and applications. i. methods. *Automation and Remote Control*, 64(5) :673–713, 2003.

[2] H. Zhang, D. Liu, and Z. Wang. Controlling chaos : Suppression, synchronization and chaotifcation. *(Communications and Control Engineering*, 2009.

[3] T. S. Parker and L. O. Chua. Practical numerical algorithms for chaotic systems. *Springer-Verlag*, 1989.

[4] D. R. Stinson. Cryptography : Theory and practice. *CRC Press*, 1995.

[5] G. Alvarez and S. Li. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. of Bifurcat. and Chaos*, 16(8) :2129–2151, 2006.

[6] G. Kolumban, M. P. Kennedy, and L. O. Chua. The role of synchronization in digital communications using chaos - part ii : chaotic modulation and chaotic synchronization. *IEEE Trans. on Circ. Syst. I*, 45, 1998.

[7] L. M. Pecora and T. L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64(8) : 821–824, 1990.

[8] M. Ahan, X. Wang, X. Gong, G.W. Wei, and C. H. Lai. Complete synchronization and generalized synchronization of one-way coupled time-delay systems. *Phys. Rev. E*, 86(3), 2003.

[9] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and H. D. I. Abarbanel. Generalized synchronization of chaos in directionally coupled chaotic systems. *Phys. Rev. E*, 51, 1995.

[10] C. Li, X. Liao, and K. Wong. Chaotic lag synchronization of coupled time-delayed systems and its applications in secure communication. *Physica D*, 194 :187–202, 2004.

[11] R. Mainieri and J. Rehace. Projective synchronization in three-dimensional chaotic systems. *Phys. Rev. Lett.*, 82(15) :3042–3045, 1999.

[12] T. Yang and L. Chua. Impulsive stabilization for control and synchronization of chaotic systems : Theory and application to secure communication. *IEEE Trans. on Circ. Syst. I : Regular Papers*, 44 :976–988, 1997.

[13] K. W. Wong J. Y. Chen and L. M. Cheng. A secure communication scheme based on the phase synchronization of chaotic systems. *Chaos*, 13(2) :508–514, 2003.

[14] A. Loria, E. Panteley, and A. Zavala. Adaptive observers with persistency of excitation for synchronization of chaotic systems. *IEEE Trans. on Circ. Syst. I : Regular Papers*, 56(12) : 2703–2716, 2009.

[15] Z. Huang and J. Ruan. Synchronization of chaotic systems by linear feedback controller. *Commun Nonlinear Sci Numer Simul*, 3 :27–30, 1998.

[16] M.Yassen. Controlling, synchronization and tracking chaotic liu system using active backstepping design. *Phys Lett A*, 360 :582–587, 2007.

[17] Y. Feng, J. Zheng, and L. Sun. Chaos synchronization based on sliding mode observer. *Systems and Control in Aerospace and Astronautics*, pages 1366–1373, 2006.

[18] G.Jiang, W.Zheng, W.Tang, and G.Chen. Integral observer approach for chaos synchronization with transmission disturbances. *IEEE Trans Circuits Syst I Fundam Appl*, 53 :110–114, 2006.

[19] H. Nijmeijer and I. Mareels. An observer looks at synchronization. *IEEE Trans. on Circ. Syst. I : Fundamental Theory and Applications*, 44(10) :882–890, 1997.

[20] O. Morgül and E. Solak. Observer based synchronization of chaotic systems. *Phys. Rev. E*, 54, 1996.

[21] A. V. Oppenheim K. M. Cuomo and S. H. Strogatz. Synchronization of lorenz-based chaotic circuits with applications to communications. *IEEE Trans. on Circ. Syst. II*, 40(10) :626–633, 1993.

[22] M. Feki. An adaptive chaos synchronization scheme applied to secure communication. *Chaos, Solitons and Fractals*, 18 :141–148, 2003.

[23] H. Dedieu, M. P. Kennedy, and M. Hasler. Chaos shift keying : modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits. *IEEE Trans. on Circ. Syst. I : Regular Papers*, 40(10) :634–642, 1993.

[24] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang. Trnasmission of digital signals by chaotic synchronization. *Int. J. of Bifurcat. and Chaos*, 2, 1993.

[25] M. Chen, D. Zhou, and Y. Shang. A sliding mode observer based secure communication scheme. *Chaos, Solitons and Fractals*, 25 :573–578, 2005.

[26] G. Millérioux and C. Mira. Coding scheme based on chaos synchronization from noninvertible maps. *Int. J. of Bifurcat. and Chaos*, 8(10) :2019–2029, 1998.

[27] T. Yang, C. W. Wu, and L. O. Chua. Cryptography based on chaotic systems. *IEEE Trans. on Circ. Syst. I : Regular Papers*, 44(5) :469–472, 1997.

[28] G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Breaking parameter modulated chaotic secure communication system. *Chaos, Solitons and Fractals*, 21, 2003.

[29] A. J. Menezes, P. C. Van Oorschot, and S. A.Vanstone. Handbook of applied cryptography. *CRC Press*, 1997.

[30] J. Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. of Bifurcat. and Chaos*, 8, 1998.

[31] G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Breaking two secure communication systems based on chaotic masking. *IEEE Trans. on Circ. Syst. I : Regular Papers*, 51 :505–506, 2004.

[32] G. Alvarez, L. Hernandez, J. Munoz, F. Montoya, and S. Li. Security analysis of communication system based on the synchronization of different order chaotic systems. *Phys. Lett. A*, 345 (4) :245–250, 2005.

[33] T. Yang, L. B. Yang, and C. M. Yang. Cryptanalysing chaotic secure communications using return maps. *Phys. Lett. A*, 245, 1998.

[34] T. Yang, L. Yang, and C. Yang. Breaking chaotic switching using generalized synchronization : examples. *IEEE Trans. on Circ. Syst. I : Regular Papers*, 45 :1062–1067, 1998.

[35] G. Besaçon. *Nonlinear Observers and Applications*. Series Lecture Notes in Control and Information Science,. Springer Verlag, Berlin Heidelberg NewYork, 2007. ISBN-13 : 978-3-540-73502-1.

[36] J. P. Gauthier H. Hammouri and S. Othman. A simple observer for nonlinear systems. applications to bioreactors. *IEEE Trans. on Automat. Contr.*, 37(6) :875–880, 1992.

[37] D. G. Luenberger. Observing the state of a linear system. *IEEE Trans. Mil. Electron.*, 8, 1964.

[38] R. E. Kalman et J. E. Betram. Control system analysis and design via the second method of lyapunov -i : Continuous-time system. *ASME journal of Basic Engineering*, 82, 1960.

[39] F. E. Thau. Observing the state of nonlinear dynamic systems. *Int. J. of Contr.*, 17(3) : 471–479, 1973.

[40] M. Arcak and P. Kokotović. Observer-based control of systems with slope-restricted nonlinearities. *IEEE Trans. on Automat. Contr.*, 46(7) :1146–1150, 2001.

[41] A. Zemouche, M. Boutayeb, and G. I. Bara. Observers for a class of lipschitz systems with extension to h_∞ performance analysis. *Syst. & Contr. Letters*, 57(3) :18–27, 2008.

[42] S. Raghavan and J. K. Hedrick. Observers for a class of lipschitz systems with extension to h∞ performance analysis. *Int. J. of Contr.*, 59(2) :515–528, 1994.

[43] R. Rajamani. Observers for a class of lipschitz systems with extension to h∞ performance analysis. *IEEE Trans. on Automat. Contr.*, 43(3) :397–401, 1998.

[44] M. Abbaszadeh and H. J. Marquez. A robust observer design method for continuous-time lipschitz nonlinear systems. In *45th IEEE Conf. on Dec. and Contr.*, pages 3795–3800, San Diego, USA, 2006.

[45] X. Fan and M Arcak. Observer design for systems with multivariable monotone nonlinearities. *Syst. & Contr. Letters*, 50, 2003.

[46] M. Boutayeb A. Zemouche. A unified adaptive observer synthesis method for a class of systems with both lipschitz and monotone nonlinearities. *Syst. & Contr. Letters*, 58, 2009.

[47] M. Farza, K. Busawon, and H. Hammouri. Simple nonlinear observers for on-line estimation of kinetic rates in bioreactors. *Automatica*, 34(3) :301–318, 1998.

[48] M. Farza, M. Msaad, M. Triki, and T. Maatoug. High gain observer for a class of non-triangular systems. *Syst. & Contr. Letters*, 60, 2011.

[49] L. Praly. Asymptotic stabilization via output feedback for lower triangular systems with output dependent incremental rate. *IEEE Transactions on Automatic Control*, 48(6) :1103–1108, 2003.

[50] L. Praly V. Andrieu and A. Astolfi. High gain observers with updated gain and homogeneous correction terms. *Automatica*, 45, 2009.

[51] G. Besançon. Remarks on nonlinear adaptive observer design. *Systems and Control Letters*, 41 :271–280, 2000.

[52] Y. M. Cho and R. Rajamani. A systematic approach to adaptive observer synthesis for nonlinear systems. *IEEE Trans.Automat. Contr.*, 42(4) :534–537, 1997.

[53] Q. Zhang. Adaptive observers for mimo linear time-varying systems. *IEEE Trans. on Automat. Contr.*, 47 :525–529, 2002.

[54] A. Xu and Q. Zhang. Nonlinear system fault diagnosis based on adaptive estimation. *Automatica*, 40 :1183–1193, 2004.

[55] M. Farza, M. Msaad, T. Maatoug, and M. Kamounb. Adaptive observers for nonlinearly parameterized class of nonlinear systems. *Automatica*, 45 :2292–2299, 2009.

[56] B. L. Walcott et S. H. Zak. Combined observer-controller synthesis for uncertain dynamical systems with applications. *IEEE Trans. on Systems*, 18, 1988.

[57] B. L. Walcott and S. H. Zak. State observation of nonlinear uncertain dynamical systems. *IEEE Trans. on Automat. Contr.*, 32(2) :166–170, 1987.

[58] C. Edwards, S. K. Spurgeon, and R.J. Patton. Sliding mode observers for fault detection and isolation. *Automatica*, 36 :541–553, 2000.

[59] J. P Barbot and T. Floquet. Iterative higher-order sliding-mode observer design for nonlinear systems with unknown inputs. Technical report, INRIA, 2009. `http://hal.inria.fr/inria-00442129`.

[60] T. Floquet and J. P Barbot. *A canonical form for the design of unknown input sliding mode observers*, volume 334, "Advances in Variable Structure and Sliding mode control". Springer, Lecture Notes in Control and Information Science, Berlin, 2006. `http://hal.inria.fr/inria-00293867`.

[61] A. Levant. Robust exact differentiation via sliding mode technique. *Automatica*, 34 :379–384, 1998.

[62] A. Levant. Higher-order sliding modes, differentiation and output-feedback control. *International Journal of Control*, 76 :924–941, 2003.

[63] S. H. Wang, E. J. Davison, and P. Dorato. Observing the states of systems with unmeasurable disturbances. *IEEE Trans. on Automat. Contr.*, 20, 1975.

[64] M. Darouach, M. Zasadzinski, and S. J. Xu. Full-order observers for lienar systems with unknown inputs. *IEEE Trans. on Automat. Contr.*, 39(3) :606–609, 1994.

[65] J. Chen and H. Zhang. Robust detection of faulty actuators via unknown input observers. *International Journal of Systems Science*, 22, 1991.

[66] M. Darouach. Complements to full order observer design for linear systems with unknown inputs. *Applied Mathematics Letters*, 22 :1107–1111, 2009.

[67] V. Syrmos. Observer design for descriptor systems with unmeasurable disturbances. In *Proc. 31th. IEEE Conf. Decision Contr.*, Tucson, Arizona, USA, 1992.

[68] S. Kawaji and K. Sawada. Observer design for linear descriptor systems with unknown inputs. *IECON'91*, 1991.

[69] D. Koenig and S. Mammar. Design of proportional-integral observer for unknown input descriptor systems. *IEEE Trans. on Automat. Contr.*, 47(12) :2057–2062, 2002.

[70] A. L. Fradkov and A. Yu. Pogromsky. *Introduction to Control of Oscillations and Chaos*. World Scientific, Singapore, 1998.

[71] R. Kelly, V. Santibáñez, and A. Loría. *Control of robot manipulators in joint space*. Series Advanced textbooks in control engineering. Springer Verlag, 2005. ISBN : 1-85233-994-2.

[72] A. Loria and A. Zavala. Adaptive tracking control of chaotic systems with applications to synchronization. *IEEE Trans. on Circ. Syst. I : Regular Papers*, 54(9) :2019–2030, 2007.

[73] A. Loria, E. Panteley, D. Popovic, and A. R. Teel. δ-persistency of excitation : A necessary and sufficient condition for uniform attractivity. In *IEEE Conf. on Dec. and Contr.*, volume 3.

[74] A. Loria, E. Panteley, D. Popovic, and A. R. Teel. A nested matrosov theorem and persistency of excitation for uniform convergence in stable nonautonomous systems. *IEEE Transactions on Automatic Control*, 50(2) :183–198, 2005.

[75] M. Corless and J. Tu. State and input estimation for a class of uncertain systems. *Automatica*, 34 :757–764, 1998.

[76] A. Loria and S. Poinsard. Robust communication-masking via a synchronized chaotic lorenz transmission system. In *Conf. on Nonlinear Science and Complexity*, 2008.

[77] L. Fridman, J. Davila, and A. Levant. High-order sliding-mode observation for linear systems with unknown inputs. *Nonlinear Analysis : Hybrid Systems*, 5 :189–205, 2011.

[78] B. L. Walcott and S. Zak. State observation of nonlinear uncertain dynamical systems. *IEEE Trans. on Automat. Contr.*, 32 :166–170, 1987.

[79] X. Yan and C. Edwards. Nonlinear robust fault reconstruction and estimation using a sliding mode observer. *Automatica*, 43 :1605–1614, 2007.

[80] C. PinTan and C. Edwards. Sliding mode observers for detection and reconstruction of sensor faults. *Automatica*, 38 :1815–1821, 2002.

[81] W. Respondek. Right and left invertibility of nonlinear control systems. *Nonlinear controllability and optimal control, Dekker, New York*, 1990.

[82] H. Nijmeijer W. Respondek, A. Pogromsky. Time scaling for observer design with linearizable error dynamics. *Automatica*, 40 :277–285, 2004.

[83] M. Fliess. Generalized controller canonical forms for linear and nonlinear dynamics. *IEEE Transactions on Automatic Control*, 35(9) :994–1000, 1990.

[84] P. Martin M. Fliess, J. Levine and P. Rouchon. Flatness and defect of non-linear systems : Introductory theory and examples. *International Journal on Control*, 61(6) :1327–1361, 1995.

[85] G. R. Duan, A. G. Wu, and W. N. Hou. Parametric approach fo luenberger observers for descriptor linear systems. *Bull. of the Polish Academy of Sciences*, 55(1) :15–18, 2007.

[86] M. Boutayeb, M. Darouach, and H. Rafaralahy. Generalized state-space observers for chaotic synchronization and secure communication. *IEEE Trans. on Circ. Syst. I : Regular Papers*, 49 :271–280, 2002.

[87] R. J Patton, D. Putra, and S. Klinkhieo. Friction compensation as a fault tolerant control problem. *International Journal of Systems Science*, 41(8) :987–1001, 2010.

[88] C. Edwards and S. K. Spurgeon. *Sliding mode control : theory and applications*. Taylor and Francis, London, 1998.

[89] H. Khalil. *Nonlinear systems*. Prentice Hall, 3rd ed., New York, 2002.

[90] K. Kalsi, J. Lian, S. Hui, and H. Zak. Sliding-mode observers for systems with unknown inputs : A high-gain approach. *Automatica*, 46 :347–353, 2010.

[91] S. Yu, J. Lü, and G. Chen. A modulated-based and unified approach to chaotic circuit design and its applications. *Int J Bifurcat Chaos*, 17(5) :1785–1800, 2007.

[92] M. E. Yalcin, J. A. K. Suykens, and J. Vandewalle. Master-slave synchronization of lur'e systems with time-delay. *Int. J. of Bifurcat. and Chaos*, 11 (6) :1707–1722, 2001.

[93] J. Cao, H. X Li, and D. W. C. Ho. Synchronization criteria of lur'e systems with time-delay feedback control. *Chaos, Solitons and Fractals*, 23 :1285–1298, 2005.

[94] Q. L. Han. New delay-dependent synchronization criteria for lur'e systems using time delay feedback control. *Phys. Lett. A*, 360 :563–569, 2007.

[95] Q. L. Han. On designing time-varying delay feedback controllers formaster-slave synchronization of lur'e systems. *IEEE Trans. on Circ. Syst. I : Regular Papers*, 54 :1573–1583, 2007.

[96] S. M. Lee, S. J. Choi, D. H. Ji, J. H. Park, and S. C.Won. Synchronization for chaotic lur'e systems with sector-restricted nonlinearities via delayed feedback control. *Nonlinear Dyn*, 59 : 277–288, 2010.

[97] A. Germani, C. Manes, and P. Pepe. A new approachto state observation of nonlinear systems with delayed output. *IEEE Trans. on Automat. Contr.*, 47 (1) :96–101, 2000.

[98] N. Kazantzis and R. A. Wright. Nonlinear observer design in the presence of delayed output measurements. *Sys.& Control Letters*, 54 :877–886, 2005.

[99] F. Cacace, A. Germani, and C. Manes. An observer for a class of nonlinear systems with time varying observation delay. *Sys.& Control Letters*, 59 :305–312, 2010.

[100] T. Ahmed-Ali, E. Cherrier, and M. Msaad. Cascade high gain observers for nonlinear systems with delayed output. In *Proc. 48th. IEEE Conf. Decision Contr.*, pages 8226 –8231, Shanghai, China, 2009.

[101] V. Van Assche, T. Ahmed-Ali, C. A. B. Hann, and F. Lamnabhi-Lagarrigue. High gain observer design for nonlinear systems with time varying delayed measurements. In *18th IFAC World congress*, pages 692–696, Milano, Italia, 2011.

[102] D. H. Ji, J. H. Park, and S. C.Won. Master-slave synchronization of lur'e systems with sector and slope restricted nonlinearities. *Phys. Lett. A*, 373 :1044–1050, 2009.

[103] Q. L. Han. On designing time-varying delay feedback controllers for master–slave synchronization of lur'e systems. *IEEE Trans. on Circ. Syst. I : Regular Papers*, 54 (7) :1573–1583, 2007.

[104] A. Loria, F. Lamnabhi-Lagarrigue, and E. Panteley. *Advanced topics in control systems theory*. Series Lecture Notes in Control and Information Science, Springer Verlag, London, ISBN : 1-84628-313-2., 2005.

[105] V. L. Kharithonov. Lyapunov functionals and matrices. *Annual reviews in control*, 34, 2010.

[106] L.F. da Cruz Figueredo, J.Y. Ishihara, G.A. Borges, and A. Bauchspiess. New delay-and-delay-derivative-dependent stability criteria for systems with time-varying delay. In *Proc. 49th. IEEE Conf. Decision Contr.*, pages 1004–1009, Atlanta, USA, 2010.

[107] C. Zhu. A novel image encryption scheme based on improved hyperchaotic sequences. *Optics Communications*, 285(1) :29–37, 2010.

[108] F. Sun and Z .L. S. Liu. A new cryptosystem based on spatial chaotic system. *Optics Communications*, 283(10) :2066–2073, 2010.

[109] V. Patidar, N. Pareek, and K. Sud. A new substitution-diffusion based image cipher using chaotic standard and logistic maps. *Communications in Nonlinear Science and Numerical Simulation*, 14(7) :3056–3075, 2009.