Fiabilité de l'intégrité des informations par observateur à mémoire finie pour un système commandé en réseau

Julien Thuillier

INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

INSA Centre Val de Loire

ÉCOLE DOCTORALE
MATHÉMATIQUES, INFORMATIQUE, PHYSIQUE THÉORIQUE ET INGÉNIERIE DES SYSTÈMES

Laboratoire PRISME

THÈSE présentée par :

Julien THUILLIER

soutenue le : **16 décembre 2019**

pour obtenir le grade de : **Docteur de l'INSA Centre Val de Loire**
Discipline/ Spécialité : Sciences et Technologies industrielles/ Automatique

---

Fiabilité de l'intégrité des informations par observateur à mémoire finie pour un système commandé en réseau

---

THÈSE dirigée par :

Frédéric KRATZ	Professeur, INSA Centre-Val de Loire

RAPPORTEURS :

Mireille BAYART	Professeure, Université de Lille
Jean-Marie FLAUS	Professeur, Université Grenoble-Alpes

Président de jury :

Didier DUMUR	Professeur, Ecole CentraleSupelec

JURY :

Mireille BAYART	Professeure, Université de Lille, CRIStAL
Jean-Marie FLAUS	Professeur, Université Grenoble-Alpes, G-SCOP
Marion GILSON	Professeure, Université de Lorraine, CRAN
Didier DUMUR	Professeur, Ecole CentraleSupelec, L2S
Michel KINNAERT	Professeur, Université Libre de Bruxelles, SAAS
Frédéric KRATZ	Professeur, INSA Centre-Val de Loire, PRISME
David DELOUCHE	Enseignant Chercheur, HEI campus Centre, PRISME
Jacques FANTINI	Maître de Conférences, Université d'Orléans, PRISME

Table des matières

Liste des figures

Liste des tableaux

Lexique

API : Automate Programmable Industriel

CIA : Confidentiality Integrity Availability

ERP : Enterprise Resource Planning

FMO : Finite Memory Observer

IO : Internet des Objets

IIoT : Industrial Internet of Things

IoT : Internet of Things

IP : Internet Protocol

M2M : Machine to Machine

SCADA : Supervisory Control And Data Acquisition

SNCC : Système Numérique de Contrôle-Commande

TCP : Transmission Control Protocol

$\mathcal{N}(\mu, \mathbb{V})$: Loi binomiale de moyenne μ et de variance $\mathbb{V}$.

Remerciements

À mes parents,

Je remercie Frédéric KRATZ et David DELOUCHE pour leurs confiances, qu'ils m'ont accordée durant ces dernières années au sein du laboratoire PRISME sur les sites de HEI campus Centre, l'IUT de l'Indre et l'INSA Centre Val de Loire.

La rencontre, les échanges et les conseils que j'ai pu avoir avec Jacques FANTINI ont permi d'élargir mon approche des diverses thématiques liées à ma thèse. Je le remercie pour cela.

Je remercie le professeur Didier DUMUR d'avoir accepté d'être président de mon jury de thèse.

Je remercie la professeure Mireille BAYART et le professeur Jean-Marie FLAUS d'avoir accepté d'être mes rapporteurs ainsi que pour leurs remarques pertinentes m'ayant permis d'améliorer le contenu de mon manuscrit de thèse.

Je remercie les professeurs Marion GILSON et Michel KINNAERT d'avoir accepté de faire partie de mon jury.

Egalement une pensée à tous mes collègues proches sur ces différents sites de recherche.

Je remercie PRISME et plus particulèrement son directeur Azzedine KOURTA pour m'avoir reçu au sein de cette structure.

Introduction Générale

L'Internet des Objets (Internet of Things : IoT) est devenu une réalité puisque 79 milliards d'objets connectés devraient être déployés sur la planète à l'horizon 2020 [Forbes, 2020]. Le déploiement à grande échelle de l'Internet des Objets sera une des briques de base pour l'usine du futur. La capacité d'une "intelligence" embarquée dans les objets connectés ne permet pas actuellement à elle seule, d'assurer la conformité des échanges numériques. Ces objets sont dans l'incapacité d'effectuer un chiffrement de haut niveau tout en garantissant une qualité de service attendu notamment dans le cas du contrôle/commande de système. Dans ces conditions, il faut assurer aux données transmises une Confidentialité, une Intégrité et une Accessibilité (au sens de la disponibilité), contraintes connues sous l'acronyme CIA (Confidentiality-Integrity-and Availability)(Figure 1).

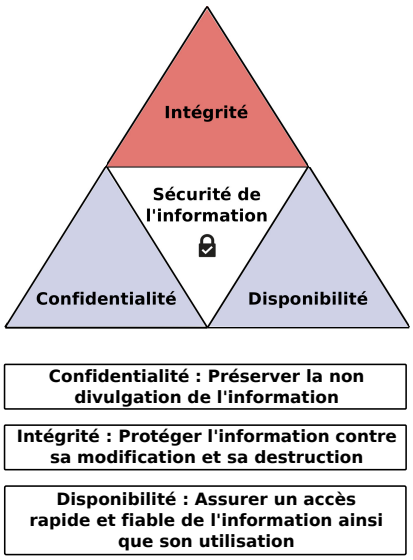


Figure 1 – Sécurité de l'information - Confidentialité, Intégrité et Disponibilité

L'arrivée des objets communicants dans le monde industriel a provoqué la quatrième révolution industrielle, appelée Industrie du futur ou Industrie 4.0 (Figure 2). L'efficience des

systèmes de production est au cœur des préoccupations actuelles. Dans ce contexte, il est incontournable de mettre en place une politique de maintenance prédictive. Les échanges numériques de type Tout IP sur lesquelles reposent l'Internet des Objets (IO) ne sont pas déterministes (c'est-à-dire que l'information est émise mais sa réception n'est pas garantie).

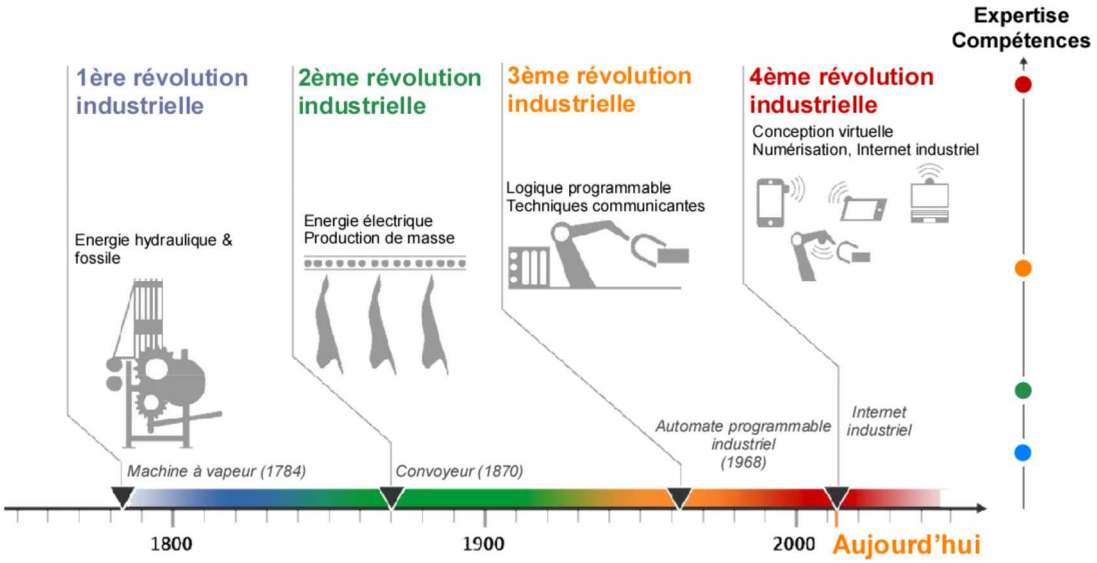


Figure 2 – Croissance des objets connectés, [Blanchet et Bergerried, 2014]

Suite à un appel à projet - Initiative Académique de la région Centre-Val de Loire les laboratoires LIFO et PRISME ont déposé conjointement un projet (IoT-CIA) dont l'objectif vise à garantir l'intégrité et la fiabilité des informations numériques au cours de leur cycle de vie dans le cadre d'un environnement SCADA (Système de Contrôle et d'Acquisition de Données). Dans ces conditions, le défi des travaux engagés résidera à concevoir un outil capable de détecter différentes attaques (par exemples : perte de paquets, délai de transmission aléatoire, congestion, données manquantes ...).

Le manuscrit est organisé en quatre chapitres.

Chapitre 1 : Une présentation du contexte des systèmes interconnectés vis-à-vis de leur sécurité sera réalisée afin d'introduire notre contribution à l'élaboration d'outils permettant de garantir l'intégrité des données transitant dans ces systèmes. Une présentation des systèmes comportant des incertitudes sera également réalisée afin d'introduire l'extension d'outils à ce cas de figure.

Chapitre 2 : L'outil que nous proposons repose sur une estimation des états du système. Nous avons fait le choix d'utiliser un observateur à fenêtre glissante, connu dans la littérature sous le nom d'observateur à mémoire finie [Medvedev et Toivonen, 1992]. Une description de

l'observateur à mémoire finie sera réalisée dans ce chapitre. Puis, nous présenterons différentes propriétés de cet observateur utiles à nos travaux. Enfin, la conception d'outils à base d'observateur à mémoire finie pour le cas de perte de paquets et de perte d'intégrité sera réalisée afin de répondre aux problématiques concernant la sécurité des systèmes interconnectés.

Chapitre 3 : Le chapitre 3 propose une extension de l'observateur à mémoire finie de manière à pouvoir traiter le cas des systèmes présentant des incertitudes de modélisation (FMO à intervalle) ainsi que le cas des systèmes où bruits de mesures et bruits d'états sont corrélés (problème que l'on rencontre, par exemple dans le calcul du positionnement d'un mobile par fusion de données [Mambou Kuipou, 2016])

Chapitre 4 : Dans ce dernier chapitre, une partie sera consacrée à la modélisation de systèmes télé-opérés. L'objectif de ce chapitre est de présenter le comportement de certains de nos outils pour ce type de systèmes sensibles soumis à des attaques plus élaborées.

La recherche présentée dans ce manuscript de thèse a été financée par la Région Centre-Val de Loire dans le cadre du projet APR IA IoT-CIA.

Chapitre 1

Introduction aux systèmes interconnectés en réseau

Contenu du chapitre

1.1 Introduction

Ce chapitre a pour objectif de présenter le contexte de nos travaux de thèse dont la thématique concerne les nouvelles problématiques rencontrées sur les systèmes interconnectés par un réseau de communication et plus particulièrement les conséquences sur la sécurité et la sûreté des installations industrielles comportant de tels systèmes.

Dans un premier temps, les réseaux industriels, l'interconnexion des sous-systèmes ainsi que les échanges de données sont définis, décrits et analysés. Ensuite, l'aspect sécurité de ces systèmes sera abordé au travers de différents éléments. Plus particulièrement, nous nous intéressons à l'influence des incertitudes de modélisation sur le fonctionnement du système ainsi qu'aux aspects *intégrité* et *disponibilité* des données dans les réseaux de communcation. Un focus sur les méthodologies utilisées dans le cadre de la problématique traitée est également proposée. Il est évident que de part la richesse de la littérature dans ces domaines, l'état de l'art présenté ne sera pas exhaustif.

1.2 Systèmes interconnectés en réseau

La transition numérique, apportée par le concept de l'usine du futur, ou industrie 4.0 (voire cyber-usine), au sein des installations industrielles, repose sur le développement et l'utilisation croissante de systèmes connectés par des réseaux de communication. Cette transformation s'effectue à la fois par l'extension de la masse de données transitant dans le réseau mais également par la pluralité des types de réseau industriels. En effet, aujourd'hui les fonctionnalités de suivi de production, de supervision et de maintenance sont principalement réalisées grâce à la mise en réseau des entités composant un ensemble de systèmes (*exemple :* ligne de production, avion, centrale électrique, ...).

1.2.1 Réseaux industriels et échange de données

Les architectures de transmissions de données IIoT (Industrial Internet of Things) et M2M (Machine to Machine) partagent l'utilisation d'un réseau local et permettent la circulation de données provenant d'objets industriels communiquants : capteurs, actionneurs, Automates Programmables Industriels (API), ... ([Mukhopadhyay, 2014] et [Lele, 2019]).

De manière historique, le câblage des équipements électriques industriels était uniquement assuré par des liaisons fil à fil. L'émergence de l'usine du futur et des technologies de communication a orienté la conception et l'utilisation de matériels connectés. Cherchant à tirer les bénéfices de cette évolution de ces nouveaux équipements (simplification du câblage, coût, échanges importants de données, ...), l'architecture des communications des systèmes

industriels s'est orientée vers une structure à quatre niveaux distincts mais interconnectés :

— Niveau 0 : capteurs,
— Niveau 1 : machine,
— Niveau 2 : atelier (localisation et gestion des lots),
— Niveau 3 : entreprise (ERP)

Les différents niveaux correspondent à des besoins ou des caractéristiques à satisfaire (Figure 1.1). Parmi ces besoins, nous retrouvons entre autre le temps de réponse de l'équipement, le volume d'échange de données (nombre et fréquence des échanges de données) et l'interopérabilité.

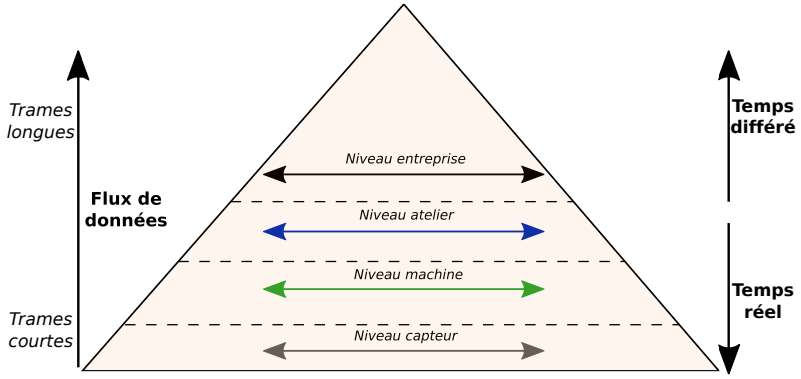


Figure 1.1 – Flux de données - CIM ([Debaene et Vidal, 1990])

Ces différents niveaux interopérables entre eux communiquent à l'aide de routeurs, de passerelles, d'automates programmables industriels et de concentrateurs. Un exemple des différents niveaux et des interconnexions associées est illustré par la Figure 1.2.

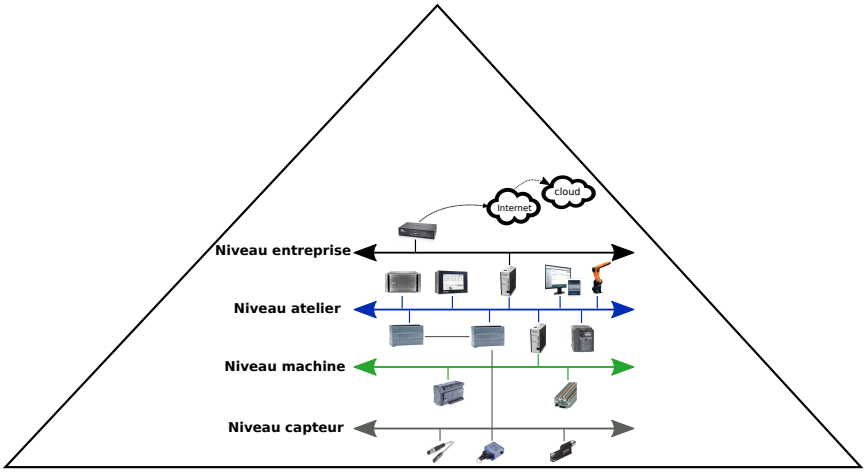


Figure 1.2 – Réseau pyramide - CIM

1.2.1.1 Topologies des réseaux industriels

Les différentes technologies utilisées par les différents niveaux des réseaux impliquent l'organisation d'une structuration des composants au sein de l'installation. La topologie structure l'échange des informations au niveau des réseaux. Parmi les topologies existantes citons la topologie en bus, en étoile, en anneau et maillée ([Knezic *et al.*, 2010] et [Trinquet et Elloy, 2010]).

Le développement des technologies et la baisse des coûts des équipements industriels communicants permettent une constante évolution sur l'utilisation de nouveaux objets connectés. Parmi ceux-ci, on note l'apparition de capteurs communiquants appelés également capteurs connectés qui aujourd'hui intègrent une partie opérative permettant de générer et traiter des informations supplémentaires utiles à la bonne gestion du système tant pour le suivi de production que pour la maintenance.

1.2.1.2 Capteurs connectés

Le développement de la maîtrise de systèmes complexes implique la mise en place d'un nombre de plus en plus important de capteurs. Parallèlement, la demande croissante de traitements numériques locaux de plus en plus complexes a imposé aux capteurs de posséder des unités de calcul. Ces derniers possèdent également un composant permettant la mise à disposition des données aux utilisateurs via le réseau de communication. Un schéma simplifié, construit autour d'un capteur traditionnel, présente le capteur connecté en Figure 1.3.

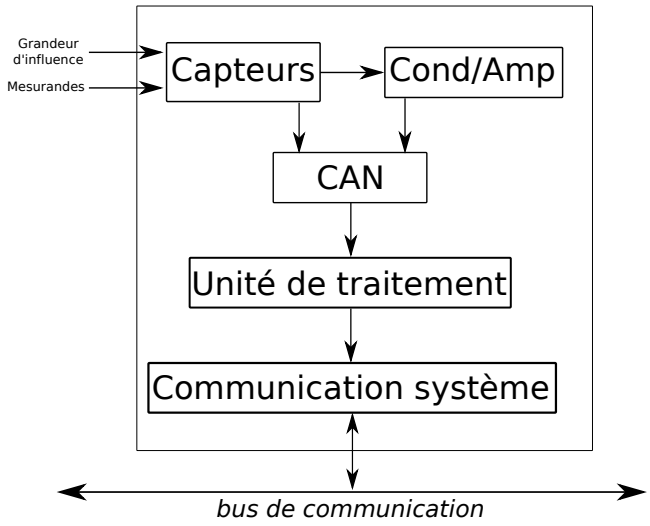


Figure 1.3 – Structure d'un capteur intelligent

Telle que présentée par ([Kyung *et al.*, 2016], [Yasuura *et al.*, 2017] et [Kim et Tran-Dang, 2019]), la virtualisation des objets physiques est l'essence même de l'Internet des objets, permettant à ceux-ci d'être connectés et de communiquer dans un

cyber-espace. Le fonctionnement de systèmes interconnectés nécessite d'intégrer la virtualisation des fonctions des capteurs, des actionneurs, des traitements, des tâches de diagnostic (surveillance de processus, détection, filtrage et analyse de données), de contrôle-commande, de communication ainsi que la gestion de l'énergie.

Les travaux ([Peng *et al.*, 2015], [I-Scoop, 2017] et [Gravina *et al.*, 2018]), montrent que pour chaque équipement, il existe de multiples compositions entre grandeur physique mesurée, protocole de communication, technologie.... Cette pluralité des offres proposées participe à l'expansion des équipements connectés et donc au développement des systèmes interconnectés.

1.2.1.3 Réseau de communication

Dans un scénario de transitions des communications vers des solutions IIOT ou M2M, les problématiques de coût, d'entretien, de maintenance et d'efficience orienteront le choix des architectures, des technologies et des équipements utilisés [Zervakis, 2019].

L'utilisation de technologies de communicantion via un réseau (ex : réseau filaire ou sans fil), permet de réduire les coûts d'installation et de maintenance. Néanmoins, l'aspect sûreté de fonctionnement du système et la sécurité des informations doivent nécessiter une étude afin de garder ou de garantir un certain niveau de sûreté. C'est ce point qui est le plus complexe lors de la conception et la réalisation de l'architecture réseau pour les systèmes interconnectés, d'où un grand nombre de travaux sur la résilience de ces nouvelles technologies ([Neumann, 2007], [Gertsbakh et Shpungin, 2011], [Frotzscher *et al.*, 2014], [Ali, 2019], ...). De nombreux travaux se sont également intéressés à la performance des réseaux et des protocoles associés ([Tovar et Vasques, 1999], [Decotignie, 2005], [Dang et Devic, 2008], [Peijiang et Xuehua, 2008], [Prytz, 2008], [Yi *et al.*, 2011] et [Adame *et al.*, 2014]).

Le choix parmi les différentes architectures réseaux est motivé par la flexibilité offerte et dans certains cas par la réduction de la longueur de cablâge nécessaire ou de la facilité de déploiement ([Thomesse, 2005], [Morel *et al.*, 2007] et [Gaj *et al.*, 2013]).

Ces technologies répondent aux problématiques de communication, menant les systèmes à être connectés et plus vraisemblablement, avec le temps, totalement interconnectés.

1.2.2 Structure des systèmes interconnectés

Les systèmes interconnectés en réseau présentés dans [Xia *et al.*, 2011], [Kyriakides et Polycarpou, 2015] et [Garas, 2016] sont des systèmes dont les entrées et sorties (consigne, commande, mesures, ...) sont reçues et/ou transmises par un réseau de communication (Figure 1.4) et dont l'analyse à fait l'objet de différents articles ([Wang et Liu, 2008], [Pietrabissa et Priscoli, 2009] et [Blume, 2016]).

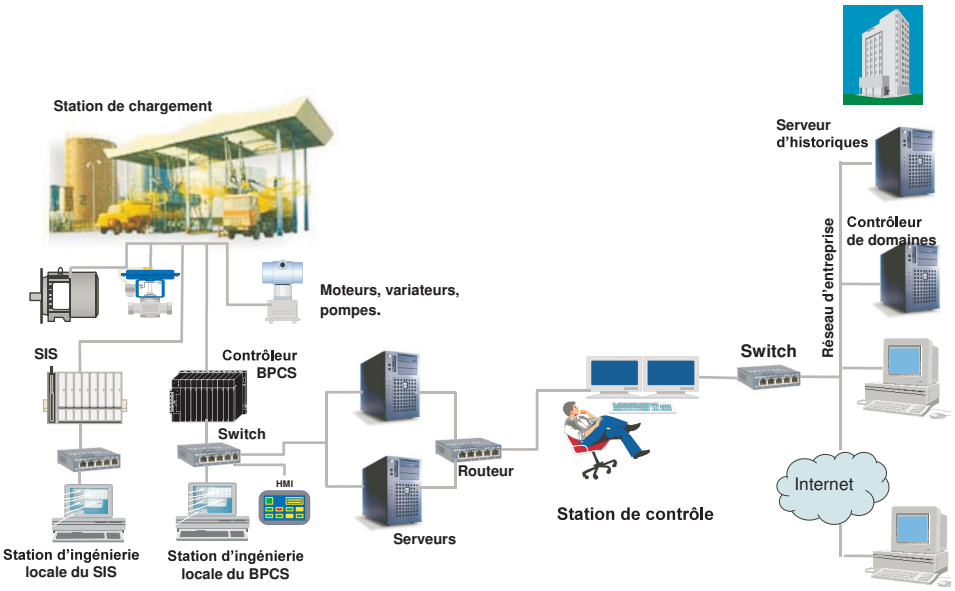


Figure 1.4 – Exemple d'une station de remplissage de camions en produits chlorés, [Hauet, 2016]

La Figure 1.5 représente un ensemble de deux systèmes interconnectés. Le système numéro 1 reçoit ses commandes et envoie ses mesures à l'API A. Cet API reçoit également les données du système numéro 2 grâce aux capteurs IoT (site déporté) et redirigées vers un réseau de communication principal. Les éléments de supervision, de maintenance, de serveurs et de cloud sont également présents afin d'assurer toutes les tâches inhérentes à la maintenance et la gestion de production.

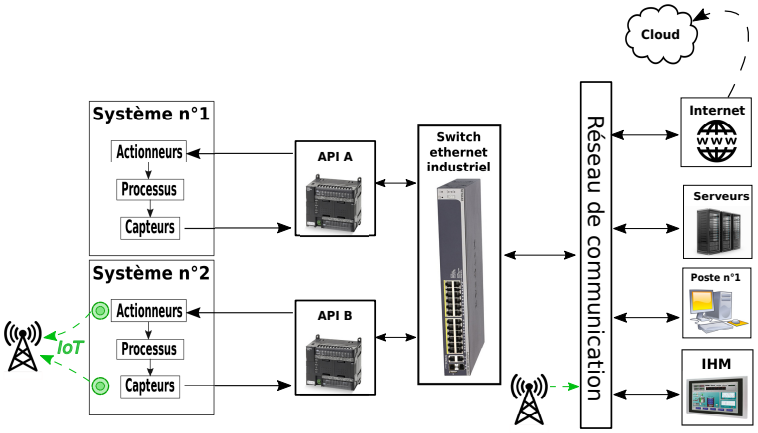


Figure 1.5 – Système industriel interconnectés en réseau

Les principaux avantages et inconvénients rencontrés dans l'utilisation de systèmes interconnectés sont :

Avantages :

— facilité d'installation,
— aide à la maintenance,
— très bon rapport coût/efficacité,
— ...

Inconvénients :

— problématique des perturbations réseau : perte de paquets, retard, congestion ...
— risque de cyber-attaque,
— ...

1.2.3 Modélisation des systèmes interconnectés en réseau

Les travaux de cette thèse, s'appuient sur la représentation d'état linéaire à temps continu afin de caractériser les modèles des systèmes étudiés. La représentation d'état classique sera adoptée, sachant que les composantes des entrées et des sorties sont reçues ou envoyées sur le réseau de communication (Figure 1.6).

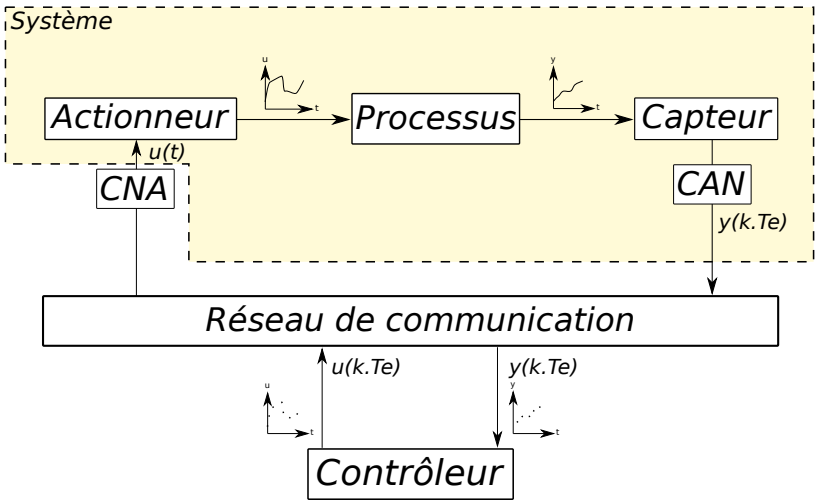


Figure 1.6 – Représentation d'un système interconnecté

La représentation d'état d'un système interconnecté en réseau est donnée par :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(k * Te) = Cx(k * Te) + v(k * Te) \end{cases} \tag{1.1}$$

avec les matrices de la représentation d'état A, B et C de dimensions appropriées, $x \in \mathbb{R}^n$ est le vecteur d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée, $y \in \mathbb{R}^p$ est le vecteur de mesure et $v \in \mathbb{R}^p$ est le vecteur de bruit de mesure. Te est la période d'échantillonnage (dans la suite du manuscript, cette période d'échantillonage est implicite dans l'équation de mesure : $y(k) = Cx(k) + v(k)$ et $k \in \mathbb{N}$ représente l'indice de l'échantillon.

Cette représentation continue pour l'évolution de l'état et discrète pour la mesure, présente l'avantage de garder la signification physique de l'état obtenue par la modélisation et la prise en compte de la réalité de l'instrumentation avec une mesure échantillonnée.

De plus, ce choix de la représentation d'état permet d'intégrer plus facilement les éventuelles perturbations inhérentes au réseau et d'obtenir une présentation plus claire des échanges et de leurs impacts. Dans la suite de ce chapitre, les différentes perturbations réseau, leurs comportements et le choix de leurs modélisations sont abordés.

1.3 Sécurité des systèmes interconnectés et cyber-attaque

1.3.1 Sécurité de l'information

Le développement et l'augmentation du volume des communications amènent à diffuser toutes les informations, y compris celles classées sensibles. L'ouverture des réseaux pose la question de la sécurité des données transitant au sein des réseaux industriels. Plus particulièrement, nous nous focalisons sur les aspects de confidentialité, intégrité et disponibilité des données. Le modèle de sécurité *CIA* (Confidentiality, Integrity and Availability) traite de ces aspects de sécurité de l'information (Figure 1.7), ([Evans *et al.*, 2004], [Grance *et al.*, 2004], [Chaeikar *et al.*, 2012], [Von Solms et Van Niekerk, 2013] et [Teixeira *et al.*, 2015]).

Plus particulièrement, ce modèle permettra de traiter la sécurité de l'information selon les trois critères :

— **Confidentialité :** Elle assure le non-accès des données à des personnes non autorisées, et assure à celles autorisées l'exclusivité d'accès. Bien souvent, la confidentialité des données est implémentée au travers de mécanismes de cryptage, de mots de passe et de l'utilisation de protocoles spécifiques. Un tri du niveau de confidentialité des données lors de la phase de développement d'un système est réalisé, afin de minimiser la mise en place de ces mécanismes de protection.

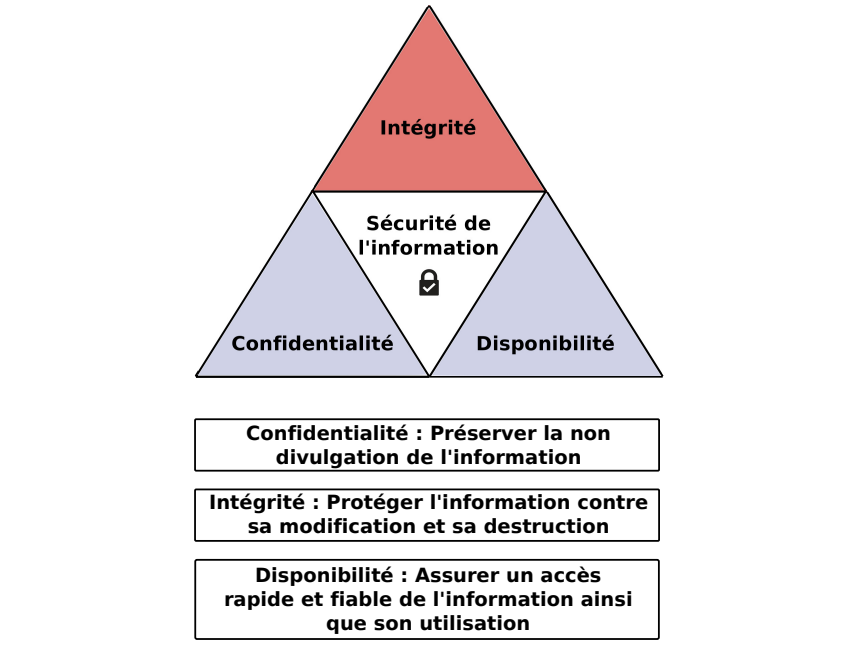


Figure 1.7 – Schéma - Confidentialité, Intégrité et Disponibilité

La Figure 1.8 présente la perte de confidentialité des mesures du système. La mesure y_k (en l'occurrence [2 13]) est ici captée par un adversaire sur le réseau de communication.

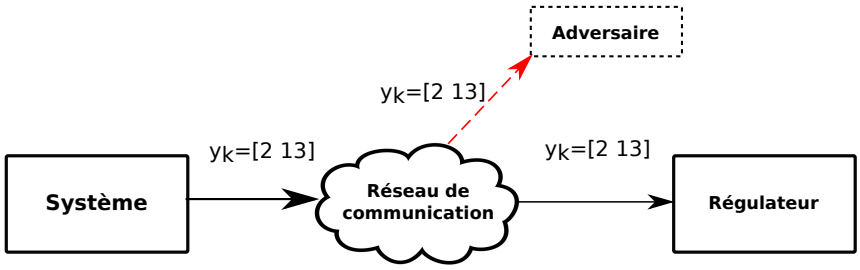


Figure 1.8 – Confidentialité

— **Intégrité :** L'intégrité des données caractérise la validité des données, selon leurs formats, leurs valeurs. Elle permet, entre autre de maintenir la correspondance des données reçues par rapport aux données originales communiquées. Ainsi, les personnes ou les appareils autorisés peuvent modifier le contenu des données. Les procédés de cryptage et de *hash* (également appelé tatouage numérique) sont implémentés pour maintenir l'intégrité des données.

La perte d'intégrité présentée sur la Figure 1.9 montre que les données transmises par

le système ([2 13]) vont être modifiées par l'ajout des valeurs [3 1] injectées par un adversaire. Cette injection tend à modifier les informations reçues par le régulateur afin d'orienter le système vers un mode de fonctionnement imposé par l'adversaire.

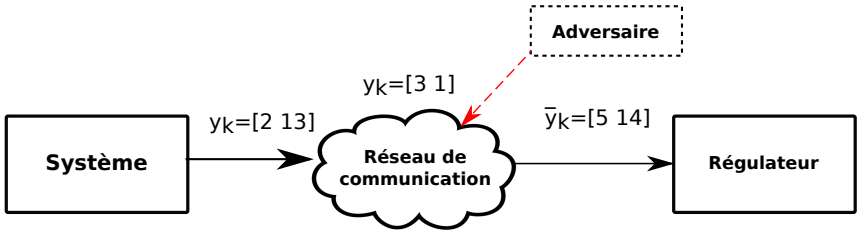


Figure 1.9 – Intégrité

— **Disponibilité :** Elle permet d'assurer aux données d'être reçues et disponibles à temps aux éléments les nécessitant. Le matériel hardware et l'optimisation des réseaux permettent de répondre à cette problématique.
Sur la Figure 1.10, il apparait que les données envoyées à travers le réseau de communication ne sont pas reçues en temps requis par le régulateur. Cette disponibilité peut être menacée par des phénomènes de retards ou de pertes de paquets provoqués par la nature du réseau de communication ou de la part d'une personne malveillante présente sur ce réseau.

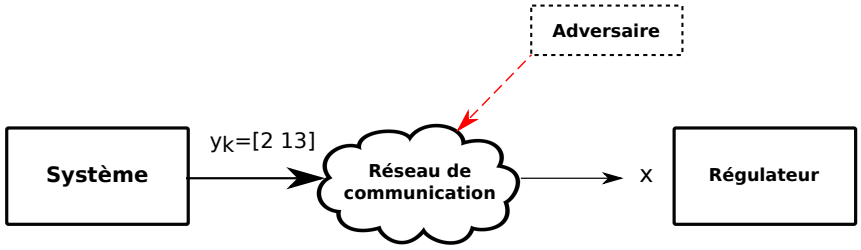


Figure 1.10 – Disponibilité

1.3.2 Risques industriels

Suite aux évènements du 11 septembre 2001, où des terroristes étaient arrivés à se former au pilotage d'avions sophistiqués, la nécessité d'être attentif à la sécurité des systèmes automatisés et au contrôle de procédé est apparue évidente aux USA ainsi qu'en Europe. En effet, cet acte montrait la possibilité pour des terroristes de s'initier au fonctionnement des systèmes contrôlant des infrastructures stratégiques : alimentation en eau, centrales et réseaux électriques,

moyens de transports, installations réputées sensibles : chimie, pharmacie, agro-alimentaire.

Risque d'autant plus accru, que depuis la fin des années 1990, l'informatique s'est largement introduite dans les systèmes de contrôle :

— au niveau des réseaux, avec Ethernet, TCP-IP, les connexions à Internet,
— au niveau des équipements, avec l'usage de matériels non spécifiques et l'utilisation croissante de systèmes d'exploitation grand public tel que Microsoft (Windows).

Cette évolution a été bénéfique sur le plan des coûts et des fonctionnalités, en permettant un accès aux données de production et aux historiques depuis l'informatique de gestion, ainsi qu'un accès distant, pour la collecte d'information, la configuration et la maintenance. Cela a également permis une ouverture au partenariat d'ingénierie par l'utilisation d'outils communicants. Toutefois, les points d'accès aux systèmes de contrôle ont été multipliés et il devient aujourd'hui difficile de savoir qui est autorisé à accéder à un système d'information, quand cet accès est autorisé et quelles données peuvent être rendues accessibles.

Après la banalisation des équipements de traitement de l'information, le développement des réseaux locaux de radiocommunications, du type Wi-Fi, ZigBee, Bluetooth, dans des bandes de fréquence ouvertes à tous, va générer de nouveaux points d'entrée possibles dans les systèmes de contrôle et donc potentiellement de nouvelles failles sécuritaires.

La sécurité dont il est ici question, concerne la prévention des risques associés à des interventions malintentionnées sur des systèmes programmés de contrôle de procédé (SCADA, SNCC, API...) s'appuyant sur les techniques, matérielles ou logicielles, du monde de l'informatique et sur les réseaux de communication, y compris des réseaux sans fil. Les auteurs de ces interventions peuvent être des "professionnels" de l'intrusion frauduleuse, y compris des criminels ayant des visées terroristes. Mais ils peuvent être plus simplement des "hackers" faisant du piratage leur distraction favorite et utilisant des logiciels téléchargés sur Internet, des concurrents peu scrupuleux, ou bien des personnels de l'entreprise ou l'ayant récemment quittés et ayant, pour une raison ou pour une autre, une réelle intention de nuire. Souvent d'ailleurs les tentatives passent inaperçues et sont découvertes très tardivement. Cependant beaucoup d'articles publiés font état d'un nombre croissant de tentatives non autorisées d'accès à des systèmes d'information dédiés au contrôle [KEMA, 2005], [Symantec Corporation, 2010] et [Kaspersky Laboratory, 2018].

1.3.2.1 Perte de l'intégrité des données

Un nouveau type d'assaillant possédant des connaissances en informatique et automatique pourrait tenter de corrompre les données transitant sur le réseau afin de modifier le fonctionnement d'un système. Cette modification, pouvant être appelée "intelligente" affecte

l'intégrité des données des réseaux industriels. L'intégrité est de plus en plus menacée face aux attaques visant à modifier les données, étant donné l'expansion rapide d'équipements électriques communicants. Ces attaques sont parfaitement intégrées au sein des systèmes industriels, transparentes vis-à-vis des organes de sécurité et permettent à l'assaillant des modifications importantes sur les installations pouvant aller jusqu'à la destruction. Le prochain paragraphe, définit deux catégories d'attaques sur les systèmes industriels.

Attaque modifiant le comportement et les informations transmises par l'API :

Ce type d'attaque est généré après l'intégration dans un API d'un code malveillant. Ce dernier, cherchera sur certains points de fonctionnement, à modifier dans la plupart du temps les commandes générées et envoyées vers les actionneurs. Cette modification doit être confinée dans une zone acceptable (cohérence des données) par le système afin de garantir l'invisibilité de l'attaque, notamment vis-à-vis des automates de sécurité et de la supervision. Concernant la supervision, le code malveillant peut tout à fait être conçu afin d'alimenter celle-ci en données considérées correctes, masquant ainsi celles de l'attaque réellement envoyées. La réalisation de ces cas d'attaques s'appuient sur deux contraintes :

— La non visibilité du code malveillant dans le code original de l'API. Ceci par l'effacement du code malveillant et une réécriture constante du programme de ce code contenu dans l'API (de manière automatique par le code malveillant lui même ([Langner, 2011]).

— La modification ne peut quasiment être réalisée que sur la commande envoyée. Pour être efficace cette attaque doit correspondre à des modifications de commande en cohérence avec le système mais cherchant à modifier l'efficacité ou à rendre instable le système.

Attaque modifiant les données transitant sur le réseau :

Les attaques modifiant l'intégrité des données en transit sur le réseau de communication, possèdent les avantages de pouvoir être plus facilement non détectables et mener le système vers un fonctionnement anormal ou tout du moins avoir suffisamment de temps pour réaliser des dommages. En effet, l'accès des données portant sur les mesures et les commandes par la modification d'intégrité peut chercher à faire dévier le système de sa trajectoire de fonctionnement, en gardant un niveau de cohérence du modèle (entrées/sorties) satisfaisant pour la plupart des outils traditionnels de diagnostic.

Néanmoins, cette attaque nécessite elle aussi deux pré-requis :

— L'accès au réseau de communication et la modification de(s) donnée(s) en transit,

— La connaissance du fonctionnement du système et de ses équipements (régulateur, supervision, outil de diagnostic implémenté).

Ce type d'attaque est donc réalisé par l'association de deux profils de personne, la première avec un profil orienté sécurité des réseaux et la deuxième compétente en ingénierie des systèmes automatisés et du diagnostic. L'avantage étant ici, une non visibilité immédiate des modifications par les organes de sécurité traditionnels.

Exemple d'attaque :

L'attaque Stuxnet (étudiée par [Langner, 2011]) est l'une des premières de ce type avec un impact considérable sur les installations. Cette attaque des automates programmables industriels modifiait le fonctionnement de la régulation des centrifugeuses. Une fois la tâche de la machine effectuée, il ne paraissait aucun changement dû à l'attaque au sein de l'automate programmable industriel.

L'attaque contre une centrale de production d'énergie électrique d'Ukraine (dont la provenance est explicitée par ([Hultquist, 2016] et [Security, 2018]) modifiait les données de mesure et de commande sur le réseau de communication menant à la perte de puissance puis à l'îlotage de la centrale électrique (mode de repli). Un nombre important de travaux se sont intéressés à la possibilité de nouvelles attaques plus complexes ([Liu *et al.*, 2009], [Kundur *et al.*, 2010], [Chen *et al.*, 2012], [Kim et Tong, 2013] et [Bretas *et al.*, 2017]). Le Tableau 1.1 représente une liste non-exhaustive de différentes attaques ayant eu cours sur des systèmes industriels.

1.3.2.2 Perturbations réseaux

Les perturbations réseaux concernent les propriétés des réseaux de communication et des protocoles associés. Les systèmes interconnectés en réseau nécessitent un flux de données important sur les réseaux, tout en possédant une bande passante limitée en fonction de leurs technologies.

La surcharge des réseaux peut conduire à une perte de données, à un retard de transmission ou à une congestion du réseau. Mais, il existe également des menaces extérieures provoquant ce type de perturbations sur les réseaux dans le but de ralentir voire arrêter le fonctionnement du système.

Dans les deux cas, ces perturbations ne permettent pas aux données d'être reçues en temps voulu ou d'être reçues tout simplement par leurs destinataires. Les conséquences de ces perturbations peuvent être un dysfonctionnement ou arrêt du système. Ces perturbations sur les entrées/sorties sont présentées par la Figure 1.11.

Années	**Nom de l'attaque**	**Méthodologies et conséquences**	**Publications**
2007-2010	Stuxnet	Impact sur la régulation des centrifugeuses	[Karnouskos, 2011], [Langner, 2011]
2011	Duqu	Récupération d'information	[Bencsáth *et al.*, 2012a], [Bencsáth *et al.*, 2012b]
2011	*	Corruption de la partie SCADA impliquant des perturbations sur la fourniture d'énergie	[Giani *et al.*, 2011], [Kosut *et al.*, 2011], [Mo *et al.*, 2012]
2017	Petya	Blocage et effacement de données impliquant une interruption d'activité d'un nombre important d'entreprises	[Symantec Corporation, 2002], [Vasiliadis *et al.*, 2015]
2017	Triton	Tentative de modification de données afin d'outrepasser les fonctions de contrôle des système de sécurité inter-automate	[Baliga *et al.*, 2014], [Mansfield-Devine, 2018]

Tableau 1.1 – Tableau présentant des attaques sur des systèmes industriels

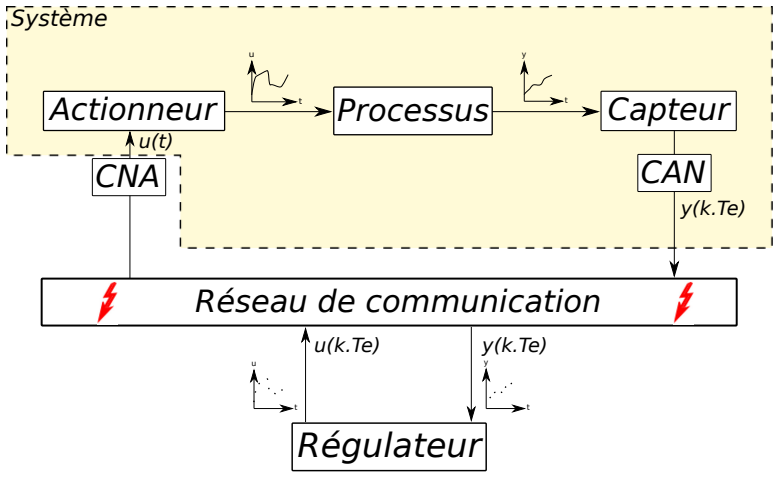


Figure 1.11 – Envoi et réception des données pour un système interconnecté en présence de pertes de paquets

Les différentes perturbations que nous allons prendre en compte sont :

Pertes de données :

De nombreux travaux se sont intéressés à la problématique des pertes de données sur les systèmes ([Lin *et al.*, 2003], [Zhang *et al.*, 2013] et [Liu *et al.*, 2018]). Parmi ces travaux, plusieurs auteurs apportent une solution au sens de l'automatique par l'utilisation d'observateurs et/ou filtres.

L'observateur à horizon glissant a été majoritairement utilisé pour répondre à cette problématique pour les systèmes linéaires ([Liu *et al.*, 2012], [Wu *et al.*, 2012] et [Liu *et al.*, 2013]) et non linéaires ([Alessandri *et al.*, 2007], [Wang *et al.*, 2007] et [Li *et al.*, 2010]). En effet, les propriétés intrinsèques à ce type d'observateur qui utilisent une fenêtre temporelle sont efficaces dans le cadre de ces perturbations.

Retard de transmission :

Concernant les retards de transmission, une pluralité de classes d'observateurs existent. Les principaux travaux traitent les problématiques liées au retard de transmission sur les commandes par une solution H_∞ ([Wu *et al.*, 2012] et [Jiang et Fang, 2014]). Les filtres, dans le cas de la détection de défaut, ont été proposés par [Shi *et al.*, 2009] et [Wan *et al.*, 2012] ainsi qu'une approche par observateurs distribués par [Lu *et al.*, 2015].

Congestion du trafic :

L'augmentation du trafic du réseau peut ajouter des phénomènes de file d'attente sur les données en émission et en réception. Afin d'être dans la capacité de permettre au système d'émettre et de recevoir les données de manière correcte d'un point de vue temporel, les travaux suivants ([Kubo *et al.*, 2008], [Zhou *et al.*, 2008] et [Wang *et al.*, 2010]) ont apporté des solutions à l'aide d'observateurs pour la gestion du trafic lors de congestion. La détection de ces congestions a été traitée dans différents travaux dont [Chiabaut *et al.*, 2009] et [Harrou *et al.*, 2018].

Modélisation de la perte de paquets et des retards :

La modélisation des perturbations réseaux est très souvent dans la littérature représentée par un processus stochastique dynamique. Les travaux de [Jia *et al.*, 2005], [Flavia *et al.*, 2006] et plus récemment [Jungers *et al.*, 2018] et [Tanwani *et al.*, 2019] proposent de modéliser ces perturbations à l'aide d'un automate fini et plus spécifiquement sous forme d'une chaine de Markov. Cette modélisation est intégrée à celle du système, afin de prendre en compte les pertes occasionnées éventuellement sur les données d'entrées et de sorties circulant dans le réseau.

Considérons la structure à base de chaine de Markov proposée par [Jungers *et al.*, 2018] composée de deux états $\phi = 0$ et $\phi = 1$, correspondant respectivement à la non apparition et la réalisation d'une perturbation (retard ou perte de paquets) à chaque instant d'échantillonnage k (cf. Eq. (1.1)).

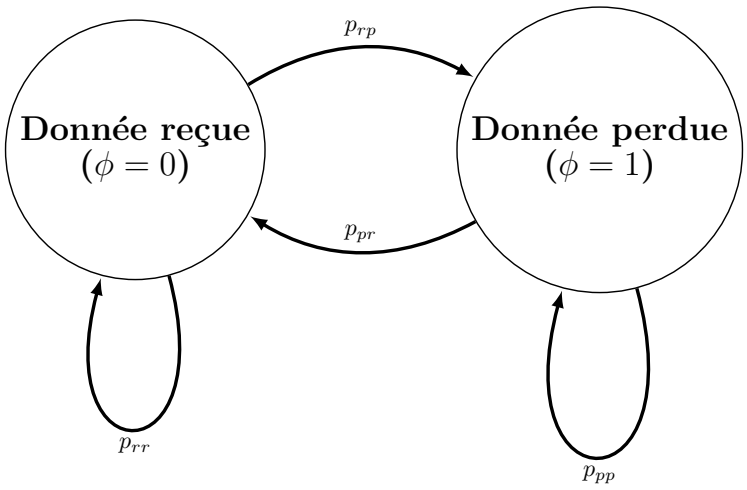


Figure 1.12 – Chaine de Markov modélisant la perte de paquets

Les transitions entre états sont définies par le système d'équation :

$$\begin{cases} \mathbb{P}\{\phi(k+1)=0|\phi(k)=0\} = p_{rr} \\ \mathbb{P}\{\phi(k+1)=1|\phi(k)=0\} = p_{rp} \\ \mathbb{P}\{\phi(k+1)=1|\phi(k)=1\} = p_{pp} \\ \mathbb{P}\{\phi(k+1)=0|\phi(k)=1\} = p_{pr} \end{cases} \tag{1.2}$$

Les probabilités associées correspondent à :
— p_{rr} probabilité de transition de donnée reçue à donnée reçue,
— p_{rp} probabilité de transition de donnée reçue à donnée perdue,
— p_{pp} probabilité de transition de donnée perdue à donnée perdue,
— p_{pr} probabilité de transition de donnée perdue à donnée reçue.

Ces différentes probabilités peuvent être modélisées sous forme matricielle, appelée matrice de transition, notée P, et définie par :

$$P = \begin{pmatrix} p_{rr} & p_{rp} \\ p_{pr} & p_{pp} \end{pmatrix}$$

Une autre représentation graphique de cette matrice est donnée par la chaine présentée Figure 1.12. Cette représentation permet de simuler les différents scénarios possibles de l'apparition de la perturbation. Évidemment, les statistiques obtenues à partir de l'étude des occurrences des perturbations sur un système réel permettent d'obtenir une expression quantitative des probabilités utilisées dans l'Eq. (1.2).

Si pour des raisons pratiques, nous sommes amenés à prendre en compte un nombre maximal de pertes consécutives de paquets, la modélisation par une chaîne de Markov doit prendre en compte l'historique. Un exemple de chaine de Markov modélisant trois pertes consécutives de paquets au maximum sera présenté.

1.4 Système comportant des incertitudes

Des attaques peuvent être conçues afin d'exploiter les incertitudes de modèle afin de rester "transparentes" pendant une certaine durée. Celles-ci modifient les données afin de les faire évoluer dans le domaine des incertitudes. Ce comportement a pour objectif de ne pas alerter les outils de surveillance associés à ces modèles.

Dans le cadre de nos travaux de thèse, nous nous sommes intéressés à deux types d'incertitudes pouvant modéliser une classe de systèmes rencontrés : les incertitudes paramétriques et les bruits corrélés.

1.4.1 Modèle avec incertitudes paramétriques

Certains paramètres du modèle mathématique décrivant le comportement physique de systèmes réels sont connus avec une certaine précision. Ces éléments d'incertitudes sur les valeurs numériques des paramètres du modèle proviennent de la méthode de mesure de cette valeur, de la précision de l'algorithme d'identification utilisé pour obtenir cette valeur, de la variabilité de la dynamique négligée de ce paramètre, ...

L'étude de ces systèmes, appelés également systèmes incertains, a conduit à différentes modélisations en fonction des incertitudes, et est largement discutée dans les travaux ([Weinmann, 1991], [Bubnicki, 2007] et [Yao, 2016]).

Plus particulièrement, dans nos travaux, nous nous sommes intéressés à la modélisation du comportement d'un système incertain à partir d'une représentation d'état (Eq. (1.3)) où l'incertitude est localisée uniquement au niveau de la matrice d'action. Le modèle ainsi obtenu (extension du modèle donné par Eq. (1.1)) est :

$$\begin{cases} \dot{x}(t) = & (A + \Delta A)x(t) + Bu(t) \\ y(k) = & Cx(k) + v(k) \end{cases} \tag{1.3}$$

L'incertitude du modèle est portée par le terme ΔA. Pour un système en fonctionnement normal, les bornes des incertitudes ΔA sont connues, vérifiant la condition de bornitude c'est-à-dire $\Delta A \in [\Delta A_{inf}, \Delta A_{sup}]$.

Ce type de modélisation des incertitudes a pu prendre son essor par l'utilisation de l'arithmétique à intervalle développée au début des années 1960 et dont l'usage en automatique s'est intensifié au début des années 1990 ([Kearfott et Kreinovich, 1996], [Milanese *et al.*, 1996], [Jaulin *et al.*, 2002] et [Moore *et al.*, 2009]).

Il est important de noter que l'arithmétique par intervalle n'est pas le seul outil permettant de traiter les problèmes de systèmes incertains. Un apport particulier a été réalisé à l'aide de l'utilisation de fonction de croyance ([Smith, 1961], [Smith et Shafer, 1976] et [Smets, 2005]), ainsi qu'à l'aide de logique floue ([Sugeno et Yasukawa, 1993] et [Wedding, 1997], ...)

De nombreux travaux sur les observateurs de systèmes incertains sont présents dans la littérature. Nous pouvons citer les travaux pour les systèmes non-linéaires ([Raïssi *et al.*, 2010]

et [Efimov *et al.*, 2013]), linéaires ([Mazenc et Bernard, 2011] et [Cacace *et al.*, 2015]) et pour le diagnostic ([Meseguer *et al.*, 2007], [Montes De Oca *et al.*, 2012] et [Blesa *et al.*, 2014]).

1.4.2 Système comportant des bruits corrélés

Les domaines de l'aéronautique, du spatial et du génie chimique induisent des problématiques vibratoires et d'incertitudes additives et/ou multiplicatives. Lors de la modélisation de tels systèmes, il est nécessaire d'introduire des termes d'incertitudes pour représenter au mieux le comportement du système. Une manière de modéliser ces incertitudes est l'utilisation de bruits de processus. Dans certains cas ces bruits de processus peuvent être corrélés avec les bruits de mesures. Ces bruits corrélés sous certaines conditions limitent l'utilisation des outils d'estimation développés dans le cadre classique (observateurs et filtres).

Face à cette problématique un nombre important de travaux tend à développer ou adapter les outils de l'automatique afin de filtrer ce type de système. La modélisation en temps discret de systèmes possédant des bruits corrélés a obtenu un grand intérêt de la part de la communauté scientifique ([Gao et Li, 2014] et [Yao, 2016]). Pour le filtre de Kalman ([Simon, 2006] et [Ghahremani et Kamwa, 2011]) a retenu une attention particulière pour ses propriétés de mise à jour de la variance des bruits. Plus récemment ([Deshpande, 2017] et [Zhao, 2017]) ont permis d'améliorer l'estimation de la variance des bruits considérés.

Néanmoins, la modélisation de système à temps continu en considérant les bruits corrélés est moins étudiée dans la littérature. Les systèmes linéaires considérés sont représentés sous la forme suivante :

$$\begin{cases} \dot{x}(t) = & Ax(t) + Bu(t) + Gw(t) \\ y(t) = & Cx(t) + Hw(t) + v(t) \end{cases} \tag{1.4}$$

avec $x \in \mathbb{R}^n$ le vecteur d'état, $u \in \mathbb{R}^m$ le vecteur d'entrée, $w \in \mathbb{R}^n$ le bruit de processus, $y \in \mathbb{R}^p$ le vecteur de mesure et $v \in \mathbb{R}^p$ le bruit de mesure. Les matrices A, B, G, C et H sont de dimensions appropriées.

La prise en compte des incertitudes de modèle est une thématique importante afin de réaliser le développement d'outils robustes aux incertitudes tout en conservant un niveau de performance souhaité.

1.5 Conclusion

Les travaux concernant les enjeux dans le cadre de l'industrie du futur autour des sujets de la sécurité des systèmes interconnectés ont été présentés dans ce chapitre d'introduction ainsi

que ceux portant sur la perte d'intégrité des données et des perturbations réseaux.

Concernant l'intégrité des données, plusieurs approches correspondant au type d'attaques sont décrites. La plupart de ces descriptions concernent des attaques réelles. Dans la suite de nos travaux, nous allons chercher à formaliser une méthodologie permettant de répondre aux problématiques présentées lors de ce chapitre d'introduction.

Chapitre 2

Observateur à mémoire finie : Perte de paquets et perte d'intégrité

Contenu du chapitre

2.1 Introduction

2.1.1 Formulation de l'observateur à mémoire finie

L'observateur à mémoire finie a été développé dans le cas des systèmes linéaires standards et a été documenté dans les travaux suivants [Medvedev et Toivonen, 1992], [Medvedev, 1996] et [Medvedev, 1998].

Son application a été étendue à la détection de défauts pour plusieurs classes de système ainsi que pour la réconciliation de données. La détection pour les systèmes linéaires a été proposée dans les travaux de [Kratz *et al.*, 1993] et [Nuninger *et al.*, 1998]. L'application aux systèmes hybrides linéaires et non linéaires a également été montrée dans les travaux de [Kratz et Aubry, 2003], [Kajdan *et al.*, 2006] et [Kajdan *et al.*, 2007] ainsi que la réconciliation de données par [Bousghiri *et al.*, 1994] et [Kratz-Bousghiri *et al.*, 1996].

Dans cette partie, nous souhaitons présenter le fonctionnement de l'observateur à mémoire finie dans le cas de modèle à dynamique en temps continu et à mesures discrètes. Cette présentation abordera la structure de l'observateur et ses propriétés.

2.1.1.1 Observateur à mémoire finie : modèle

L'objectif de l'observateur à mémoire finie est d'estimer les états du système connaissant le modèle du système étudié (Eq. (1.1) et Eq. (2.1)), les mesures et les commandes sur une fenêtre temporelle donnée.

La formulation de l'observateur à mémoire finie, sur laquelle nos travaux reposent, est celle des modèles des systèmes linéaires à temps continu et à mesures discrètes :

$$\left\{ \begin{array}{rcl} \dot{x}(t) & = & Ax(t) + Bu(t) \\ y(k.Te) & = & Cx(k.Te) + v(k.Te) \end{array} \right. \tag{2.1}$$

où les matrices de la représentation d'état A, B et C sont de dimensions appropriées, $x \in \mathbb{R}^n$ est le vecteur d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée, $y \in \mathbb{R}^p$ est le vecteur de mesure et $v \in \mathbb{R}^p$ est le vecteur de bruit de mesure défini gaussien, stationnaire et non corrélé, dont la matrice de covariance associée est notée R. La période d'échantillonnage est notée Te. Dans la suite du manuscrit, cette période d'échantillonnage sera implicite dans l'équation de mesure : $y(k) = Cx(k) + v(k)$ où $k \in \mathbb{N}$ représente l'indice de l'échantillon.

La solution de l'équation différentielle à l'instant t en fonction de l'instant initial pris en $t-\tau_i$ est donnée ([Cellier, 1991] et [Shmaliy, 2006]) par :

$$x(t) = e^{A\tau_i}x(t-\tau_i) + \int_{t-\tau_i}^{t} e^{A(t-\theta)}Bu(\theta)d\theta \tag{2.2}$$

Nous souhaitons pouvoir exprimer $x(t)$ en fonction des mesures, pour cela nous effectuons les transformations suivantes :

$$x(t-\tau_i) = e^{-A\tau_i}x(t) - \int_{t-\tau_i}^{t} e^{A(t-\tau_i-\theta)}Bu(\theta)d\theta$$

$$y(t-\tau_i) = Ce^{-A\tau_i}x(t) - \int_{t-\tau_i}^{t} Ce^{A(t-\tau_i-\theta)}Bu(\theta)d\theta + v(t-\tau_i) \tag{2.3}$$

A un instant t quelconque, l'expression de $x(t)$ peut être obtenue à partir de mesures prises à des instants différents. Du fait de l'acquisition numérique des données, les mesures ne sont disponibles qu'à des instants multiples de la période d'échantillonnage sous l'hypothèse d'échantillonnage à pas fixe que nous avons retenue ici. Ceci se traduit d'un point de vue mathématique par le fait que $y(t-\tau_j)$ existe, si et seulement si, il existe $i_j \in \mathbb{N}$ tel que $t-\tau_j = i_j \times Te$.

L'expression de $x(t)$ en fonction de mesures prises à différents instants permet d'obtenir le système d'équations suivant :

$$\left\{\begin{array}{lcl} y(t-\tau_0) & = & Ce^{-A\tau_0}x(t) - \int_{t-\tau_0}^{t} Ce^{A(t-\tau_0-\theta)}Bu(\theta)d\theta + v(t-\tau_0) \\ y(t-\tau_1) & = & Ce^{-A\tau_1}x(t) - \int_{t-\tau_1}^{t} Ce^{A(t-\tau_1-\theta)}Bu(\theta)d\theta + v(t-\tau_1) \\ \vdots & \vdots & \\ y(t-\tau_{L-1}) & = & Ce^{-A\tau_{L-1}}x(t) - \int_{t-\tau_{L-1}}^{t} Ce^{A(t-\tau_{L-1}-\theta)}Bu(\theta)d\theta + v(t-\tau_{L-1}) \end{array}\right. \tag{2.4}$$

Ce système d'équations peut être écrit sous forme matricielle :

$$W_L x(t) = Y_L(t) - V_L(t) \tag{2.5}$$

Les différents vecteurs et matrices intervenant dans cette équation possèdent $p \times L$ lignes et

sont définis par :

$$Y_L(t) = \begin{pmatrix} y(t-\tau_0) + \int_{t-\tau_0}^{t} e^{A(t-\tau_0-\theta)}Bu(\theta)d\theta \\ y(t-\tau_1) + \int_{t-\tau_1}^{t} e^{A(t-\tau_1-\theta)}Bu(\theta)d\theta \\ \vdots \\ y(t-\tau_{L-1}) + \int_{t-\tau_{L-1}}^{t} e^{A(t-\tau_{L-1}-\theta)}Bu(\theta)d\theta \end{pmatrix}, \quad W_L = \begin{pmatrix} Ce^{-A\tau_0} \\ Ce^{-A\tau_1} \\ \vdots \\ Ce^{-A\tau_{L-1}} \end{pmatrix}$$

$$V_L(t) = \begin{pmatrix} v(t-\tau_0) \\ v(t-\tau_1) \\ \vdots \\ v(t-\tau_{L-1}) \end{pmatrix}$$

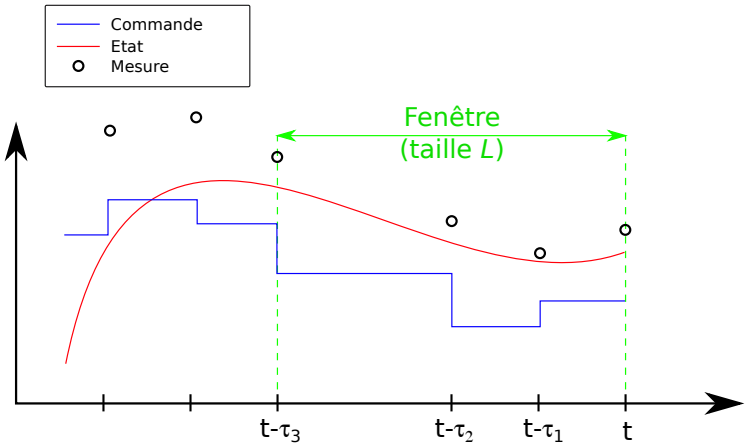


Figure 2.1 – Fenêtre de l'observateur à mémoire finie

Sur l'exemple de la Figure 2.1, nous allons chercher à connaître la valeur de l'état à l'instant t, à partir des quatre mesures disponibles aux instant $(t,\ t-\tau_1,\ t-\tau_2,\ t-\tau_3)$ ainsi que les commandes sur cette fenêtre temporelle.

Les mesures sont perturbées par un bruit $v(t)$ considéré gaussien à moyenne nulle et de matrice de covariance R. Le vecteur $V_L(t)$ qui est la collection de ces bruits de mesure sur la fenêtre temporelle considérée est donc un vecteur de bruit gausssien à moyenne nulle et dont la matrice de covariance est $P_L = \mathbb{E}[V_L V_L^T]$.

L'estimation de l'état $\hat{x}_L(t)$ s'obtient par minimisation, au sens des moindres carrés, du critère de coût $J(t)$:

$$J(t) = \frac{1}{2} \left\| Y_L(t) - W_L x(t) \right\|^2_{P_L^{-1}} \tag{2.6}$$

L'estimation est donnée ([Graton, 2005]) par :

$$\hat{x}_L(t) = (W_L^T P_L^{-1} W_L)^{-1} W_L^T P_L^{-1} Y_L(t) = \Omega_L^{-1} W_L^T P_L^{-1} Y_L(t) \tag{2.7}$$

où $\Omega_L = \left(W_L^T P_L^{-1} W_L\right)$ et $P_L = \begin{pmatrix} R & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & R \end{pmatrix}$.

Pour le cas déterministe, l'estimation s'exprime :

$$\hat{x}_L(t) = (W_L^T W_L)^{-1} W_L^T Y_L(t) = \Omega_L^{-1} W_L^T Y_L(t) \tag{2.8}$$

avec, $\Omega_L = \left(W_L^T W_L\right)$.

2.1.1.2 Observabilité

L'estimation $\hat{x}_L(t)$ obtenue par l'observateur (Eq. (2.7) ou Eq. (2.8)) dépend de la taille de la fenêtre L choisie. Il est nécessaire que la matrice Ω_L soit inversible pour le calcul de $\hat{x}_L(t)$, ce qui nous donne une condition sur la taille minimale de la fenêtre L ([Graton *et al.*, 2014]) et qui est conforme à l'indice d'observabilité. Cette condition d'existence est identique au critère d'observabilité de Kalman (observabilité de la paire (A, C)).

Dans ses travaux, [Graton, 2005] montre que la covariance de l'erreur d'estimation est directement donnée par l'inverse de la matrice Ω_L. Le calcul de Ω_{L+1}^{-1} en fonction de Ω_L^{-1} obéit à une équation de Riccati, dont les solutions, à partir d'une certaine valeur de L, sont stationnaires (comme l'illustre la Figure 2.2). Cette valeur de L donnant cette stationnarité est généralement retenue pour construire l'estimateur. [Byrski et Byrski, 2019] dans leurs travaux retrouvent ce résultat à partir du calcul d'une norme.

2.1.2 Système continu à mesures discrètes : observateur à mémoire finie

Nous souhaitons au travers d'un exemple, illustrer la synthèse et quelques propriétés de l'observateur à mémoire finie.

Considérons le système dont le modèle en temps continu est conforme à l'Eq (2.1) avec les valeurs numériques suivantes :

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 \end{pmatrix}, Te = \frac{\pi}{30} s.$$

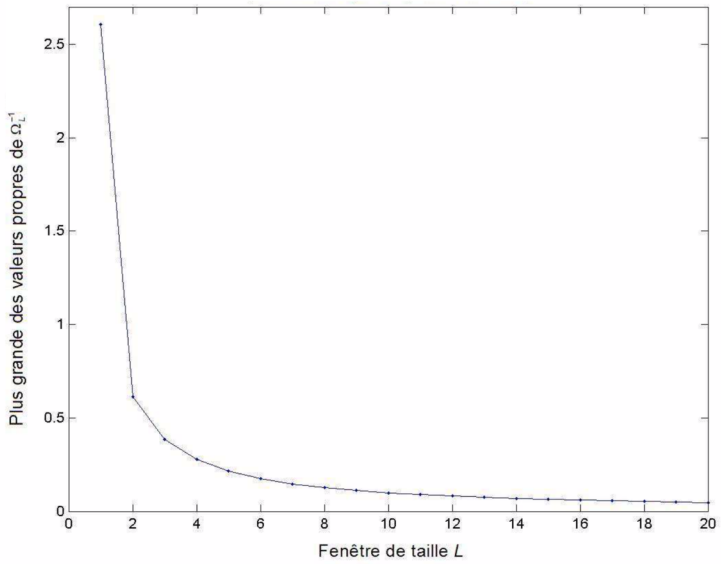


Figure 2.2 – Décroissance asymptotique des valeurs propres, [Graton, 2005]

La commande, la mesure et les états simulés de ce système sont présentés en Figure 2.3.

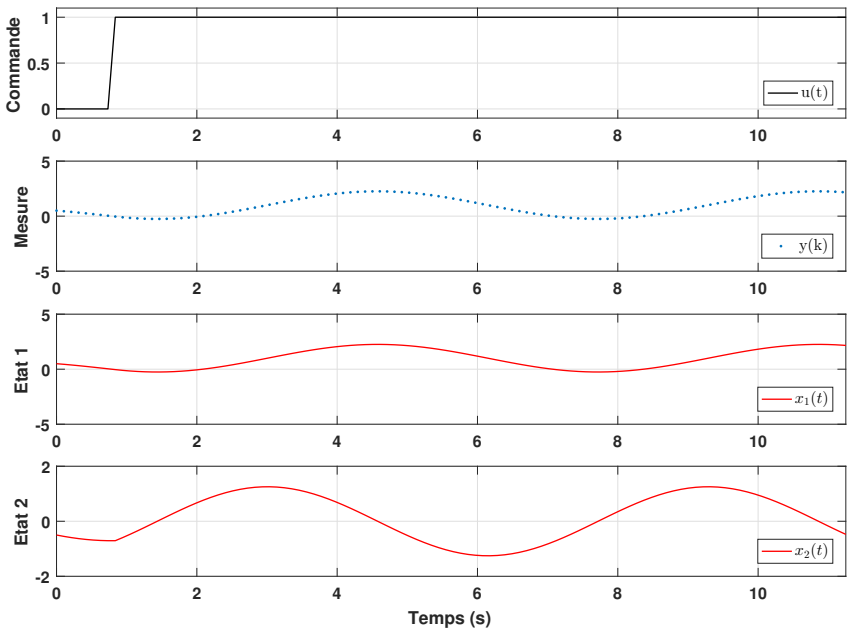


Figure 2.3 – Évolution de la commande, de la mesure et des états du système

La matrice d'observabilité (Eq. (2.9)) satisfait la condition de rang, la paire (A, C) est donc observable.

$$\text{rang}\left[\begin{pmatrix} C \\ CA \end{pmatrix}\right] = \text{rang}\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right] = 2 \tag{2.9}$$

Regardons, l'observabilité dans le cas du modèle discret. L'équation d'état discrète est donnée (sachant que $u = constante$ entre 0 et Te) par :

$$x(k+1) = e^{ATe}x(k) + \int_0^{Te} e^{A\theta}d\theta Bu(k) \tag{2.10}$$

Nous obtenons :

$$e^{ATe} = \begin{pmatrix} cos(Te) & sin(Te) \\ -sin(Te) & cos(Te) \end{pmatrix}$$

et

$$\begin{aligned} \int_0^{Te} e^{A\theta}d\theta B &= \begin{pmatrix} \int_0^{Te} sin(\theta)d\theta \\ \int_0^{Te} cos(\theta)d\theta \end{pmatrix} \\ &= \begin{pmatrix} 1 - cos(Te) \\ sin(Te) \end{pmatrix} \end{aligned} \tag{2.11}$$

La représentation discrète du système est donc :

$$\begin{aligned} x(k+1) &= A_d x(k) + B_d u(k) \\ &= \begin{pmatrix} cos(Te) & sin(Te) \\ -sin(Te) & cos(Te) \end{pmatrix} x(k) + \begin{pmatrix} 1 - cos(Te) \\ sin(Te) \end{pmatrix} u(k) \end{aligned}$$

La matrice d'observabilité du système s'écrit :

$$\begin{pmatrix} C \\ CA_d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ cos(Te) & -sin(Te) \end{pmatrix} \tag{2.12}$$

Pour vérifier la condition de rang, il est nécessaire de calculer le déterminant de la matrice d'observabilité (Eq. (2.12)).

$$\det\left[\begin{pmatrix} C \\ CA_d \end{pmatrix}\right] = -sin(Te) \tag{2.13}$$

On constate que la condition de rang peut ne pas être respectée, et donc que l'observabilité du système est perdue pour toute période d'échantillonnage multiple de π.

2.1.2.1 Synthèse de l'observateur à mémoire finie

L'existence de l'observateur à mémoire finie est donnée par l'inversibilité de la matrice Ω_L qui dans le cas présent s'écrit pour une fenêtre de taille deux ($\tau_0 = 0$ et $\tau_1 = Te$) :

$$\begin{aligned} \Omega_L &= \left(W_L^T W_L\right) = \begin{pmatrix} C^T & e^{-A^T \times Te} C^T \end{pmatrix} \begin{pmatrix} C \\ Ce^{-A \times Te} \end{pmatrix} \\ &= C^T C + e^{-A^T \times Te} C^T C e^{-A \times Te} \\ &= \begin{pmatrix} 1 + cos^2(Te) & -cos(Te)sin(Te) \\ -cos(Te)sin(Te) & sin^2(Te) \end{pmatrix} \end{aligned} \tag{2.14}$$

$$\det\left[\Omega_L\right] = sin^2(Te) \tag{2.15}$$

On remarque que le déterminant est nul lorsque la période d'échantillonnage est un multiple de π, la synthèse de l'observateur à mémoire finie ne peut pas être réalisée pour de telles périodes d'échantillonnage.

2.1.2.2 Synthèse pour différentes périodes d'échantillonnage

Dans la suite, nous présenterons les estimations produites par le FMO suivant trois cas de période d'échantillonnage des mesures ($Te = \frac{\pi}{30}s$, Te proche de π par valeur inférieure puis par valeur supérieure *i.e.* $Te = \pi^-$ et $Te = \pi^+$).

Estimation : Cas $Te = \frac{\pi}{30}s$

La Figure 2.4 présente l'évolution des états du système (en rouge) et leur estimation (en bleu) reconstruite par le FMO avec $Te = \frac{\pi}{30}s$. L'estimation des états est correcte vis-à-vis de l'évolution réelle de ceux-ci.

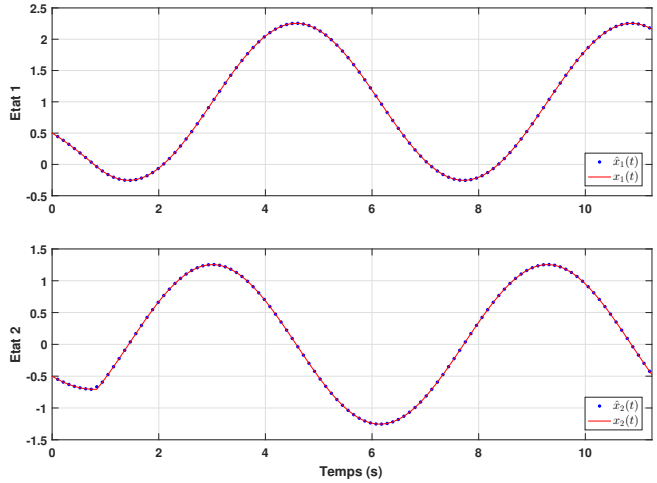


Figure 2.4 – Estimations et évolution des états : Cas $Te = \frac{\pi}{30}s$

Estimation : Cas $Te = \pi^- s = \frac{29\pi}{30}s \approx 0.97\pi s$

La Figure 2.5 présente l'évolution des états du système et leurs estimation. L'estimation des états est correcte malgré un temps d'échantillonnage proche de π ($Te = 0.97\pi s$).

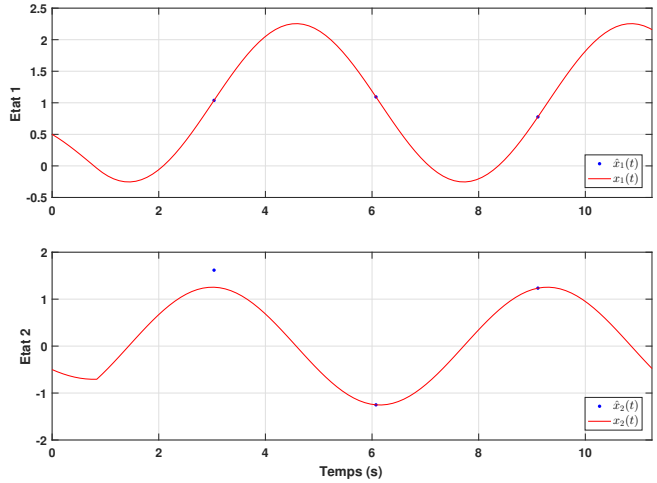


Figure 2.5 – Estimations et évolution des états : Cas $Te = \pi^- s$

Estimation : Cas $Te = \pi^+ s = \frac{31\pi}{30}s \approx 1.03\pi s$

Dans le cas où $Te = 1.03\pi s$, l'observateur à mémoire finie est capable d'estimer correctement les états du système (Figure 2.6).

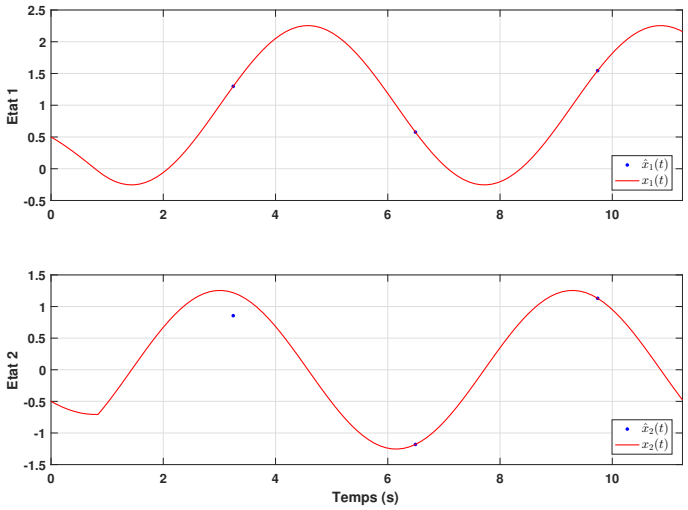


Figure 2.6 – Estimations et évolution des états : Cas $Te = \pi^+ s$

Nous avons montré, au travers de ces trois simulations, qu'à partir du moment où le système est observable, l'observateur FMO est en mesure d'estimer les états du système correctement.

2.1.2.3 Propriétés supplémentaires du FMO

Estimation asynchrone des états

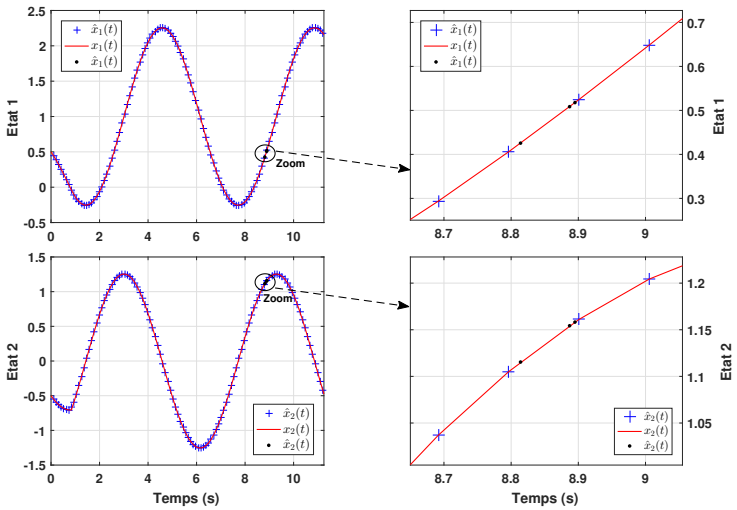


Figure 2.7 – Estimation asynchrone des états

De part l'écriture de l'observateur à mémoire finie, une de ses propriétés est sa capacité à

estimer les états à n'importe quel instant t, et en particulier même si t n'est pas un instant d'échantillonnage.

Par exemple, l'estimation aux instants $t = 10.917s$, $t = 10.930s$ et $t = 10.980s$ (instants non échantillonnés) est correcte vis-à-vis des états réels, comme le montre la Figure 2.7.

De plus, la condition d'échantillonnage à pas fixe retenue, n'est pas une obligation, ce choix a été fait de manière à simplifier la présentation. L'estimation peut être calculée à n'importe quel instant t à partir de L mesures disponibles.

Une troisième propriété du FMO est donnée par le théorème suivant :

Théorème 1 - [Medvedev et Toivonen, 1992]

Si la matrice Ω_L est définie positive alors $\hat{x}_L(t)$ satisfait à l'équation ci-dessous :

$$\frac{d\hat{x}_L(t)}{dt} = Ax(t) + Bu(t) \tag{2.16}$$

Démonstration : Sans perte de généralité, nous nous plaçons dans le cas déterministe. L'estimation de l'état est donnée par l'Eq. 2.8 qui peut être exprimée par :

$$\hat{x}_L(t) = \Omega_L^{-1} \sum_{i=0}^{L-1} e^{-A^\top \tau_i} C^\top \left(y(t-\tau_i) + C \int_{t-\tau_i}^{t} e^{A(t-\tau_i-\theta)} Bu(\theta) d\theta \right) \tag{2.17}$$

La dérivée de cette dernière équation s'écrit :

$$\frac{d\hat{x}_L(t)}{dt} = \Omega_L^{-1} \sum_{i=0}^{L-1} e^{-A^T \tau_i} C^T C \left[Ax(t-\tau_i) + Bu(t-\tau_i) + \frac{d}{dt} \int_{t-\tau_i}^{t} e^{A(t-\tau_i-\theta)} Bu(\theta) d\theta \right] \tag{2.18}$$

or, d'après le théorème de dérivée d'une intégrale (Leibniz) :

$$\frac{d}{dt} \int_{a(t)}^{b(t)} f(t,\tau) d\tau = \int_{a(t)}^{b(t)} \frac{d}{dt} f(t,\tau) d\tau + f(t,b) \frac{db(t)}{dt} - f(t,a) \frac{da(t)}{dt}$$

nous obtenons,

$$\frac{d}{dt} \int_{t-\tau_i}^{t} e^{A(t-\tau_i-\theta)} Bu(\theta) d\theta = e^{-A\tau_i} \left(\int_{t-\tau_i}^{t} Ae^{A(t-\theta)} Bu(\theta) d\theta + Bu(t) - e^{A\tau_i} Bu(t-\tau_i) \right) \tag{2.19}$$

Ainsi

$$\begin{aligned}
\frac{d\hat{x}_L(t)}{dt} &= \Omega_L^{-1} \sum_{i=0}^{L-1} e^{-A^T\tau_i} C^T C \left[Ax(t-\tau_i) + A \int_{t-\tau_i}^{t} e^{A(t-\tau_i-\theta)} Bu(\theta) d\theta + e^{-A\tau_i} Bu(t) \right] \\
&= \Omega_L^{-1} \sum_{i=0}^{L-1} e^{-A^T\tau_i} C^T C \left[Ae^{-A\tau_i} x(t) + e^{-A\tau_i} Bu(t) \right] \\
&= \Omega_L^{-1} \sum_{i=0}^{L-1} e^{-A^T\tau_i} C^T CAe^{-A\tau_i} x(t) + \Omega_L^{-1} \sum_{i=0}^{L-1} e^{-A^T\tau_i} C^T Ce^{-A\tau_i} Bu(t) \\
&= \Omega_L^{-1} \sum_{i=0}^{L-1} e^{-A^T\tau_i} C^T CAe^{-A\tau_i} x(t) + Bu(t) \\
&= \Omega_L^{-1} \sum_{i=0}^{L-1} e^{-A^T\tau_i} C^T Ce^{-A\tau_i} Ax(t) + Bu(t) \quad \text{car} \quad Ae^{-At} = e^{-At}A \\
&= Ax(t) + Bu(t)
\end{aligned} \tag{2.20}$$

$\diamond$

De plus, à partir de l'équation de mesure (2.3), avec $v(t-\tau_i) = 0$ (cas déterministe), que nous injectons dans l'Eq. (2.17).

$$\hat{x}_L(t) = \Omega_L^{-1} \sum_{i=0}^{L-1} e^{-A^\top\tau_i} C^\top C \left(e^{-A\tau_i} x(t) - \int_{t-\tau_i}^{t} e^{A(t-\tau_i-\theta)} Bu(\theta) d\theta + \int_{t-\tau_i}^{t} e^{A(t-\tau_i-\theta)} Bu(\theta) d\theta \right) \tag{2.21}$$

donc,

$$\begin{aligned}
\hat{x}_L(t) &= \Omega_L^{-1} \sum_{i=0}^{L-1} e^{-A^T\tau_i} C^T Ce^{-A\tau_i} x(t) \\
&= x(t)
\end{aligned} \tag{2.22}$$

Ainsi $x(t) - \hat{x}_L(t) = 0$ pour $t > \tau_{L-1}$.

2.1.3 Conclusion

Dans cette section, nous avons présenté l'utilisation de mesures discrètes par l'observateur à mémoire finie, utilisant un modèle en temps continu, pour estimer à chaque instant l'état. Le critère d'observabilité des modèles en temps discret conditionne l'existence de cet observateur. Si ce critère est respecté, alors l'observateur à mémoire finie existe et est en capacité de réaliser l'estimation des états du système considéré à n'importe quel instant, synchrone ou non par rapport à la période d'échantillonnage. Nous avons également démontré les propriétés de convergence, dans le cas déterministe, de cet observateur.

2.2 Synthèse d'un observateur à mémoire finie soumis à des pertes de paquets

Les flux de communication liés à l'émergence de l'industrie du futur ont révélé de nouveaux besoins et de nouvelles contraintes. L'industrie a intégré rapidement dans ses lignes ou processus de production l'utilisation des réseaux de communication. Aujourd'hui, la plupart des systèmes industriels sont victimes de perturbations des réseaux, telles que les pertes de paquets ou les retards.

Dans ces conditions et afin d'être capable de développer un outil efficace, nous devons mieux connaitre le comportement de ces perturbations. Les travaux de [Jia *et al.*, 2005], [Naghshtabrizi et Hespanha, 2005], [Xue *et al.*, 2012] et [Jiang et Fang, 2014] se sont intéressés à la modélisation et à l'analyse du comportement de ce type de dégradation. En effet, les pertes de paquets sur les mesures et les commandes impactent de façon importante la réactivité de la régulation et de la supervision, donc du fonctionnement global du système.

De nombreux travaux ont développé une analyse de la performance des systèmes subissant ces perturbations et en particulier le fait de ne plus être en capacité de calculer la commande ou d'estimer les états. Les pertes de paquets sur les réseaux de communication sont un obstacle à la performance des systèmes pour ce type d'architecture ([Zhang *et al.*, 2001], [Hadjicostis et Touri, 2002], [Hu et Yan, 2008] et [Schenato, 2008]).

Afin de pouvoir répondre à ces problématiques, nous proposons un outil utilisant des observateurs à mémoire finie. Cet outil doit être capable d'estimer et de prédire les données perdues afin de fournir au système une mesure fiable lui permettant de continuer son fonctionnement. L'observateur jouant ici le rôle de capteur logiciel.

Pour cela, dans la suite de la section, nous présentons la modélisation des pertes de paquets et sa prise en compte dans le modèle du système Eq. (2.24). Dans un second temps, à partir des informations du système, nous proposons une adaptation de l'observateur à mémoire finie permettant de répondre aux problématiques associées à ces pertes de paquets. Le comportement de l'observateur proposé, au travers de diverses simulations, montre ses qualités d'estimations et de prédictions dans le cas étudié.

2.2.1 Modélisation de la perte de paquets de mesure

La modélisation des pertes de paquets présentée au paragraphe 1.3 est utilisée dans ce paragraphe. Nous considérons une chaîne de Markov qui modélise les transistions possibles pour une fenêtre de trois données transmises. La chaîne présentée fournit une variable prenant deux

valeurs différentes possibles ($\phi = 0$ et $\phi = 1$) correspondant respectivement à la réception correcte des mesures (*i.e.* pas de perte de paquets) et à la perte de la mesure. La chaîne est définie par sa matrice de transition T donnée ci-dessous et présentée en Figure 2.8.

$$T = \begin{pmatrix} P_r & P_p & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & P_r & P_p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & P_r & P_p & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & P_r & P_p \\ P_r & P_p & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & P_r & P_p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & P_r & P_p & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & P_r & P_p \end{pmatrix} \tag{2.23}$$

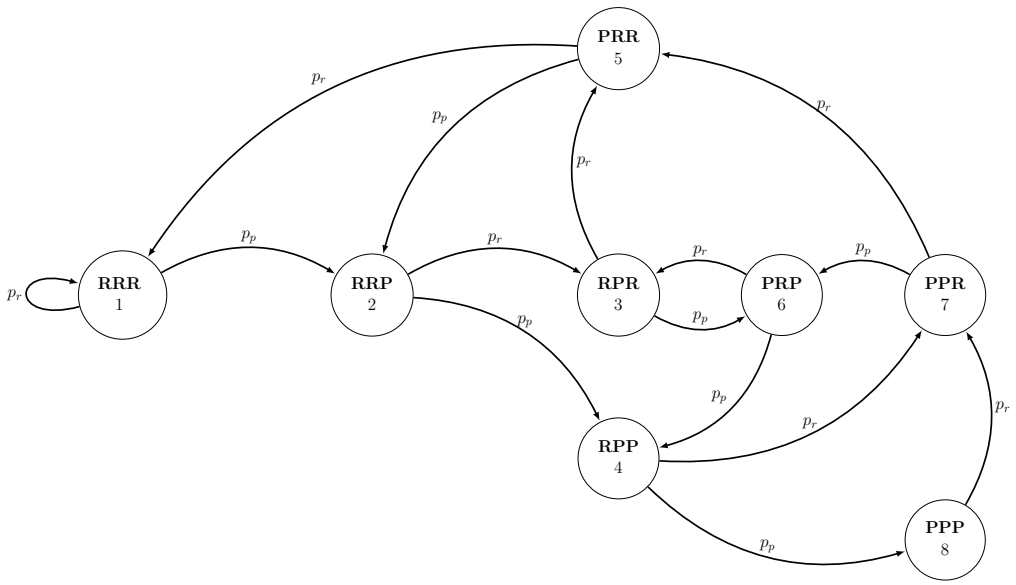


Figure 2.8 – Chaîne de Markov modélisant au plus trois pertes de paquets

Les états à l'instant k de cette chaine sont définis par la réception des données aux instants $k-2$, $k-1$ et k. Ainsi l'état RRP indique qu'à l'instant $k-2$, le paquet de données est reçu (R), idem pour l'instant $k-1$ et qu'à l'instant k le paquet n'est pas reçu (P). La transition entre les instants k et $k+1$ ne peut donc être réalisée que vers les états RPR ou RPP suivant que le paquet soit reçu (R) à l'instant $k+1$ ou non (P).

La prise en compte de cette modélisation dans le modèle du système (Eq. (2.1)) se traduit

par le système d'équations suivant :

$$\begin{cases} \dot{x}(t) &= Ax(t) + Bu^*(t) \\ y(k) &= Cx(k) + v(k) \\ y^*(k) = \begin{cases} y(k) & \text{si } \phi = 0 \\ \emptyset & \text{si } \phi = 1 \end{cases} \end{cases} \tag{2.24}$$

Le système représenté dans la Figure 2.9, dont le modèle est donné par l'Eq. (2.24), délivre des mesures capteurs $y(k)$. La transmission de ces mesures par le réseau de communication est notée $y^*(k)$. Lorsque la donnée reçue correspond à celle envoyée, la chaîne de Markov est à l'état $\phi = 0$ (pas de perte de paquets). Dans le cas contraire (perte de paquets sur les mesures), la mesure n'est pas reçue, on impose $y^*(k) = \emptyset$ (vide) (chaîne de Markov à l'état $\phi = 1$). La transmission des commandes par le réseau de communication est notée $u^*(k)$.

Remarque : le cas de la perte de paquets affectant les commandes n'est pas considéré dans nos travaux actuels.

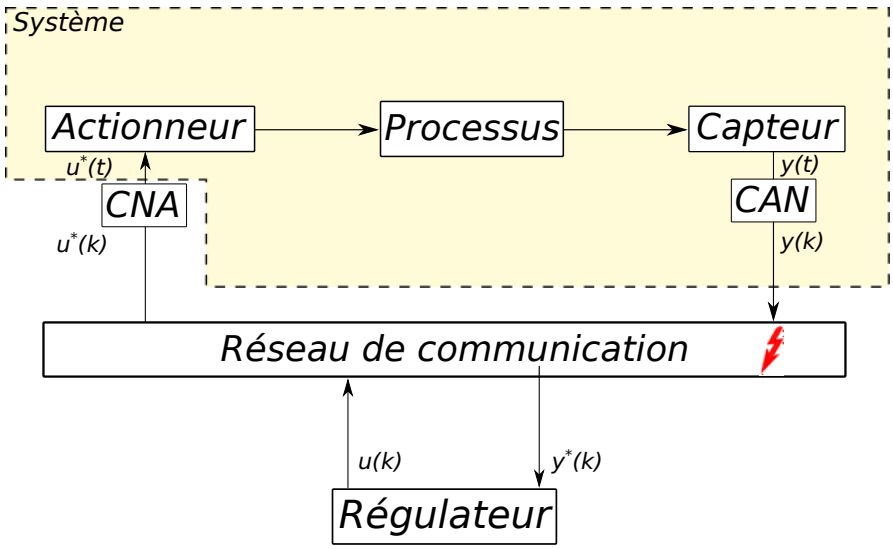


Figure 2.9 – système interconnecté en réseau - perte de paquets

2.2.2 Synthèse de l'observateur à mémoire finie : cas des pertes de paquets

Notre objectif est de synthétiser un observateur à mémoire finie capable d'estimer les états du système que la donnée soit reçue ou perdue. Lorsqu'il y a perte de paquets, l'observateur doit adapter sa fenêtre temporelle en fonction des mesures disponibles et de leur horodatage associé.

Soit à un instant t une collection de L mesures disponibles notée $Z_L(t, T_t)$ (Eq. (2.25)). La taille de la fenêtre de longueur L est constante. Cette fenêtre contient donc les L dernières

mesures collectées et horodatées (par T_t) à cet instant t. Le vecteur T_t concatène les relations d'horodatage relatif des mesures disponibles à l'instant t dans la fenêtre temporelle considérée : $T_t = [\tau_0, \tau_1, ..., \tau_{L-1}]^T$ avec $\tau_0 < \tau_1 < ... < \tau_{L-1}$.

Cette collection de mesures notée $Z_L(t, T_t)$ s'écrit :

$$Z_L(t, T_t) = \begin{pmatrix} y(t-\tau_0) \\ y(t-\tau_1) \\ \vdots \\ y(t-\tau_{L-1}) \end{pmatrix} \tag{2.25}$$

Nous rappellons que les $t - \tau_i$ doivent être multiples de Te (cf. § 2.1.1.1), pour que les mesures correspondantes existent.

En cohérence avec les Eq. (2.4) et (2.5), nous devons introduire le vecteur $\Phi_L(t, T_t)$ défini par :

$$\Phi_L(t, T_t) = \begin{pmatrix} C \int_{t-\tau_0}^{t} e^{A(t-\tau_0-\theta)} B u(\theta) d\theta \\ C \int_{t-\tau_1}^{t} e^{A(t-\tau_1-\theta)} B u(\theta) d\theta \\ \vdots \\ C \int_{t-\tau_{L-1}}^{t} e^{A(t-\tau_{L-1}-\theta)} B u(\theta) d\theta \end{pmatrix}.$$

En exprimant $Y_L(t, T_t) = Z_L(t, T_t) + \Phi_L(t, T_t)$, l'estimation de l'état à l'instant t (cf. Eq. (2.7)) en tenant compte de l'horodatage relatif, devient dans le cas présent :

$$\hat{x}_L(t|T_t) = (W_L^T P_L^{-1} W_L)^{-1} W_L^T P_L^{-1} Y_L(t, T_t) \tag{2.26}$$

Les travaux précédents [Graton, 2005] ont montré que la matrice de covariance des erreurs d'estimation $\Omega_L(T_t)$ est donnée par :

$$\Omega_L(T_t) = (W_L^T P_L^{-1} W_L) \tag{2.27}$$

avec,

$$P_L = \begin{pmatrix} R & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & R \end{pmatrix}$$

où P_L est la matrice de covariance des bruits de mesure supposés gaussiens.

$$P_L = \mathbb{E}[V_L(t)V_L^T(t)] \tag{2.28}$$

2.2.3 Comportement de l'observateur

Ce paragraphe présente la stratégie du FMO mise en œuvre pour estimer les états lors d'une perte d'information. Nous présentons dans le Tableau 2.1, l'évolution de la fenêtre de l'observateur en fonction de la perte de mesures. Le scénario de perte de mesures est composé de trois pas d'évolution du système. La taille de la fenêtre de l'observateur est fixée à $L = 3$, nous précisons que cette évolution est un exemple illustratif du formalisme utilisé et non une simulation.

2.2.3.1 Principe de fonctionnement

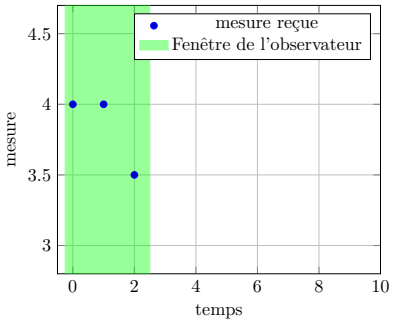
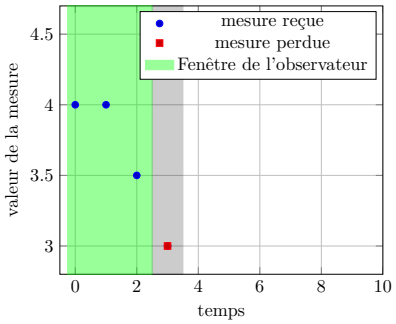
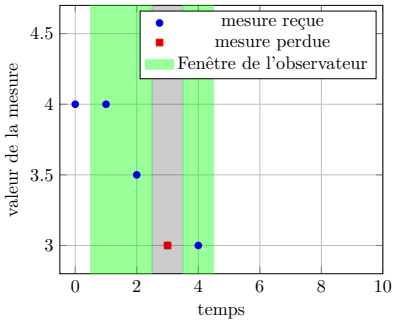
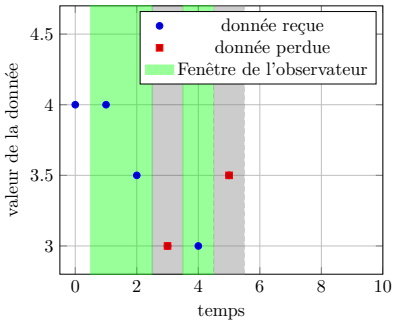
À l'instant $t = 2$, la fenêtre de l'observateur (en vert dans le Tableau 2.1) est composée des trois dernières mesures reçues (en bleu), le vecteur T_t comporte les horodatages relatifs à t et est défini par $T_2 = [0, 1, 2]^T$. Le FMO va donc réaliser l'estimation des états à $t = 2$. Nous souhaitons mettre en avant l'évolution de T_t lors du déroulement de ce scénario.

À $t = 3$, la mesure n'est pas reçue (en rouge), la fenêtre (en vert) du FMO sera alors composée des trois dernières mesures disponibles et la zone grise dans le Tableau 2.1 correspond à une zone de non réception. On observe que l'horodatage du FMO va évoluer suivant $T_3 = [1, 2, 3]^T$. $\hat{x}(t|T_3)$ est dans le cas présent une prédiction à un pas de temps. La chronologie de T_t devient :

$$\begin{matrix} T_2 \\ \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \end{matrix} \begin{matrix} \Rightarrow \\ \Rightarrow \end{matrix} \begin{matrix} T_3 \\ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \end{matrix}$$

À $t = 4$, une nouvelle mesure est reçue. La fenêtre (en vert) est composée des trois dernières mesures disponibles (en bleu), c'est-à-dire $Z_L(4, T_4) = [y(4), y(2), y(1)]^T$. On remarque alors que la fenêtre du FMO est composée de deux parties (pré et post perte de mesures à $t = 3$).

Tableau 2.1 – Évolution de la collection de mesures pour le FMO dans un scénario spécifique de pertes de paquets

	Scénario	**Collection des mesures**
$t = 2$		$Z_L(t\|T_2) = \begin{pmatrix} y(2) & = & 3.5 \\ y(1) & = & 4 \\ y(0) & = & 4 \end{pmatrix}$, avec $T_2 = \begin{pmatrix} \tau_0 = 0 \\ \tau_1 = 1 \\ \tau_2 = 2 \end{pmatrix}^T$
$t = 3$		$Z_L(t\|T_3) = \begin{pmatrix} y(2) & = & 3.5 \\ y(1) & = & 4 \\ y(0) & = & 4 \end{pmatrix}$, avec $T_3 = \begin{pmatrix} \tau_0 = 1 \\ \tau_1 = 2 \\ \tau_2 = 3 \end{pmatrix}^T$
$t = 4$		$Z_L(t\|T_4) = \begin{pmatrix} y(4) & = & 3 \\ y(2) & = & 3.5 \\ y(1) & = & 4 \end{pmatrix}$, avec $T_4 = \begin{pmatrix} \tau_0 = 0 \\ \tau_1 = 2 \\ \tau_2 = 3 \end{pmatrix}^T$
$t = 5$		$Z_L(t\|T_5) = \begin{pmatrix} y(4) & = & 3 \\ y(2) & = & 3.5 \\ y(1) & = & 4 \end{pmatrix}$, avec $T_5 = \begin{pmatrix} \tau_0 = 1 \\ \tau_1 = 3 \\ \tau_2 = 4 \end{pmatrix}^T$

Le vecteur T_t évolue tel que $T_4 = [0, 2, 3]^T$ (ce qui correspond pour $\hat{x}(t|T_4)$ à un cas d'estimation). La récupération de mesure impacte T_4 telle que :

$$\begin{matrix} T_2 & \Rightarrow & T_3 & \Rightarrow & T_4 \\ \begin{pmatrix}0\\1\\2\end{pmatrix} & \Rightarrow & \begin{pmatrix}1\\2\\3\end{pmatrix} & \Rightarrow & \begin{pmatrix}0\\2\\3\end{pmatrix} \end{matrix}$$

Puis à $t = 5$, la mesure n'est pas reçue. La fenêtre (en vert) du FMO est alors basée sur les trois dernières mesures disponibles. Le vecteur T_t va ainsi évoluer vers la forme $T_5 = [1, 3, 4]^T$ impliquant pour le FMO une prédiction à un pas :

$$\begin{matrix} T_2 & \Rightarrow & T_3 & \Rightarrow & T_4 & \Rightarrow & T_5 \\ \begin{pmatrix}0\\1\\2\end{pmatrix} & \Rightarrow & \begin{pmatrix}1\\2\\3\end{pmatrix} & \Rightarrow & \begin{pmatrix}0\\2\\3\end{pmatrix} & \Rightarrow & \begin{pmatrix}1\\3\\4\end{pmatrix} \end{matrix}$$

La chronologie de l'évolution de T_t est présentée (Tableau 2.2) en fonction de la réception de la mesure à chaque instant.

Tableau 2.2 – Evolution de la structure du FMO en fonction de la perte de paquets

t	2	3	4	5
Mesure	R	P	R	P
T_t	$\begin{pmatrix}0\\1\\2\end{pmatrix}$	$\begin{pmatrix}1\\2\\3\end{pmatrix}$	$\begin{pmatrix}0\\2\\3\end{pmatrix}$	$\begin{pmatrix}1\\3\\4\end{pmatrix}$

L'observateur FMO répond correctement à des scénarios de perte de mesures par la réalisation d'estimation ou de prédiction et ceci uniquement à partir de l'horodatage des mesures disponibles tout en conservant constante la taille de la fenêtre.

Remarque : À l'instant $t = 4$, il est possible de réaliser une prédiction à deux pas de temps pour obtenir l'estimation $\hat{x}_L(4|T_2)$. Mais la qualité de l'estimation donnée par le FMO est intrinsèquement liée aux mesures et donc à l'apport d'information récente dans l'équation d'estimation. Nous privilégions donc le scénario présenté.

2.2.4 Exemple d'application

L'exemple d'application utilisé est un moteur électrique composant une chaine cinématique de machine-outil (Figure 2.10). Le moteur électrique est régulé en vitesse $y(k)$ à l'aide d'un

correcteur PI afin de satisfaire une consigne. Le modèle comprend les frottements visqueux. La commande $u_2(t)$ provient du régulateur et $u_1(t)$ de la force de Coulomb modélisant une force de friction (supposée connue et maitrisée, par exemple le cas de freinage sur les bancs de test moteur), la variance du bruit de mesure est définie telle que $\mathbb{V} = 0.0025$. La période d'échantillonnage est définit à $Te = 1ms$.

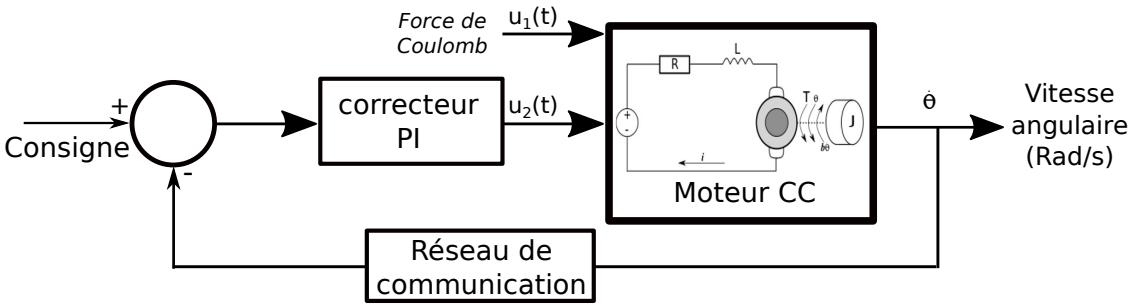


Figure 2.10 – Système étudié

Les valeurs numériques suivantes ont permis de simuler le système.

$$A = \begin{pmatrix} -0.1462 & 22.9066 \\ -247.3684 & -321.0526 \end{pmatrix}, \quad B = \begin{pmatrix} -48.7374 & 0 \\ 0 & 526.3158 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 \end{pmatrix} \tag{2.29}$$

La donnée de vitesse transite par le réseau de communication jusqu'au régulateur décentralisé. Dans ce cadre, nous synthétisons un observateur à mémoire finie de manière à fournir au régulateur des"mesures fiables" en particulier dans le cas de la non-réception des paquets de mesure. L'intégration de l'observateur au système est illustrée en Figure 2.11.
Si aucune perte de paquets n'intervient alors les mesures sont reçues par les parties régulateur

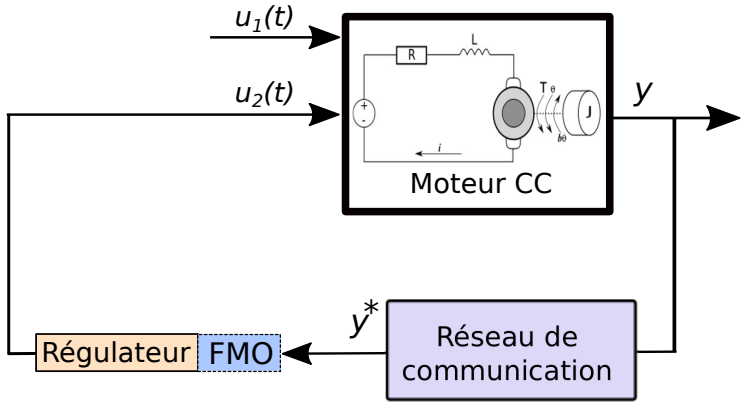


Figure 2.11 – Connexion entre la régulation, le capteur logiciel et le système

et capteur logiciel. Dans le cas où une perte de paquets intervient, le régulateur utilisera une

copie des mesures précédentes (procédure classiquement intégrée dans les régulateurs industriels) afin de commander le système. La fenêtre de l'observateur à mémoire finie s'adaptera (la mesure est non reçue) afin de réaliser une prédiction dans le cadre de la partie capteur logiciel.

Nous allons illustrer, à l'aide de la simulation, l'évolution des estimations réalisées par le FMO dans le cas d'un système présentant trois pertes de paquets consécutives.

Les évolutions de la mesure, de la commande et des états sont présentées en Figure 2.12.

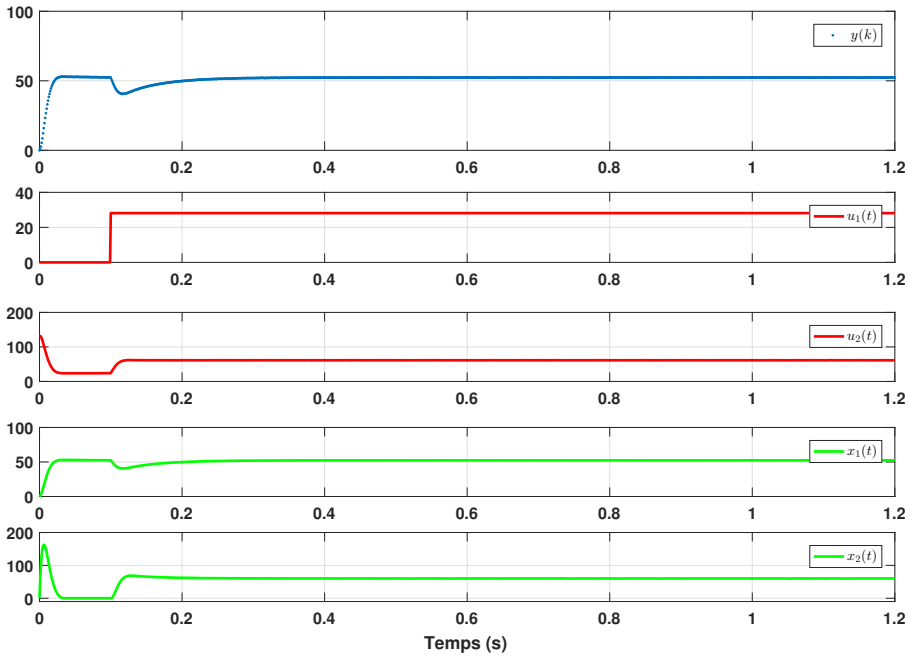


Figure 2.12 – Évolution de la mesure, des entrées et des états du système sain sans perte de paquets

Nous observons sur la Figure 2.13 la perte des paquets des mesures aux instants $t = 0.149s$, $t = 0.150s$ and $t = 0.151s$. Lors d'une perte de mesure, le régulateur maintient la commande à sa valeur, d'où l'apparition d'un pic sur le zoom de la commande $u_2(t)$.

Les résultats Figure 2.14 comparent l'évolution du système sous perte de données avec la formulation du FMO et sans le FMO. Quand les mesures sont perdues, la formulation du FMO proposée précédemment est capable de produire une estimation correcte. Le régulateur utilisant les estimations du FMO produit une commande similaire au cas sans perte de paquets.

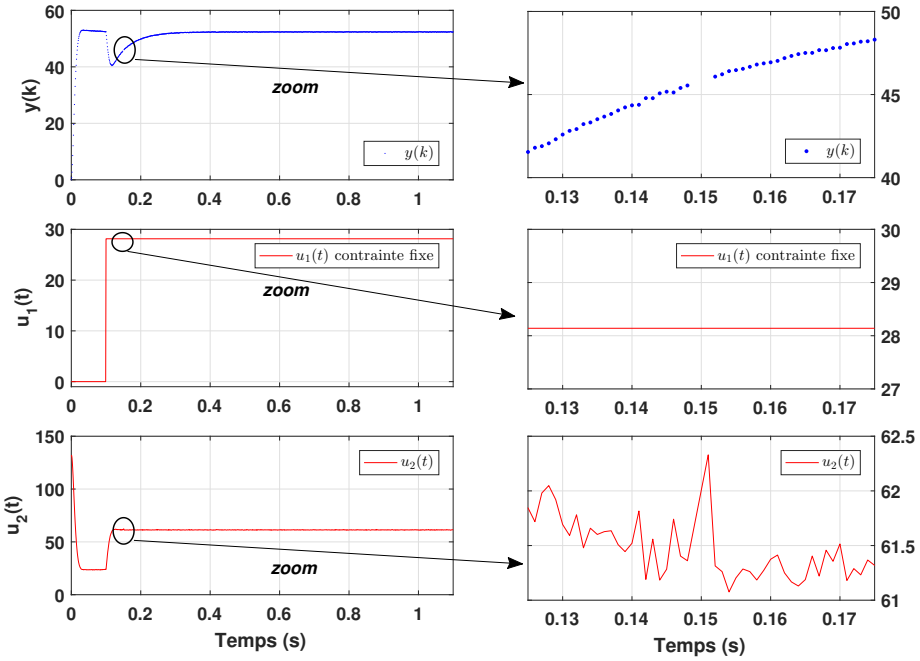


Figure 2.13 – Système soumis à un scénario de trois pertes de mesures consécutives

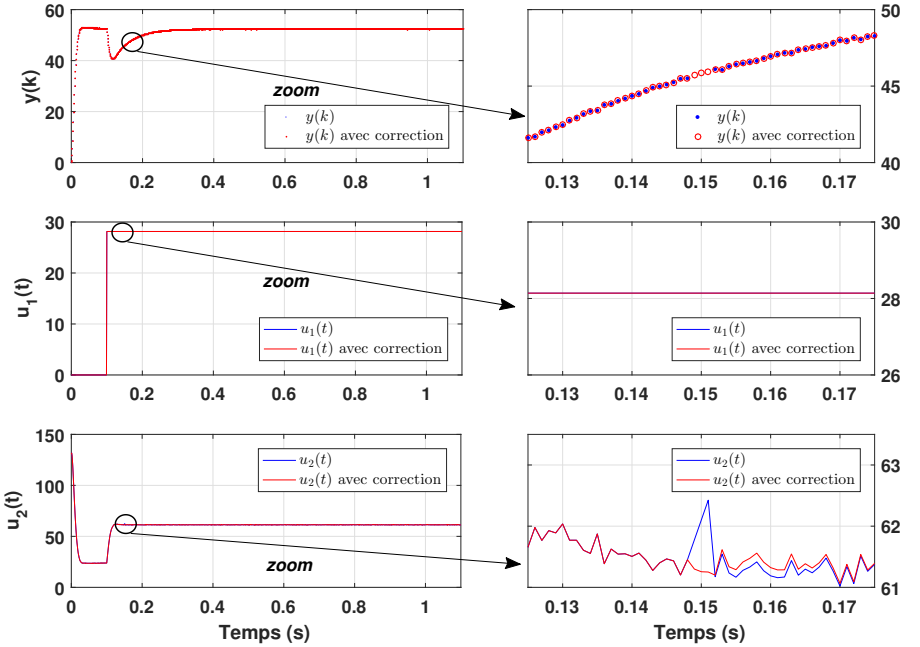


Figure 2.14 – Mesure et commande avec et sans correction FMO

2.3 Élaboration d'une stratégie de détection/correction de perte d'intégrité par observateur à mémoire finie

Dans cette partie, les estimations robustes de l'observateur à mémoire finie sont associées à une stratégie spécifique. Dans un premier temps, elle permet de détecter la perte d'intégrité des mesures transmises par le réseau de communication. Puis, elle corrige les données corrompues à l'aide d'un observateur à mémoire finie construit à partir de mesures dont l'intégrité a été validée.

2.3.1 Modélisation de la perte d'intégrité

La modélisation de la perte d'intégrité sur un système interconnecté est présentée par l'Eq. (2.30) et la Figure 2.15.

$$\begin{cases} \dot{x}(t) &= Ax(t) + Bu^*(t) \\ y(k) &= Cx(k) + v(k) \\ u^*(k) &= u(k) + \zeta(k) \\ y^*(k) &= y(k) + \sigma(k) \end{cases} \tag{2.30}$$

$\zeta \in \mathbb{R}^m$ est la modélisation de la perturbation agissant sur les commandes via le réseau de communication et $\sigma \in \mathbb{R}^p$ est la perturbation sur les mesures transmises par le réseau. u^* représente les commandes reçues du réseau de communication par le système et y^* ayant la même définition que précèdemment, c'est-à-dire les mesures reçues du réseau de communication par le régulateur.

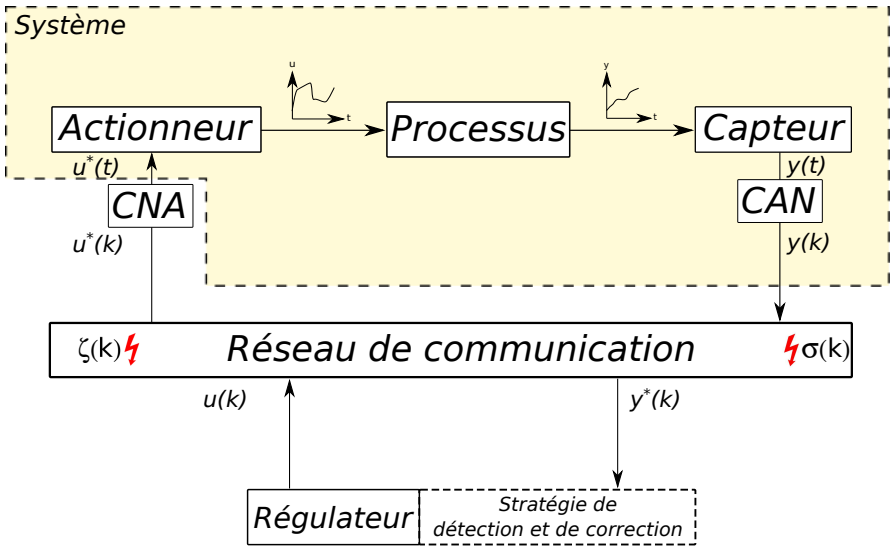


Figure 2.15 – Système interconnecté en réseau - perte d'intégrité

2.3.2 Stratégie de détection et de correction

Les principaux objectifs de cette stratégie sont :

— Détecter et neutraliser les cyber-attaques modifiant l'intégrité des données afin de protéger le système en fonctionnement. La stratégie de détection est réalisée grâce à l'observateur à mémoire finie, utilisant le modèle du système et les informations des mesures et commandes.

— Permettre au système de continuer à fonctionner. Quand une attaque est détectée, elle est alors corrigée en recouvrant l'intégrité des données reçues. La donnée corrigée est produite par une prédiction. Cette dernière est construite à l'aide des données précédemment acquises et/ou validée avant la détection de la perte d'intégrité en cours.

La réalisation de ces deux objectifs sera intégrée en amont du régulateur (cf. Figure 2.15), et est présentée par l'organigramme (Figure 2.16). Cet organigramme décompose le fonctionnement de cette stratégie en trois phases (*Détection - Décision - Correction*).

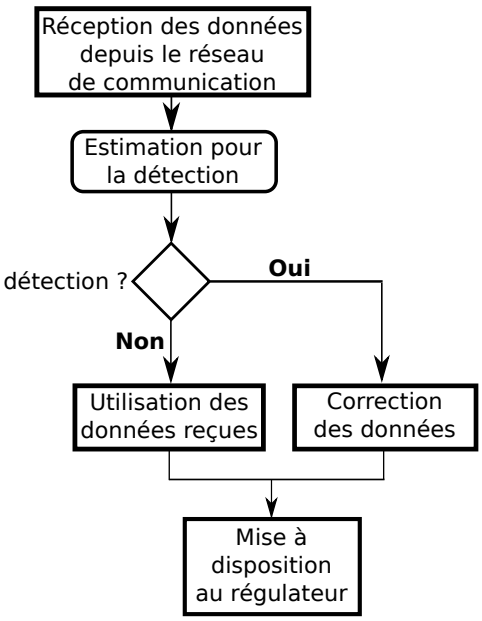


Figure 2.16 – organigramme : Détection - Décision - Correction

Après réception des données, une estimation est réalisée à partir d'un observateur spécifique (appelé observateur de détection) utilisant une fenêtre de données notée $Z_{L_{D_1}}$. L'écart entre ces estimations et les mesures reçues forme un signal appelé résidu. À partir de l'évaluation de ce résidu (par comparaison à un seuil de détection), un indicateur (alarme) est généré avertissant de la modification de l'intégrité.

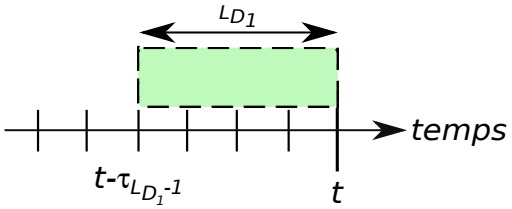


Figure 2.17 – Fenêtre $Z_{L_{D_1}}$ de l'observateur de détection

Un second résidu similaire au précèdent est généré par un observateur de détection utilisant une fenêtre de données notée $Z_{L_{D_2}}$, décalée temporelle vis-à-vis de l'instant d'estimation (Figure 2.18). Cette fenêtre comporte une mesure de moins que $Z_{L_{D_1}}$. L'évaluation de ce deuxième résidu sera réalisée de manière équivalente à celle du résidu précédent.

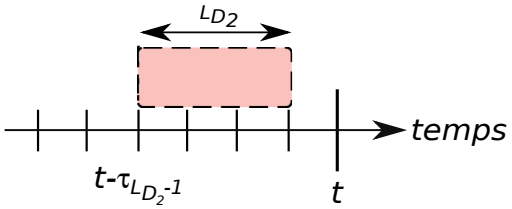


Figure 2.18 – Fenêtre $Z_{L_{D_2}}$ de l'observateur de détection

Un troisième résidu peut être généré par comparaison de deux estimations produites par des observateurs dont les fenêtres temporelles diffèrent comme l'illustre la figure suivante :

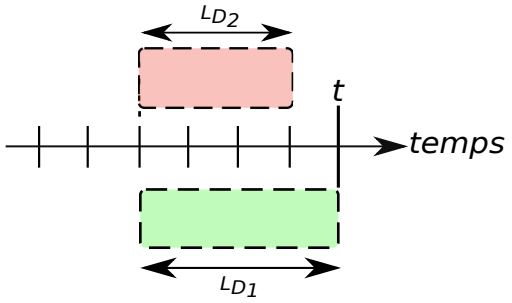


Figure 2.19 – Fenêtre $Z_{L_{D_1}}$ et$Z_{L_{D_2}}$ des observateurs de détection

Dans le cas d'une perte d'intégrité, une correction est effectuée à l'aide d'un observateur dédié (nommé observateur de correction). Une prédiction, à partir de la dernière séquence valide des mesures et des commandes du système notée Z_{L_C}, est réalisée. Cette prédiction permet de recouvrer l'intégrité du système et ainsi lui assurer un fonctionnement normal.

Cette stratégie s'appuie sur l'utilisation de deux fenêtres de données $Z_{L_{D_i}}$ (pour la détection) et Z_{L_C} (pour la correction). Les temporalités des données utilisées par ces fenêtres sont présentées sur la Figure 2.20.

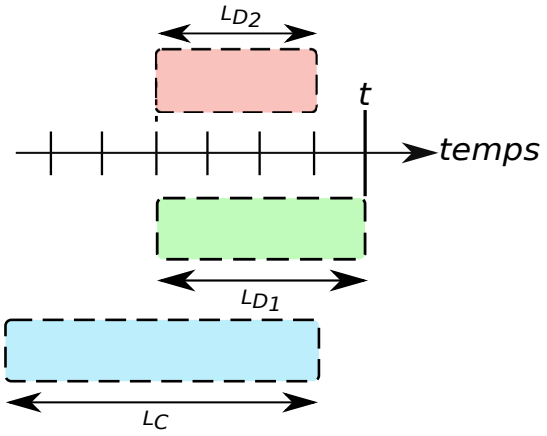


Figure 2.20 – Fenêtre $Z_{L_{D_1}}$, $Z_{L_{D_2}}$ et Z_{L_C} des observateurs de détection et de correction

2.3.2.1 Détection de la perte d'intégrité

La détection est basée sur l'estimation des états courants à partir des mesures reçues depuis le réseau de communication. L'objectif est de détecter des changements significatifs entre la mesure et son estimation. Nous faisons l'hypothèse que le changement provient d'une cyber-attaque à injection de biais.

La conception de la méthode de détection d'une cyber-attaque, n'est possible qu'après la spécification du modèle de l'attaque. Les attaques peuvent être divisées en différentes catégories, dont les deux principales sont les attaques par déni de service (DoS) et les attaques par interception de communication.

Les attaques DoS n'ont besoin que d'un accès au réseau du système et ne nécessitent pas d'intelligence, alors qu'une attaque par interception de communication, nécessite la connaissance du modèle du système et parfois aussi la connaissance du système de surveillance.

Les attaques par interception de communication (également appelées attaques par injection de données) sont effectuées pour altérer les composantes du système et modifier l'intégrité des données. Ainsi, les attaques par injection de biais "Bias injection attacks" sont un type d'attaque lorsque de fausses données sont injectées dans les canaux de sortie des capteurs ou les canaux d'entrée des régulateurs et introduisent un biais dans les signaux correspondants.

L'attaque par injection de biais peut être modélisée par un signal d'attaque additif aux signaux de commande ou aux signaux de sortie du capteur. Lorsque l'attaque par injection de biais est conçue pour rester furtive, elle devient une stratégie d'attaque intelligente et nécessite une grande connaissance du système ([Mo *et al.*, 2010], [Pasqualetti *et al.*, 2013], [Fawzi *et al.*, 2014], [Hoehn et Ping Zhang, 2016] et [Keller *et al.*, 2016]).

Afin de détecter une attaque, il est nécessaire que l'estimation produite par le FMO avec une fenêtre de données de taille L_D soit sensible à cette attaque. Dans le cadre de nos travaux, nous présentons seulement les résultats concernant l'attaque par injection de biais sur la mesure et nous imposons $\tau_0 = 0$.

Suite à une attaque $\sigma(t)$ à un instant t sur la mesure, l'estimation à cet instant est donnée par :

$$\hat{x}_{L_D}(t) = \Omega_{L_D}^{-1} \left(\left(\sum_{i=1}^{L_D-1} e^{A^T \tau_i} C^T R \left(y^*(t-\tau_i) + \int_{t-\tau_i}^{t} e^{A(t-\tau_i-\theta)} B u(t-\tau_i) d\theta \right) \right) + y^*(t) \right) \tag{2.31}$$

L'Eq. (2.31) montre que l'estimation est sensible à la perturbation $\sigma(t)$.

Afin de visualiser, analyser et réaliser des décisions, il est communément choisi de réaliser la génération de résidu. Cette génération est équivalente à celle que l'on rencontre dans le cadre du diagnostic et que l'on retrouve dans les travaux de [Himmelblau, 1978], [Patton *et al.*, 1989], [Frank, 1990], [Gertler, 1992], [Blanke *et al.*, 2006] et [Isermann, 2006].

Nous proposons de générer trois résidus, le premier r_1 comme l'écart entre l'estimation à l'aide d'une fenêtre temporelle L_{D_1} et la mesure réelle à l'instant t, le second résidu r_2 est également défini comme l'écart entre l'estimation et la mesure réelle à l'instant t mais cette fois ci avec une fenêtre temporelle L_{D_2}. Le dernier résidu r_3 est défini comme l'écart entre les estimations construites sur des fenêtre temporelles différentes (L_{D_1} et L_{D_2}).

$$\begin{aligned} r_1(t) &= y^*(t) - C\hat{x}_{L_{D_1}}(t|T_t) \\ r_2(t) &= y^*(t) - C\hat{x}_{L_{D_2}}(t|T_{t'}) \\ r_3(t) &= \hat{x}_{L_{D_1}}(t|T_t) - \hat{x}_{L_{D_2}}(t|T_{t'}) \end{aligned} \tag{2.32}$$

Remarque : même si l'écriture est en t, il est évident que la mesure doit exister et donc que t est un multiple de Te (c.f § 2.1.2.3).

L'obtention de l'espérance et de la variance des résidus (Tableau 2.3) est présentée dans l'annexe A de ce document. Les espérances des résidus r_1, r_2 et r_3 sont nulles pour le cas sans attaque. Dans le cas avec attaque, ces espérances sont sensibles à la modification réalisée par le vecteur de perturbations $\sigma(t)$. La variance des résidus pour les cas sans et avec attaque est identique. Les espérances et les variances des résidus, nous permettent d'établir que l'apparition d'une attaque par biais générera un saut de moyenne.

Les résidus suivent une loi normale dont les paramètres d'espérance et de variance sont donnés Tableau 2.3. Il est alors possible de définir une valeur de seuil notée S_i pour chaque résidu. Dans le cas, sans attaque, la relation liant le résidu au seuil est définit ci-dessous :

$$|r_{norm_i}(t)| \leq S_i \tag{2.33}$$

Dans le cas avec attaque, la moyenne n'étant pas nulle, le résidu ne vérifiera pas la condition de seuil, dont le franchissement générera une alarme de détection de perte d'intégrité. L'évaluation des résidus peut être réalisée par les test d'hypothèse présentés en annex B de ce manuscript ou par l'utilisation de CUSUM ([Basseville et Nikiforov, 1993] et [Blanke *et al.*, 2006]).

Tableau 2.3 – Espérance et variance des résidus

Résidu		Sans attaque	Avec attaque
$r_1(t)$	$\mathbb{E}$	0	$(I - C\Omega^{-1}_{L_{D_1}})\sigma$
	$\mathbb{V}ar$	$C\Omega^{-1}_{L_{D_1}}C^T + R$	$C\Omega^{-1}_{L_{D_1}}C^T + R$
$r_2(t)$	$\mathbb{E}$	0	σ
	$\mathbb{V}ar$	$C\Omega^{-1}_{L_{D_2}}C^T + R$	$C\Omega^{-1}_{L_{D_2}}C^T + R$
$r_3(t)$	$\mathbb{E}$	0	$\Omega^{-1}_{L_{D_1}}\sigma$
	$\mathbb{V}ar$	$(J-I)\Omega^{-1}_{L_{D_2}}(J-I)^T + FRF^T$	$(J-I)\Omega^{-1}_{L_{D_2}}(J-I)^T + FRF^T$

Validation numérique des propriétés des résidus

Nous réalisons la simulation du système décrit (2.29) afin de calculer les valeurs de moyenne et de variance des résidus, que nous présentons dans le Tableau 2.4 (cas sans attaque) et du Tableau 2.5 (cas avec attaque, $\sigma = 0.036$).

Tableau 2.4 – Espérance et variance des résidus sans attaque

Résidu		Obtenus par simulation	Obtenus depuis l'écriture littérale
r_1	$\overline{r_1}$	6.40×10^{-5}	0
	$\mathbb{V}ar$	6.52×10^{-5}	1.31×10^{-4}
r_2	$\overline{r_2}$	1.52×10^{-4}	0
	$\mathbb{V}ar$	1.37×10^{-4}	1.35×10^{-4}
r_3	$\overline{r_3}$	$\begin{pmatrix} 8.61 \times 10^{-5} \\ 4.81 \times 10^{-4} \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
	$\mathbb{V}ar$	$\begin{pmatrix} 1.99 \times 10^{-5} & 0 \\ 0 & 5.16 \times 10^{-4} \end{pmatrix}$	$\begin{pmatrix} 1.71 \times 10^{-5} & 0 \\ 0 & 7.55 \times 10^{-4} \end{pmatrix}$

Tableau 2.5 – Espérance et variance des résidus avec attaque

Résidu		Obtenus par simulation	Obtenus depuis l'écriture littérale
r_1	$\overline{r_1}$	-1.30×10^{-4}	1.75×10^{-2}
	$\mathbb{V}ar$	6.26×10^{-5}	1.31×10^{-4}
r_2	$\overline{r_2}$	-2.25×10^{-4}	1.75×10^{-2}
	$\mathbb{V}ar$	1.19×10^{-4}	1.35×10^{-4}
r_3	$\overline{r_3}$	$\begin{pmatrix} 9.48 \times 10^{-5} \\ 4.29 \times 10^{-4} \end{pmatrix}$	$\begin{pmatrix} 5.54 \times 10^{-7} \\ 1.16 \times 10^{-5} \end{pmatrix}$
	$\mathbb{V}ar$	$\begin{pmatrix} 1.65 \times 10^{-5} & 0 \\ 0 & 4.84 \times 10^{-4} \end{pmatrix}$	$\begin{pmatrix} 1.71 \times 10^{-5} & 0 \\ 0 & 7.55 \times 10^{-4} \end{pmatrix}$

Conservation de l'intégrité des fenêtres du FMO : Injection de l'estimation

Dans le cas où la modification de l'intégrité est réalisée à des instants successifs, les collections de données utilisées perdent leur intégrité, menant à une possible non détection. En effet, le tableau 2.6 présente la propagation des mesures dont l'intégrité a été modifiée dans les collections du FMO.

Afin de garder l'intégrité des données contenues dans les collections $Z_{L_{D_1}}$ et $Z_{L_{D_2}}$, après une première détection nous injecterons la mesure reconstruite à partir de la prédiction $\hat{x}_{L_C}(k|T_{k-1})$. Ce phénomène permet de conserver l'intégrité des données contenues dans les collections des deux observateurs de détection et est présenté dans le Tableau 2.7.

Nous avons présenté dans cette section l'élaboration d'une stratégie de détection et de correction concernant l'intégrité des données perturbées par des attaques par injection de biais. L'utilisation de l'observateur à mémoire finie proposé dans la section 2.2 a permis d'améliorer la détection et l'intégrité.

Tableau 2.6 – Propagation de la perte d'intégrité dans la fenêtre de l'observateur à mémoire finie

	$\hat{x}_{L_{D_1}}(k\|T_k)$	$\hat{x}_{L_{D_2}}(k\|T_{k-1})$	$\hat{x}_{L_C}(k\|T_{k-1})$
instant k	$Z_{L_{D_1}}(k\|T_k) = \begin{pmatrix} y^*(k) \\ y^*(k-1) \\ \vdots \\ y^*(k-L_{D_1}-1) \end{pmatrix}$	$Z_{L_{D_2}}(k,T_{k-1}) = \begin{pmatrix} y^*(k-1) \\ y^*(k-2) \\ \vdots \\ y^*(k-L_{D_2}-1) \end{pmatrix}$	$Z_{L_C}(k,T_{k-1}) = \begin{pmatrix} y^*(k-1) \\ y^*(k-2) \\ \vdots \\ y^*(k-L_C-1) \end{pmatrix}$
instant $k+1$	$\hat{x}_{L_{D_1}}(k+1\|T_{k+1})$	$\hat{x}_{L_{D_2}}(k+1\|T_k)$	$\hat{x}_{L_C}(k+1\|T_k)$
	$Z_{L_{D_1}}(k\|T_k) = \begin{pmatrix} y^*(k+1) \\ y^*(k) \\ y^*(k-1) \\ \vdots \\ y^*(k-L_{D_1}-2) \end{pmatrix}$	$Z_{L_{D_2}}(k,T_{k-1}) = \begin{pmatrix} y^*(k) \\ y^*(k-1) \\ \vdots \\ y^*(k-L_{D_2}-2) \end{pmatrix}$	$Z_{L_C}(k,T_{k-1}) = \begin{pmatrix} y^*(k) \\ y^*(k-1) \\ \vdots \\ y^*(k-L_C-2) \end{pmatrix}$

Tableau 2.7 – Conservation de l'intégrité dans la fenêtre de l'observateur à mémoire finie

	$\hat{x}_{L_{D_1}}(k\|T_k)$	$\hat{x}_{L_{D_2}}(k\|T_{k-1})$	$\hat{x}_{L_C}(k\|T_{k-1})$
instant k	$Z_{L_{D_1}}(k\|T_k) = \begin{pmatrix} y^*(k) \\ y^*(k-1) \\ \vdots \\ y^*(k-L_{D_1}-1) \end{pmatrix}$	$Z_{L_{D_2}}(k,T_{k-1}) = \begin{pmatrix} y^*(k-1) \\ y^*(k-2) \\ \vdots \\ y^*(k-L_{D_2}-1) \end{pmatrix}$	$Z_{L_C}(k,T_{k-1}) = \begin{pmatrix} y^*(k-1) \\ y^*(k-2) \\ \vdots \\ y^*(k-L_C-1) \end{pmatrix}$
instant $k+1$	$\hat{x}_{L_{D_1}}(k+1\|T_{k+1})$	$\hat{x}_{L_{D_2}}(k+1\|T_k)$	$\hat{x}_{L_C}(k+1\|T_k)$
	$Z_{L_{D_1}}(k\|T_k) = \begin{pmatrix} y^*(k+1) \\ C\hat{x}_{L_C}(k\|T_{k-1}) \\ y^*(k-1) \\ \vdots \\ y^*(k-L_{D_1}-2) \end{pmatrix}$	$Z_{L_{D_2}}(k,T_{k-1}) = \begin{pmatrix} C\hat{x}_{L_C}(k\|T_{k-1}) \\ y^*(k-1) \\ \vdots \\ y^*(k-L_{D_2}-2) \end{pmatrix}$	$Z_{L_C}(k,T_{k-1}) = \begin{pmatrix} C\hat{x}_{L_C}(k\|T_{k-1}) \\ y^*(k-1) \\ \vdots \\ y^*(k-L_C-2) \end{pmatrix}$

2.3.3 Exemple d'application

Nous utilisons l'exemple précédent (c.f § 2.2) afin de présenter les résultats de la stratégie de *détection-décision-correction*. Les tailles des observateurs sont fixées telles que $L_{D_1} = 6$, $L_{D_2} = 5$ et $L_C = 12$. Une attaque est réalisée de l'instant $0.999s$ à l'instant $1.004s$ compris, c'est à dire

6 échantillons consécutifs. L'attaque est une injection de biais, dont la valeur est $\sigma = 0.036$, ce qui représente 3% de la valeur considérée.

Les mesures et les commandes d'un système soumis à l'attaque par injection de biais est comparées au cas sans attaque (Figure 2.21). Lors de l'attaque, les mesures en rouge du système

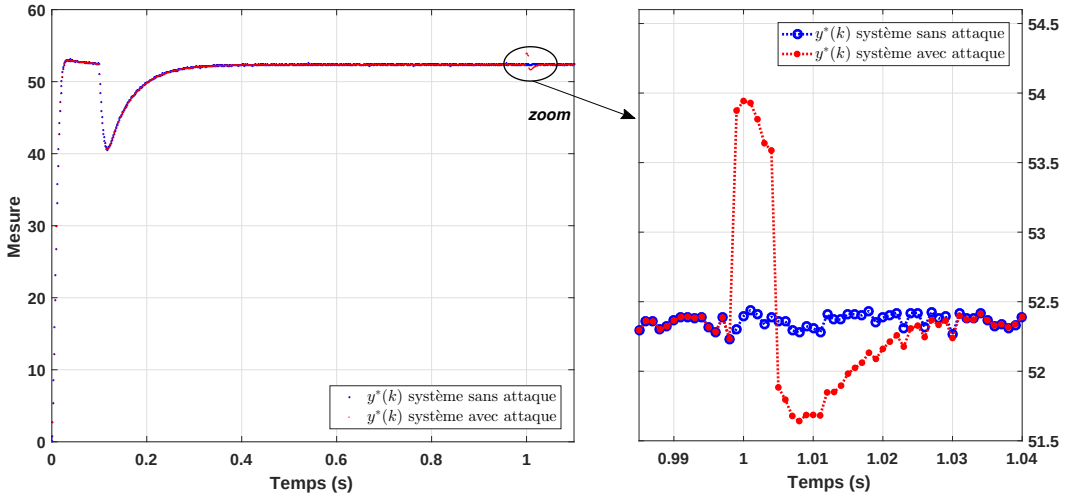


Figure 2.21 – Impact sur les mesures de la modification d'intégrité

impacté sont modifiées et provoquent une oscillation de la sortie. De manière équivalente, la modification de la mesure impacte la régulation et mène la commande à s'ajuster en fonction des données reçues modifiées.

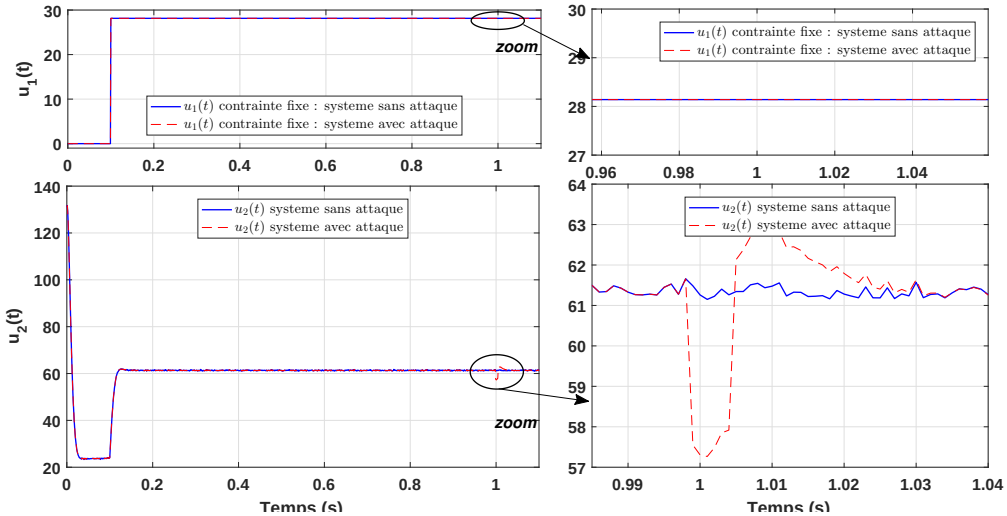


Figure 2.22 – Impact sur les entrées de la modification d'intégrité

En appliquant notre stratégie sur ce système, nous visualisons les résidus obtenus (Figure 2.23) et les alarmes générées (Figure 2.24) à l'aide des seuils de détection (c.f § 2.3.2.1).

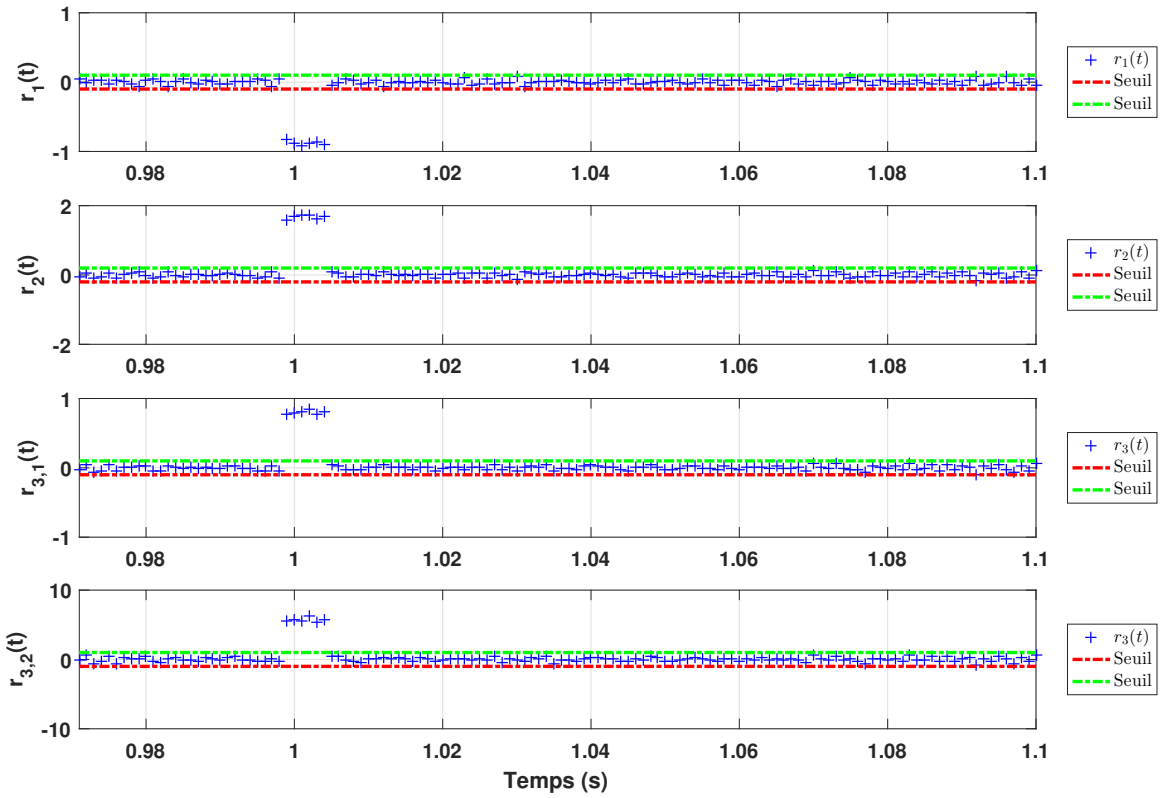


Figure 2.23 – Évolution des résidus générés

Lors de l'attaque entre $t = 0.999s$ et $t = 1.004s$, le résidu dépasse le seuil fixé pour chaque résidu.

Suite au dépassement de seuil, on remarque que l'attaque est détectée à son apparition et l'alarme est stoppée lors de l'arrêt de l'attaque.

Nous souhaitons dans la suite des résultats comparer la donnée reçue modifiée par le régulateur à celle produite par l'observateur de correction dans la stratégie proposée.

La mesure produite par l'observateur de correction (Figure 2.25) ne suit pas la modification appliquée et permet ainsi au régulateur de recevoir des valeurs intègres. La stratégie proposée permet donc de détecter et de corriger efficacement la perte d'intégrité des mesures reçues par le réseau de communication.

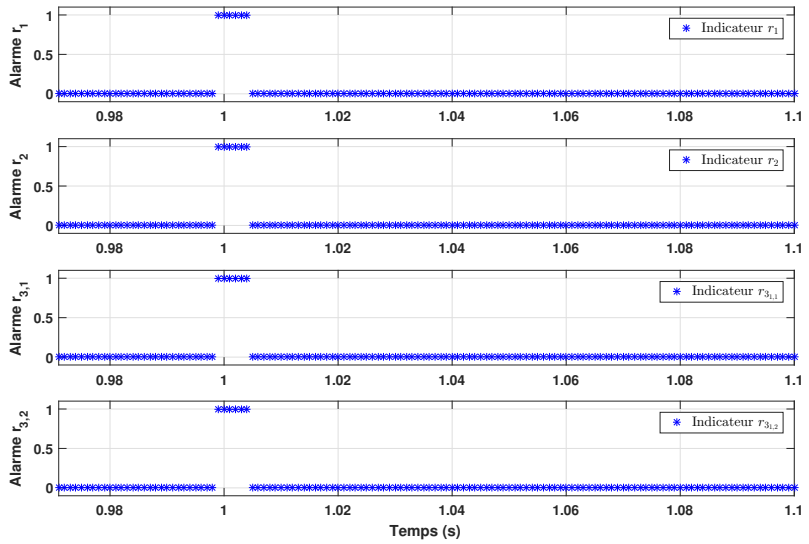


Figure 2.24 – Activation des alarmes par dépassement des seuils des résidus

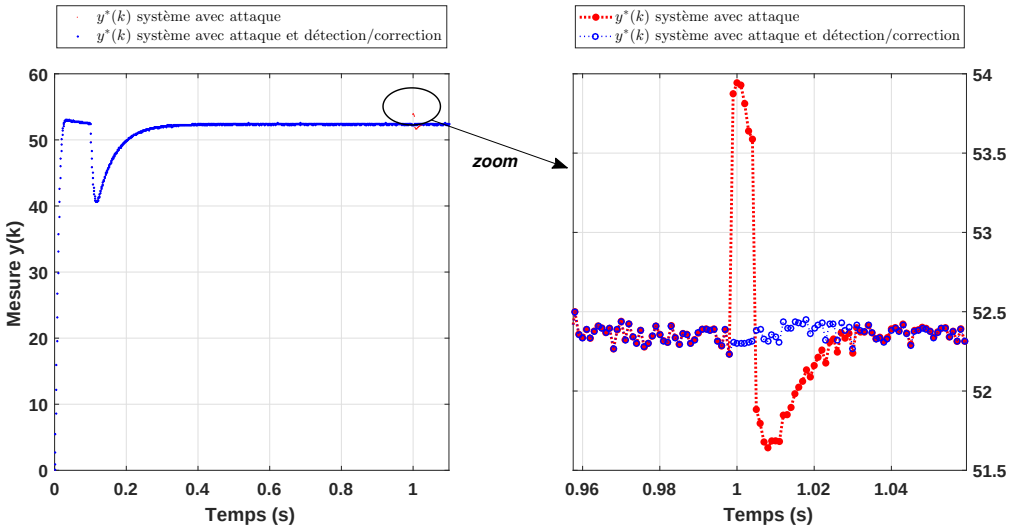


Figure 2.25 – Évolution de la mesure avec attaque et avec attaque + détection/correction

2.4 Conclusion

Ce chapitre avait pour ambition de présenter l'essentiel des résultats obtenus dans l'utilisation de l'observateur à mémoire finie pour résoudre le problème des cyber-attaques simples (perte de paquets, perte d'intégrité avec dynamique non nulle). Les propositions développées dans ce chapitre ont été illustrées par des exemples de simulation. Ces exemples ont permis de visualiser les bons résultats de nos propositions.

Chapitre 3

Observateur à mémoire finie et incertitudes de modélisation

Contenu du chapitre

3.1 Systèmes incertains

Dans le cas de systèmes incertains, les attaques peuvent mettre à profit les incertitudes de modélisation de manière à être difficilement détectable. En prolongement de nos travaux présentés au chapitre précédent, nous proposons une formulation de l'observateur à mémoire finie pour prendre en compte ces incertitudes pour les systèmes incertains.

3.1.1 Modélisation des systèmes incertains

Nous considérons dans cette partie, l'étude de système à représentation d'état à temps continu et à mesures discrètes comportant des incertitudes uniquement sur la matrice A du modèle. Seules les bornes des incertitudes sont connues *a priori*.

La représentation d'état d'un tel système peut être définie par :

$$\begin{cases} \dot{x}(t) = (A + \Delta A)x(t) + Bu(t) \\ y(k) = Cx(k) + v(k) \end{cases} \tag{3.1}$$

avec les matrices de représentation d'état A, B et C de dimensions appropriées. $x \in \mathbb{R}^n$ est le vecteur d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée, $y \in \mathbb{R}^p$ est le vecteur de mesure et $v \in \mathbb{R}^p$ est le vecteur des bruits de mesure. L'incertitude ΔA vérifie les conditions de bornitude telles que $\Delta A \in [\Delta A_{inf}, \Delta A_{sup}]$ équivalent à $(\underline{A}_{i,j} \leqslant (A + \Delta A)_{i,j} \leqslant \overline{A}_{i,j}$, où i et j correspondent aux indices des lignes et des colonnes. Ces conditions de bornitude permettent de réecrire l'Eq. (3.1) sous la forme suivante en introduisant la matrice intervalle $[A]$.

$$\begin{cases} \dot{x}(t) = [A]x(t) + Bu(t) \\ y(k) = Cx(k) + v(k) \end{cases} \tag{3.2}$$

avec $[A]$ la matrice intervalle dont chaque élément est un intervalle de la forme $[\underline{A}_{i,j}, \overline{A}_{i,j}]$:

$$[A] = \begin{pmatrix} [\underline{A}_{1,1}, \overline{A}_{1,1}] & \dots & [\underline{A}_{1,n}, \overline{A}_{1,n}] \\ \vdots & \ddots & \vdots \\ [\underline{A}_{n,1}, \overline{A}_{n,1}] & \dots & [\underline{A}_{n,n}, \overline{A}_{n,n}] \end{pmatrix}$$

Cette représentation par intervalle de l'état, nous permet de synthétiser un observateur à mémoire finie, qui à partir des mesures et des commandes disponibles, estime une enveloppe dans laquelle l'état réel du système évolue.

3.1.2 Synthèse de l'observateur

L'objectif de cette section est l'adaptation de l'observateur à mémoire finie sous une forme intervalle. Cette adaptation nécessite de calculer les matrices intervalles présentes dans l'équation de l'observateur.

La forme générale de cet observateur est alors définie par l'équation 3.3, obtenue à partir de l'équation (2.1.2) (p. 29 du chapitre 2) en remplaçant les vecteurs et matrices réels par leurs correspondants intervalles.

$$[\hat{x}_L(t)] = ([W_L^T][P_L^{-1}][W_L])^{-1}[W_L^T][P_L^{-1}][Y_L(t)] \tag{3.3}$$

L'obtention de $[\hat{x}_L(t)]$ nécessite le calcul sous forme intervalle des différentes matrices intervenant dans cette équation et plus particulièrement le calcul de W_L nécessitant l'exponentielle ainsi que le calcul de l'inverse de matrices.

Pour calculer le terme $e^{(-[A]\tau)}$, puis l'évaluation de la matrice W_L, plusieurs méthodes de la littérature [Oppenheimer et Michel, 1988] et [Higham, 2009] peuvent être appliquées par l'utilisation de séries de Taylor et de la méthode de décompositions polynomiales.

La méthode retenue ([Goldsztejn et Neumaier, 2014]), utilise un "schéma de réduction-élévation" également nommé "schéma de Horner". En effet, les auteurs ont démontré que la méthodologie proposée permet de réduire l'effet de perte de corrélation entre les éléments de la matrice lors de la mise en exponentielle. La précision du calcul des éléments de la matrice est également améliorée, notamment grâce au processus de "réduction-élévation".

La première étape consiste à calculer la décomposition complète avec compensation d'erreur de $e^{(-[A]\tau)}$ notée $\tilde{H}_K(-[A]\tau)$ et définie par :

$$\tilde{H}_K(-[A]\tau) = H_K(-[A]\tau) + R_K(-[A]\tau) \tag{3.4}$$

La matrice H_K est la représentation de la décomposition de Horner et la matrice R_K celle des compensations des erreurs provenant du calcul en série de Taylor. Elles sont données par :

$$H_K(-[A]\tau) = I + \frac{-[A]\tau}{1}(I + \frac{-[A]\tau}{2}(I + \frac{-[A]\tau}{3}\cdots(I + \frac{-[A]\tau}{K}))) \tag{3.5}$$

$$R_K(-[A]\tau) = p(\| - [A]\tau\|_\infty, K)[-[E], [E]] \tag{3.6}$$

Le calcul de la matrice $R_k(-[A]\tau)$ est réalisé à l'aide de la matrice E composée de 1 et de dimension $n \times n$. La fonction p est définie par :

$$p(\alpha, K) = \frac{\alpha^{K+1}}{(K+1)!(1 - \frac{\alpha}{K+2})} \tag{3.7}$$

Le procédé de "réduction-élévation" proposé par [Goldsztejn et Neumaier, 2014] est appliqué à la matrice $\tilde{H}_K(-[A]\tau)$ et donne $S_K(-[A]\tau)$. Cette méthode nécessite l'utilisation de deux paramètres K et γ solutions de $(K+2)2^\gamma \geq \| A \|_\infty$. Le choix de ces deux paramètres influe la précision du calcul de la matrice intervalle. Dans notre travail, nous n'explorons pas le choix de ces paramètres mais assurons la précision de la matrice intervalle calculée par cette méthode.

$$S_K(-[A]\tau) = (\frac{\tilde{H}_K(-[A]\tau)}{2^\gamma}) \tag{3.8}$$

La matrice $[W_L]$ est obtenue d'après les calculs précédents :

$$[W_L] = \begin{pmatrix} [C]S_K(-[A]\tau_0) \\ [C]S_K(-[A]\tau_1) \\ \vdots \\ [C]S_K(-[A]\tau_{L-1}) \end{pmatrix} \tag{3.9}$$

Il est également nécessaire de calculer la matrice $[Y_L(t)]$. Pour cela, les règles simples du calcul intervalle notamment énoncées par [Moore, 1979] et [Neumaier et Hansen, 1994] sont appliquées. Nous obtenons alors :

$$[Y_L(t)] = \begin{pmatrix} y(t-\tau_0)[I_p] + [\phi(t-\tau_0)] \\ y(t-\tau_1)[I_p] + [\phi(t-\tau_1)] \\ \vdots \\ y(t-\tau_{L-1})[I_p] + [\phi(t-\tau_{L-1})] \end{pmatrix} \tag{3.10}$$

avec, $\forall i \in [0, ..., L-1]$, l'intervalle $[\phi]$ défini par :

$$\Big[\underline{\phi}(t-\tau_i)\ \overline{\phi}(t-\tau_i)\Big] = \Big[min(a,b)\ max(a,b)\Big]$$

où $[I_p]$ est la matrice intervalle identité d'ordre p et les termes a et b tels que :

$$a = \int_{t-\tau_i}^{t} e^{\underline{A}(t-\tau_i-\theta)} Bu(\theta)d\theta \text{ et } b = \int_{t-\tau_i}^{t} e^{\overline{A}(t-\tau_i-\theta)} Bu(\theta)d\theta$$

.

La synthèse de l'observateur nous permet d'obtenir des estimations sous formes intervalles :

$$[\hat{x}_L(t)] = [\underline{\hat{x}}_L(t), \overline{\hat{x}}_L(t)] = \begin{pmatrix} [\underline{\hat{x}}_{L,1}(t), \overline{\hat{x}}_{L,1}(t)] \\ [\underline{\hat{x}}_{L,2}(t), \overline{\hat{x}}_{L,2}(t)] \\ \vdots \\ [\underline{\hat{x}}_{L,n}(t), \overline{\hat{x}}_{L,n}(t)] \end{pmatrix} \tag{3.11}$$

La trajectoire de cet intervalle, au cours du temps, va générer une enveloppe, que l'on nommera intervalle d'estimation. En effet, le vecteur d'état réel, dans le cas d'un fonction normal, est élément de cet intervalle.

3.1.3 Résultats

3.1.3.1 Modélisation

Le système étudié est un pont roulant illustré par la figure 3.1.

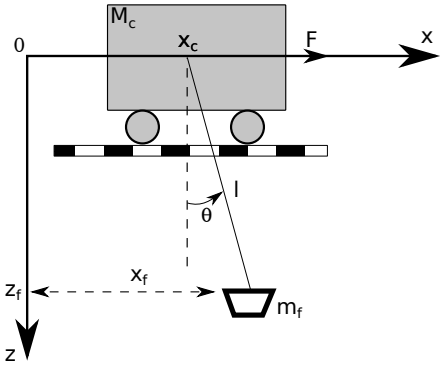


Figure 3.1 – Schéma du pont roulant

avec respectivement, x_c la position du chariot, M_c la masse du chariot, F la force de traction exercée sur le chariot, (x_f, z_f) la position de la benne, m_f la masse de la benne, g la gravité et l la longueur du filin et θ l'angle du filin par rapport à la verticale.

À partir des équations mécaniques, nous obtenons la représentation d'état linéarisée suivante :

$$\frac{d}{dt}\begin{pmatrix} x_c(t) \\ \dot{x}_c(t) \\ \theta(t) \\ \dot{\theta}(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{F}{M_c} + \frac{m_f}{M_c} g & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -\frac{F}{M_c l} - \left(\frac{m_f}{M_c} + 1\right) \frac{g}{l} & 0 \end{pmatrix} \begin{pmatrix} x_c(t) \\ \dot{x}_c(t) \\ \theta(t) \\ \dot{\theta}(t) \end{pmatrix} + \begin{pmatrix} 0 \\ \frac{1}{M_c} \\ 0 \\ -\frac{1}{M_c l} \end{pmatrix} u(t) \tag{3.12}$$

et des équations de mesures :

$$y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_c(t) \\ \dot{x}_c(t) \\ \theta(t) \\ \dot{\theta}(t) \end{pmatrix} + v(t) \tag{3.13}$$

Deux capteurs fournissent, la mesure de la position du chariot et la mesure de l'angle du filin.

3.1.3.2 Système incertain

Pour un exemple démonstratif, nous prenons pour l'encadrement du système $(\underline{A})_{i,j} \leq (A + \Delta A)_{i,j} \leq (\overline{A})_{i,j}$ les valeurs numériques suivantes :

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 39.24 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -4.905 & 0 \end{pmatrix}, (\underline{A})_{i,j} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 39.043 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -4.905 & 0 \end{pmatrix}, (\overline{A})_{i,j} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 39.436 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -4.905 & 0 \end{pmatrix}$$

$$[A] = \begin{pmatrix} [0\ ,\ 0] & [1\ ,\ 1] & [0\ ,\ 0] & [0\ ,\ 0] \\ [0\ ,\ 0] & [0\ ,\ 0] & [39.043\ ,\ 39.436] & [0\ ,\ 0] \\ [0\ ,\ 0] & [0\ ,\ 0] & [0\ ,\ 0] & [1\ ,\ 1] \\ [0\ ,\ 0] & [0\ ,\ 0] & [-4.905\ ,\ -4.905] & [0\ ,\ 0] \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 \\ 10^3 \\ 0 \\ -10^4 \end{pmatrix}$$

avec une période d'échantillonnage $Te = 10^{-1}$ s et le vecteur des bruits des mesures tel que $v \sim \mathcal{N}\left(0, \left(\begin{smallmatrix} 10^{-4} & 0 \\ 0 & 10^{-5} \end{smallmatrix}\right)\right)$. Les évolutions des mesures du système pour une entrée en échelon d'amplitude 300 N (force de traction) sont présentées en Figure 3.2.

3.1.3.3 Estimation

Les résultats obtenus à partir de l'observateur à mémoire finie intervalle sont confrontés à l'évolution des états du système. Pour chaque état réel du système incertain, nous présentons l'évolution de l'intervalle d'estimation correspondant (colonne de gauche sur la Figure 3.3). Un zoom est également proposé sur la colonne de droite (Figure 3.3) entre les instants $10s$ et $15s$. Les estimations encadrent correctement l'évolution des états réels du système.

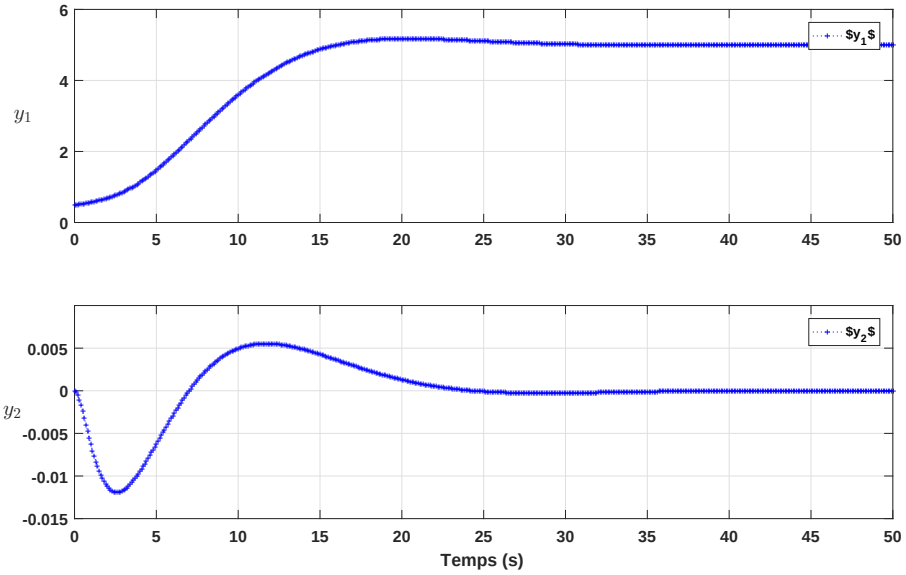


Figure 3.2 – Évolution des mesures du système

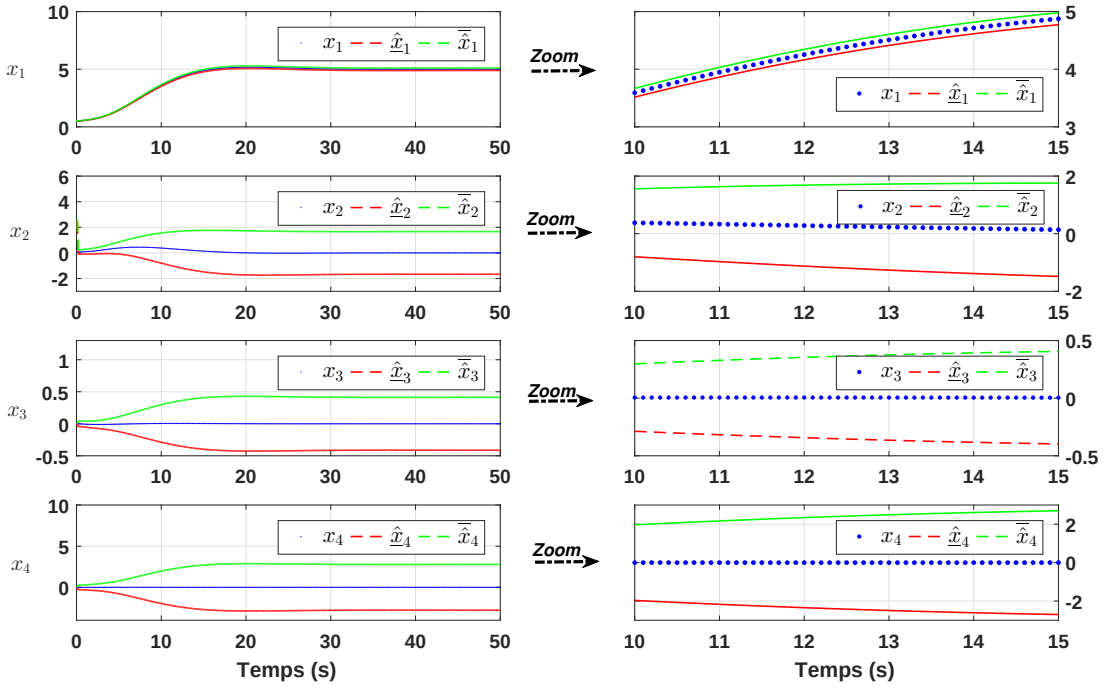


Figure 3.3 – Estimations des états du système

3.2 Systèmes à bruits corrélés

Dans ce paragraphe, l'étude porte sur des systèmes où les bruits d'états sont corrélés avec les bruits de mesures qui ont déjà été étudiés ([Simon, 2006], [Richter, 2012], [Avella et Mancini, 2013], ...) ainsi que leur diagnostic. Il est acquis que le diagnostic de ces systèmes, nécessite la prise en compte de la corrélation des bruits afin de réaliser la meilleure estimation. L'observateur à mémoire finie a été largement étudié pour différentes classes de systèmes mais aucun article, à notre connaissance, n'étudie le cas de système à bruits corrélés.

Dans ce cadre, nous proposons de synthétiser un observateur à mémoire finie capable de prendre en compte les propriétés de ce type de système. Plusieurs simulations vont confirmer les performances de l'observateur pour l'estimation.

3.2.1 Modélisation des systèmes à bruits corrélés

La formulation des systèmes étudiés est :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + Gw(t) \\ y(k) = Cx(k) + Hw(k) + v(k) \end{cases} \tag{3.14}$$

avec $x \in \mathbb{R}^n$ le vecteur d'état, $u \in \mathbb{R}^m$ le vecteur d'entrée, $w \in \mathbb{R}^n$ le bruit de processus, $y \in \mathbb{R}^p$ le vecteur de mesure et $v \in \mathbb{R}^p$ le bruit de mesure. Les matrices A, B, G, C et H sont de dimensions appropriées. Les bruits w et v sont définis gaussiens à moyennes nulles avec les propriétés suivantes :

$$\begin{cases} \mathbb{E}(w(t_1)w(t_2)^T) &= Q\delta(t_1 - t_2) \\ \mathbb{E}(v(t_1)v(t_2)^T) &= R\delta(t_1 - t_2) \\ \mathbb{E}(w(t_1)v(t_2)^T) &= J\delta(t_1 - t_2) \end{cases} \tag{3.15}$$

où J, R et Q sont des matrices aux dimensions appropriées et δ la distribution de Dirac.

3.2.2 Synthèse de l'observateur

A partir de la représentation d'état (Eq. (3.14)), nous sommes en mesure d'exprimer la relation entre l'état courant $x(t)$ et la mesure $y(t - \tau_i)$:

$$\begin{aligned} y(t-\tau_i) = Ce^{-A\tau_i}x(t-\tau_i) - \int_{t-\tau_i}^{t} Ce^{A(t-\tau_i-\theta)}Bu(\theta)d\theta + \int_{t-\tau_i}^{t} Ce^{A(t-\tau_i-\theta)}Gw(\theta)d\theta \\ + Hw(t-\tau_i) + v(t-\tau_i) \end{aligned} \tag{3.16}$$

Par analogie avec le chapitre 2 et puisque l'estimation d'état $\hat{x}(t)$ est non corrélée avec la matrice des bruits $N_L(t)$ alors la résolution est donnée au sens des moindres carrés par :

$$\hat{x}(t) = (W_L^T P_L^{-1} W_L)^{-1} W_L^T P_L^{-1} Y_L(t) \tag{3.17}$$

avec,

$$Y_L = \begin{pmatrix} y(t-\tau_0) + \int_{t-\tau_0}^{t} e^{A(t-\tau_0-\theta)} Bu(\theta) d\theta \\ y(t-\tau_1) + \int_{t-\tau_1}^{t} e^{A(t-\tau_1-\theta)} Bu(\theta) d\theta \\ \vdots \\ y(t-\tau_{L-1}) + \int_{t-\tau_{L-1}}^{t} e^{A(t-\tau_{L-1}-\theta)} Bu(\theta) d\theta \end{pmatrix}, W_L(t) = \begin{pmatrix} Ce^{-A\tau_0} \\ Ce^{-A\tau_1} \\ \vdots \\ Ce^{-A\tau_{L-1}} \end{pmatrix}$$

$$N_L(t) = \begin{pmatrix} v(t-\tau_0) + Hw(t-\tau_0) + \int_{t-\tau_0}^{t} e^{A(t-\tau_0-\theta)} Gw(\theta) d\theta) \\ v(t-\tau_1) + Hw(t-\tau_1) + \int_{t-\tau_1}^{t} e^{A(t-\tau_1-\theta)} Gw(\theta) d\theta) \\ \vdots \\ v(t-\tau_{L-1}) + Hw(t-\tau_{L-1}) + \int_{t-\tau_{L-1}}^{t} e^{A(t-\tau_{L-1}-\theta)} Gw(\theta) d\theta) \end{pmatrix}$$

Cette section a permis d'appliquer la problématique des systèmes à bruits corrélés au FMO. Dans le prochain paragraphe, nous développons notre approche afin de calculer la matrice de covariance des bruits P_L.

3.2.2.1 Calcul de la matrice de covariance des bruits

L'objectif est de pouvoir définir la matrice de covariance des bruits $P_L(t)$ aux cas des systèmes à bruits corrélés afin, de rendre l'estimation robuste à ce type de système. En effet, $P_L(t)$ intervient à la fois dans l'équation d'estimation et dans l'expression de l'erreur d'estimation de l'observateur. Afin d'évaluer $P_L(t) = \mathbb{E}[N_L(t) N_L^T(t)]$, nous exprimons chaque élément (bloc de taille n) de la matrice en fonction des instants τ_i et τ_j. Les blocs d'éléments de cette matrice sont définit en fonction de leur position et l'instant correspondant donné par : $P_L(t) = [p_{i,j}(t)]_{\substack{i=0,\dots,L-1 \\ j=0,\dots,L-1}}$:

$$\begin{aligned} p_{i,j}(t) = \mathbb{E}[&Hw(t-\tau_i)w(t-\tau_j)^T H^T + Hw(t-\tau_i)v(t-\tau_j) \\ &+ Hw(t-\tau_i) \int_{t-\tau_j}^{t} w(\theta)^T G^T e^{A^T(t-\tau_j-\theta)} C^T d\theta \\ &+ v(t-\tau_i)w(t-\tau_j)H^T + v(t-\tau_i)v(t-\tau_j) + v(t-\tau_i) \int_{t-\tau_j}^{t} w(\theta)^T G^T e^{A^T(t-\tau_j-\theta)} C^T d\theta \\ &+ \int_{t-\tau_i}^{t} Ce^{A(t-\tau_i-\theta)} Gw(\theta) d\theta w(t-\tau_j)^T H^T + \int_{t-\tau_i}^{t} Ce^{A(t-\tau_i-\theta)} Gw(\theta) d\theta v(t-\tau_j)^T \\ &+ \int_{t-\tau_i}^{t} Ce^{A(t-\tau_i-\theta)} Gw(\theta) d\theta \int_{t-\tau_j}^{t} w(\theta)^T G^T e^{A^T(t-\tau_j-\theta)} C^T d\theta] \end{aligned} \tag{3.18}$$

La matrice $P_L(t)$ est définit positive et symétrique. Même, si les propriétés de symétrie de la matrice impliquent que la partie triangulaire supérieur soit la transposée de la partie triangulaire inférieur, nous souhaitons vérifier de manière littérale cette assomption. Pour cela, le calcul de la matrice $P_L(t)$ sera divisé en trois cas :

— éléments de la diagonale ($\tau_i = \tau_j$),
— éléments de la partie triangulaire inférieure ($\tau_i < \tau_j$),
— éléments de la partie triangulaire supérieure ($\tau_i > \tau_j$).

3.2.2.2 Éléments de la diagonale

Les éléments de la diagonale correspondent au produit des termes de bruit pris aux mêmes instants ($\tau_i = \tau_j$) :

$$\begin{aligned} p_{i,i}(t) &= H\mathbb{E}[w(t-\tau_i)w(t-\tau_i)^T]H^T + H\mathbb{E}[w(t-\tau_i)v(t-\tau_i)] \\ &+ H\int_{t-\tau_i}^{t} \mathbb{E}[w(t-\tau_i)w(\theta)^T]G^T e^{A^T(t-\tau_i-\theta)}C^T d\theta \\ &+ \mathbb{E}[v(t-\tau_i)w(t-\tau_i)]H^T + \mathbb{E}[v(t-\tau_i)v(t-\tau_i)] \\ &+ \int_{t-\tau_i}^{t} \mathbb{E}[v(t-\tau_i)w(\theta)^T]G^T e^{A^T(t-\tau_i-\theta)}C^T d\theta \\ &+ \int_{t-\tau_i}^{t} Ce^{A(t-\tau_i-\theta)}G\mathbb{E}[w(\theta)w(t-\tau_i)^T]d\theta H^T \\ &+ \int_{t-\tau_i}^{t} Ce^{A(t-\tau_i-\theta)}G\mathbb{E}[w(\theta)v(t-\tau_i)^T]d\theta \\ &+ \int_{t-\tau_i}^{t}\int_{t-\tau_i}^{t} Ce^{A(t-\tau_i-\theta)}G\mathbb{E}[w(\theta)w(\theta)^T]G^T e^{A^T(t-\tau_i-\theta)}C^T d\theta d\theta \end{aligned} \tag{3.19}$$

A partir des Eq. (3.15) et (3.19) et des remarques précèdentes, nous obtenons l'équation simplifiée permettant de calculer les éléments de la diagonale de la matrice $P_L(t)$.

$$\begin{aligned} p_{i,j}(t) &= HQH^T + HJ + HQG^TC^T + J^TH^T + R + J^TG^TC^T + CGQH^T \\ &+ CGJ + CGQG^TC^T \end{aligned} \tag{3.20}$$

3.2.2.3 Elements du triangle supérieur

Les éléments du triangle supérieur correspondent aux éléments de la matrice dont l'indice de colonne est supérieur à l'indice de ligne $j > i$. A partir de l'Eq. (3.18) nous obtenons la solution suivante :

$$p_{i,j}(t) = HQG^T e^{A^T(\tau_i-\tau_j)}C^T + J^TG^T e^{A^T(\tau_i-\tau_j)}C^T \tag{3.21}$$

3.2.2.4 Elements du triangle inférieur

De manière similaire,nous obtenons la solution pour le calcul des éléments de la partie triangulaire inférieure :

$$p_{i,j}(t) = Ce^{A(\tau_i - \tau_j)}GQH^T + Ce^{A(\tau_i - \tau_j)}GJ \tag{3.22}$$

Nos développements ont permis d'obtenir une écriture théorique de la matrice de covariance $P_L(t)$. De plus, les équations (Eq. (3.21) et (3.22)) des éléments des triangles supérieur et inférieur de la matrice, vérifient les propriétés de symétrie énoncées précédemment. La connaissance de cette matrice permet de réaliser la synthèse de l'observateur appliqué aux systèmes à bruits corrélés. De plus, l'équation d'estimation prend mieux en compte les propriétés de bruit du systèmes étudiés, sachant que l'erreur d'estimation (c.f chapitre 2) de l'observateur est fonction de la matrice de covariance des bruits.

3.2.3 Résultats

3.2.3.1 Modélisation du système

La simulation de l'estimation utilisant le FMO s'appuie sur un modèle sous forme de représentation d'état d'un moteur à courant continu 24V illustré par la Figure 3.4. Ce moteur correspond à une référence du catalogue Maxon, modèle F2260, numéro 885 [Maxon, 2020].

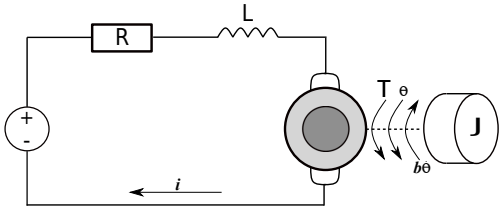


Figure 3.4 – Schéma moteur courant continu 24V

Le modèle de connaissance est construit à l'aide des équations électrique et mécanique suivantes :

$$\begin{cases} J\ddot{\theta} + b\dot{\theta} = Ki \\ L\dfrac{di}{dt} + Ri = U - K\dot{\theta} \end{cases} \tag{3.23}$$

Deux capteurs fournissent les mesures de vitesse angulaire (rad/s) et d'intensité (A). Les bruits de processus sont corrélés avec les bruits de mesures, ce qui conduit à la représentation d'état

suivante :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + Gw(t) \\ y(k) = Cx(k) + Hw(k) + v(k) \end{cases} \tag{3.24}$$

avec les matrices associées,

$$A = \begin{pmatrix} -\frac{b}{J} & \frac{K}{J} \\ -\frac{K}{L} & -\frac{R}{L} \end{pmatrix}, B = \begin{pmatrix} 0 \\ \frac{1}{L} \end{pmatrix},$$

$$A = \begin{pmatrix} -0.5581 & 775.19 \\ -178.57 & -2571.42 \end{pmatrix}, B = \begin{pmatrix} 0 \\ 1785.71 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, G = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, H = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

et les conditions initiales du système $x_0 = [0, 0]^T$.

Le système est régulé en vitesse à l'aide d'un régulateur PID (Figure 3.5).

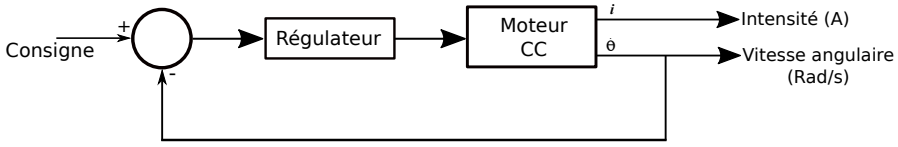


Figure 3.5 – Schéma du système avec régulation PID

Le bruit de mesure est considéré gaussien à moyenne nulle et de variance R, le bruit de processus est également considéré gaussien à moyenne nulle et de variance Q, la corrélation entre ces deux bruits est donnée par la matrice de covariance J. Les valeurs numériques seront définies pour chaque scénario. Les simulations fournissent les estimations, $\hat{x}_{L_1}(t)$ et $\hat{x}_{L_2}(t)$, à partir de deux observateurs de taille de fenêtre respective $L_1 = 3$ et $L_2 = 4$.

L'analyse des résultats est basée sur la génération de deux vecteurs de résidus, définis de la façon suivante :

$$\begin{cases} r_1(k) = y(k) - C\hat{x}_{L_1}(k) \\ r_2(k) = y(k) - C\hat{x}_{L_2}(k) \end{cases} \tag{3.25}$$

L'étude de l'espérance et de la variance de ces résidus est présentées en annexe C.

3.2.3.2 Scénario 1 : cas idéal

Les propriétés statistiques des bruits appliqués sont identiques aux valeurs prises pour la synthèse de l'observateur. Les matrices des bruits sont :

$$Q = 0.01, J = \begin{pmatrix} 0.01 & 0.01 \end{pmatrix}, R = \begin{pmatrix} 0.1 & 0 \\ 0 & 0.1 \end{pmatrix}$$

Les propriétés des vecteurs des bruits réels du système sont :

$$\overline{v} = \begin{pmatrix} 1.37 \times 10^{-3} \\ 1.29 \times 10^{-3} \end{pmatrix}, var(v) = \begin{pmatrix} 0.101 & 0.0103 \\ 0.0103 & 0.00980 \end{pmatrix}, \overline{w} = 2.18 \times 10^{-4}, var(w) = 9.80 \times 10^{-3}$$

En simulation, nous réalisons l'estimation du système présenté précédemment à l'aide de l'observateur à mémoire finie développé. La figure 3.6 présente les résidus (Eq. (3.25)). Les résidus r_1 et r_2 apportent l'erreur entre la mesure (y) et la mesure estimée $(i.e\ C\hat{x}_L)$ en utilisant respectivement les tailles de fenêtre $L_1 = 3$ et $L_2 = 4$.

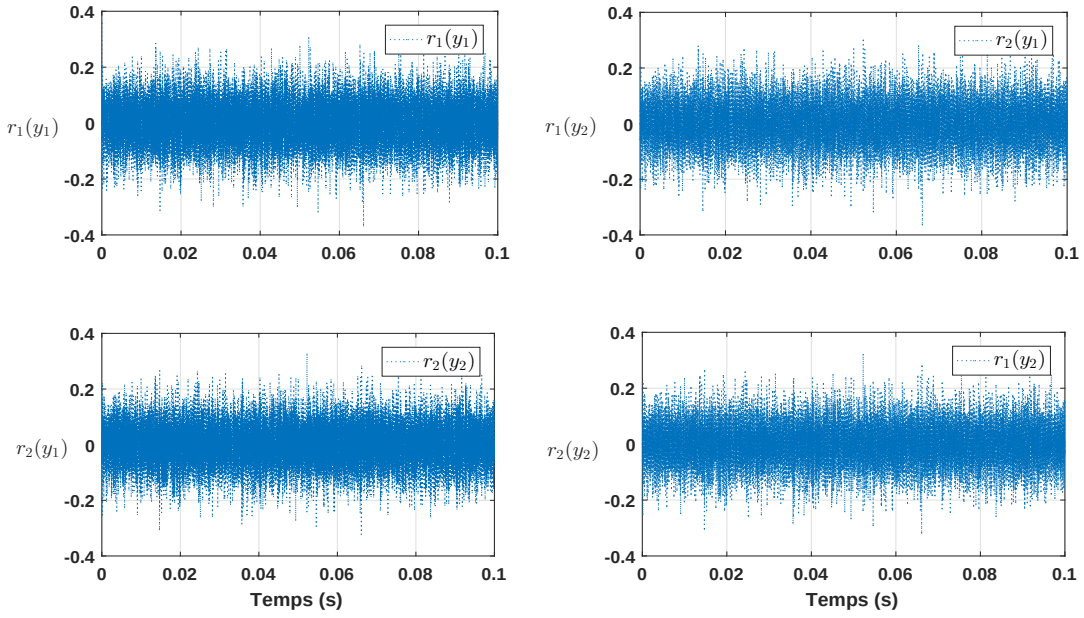


Figure 3.6 – Évolution des résidus - scénario 1

Nous remarquons que les résidus sont confinés dans un intervalle et qu'ils ne divergent pas pour chaque composante des mesures. La moyenne et la variance de ces résidus ont également été étudiées et sont présentées dans le tableau 3.1.

Tableau 3.1 – Espérance et variance des résidus - scénario 1

Résidu		Obtenus par simulation	Obtenus depuis l'écriture littérale
r_1	$\overline{r_1}$	$\begin{pmatrix} 2.51 \times 10^{-5} \\ 3.72 \times 10^{-5} \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
	$\mathbb{V}ar$	$\begin{pmatrix} 7.39 \times 10^{-3} \\ 7.59 \times 10^{-3} \end{pmatrix}$	$\begin{pmatrix} 8.10 \times 10^{-2} & 2.15 \times 10^{-2} \\ 2.15 \times 10^{-2} & 7.612.15 \times 10^{-2} \end{pmatrix}$
r_2	$\overline{r_2}$	$\begin{pmatrix} 2.08 \times 10^{-4} \\ 2.85 \times 10^{-4} \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
	$\mathbb{V}ar$	$\begin{pmatrix} 6.59 \times 10^{-3} \\ 6.75 \times 10^{-3} \end{pmatrix}$	$\begin{pmatrix} 9.43 \times 10^{-3} & 2.14 \times 10^{-3} \\ 2.14 \times 10^{-3} & 9.04 \times 10^{-3} \end{pmatrix}$

Les résultats démontrent l'efficacité de la méthode basée FMO pour des systèmes comportant une corrélations entre les bruits de mesure de système.

3.2.3.3 Scénario 2 : cas d'incertitudes sur les matrices des bruits

Nous souhaitons mettre en avant dans cette partie la robustesse de notre estimateur face aux incertitudes sur les bruits du système. Pour cela, les matrices de bruit utilisées pour la synthèse de l'observateur sont biaisées par rapport à la simulation précédente. Les bruits "réels" appliqués au système restent les mêmes.

Définissons les matrices de bruit Q, J, et R pour le système réel (3.17) telles que :

$$Q = 0.01, J = \begin{pmatrix} 0.01 & 0.01 \end{pmatrix}, R = \begin{pmatrix} 0.01 & 0 \\ 0 & 0.01 \end{pmatrix},$$

et les moyennes et variances respectives des bruits du système simulé telles que :

$$\overline{v} = \begin{pmatrix} 1.37 \times 10^{-3} \\ 1.29 \times 10^{-3} \end{pmatrix}, var(v) = \begin{pmatrix} 0.101 & 0.0103 \\ 0.0103 & 0.00980 \end{pmatrix}, \overline{w} = 2.18 \times 10^{-4}, var(w) = 9.80 \times 10^{-3}$$

Les valeurs biaisées appliquées aux matrices de bruits utilisées pour le calcul de la matrice P_L^{-1} et donc de la synthèse de l'observateur sont décrites ci-dessous :

$$Q = 0.001, J = \begin{pmatrix} 0.009 & 0.009 \end{pmatrix}, R = \begin{pmatrix} 0.01 & 0 \\ 0 & 0.01 \end{pmatrix},$$

Les résidus obtenus Figures 3.7 ne présentent ni variations brusques, ni biais. Les résidus r_1 et r_2 présentent une erreur convergente vers zéro comme lors du cas 1. Cette fois ci, la dispersion est plus importante, car provoquée par la sous-estimation des espérances mathématiques concernant les corrélations entre les bruits de processus et de mesure. Ces résultats sont confirmés par l'analyse statistique du tableau 3.2.

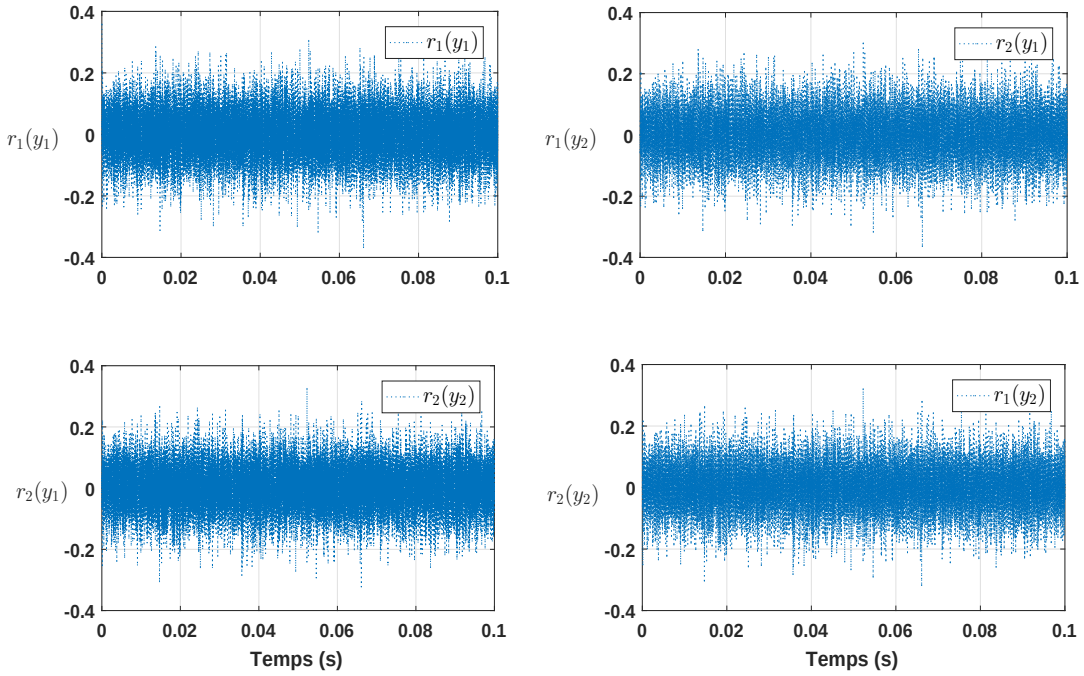


Figure 3.7 – Évolution des résidus - scénario 2

Tableau 3.2 – Espérance et variance des résidus - scénario 2

Résidu		Obtenus par simulation	Obtenus depuis l'écriture littérale
r_1	$\overline{r_1}$	$\begin{pmatrix} 2.51 \times 10^{-5} \\ 3.72 \times 10^{-5} \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
	$\mathbb{V}ar$	$\begin{pmatrix} 7.39 \times 10^{-3} \\ 7.59 \times 10^{-3} \end{pmatrix}$	$\begin{pmatrix} 8.10 \times 10^{-2} & 2.15 \times 10^{-2} \\ 2.15 \times 10^{-2} & 7.612.15 \times 10^{-2} \end{pmatrix}$
r_2	$\overline{r_2}$	$\begin{pmatrix} 2.08 \times 10^{-4} \\ 2.85 \times 10^{-4} \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
	$\mathbb{V}ar$	$\begin{pmatrix} 6.59 \times 10^{-3} \\ 6.75 \times 10^{-3} \end{pmatrix}$	$\begin{pmatrix} 9.43 \times 10^{-3} & 2.14 \times 10^{-3} \\ 2.14 \times 10^{-3} & 9.04 \times 10^{-3} \end{pmatrix}$

Les résultats confirment la performance et la robustesse de notre observateur face aux bruits de mesures processus avec les bruits de mesure. Il est intéressant de noter que la sous-estimation ou la sur-estimation des propriétés des bruits corrélés présente un impacte moindre sur l'aspect filtrage.

3.3 Conclusion

Ce chapitre avait pour but de présenter les résultats obtenues lors de l'utilisation d'observateur à mémoire finie pour les systèmes incertains et les systèmes à bruits corrélés. Chaque synthèse d'observateurs a été illustrée par un exemple de simulation.

Chapitre 4

Cyber-attaque d'un système télé-opéré

Contenu du chapitre

4.1 Introduction

Comme déjà énoncé dans les chapitres précédents, l'intégrité des données est de plus en plus menacée par les cyber-attaques visant à les modifier. L'intégrité ne pouvant pas être toujours vérifiée par les outils traditionnels, les données corrompues sont alors utilisées par le système industriel et peuvent être sources de risque en menant éventuellement le système dans un état non-acceptable.

Dans ce cadre, nous allons dans un premiers temps étudier un type d'attaque intelligente opérant sur les systèmes télé-opérés, puis nous appliquerons nos stratégies en simulation sur un système télé-opéré.

4.2 Plateforme expérimentale IoT-CIA

4.2.1 Système haptique bilatéral

Le système d'étude est composé de deux robots télé-opérés échangeant des informations via un réseau de communication. Un robot à le statut de maître et l'autre d'esclave, l'objectif étant que le robot esclave suive en position et en vitesse le robot maitre. Afin de synchroniser les deux robots, les informations de position (angulaire) et de vitesse (angulaire) de chaque robot sont transmises vers leurs contrôleurs respectifs.

Dans le cadre du projet financé par la Région Centre APR IA IoT-CIA-DATA 2017 119984, réalisé en collaboration avec le laboratoire LIFO, un démonstrateur a été mis en place. Ce démonstrateur (présenté Figure 4.1) permettra lors de la finalisation du projet de tester les solutions développées par le laboratoire LIFO et le laboratoire PRISME.

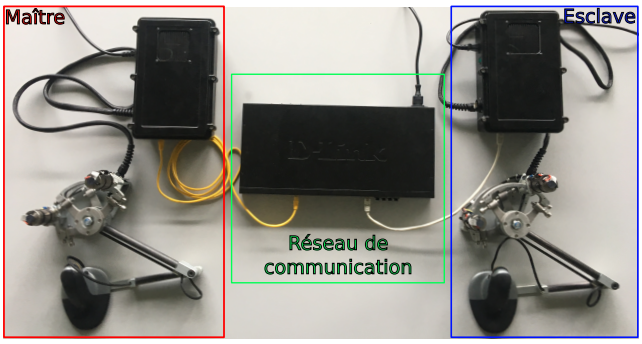


Figure 4.1 – Plateforme expérimentale d'un système de robot télé-opéré

Nous souhaitons, tester en simulation, nos outils avant toute implémentation sur cette plateforme. Pour cela, nous utilisons une modélisation (ou plateforme numérique) de la plateforme expérimentale afin d'analyser le comportement de nos outils.

4.2.2 Plateforme numérique

L'architecture de cette plateforme numérique est présentée en Figure 4.2.

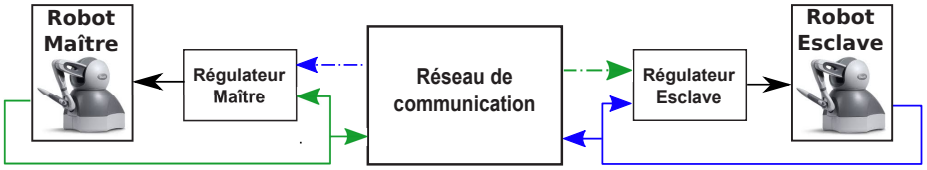


Figure 4.2 – Système téléopéré communicant à travers un réseau de communication

Pour modéliser ce système, nous utilisons les équations de la dynamique du robot, les deux robots étant identiques. Ce robot, à n degrés de libertés, sans frottement ni perturbation externe, est décrit par ([Hokayem et Spong, 2006], [Hatanaka *et al.*, 2015] et [Dong *et al.*, 2016]) :

$$\begin{cases} M_m(q_m)\ddot{q}_m + C_m(q_m,\dot{q}_m)\dot{q}_m + G_m(q_m) &= \tau_m + \tau_h \\ M_s(q_s)\ddot{q}_m + C_s(q_s,\dot{q}_s)\dot{q}_s + G_s(q_s) &= \tau_s - \tau_{env} \end{cases} \tag{4.1}$$

Les matrices d'inertie sont notées M_i, les matrices des couples centrifuges et effet Coriolis C_i et les matrices des couples gravitationels G_i. Les positions et vitesses sont respectivement notées q, $\dot{q} \in \mathbb{R}^n$. Le couple exercé par un opérateur sur le robot maître et celui exercé par l'environnement sur le robot esclave (retour de couple de l'environnement vers le couple exercé par l'opérateur) sont notés respectivement τ_h et τ_{env}. Le contrôle en couple de chaque robot est donné respectivement par τ_m et τ_s.

Dans un cas sans attaque sur le réseau de communication, les données reçues correspondent à celles envoyées. Nous notons l'information provenant du réseau de communication $(q_i^*, \dot{q}_i^*)$, et $(q_i, \dot{q}_i)$ celle du robot en local, d'où :

$$[q_m^{*T}, \dot{q}_m^{*T}, q_s^{*T}, \dot{q}_s^{*T}] = [q_m^T, \dot{q}_m^T, q_s^T, \dot{q}_s^T].$$

Les échanges de données permettant d'assurer la synchronisation des deux robots sont présentés en Figure 4.3.

Un régulateur PD est utilisé pour générer les lois de commande :

$$\begin{cases} u_m(t) = -K_d(\dot{q}_m(t) - \dot{q}_s^*(t)) - K_p(q_m(t) - q_s^*(t)) - K_{dm}\dot{q}_m(t) \\ u_s(t) = -K_d(\dot{q}_s(t) - \dot{q}_m^*(t)) - K_p(q_s(t) - q_m^*(t)) - K_{dm}\dot{q}_s(t) \end{cases} \tag{4.2}$$

Chaque loi de commande prend en compte les informations (position et vitesse) des deux robots.

Figure 4.3 – Architecture du système télé-opéré

Les couples liés à la gravité sont compensés par la régulation et les matrices C_i sont définies nulles. Dans le cas d'un robot à un degré de liberté, le modèle linéarisé autour du point de fonctionnement $(q_f, \dot{q}_f)$ donne la réprésentation d'état en boucle fermée suivante :

$$\begin{cases} \dot{x}_m(t) &= \begin{pmatrix} 0 & 1 \\ -M^{-1}K_p & -M^{-1}(K_d + K_{dm}) \end{pmatrix} x_m(t) + \begin{pmatrix} 0 \\ M^{-1} \end{pmatrix} \tau_h + \begin{pmatrix} 0 & 0 \\ K_p & K_d \end{pmatrix} \begin{pmatrix} q_s^* \\ \dot{q}_s^* \end{pmatrix} \\ \dot{x}_s(t) &= \begin{pmatrix} 0 & 1 \\ -M^{-1}K_p & -M^{-1}(K_d + K_{dm}) \end{pmatrix} x_s(t) - \begin{pmatrix} 0 \\ M^{-1} \end{pmatrix} \tau_{env} + \begin{pmatrix} 0 & 0 \\ K_p & K_d \end{pmatrix} \begin{pmatrix} q_m^* \\ \dot{q}_m^* \end{pmatrix} \end{cases} \tag{4.3}$$

$$y_i(k) = Cx_i(k) + v_i(k)$$

avec $x_i(t) = \begin{pmatrix} q_i(t) \\ \dot{q}_i(t) \end{pmatrix}$, où les indices $i = m,\ s$ correspondent respectivement au robot maitre et esclave, v_i est le vecteur des bruits de mesure et C la matrice des mesures ici égale à l'identité.

4.3 Cyber-attaques

Nous utilisons les travaux de [Dong *et al.*, 2016] qui consistent en une modification des données transitant sur le réseau de communication avant leur réception par les contrôleurs dédiés (Figure 4.4). Cette attaque modifie à la fois la position et la vitesse de manière à conserver la cohérence entre les variations de la position et la vitesse rendant ainsi la détection plus difficile. La conservation de cette cohérence justifie le terme d'attaque "intelligente" utilisée dans la littérature.

L'objectif de cette attaque est d'amener le système vers un point de fonctionnement autre que celui désiré. Dans le cas de notre système télé-opéré, ceci se traduit par une trajectoire du robot esclave différente de celle du robot maître tout en respectant le domaine admissible des états du système. Dans leurs travaux [Dong *et al.*, 2016] proposent de modifier les données transmises à l'aide de deux types d'attaque, une première statique et la seconde dynamique.

Figure 4.4 – Architecture du système télé-opéré

4.3.1 Attaque statique

Dans ce type d'attaque, les données sont altérées à l'aide d'un gain constant K, afin de modifier la loi de commande, et ainsi dévier la trajectoire du robot esclave. La relation entre les données en entrée et en sortie du réseau de communication est décrite ci-dessous :

$$[q_s^{*T}, \dot{q}_s^{*T}, q_m^{*T}, \dot{q}_m^{*T}] = K[q_s^T, \dot{q}_s^T, q_m^T, \dot{q}_m^T]$$

Les auteurs [Dong *et al.*, 2016] proposent un calcul du gain K reposant sur les propriétés de la fonction de Lyapunov.

4.3.2 Attaque dynamique

Dans le cas de ce type d'attaque, les gains évoluent au cours du temps de manière à modifier dynamiquement les données. L'objectif reste, ici aussi de modifier le fonctionnement du système, tout en ayant une attaque non détectable. En effet, la conception de ces gains repose sur le principe que les modifications respectent que le calcul de la dérivée de la position soit égal à la vitesse, c'est-à-dire :

$$\left| \dot{q}^*(t) - \frac{dq^*(t)}{dt} \right| \leq \epsilon(t). \tag{4.4}$$

Le terme $\epsilon(t)$ est introduit de manière à tenir compte des bruits de mesures et des éventuelles incertitudes.

Ce type d'attaque correspond aux équations suivantes :

$$\begin{aligned} q_s^* &= \gamma_s q_s + \alpha_s q_m \\ q_m^* &= \gamma_m q_m + \alpha_m q_s \\ \dot{q}_s^* &= \hat{\gamma}_s q_s + \hat{\alpha}_s q_m + \gamma_s \dot{q}_s + \alpha_s \dot{q}_m \\ \dot{q}_m^* &= \hat{\gamma}_m q_m + \hat{\alpha}_m q_s + \gamma_m \dot{q}_m + \alpha_m \dot{q}_s \end{aligned} \tag{4.5}$$

où les gains sont calculés par,

$$\begin{aligned}
\alpha_i(t) &= \sum_{k=0}^{\infty} \alpha_0 e^{-\frac{K_p}{K_d}(t-kT)} U_k(t) \\
\hat{\alpha}_i(t) &= -\frac{K_p}{K_d}\alpha_i(t) \\
\gamma_i(t) &= \sum_{k=0}^{\infty} \left[(\gamma_0 - 1) e^{-\frac{K_p}{K_d}(t-kT)} + 1 \right] U_k(t) \\
\hat{\gamma_i} &= -\frac{K_p}{K_d}(\gamma_i(t) - 1)
\end{aligned}$$

et $U_k(t) = U(t - kT) - U(t - (k + 1)T)$, où $U(t)$ est la fonction de Heaviside et $T = \frac{K_d}{K_p} min\left(ln(1-\gamma_0), ln(\frac{K_D}{K_{dm}}(\alpha_0 + \gamma_0 - 1))\right)$.

4.4 Système télé-opéré : attaque dynamique

4.4.1 Système d'étude

Afin de tester nos résultats, nous reprenons le système étudié dans les travaux déja cités de [Dong *et al.*, 2016]. Les robots sont considérés à un degré de liberté, une longueur de bras de 1 m et une masse de 1 kg et des positions initiales identiques pour les deux robots ($q_i = 0.1$ rad et $\dot{q}_i = 0$ rad/s $(i = m, s)$). La période d'échantillonnage est fixée à $T_e = 0.001$ s et les variances des bruits de mesure sont respectivement 10^{-5} et 10^{-7}. Les paramètres des régulateurs (Eq.4.2) sont : $K_p = 1$, $K_d = 0.5$ et $K_{dm} = 0.5$. L'opérateur déplace le robot maître, le robot esclave doit alors le suivre en position et en vitesse.

4.4.2 Estimation du système - cas sans attaque

Nous souhaitons dans un premier temps présenter les estimations réalisées par l'observateur à mémoire finie dans le cas sans attaque. Les deux tailles de fenêtre choisit sont $K_{L_{D_1}} = 6$ et $K_{L_{D_2}} = 5$. Les résidus présentés seront accompagnés par les seuils de détection (Fig 4.5 et Fig 4.6) obtenus à partir de l'étude des propriétés des résidus (c.f § 2.3.2.1).

Les résidus (robot maître et robot esclave) après convergence de l'observateur sont correctement encadrés par les seuils de détection lorsque aucune attaque n'est réalisée.

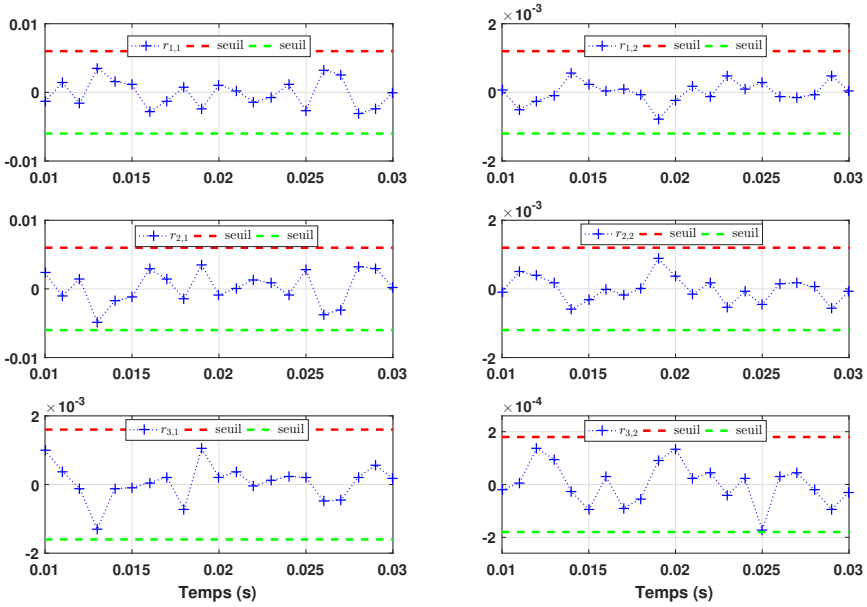


Figure 4.5 – Estimations et seuils de détection - Robot maître sans attaque

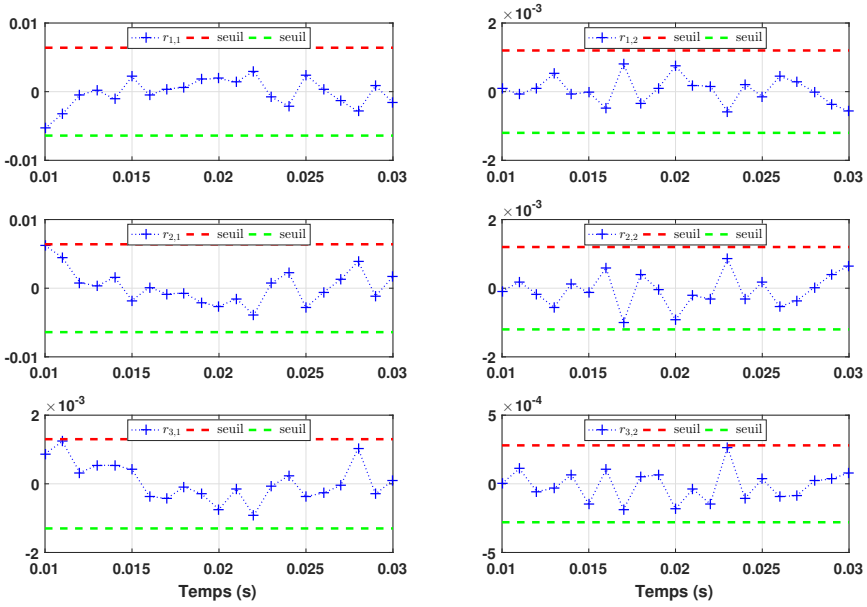


Figure 4.6 – Estimations et seuils de détection - Robot esclave sans attaque

4.4.3 Attaque synchrone

Dans les travaux de [Dong *et al.*, 2016] l'attaque est réalisée dès le premier échange de données. Cette attaque est donc synchrone avec le démarrage du système. L'observateur à

mémoire finie nécessite que la fenêtre de données soit intègre. Notre outils ne doit donc pas être en mesure de détecter ce type d'attaque.

Les données reçues du réseau de communication avec et sans attaque sont présentées Figure 4.7.

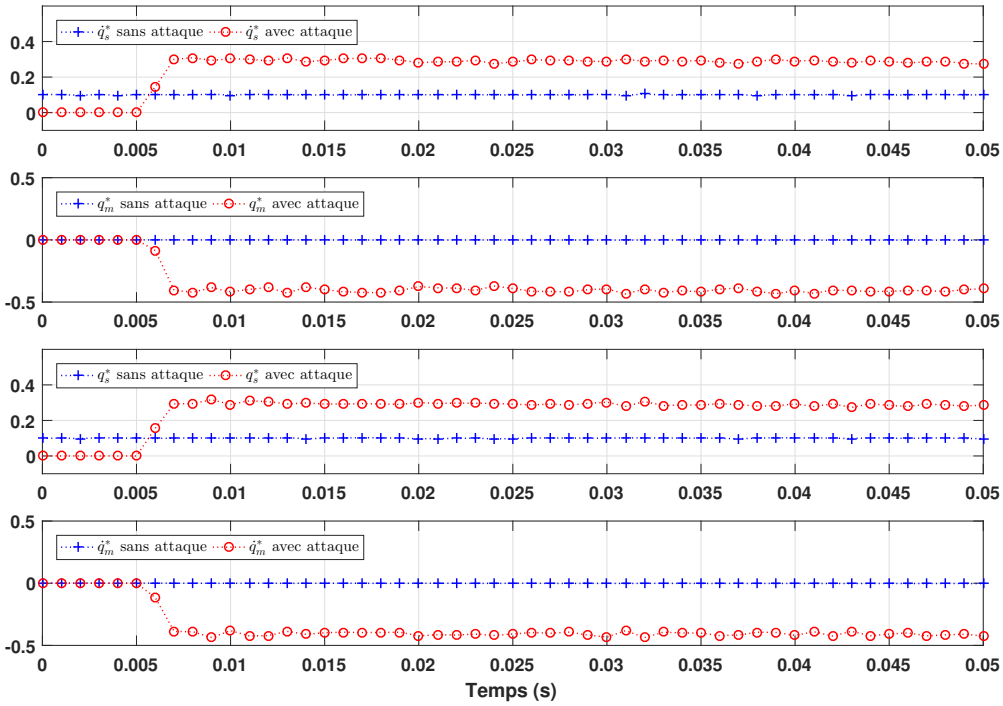


Figure 4.7 – Données reçues du réseau de communication - cas avec et sans attaque synchrone

L'attaque amène à faire croire au régulateur que les positions initiales des deux robots sont à zéro.

4.4.4 Détection de l'attaque

Les résidus obtenus sur le système comportant l'attaque décrite précédemment sont présentés Figure 4.8 et Figure 4.9.

Nous remarquons que dès la première estimation ($t = 0.005\ s$), les résidus générés dépassent les seuils de détection. Puis après une phase de convergence, malgré la perte d'intégrité de la fenêtre (attaque synchrone), les résidus oscillent en dehors des seuils. Les seuils de détection sont déterminés selon une loi normale centrée de variance $\mathbb{V}(r_{i,j})$ ($i \in \{1,2,3\}$, $j \in \{1,2\}$), en prenant un risque de première espèce égal à 5%.

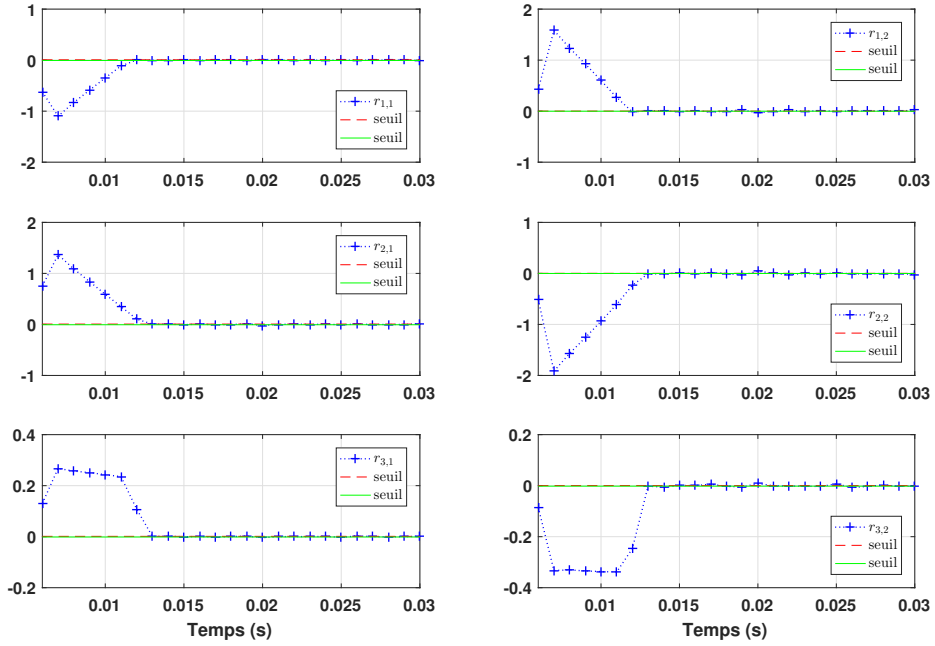


Figure 4.8 – Résidus - Robot esclave avec attaque

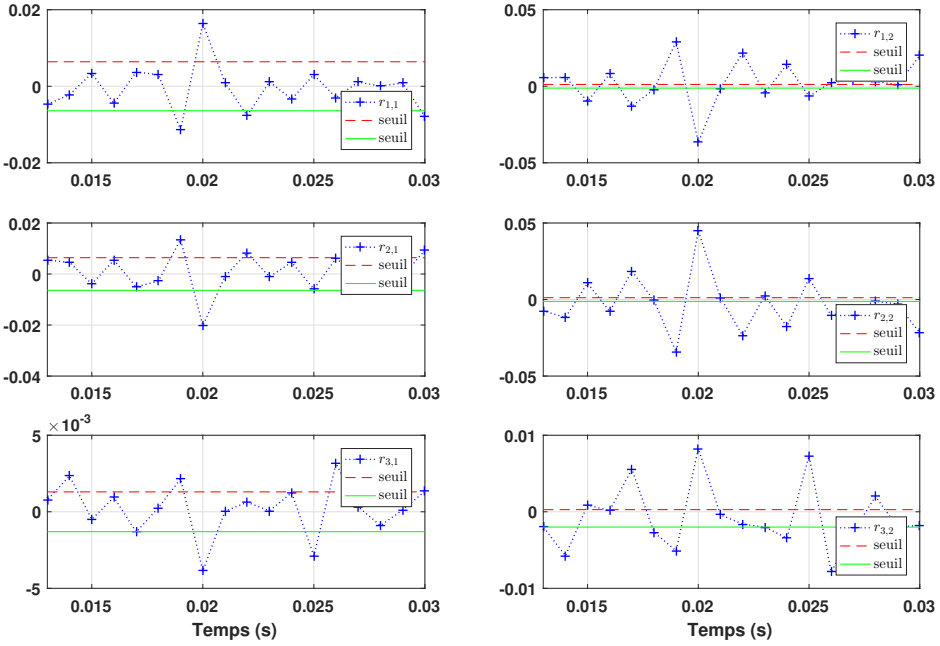


Figure 4.9 – Zoom de la Figure 4.8

Les alarmes générés par le dépassement de ces seuis sont présentées Figure 4.10.

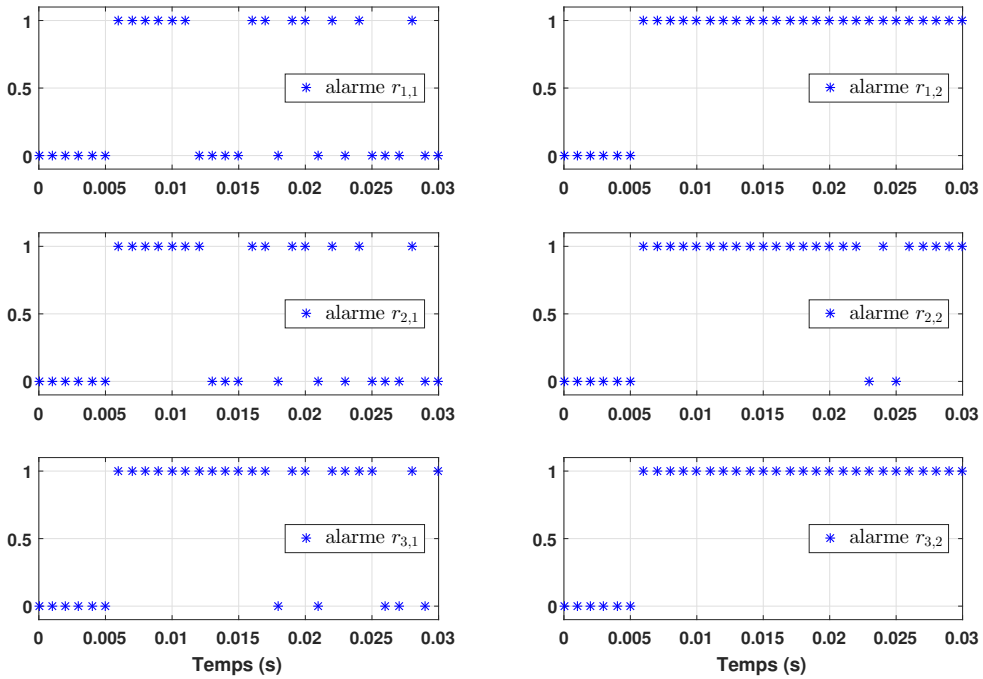


Figure 4.10 – Alarmes - Robot maître avec attaque

Nous pouvons conclure que malgré la perte d'intégrité de la fenêtre temporelle de l'observateur à mémoire finie due à l'attaque synchrone, l'estimation a permis de générer des résidus suffisamment sensibles pour alerter sur la présence d'une attaque.

Bien que la fenêtre de mesure initiale porte que des données dont l'intégrité est perdue, en raison d'une attaque synchronisé au démarrage du système, les estimations obtenues à partir de l'observateur à mémoire finie ont permis de générer des résidus suffisamment sensibles pour détecter la perte d'intégrité.

Dans le cas où l'attaque commence après le démarrage du système, la détection est bien plus facile encore.

4.5 Systèmes télé-opérés incertains : cas de l'attaque statique

4.5.1 Système incertain

Continuons avec le système télé-opéré utilisé précédemment (c.f § 4.4). Nous prendrons pour notre exemple une incertitude sur la matrice A tels que $[A]$ soit donnée par :

$$[A] \approx \begin{pmatrix} [0\ 0] & [1\ 1] \\ [-1.01010\ \ -0.99009] & [-1.01010\ \ -0.99009] \end{pmatrix}$$

Sans perte de généralité dans les résultats, nous présentons le cas déterministe. Cette hypothèse reste valable tant que le niveau de bruit est petit par rapport aux incertitudes de la matrice d'état A.

4.5.2 Attaque

L'attaque statique est perpétrée dans l'intervalle $[t = 0.21\ s, t = 0.26\ s]$ de manière à modifier de 2% les valeurs des positions et des vitesses échangées par rapport à leur valeur initialement envoyée.

4.5.3 Effet de l'attaque

L'attaque modifie les trajectoires en position et en vitesse du robot esclave. Ces trajectoires sont comparées à celles d'un système sans attaque (Figure 4.11).

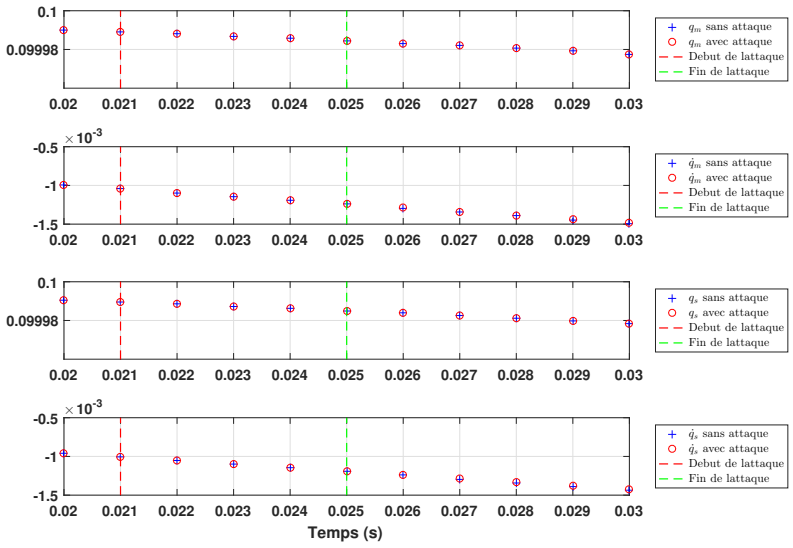


Figure 4.11 – Trajectoire du système avec et sans attaque

On remarque que les valeurs sans ou avec attaque sont relativement proches et qu'il est impossible au lecteur de les différencier.

4.5.4 Stratégie de détection dans le cas des systèmes incertains

Dans le cas de systèmes incertains, la perte d'intégrité doit être détectée dès lors que les valeurs des données reçues sortent de l'enveloppe des incertitudes du système. Pour cela, nous réalisons les estimations selon la même stratégie que précèdement (c.f § 2.3) en utilisant l'observateur à mémoire finie par intervalle proposé au chapitre 3.

Une donnée est considérée intègre dès lors que celle-ci est contenue dans l'intervalle d'estimation obtenue à partir du FMO. Si la mesure n'est pas contenue dans cet intervalle, une alarme est générée, puis une correction est effectuée. Cette stratégie repose sur trois phases *détection - décision - correction* réalisées à chaque instant d'échantillonnage.

4.5.5 Détection de l'attaque et décision

Quand l'attaque apparait à $t = 0.21s$, les données maître reçues ne sont plus contenues dans l'intervalle d'estimation (Figure 4.12), ce qui déclenche une alarme présentée en Figure 4.13.

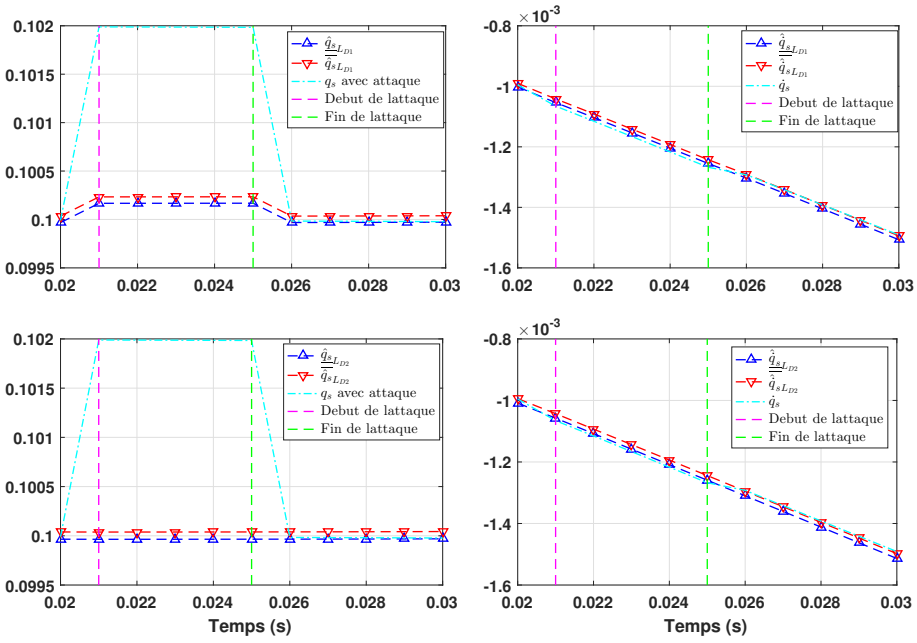


Figure 4.12 – Intervalle d'estimation des données reçues du robot esclave

Cette détection effectuée en temps voulu, permettra de corriger rapidement les données reçues, et ainsi transmettre au régulateur du robot maître des données fiabilisées.

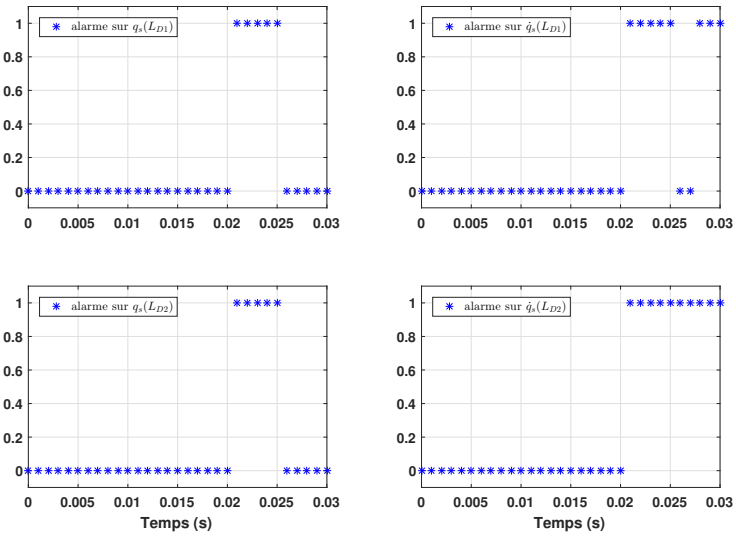


Figure 4.13 – Alarmes associées au robot maitre

4.5.6 Correction des données

Dès lors que nous avons été capables de détecter la perte d'intégrité, une correction est effectuée sur les données transmises au régulateur décentralisé. L'intérêt de cette correction est illustré (Figure 4.14) par la comparaison de l'évolution des sorties du système attaqué dans les cas avec et sans correction.

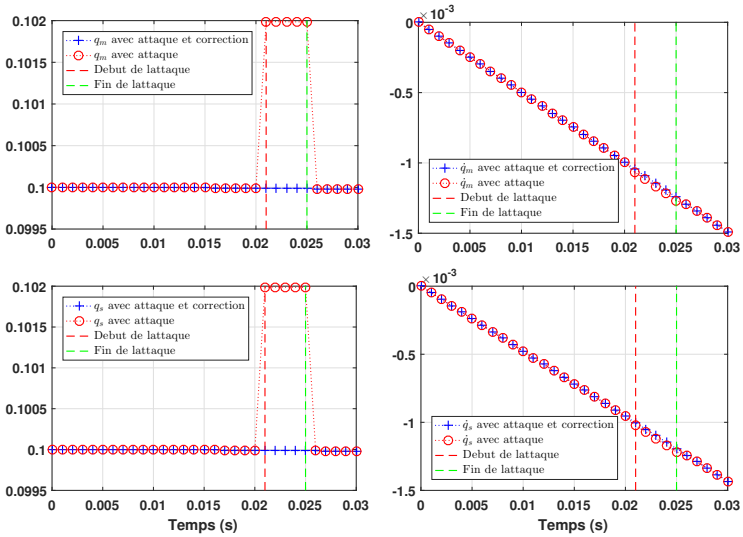


Figure 4.14 – Trajectoires du système attaqué avec et sans correction de données

La détection de la perte d'intégrité des données reçues a permis de les corriger, permettant ainsi au système de conserver la trajectoire initialement souhaitée.

4.6 Conclusion

Ce chapitre réunit les travaux effectués pour l'observateur à mémoire finie dans le contexte de cyber-attaques (c.f. Chapitre 2), et ceux réalisés pour la conception d'observateur à mémoire finie avec prise en compte des incertitudes de modélisation (c.f. Chapitre 3). L'union de ces travaux a été réalisée sur un exemple inscrit dans les problématiques soulevés dans le chapitre 1. De plus, celui-ci s'inscrit clairement dans le développement de la plateforme liée au projet IoT-CIA. Malheureusement, l'utilisation de la plateforme n'a pas pu être finalisée avant la fin de nos travaux, me privant de la confrontation simulation / expérimentation.

Conclusion Générale et Perspectives

Synthèse

Dans le premier chapitre nous avons abordé, sans être exhaustif, un état de l'art des thématiques concernant les systèmes interconnectés en réseau. Puis la structure des réseaux industriels et les échanges ayant lieu sur ceux-ci ont été explicités. Egalement, La structure et la modélisation des systèmes interconnectés a été présentée.

Dans un second temps, la sécurité de tels systèmes lors d'applications industrielles ont été étudiés. Finalement, une ouverture sur la prise en compte des incertitudes paramétriques et de corrélations de bruits a été présentée.

Le deuxième chapitre A été consacré à la conception et aux développements de l'observateur à mémoire finie dans le contexte des systèmes interconnectées en réseau. Dans un premier temps, une présentation de l'observateur à mémoire finie classique a été réalisée afin d'introduire les mécanismes d'un tel observateur. Puis, la synthèse et des propriétés temporelles ont été proposées, consolidant à notre sens l'utilisation de ce type d'observateur à modèle temps continu et mesures discrétisées.

Dans un second temps, la synthèse d'un observateur à mémoire finie dans le contexte de perte de paquets a été réalisée puis analysée. Cette synthèse propose une nouvelle formulation permettant de moduler les équations permettant l'estimation en fonction des données disponibles ainsi que de leur horodatage. L'étude numérique par simulation de cet outil a présentée la robustesse et les atouts de cet observateur.

Finalement, l'élaboration d'une stratégie utilisant l'observateur à mémoire finie dans un contexte de perte d'intégrité a été réalisée. Cette stratégie reposant sur l'utilisation de différentes fenêtres dont la composition et la taille diffèrent, a permis de réaliser un outil "détection-décision-correction" de la perte d'intégrité des données reçues via le réseau de communication. À l'appui de simulation, cette stratégie a été efficace et performante pour la détection, la décision ainsi que pour la correction.

Le troisième chapitre présente l'apport de nos travaux pour la prise en compte d'incertitudes systèmes par l'observateur à mémoire finie. La première partie, contient la synthèse d'un observateur à mémoire finie par intervalle afin de réaliser l'estimation de systèmes incertains.

La deuxième partie est composée de la synthèse d'un observateur à mémoire finie afin de permettre de prendre en compte les corrélations des bruits entre les mesures et les états. Chaque partie a été illustrée à l'aide de simulations numériques présentant le fonctionnement et les résultats des estimations des observateurs synthétisés.

Le dernier chapitre réalise le lien entre les différents observateurs synthétisés précédemment, à l'aide d'un système de robots télé-opérés. Le choix de ce système a été motivé afin de réaliser une preuve de concept de nos travaux précédents avant leurs essais sur un démonstrateur lié au projet APR IA IoT-CIA-DATA 2017 119984. Ce chapitre présente la détection d'une attaque dynamique sur un système télé-opéré illustrée par une simulation. Puis, dans un second temps, la détection d'une attaque statique sur ce système incertain est réalisée. Dans ces deux cas, l'observateur à mémoire finie a été capable de réaliser sa tâche de *détection-décision-correction*.

Perspectives sur le plan théorique

Concernant le chapitre 2, le développement de l'estimation asynchrone par l'observateur à mémoire finie pourrait être réalisé afin de répondre aux problématiques des réseaux dont l'échantillonnage ne serait pas cadencé à pas fixe. De plus, nous pourrions élargir le type de perturbation réseau, afin de répondre aux problématiques de retards, congestion... Également, la vérification de la robustesse de notre observateur, face aux pertes de paquets, pourrait être réalisée.

Le chapitre 3 se focalise sur le développement d'observateur pour des systèmes incertains. Dans le cas de l'observateur à mémoire finie par intervalle, il serait judicieux d'améliorer la forme intervalle de la modélisation par l'utilisation d'équations incertaines polytopiques ou de zonotopes.

Perspectives sur le plan applicatif

L'intégration de nos travaux sur la plateforme expérimentale est une perspective majeure. Par cette intégration, la validation expérimentale de nos travaux permettrait d'engranger un retour d'expérience sur le cas applicatif à l'aide de divers travaux :

— Tester la prise en compte des incertitudes de modélisation de la plateforme expérimentale par nos outils,

— Améliorer la détection et réaliser la localisation de la perte d'intégrité,

— Développement du FMO à entrées inconnues et prise en compte d'attaque sur la commande,

— Implémenter la génération d'attaques par perte de paquets et par perte d'intégrité à l'aide de boitiers réseaux administrables à distance,

— Réaliser la mise en situation des robots télé-opérés sur deux sites différents afin de détecter/corriger la modification d'informations à grande distance,

— Synthétiser et analyser des attaques menaçant l'estimation réalisée par l'observateur à mémoire finie,

— Développer de nouveaux types d'attaque modifiant l'intégrité des données afin de contourner certains outils de la littérature.

Références personnelles

Communications internationales avec actes

J. THUILLIER, D. DELOUCHE, J. FANTINI, F. KRATZ. Finite Memory Observer-based sensor fault detection and isolation for system when measurements are correlated with process noise. *10th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*, IFAC-PapersOnLine, 2018, vol. 51, no 24, p. 320-325.

Communications nationales avec actes

J. THUILLIER, D. DELOUCHE, P. VRIGNAT, F. KRATZ. "Impacts liés aux pertes d'informations sur un processus communiquant et contrôlé en réseau", *lm 20ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, Communication 1C-4, pp. 1-10, Saint Malo, 2016.

J. THUILLIER, D. DELOUCHE, J. FANTINI, F. KRATZ. "Observateur à mémoire finie pour systèmes incertains – Apport de l'analyse par intervalle", *Qualita 2017*, Bourges, 2017.

J. THUILLIER, D. DELOUCHE, J. FANTINI, F. KRATZ. "Diagnostic de cyber-attaque sur les systèmes télé-opérés", lm *21ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, Communication 8A, Reims, 2019.

J. THUILLIER, D. DELOUCHE, J. FANTINI, F. KRATZ. "Estimation des pertes de mesure par un observateur à mémoire finie". *In : JDJN MACS*, Bordeaux, 2019.

Bibliographie

[Adame *et al.*, 2014] Adame, T., Bel, A., Bellalta, B., Barcelo, J. et Oliver, M. (2014). IEEE 802.11AH : The WiFi approach for M2M communications. *IEEE Wireless Communications*, 21(6):144–152.

[Alessandri *et al.*, 2007] Alessandri, A., Grassia, A. F. et Punta, E. (2007). Sliding-mode state estimation for a class of multi-output nonlinear continuous-time systems. *In 2007 European Control Conference, ECC 2007*, pages 3825–3830. IEEE.

[Ali, 2019] Ali, S. R. (2019). *Next Generation and Advanced Network Reliability Analysis ; Using Markov Models and Software Reliability Engineering*. Numéro 1 de Signals and Communication Technology. Springer International Publishing, Cham.

[Avella et Mancini, 2013] Avella, A. et Mancini, F., éditeurs (2013). *Strongly Correlated Systems*, volume 176 de *Springer Series in Solid-State Sciences*. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Baliga *et al.*, 2014] Baliga, A., Bickford, J. et Daswani, N. (2014). Triton : A carrier-based approach for detecting and mitigating mobile malware. *Journal of Cyber Security and Mobility*, 3(2):181–212.

[Basseville et Nikiforov, 1993] Basseville, M. et Nikiforov, I. V. (1993). Detection of Abrupt Changes : Michele Basseville. *Change*.

[Bencsáth *et al.*, 2012a] Bencsáth, B., Pék, G., Buttyán, L. et Félegyházi, M. (2012a). Duqu : Analysis, detection, and lessons learned. *In ACM European Workshop on System Security (EuroSec)*.

[Bencsáth *et al.*, 2012b] Bencsáth, B., Pék, G., Buttyán, L. et Félegyházi, M. (2012b). The cousins of Stuxnet : Duqu, Flame, and Gauss. *Future Internet*, 4(4):971–1003.

[Blanchet et Bergerried, 2014] Blanchet, M. et Bergerried, R. (2014). Industrie 4.0-les leviers de la transformation. *Gimélec, septembre*, pages 8–11.

[Blanke *et al.*, 2006] Blanke, M., Lunze, J., Kinnaert, M., Staroswiecki, M. et Schröder, J. (2006). *Diagnosis and fault-tolerant control*.

[Blesa *et al.*, 2014] Blesa, J., Rotondo, D., Puig, V. et Nejjari, F. (2014). FDI and FTC of wind turbines using the interval observer approach and virtual actuators/sensors. *Control Engineering Practice*, 24(1):138–155.

[Blume, 2016] Blume, S. W. (2016). *Interconnected Power Systems*. Power Systems. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Bousghiri *et al.*, 1994] Bousghiri, S., Kratz, F. et Ragot, J. (1994). Comparison of the Data Reconciliation and Finite Memory Observer at the Inverted Pendulum. *IFAC Proceedings Volumes*, 27(5):561–566.

[Bretas *et al.*, 2017] Bretas, A. S., Bretas, N. G., Carvalho, B., Baeyens, E. et Khargonekar, P. P. (2017). Smart grids cyber-physical security as a malicious data attack : An innovation approach. *Electric Power Systems Research*, 149:210–219.

[Bubnicki, 2007] Bubnicki, Z. (2007). *Analysis and Decision Making in Uncertain Systems*, volume 158 de *Communications and Control Engineering*. Springer London, London.

[Byrski et Byrski, 2019] Byrski, J. et Byrski, W. (2019). State estimators and observers for continuous and discrete linear systems. Part 2. Integral observers for exact state reconstruction. *Science, Technology and Innovation*, 5(2):23–33.

[Cacace *et al.*, 2015] Cacace, F., Germani, A. et Manes, C. (2015). A New Approach to Design Interval Observers for Linear Systems. *IEEE Transactions on Automatic Control*, 60(6):1665–1670.

[Cellier, 1991] Cellier, F. E. (1991). *Continuous system modeling*, volume 33. Springer New York, New York, NY.

[Chaeikar *et al.*, 2012] Chaeikar, S. S., Jafari, M. et Taherdoost, H. (2012). Definitions and Criteria of CIA Security. *International Journal of Advanced Computer Science and Information Technology*.

[Chen *et al.*, 2012] Chen, P. Y., Cheng, S. M. et Chen, K. C. (2012). Smart attacks in smart grid communication networks. *IEEE Communications Magazine*, 50(8):24–29.

[Chiabaut *et al.*, 2009] Chiabaut, N., Buisson, C. et Leclercq, L. (2009). Fundamental diagram estimation through passing rate measurements in congestion. *IEEE Transactions on Intelligent Transportation Systems*, 10(2):355–359.

[Dang et Devic, 2008] Dang, T. et Devic, C. (2008). OCARI : Optimization of communication for ad hoc reliable industrial networks. *In IEEE International Conference on Industrial Informatics (INDIN)*, pages 688–693. IEEE.

[Debaene et Vidal, 1990] Debaene, J. D. et Vidal, P. D. (1990). Informatique industrielle. {r}obotique.

[Decotignie, 2005] Decotignie, J. D. (2005). Ethernet-based real-time and industrial communications. *Proceedings of the IEEE*, 93(6):1102–1117.

[Deshpande, 2017] Deshpande, A. S. (2017). Bridging a Gap in Applied Kalman Filtering : Estimating Outputs When Measurements Are Correlated with the Process Noise [Focus on Education]. *IEEE Control Systems*, 37(3):87–93.

[Dong *et al.*, 2016] Dong, Y., Gupta, N. et Chopra, N. (2016). On content modification attacks in bilateral teleoperation systems. *In 2016 American Control Conference (ACC)*, pages 316–321. IEEE.

[Efimov *et al.*, 2013] Efimov, D., Raïssi, T., Chebotarev, S. et Zolghadri, A. (2013). Interval state observer for nonlinear time varying systems. *Automatica*, 49(1):200–205.

[Evans *et al.*, 2004] Evans, D., Bond, P. et Bement, A. (2004). FIPS PUB 199 standards for security categorization of federal information and information systems. The National Institute of Standards and Technology (NIST).

[Fawzi *et al.*, 2014] Fawzi, H., Tabuada, P. et Diggavi, S. (2014). Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*.

[Flavia *et al.*, 2006] Flavia, F., Jia, N., Song, Y. Q. et Françoise, S. L. (2006). Impact of a (m,k)-firm data dropouts policy on the quality of control. *In IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS*, pages 353–359. IEEE.

[Forbes, 2020] Forbes (2020). 2018 Roundup Of Internet Of Things Forecasts And Market Estimates.

[Frank, 1990] Frank, P. M. (1990). Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy. A survey and some new results. *Automatica*.

[Frotzscher *et al.*, 2014] Frotzscher, A., Wetzker, U., Bauer, M., Rentschler, M., Beyer, M., Elspass, S. et Klessig, H. (2014). Requirements and current solutions of wireless communication in industrial automation. *In 2014 IEEE International Conference on Communications Workshops (ICC)*, pages 67–72. IEEE.

[Gaj *et al.*, 2013] Gaj, P., Jasperneite, J. et Felser, M. (2013). Computer Communication Within Industrial Distributed Environment—a Survey. *IEEE Transactions on Industrial Informatics*, 9(1): 182–189.

[Gao et Li, 2014] Gao, H. et Li, X. (2014). *Robust filtering for uncertain 2-D systems*. Communications and Control Engineering. Springer International Publishing, Cham.

[Garas, 2016] Garas, A., éditeur (2016). *Interconnected Networks*. Understanding Complex Systems. Springer International Publishing, Cham.

[Gertler, 1992] Gertler, J. (1992). Analytical redundancy methods in fault detection and isolation. *In IFAC Symposia Series*.

[Gertsbakh et Shpungin, 2011] Gertsbakh, I. et Shpungin, Y. (2011). *Network Reliability and Resilience*. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Ghahremani et Kamwa, 2011] Ghahremani, E. et Kamwa, I. (2011). Dynamic state estimation in power system by applying the extended kalman filter with unknown inputs to phasor measurements. *IEEE Transactions on Power Systems*, 26(4):2556–2566.

[Giani *et al.*, 2011] Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P. et Poolla, K. (2011). Smart grid data integrity attacks : Characterizations and countermeasures π. *In 2011 IEEE International Conference on Smart Grid Communications, SmartGridComm 2011*, pages 232–237. IEEE.

[Goldsztejn et Neumaier, 2014] Goldsztejn, A. et Neumaier, A. (2014). On the exponentiation of interval matrices. *Reliable Computing*.

[Grance *et al.*, 2004] Grance, B. K. T., Kent, K. et Kim, B. (2004). Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology NIST800-61.

[Graton, 2005] Graton, G. (2005). *System diagnosis using finite memory observers. Common Rail application*. Thèse de doctorat, Universite d'Orleans.

[Graton *et al.*, 2014] Graton, G., Kratz, F. et Fantini, J. (2014). Finite Memory Observers for linear time-varying systems : Theory and diagnosis applications. *Journal of the Franklin Institute*, 351(2):785–810.

[Gravina *et al.*, 2018] Gravina, R., Palau, C. E., Manso, M., Liotta, A. et Fortino, G., éditeurs (2018). *Integration, Interconnection, and Interoperability of IoT Systems*. Internet of Things. Springer International Publishing, Cham.

[Hadjicostis et Touri, 2002] Hadjicostis, C. et Touri, R. (2002). Feedback control utilizing packet dropping network links. *In Proceedings of the 41st IEEE Conference on Decision and Control.*, volume 2, pages 1205–1210. IEEE.

[Harrou *et al.*, 2018] Harrou, F., Zeroual, A. et Sun, Y. (2018). Traffic congestion detection based on hybrid observer and GLR test. *In Proceedings of the American Control Conference*, volume 2018-June, pages 604–609.

[Hatanaka *et al.*, 2015] Hatanaka, T., Chopra, N., Fujita, M. et Spong, M. W. (2015). *Passivity-Based Control and Estimation in Networked Robotics*. Communications and Control Engineering. Springer International Publishing, Cham.

[Hauet, 2016] Hauet, J.-P. (2016). Les risques de cyberattaques sur lIoT en millieu industriel.

[Higham, 2009] Higham, N. J. (2009). The scaling and squaring method for the matrix exponential revisited. *SIAM Review*.

[Himmelblau, 1978] Himmelblau, D. M. (1978). Fault Detection and Diagnosis in Chemical and Petrochemical Processes (Chemical Engineering Monographs, Vol 8). Elsevier Science Ltd.

[Hoehn et Ping Zhang, 2016] Hoehn, A. et Ping Zhang (2016). Detection of replay attacks in cyber-physical systems. *In 2016 American Control Conference (ACC)*, pages 290–295. IEEE.

[Hokayem et Spong, 2006] Hokayem, P. F. et Spong, M. W. (2006). Bilateral teleoperation : An historical survey. *Automatica*.

[Hu et Yan, 2008] Hu, S. et Yan, W.-Y. (2008). Stability of Networked Control Systems Under a Multiple-Packet Transmission Policy. *IEEE Transactions on Automatic Control*, 53(7):1706–1711.

[Hultquist, 2016] Hultquist, J. (2016). Sandworm Team and the Ukrainian Power Authority Attacks.

[I-Scoop, 2017] I-Scoop (2017). *Industrial Internet of Things definition*, volume 1 de *Springer Series in Wireless Technology*. Springer International Publishing, Cham.

[Isermann, 2006] Isermann, R. (2006). *Fault-diagnosis systems : An introduction from fault detection to fault tolerance*.

[Jaulin *et al.*, 2002] Jaulin, L., Kieffer, M., Didrit, O. et Walter, É. (2002). *Applied interval analysis*, volume 39. Springer London, London.

[Jia *et al.*, 2005] Jia, N., Song, Y. Q. et Lin, R. Z. (2005). Analysis of networked control system with packet drops governed by (m,k)-firm constraint. *In IFAC Proceedings Volumes (IFAC-PapersOnline)*, volume 38, pages 63–70.

[Jiang et Fang, 2014] Jiang, S. et Fang, H. (2014). Fault estimation for nonlinear networked systems with time-varying delay and random packet dropout. *Asian Journal of Control*, 16(1):126–137.

[Jungers *et al.*, 2018] Jungers, R. M., Kundu, A. et Heemels, W. P. (2018). Observability and controllability analysis of linear systems subject to data losses. *IEEE Transactions on Automatic Control*, 63(10):3361–3376.

[Kajdan *et al.*, 2006] Kajdan, R., Graton, G., Aubry, D. et Kratz, F. (2006). Fault Detection of a Nonlinear Switching System Using Finite Memory Observers. *IFAC Proceedings Volumes*, 39(13):992–997.

[Kajdan *et al.*, 2007] Kajdan, R., Kratz, F. et Aubry, D. (2007). Fault detection of affine hybrid systems using finite memory observers. *In 2007 European Control Conference, ECC 2007*, pages 1030–

1037. IEEE.

[Karnouskos, 2011] Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. *In IECON Proceedings (Industrial Electronics Conference)*, pages 4490–4494. IEEE.

[Kaspersky Laboratory, 2018] Kaspersky Laboratory (2018). The State of Industrial Cybersecurity 2018.

[Kearfott et Kreinovich, 1996] Kearfott, R. B. et Kreinovich, V. (1996). *Applications of Interval Computations*, volume 3 de *Applied Optimization*. Springer US, Boston, MA.

[Keller *et al.*, 2016] Keller, J. Y., Chabir, K. et Sauter, D. (2016). Input reconstruction for networked control systems subject to deception attacks and data losses on control signals. *International Journal of Systems Science*.

[KEMA, 2005] KEMA (2005). : 5ème conférence « Cyber-security of SCADA and Process Control Systems» organisée par le KEMA à Albuquerque en août 2005.

[Kim et Tran-Dang, 2019] Kim, D.-S. et Tran-Dang, H. (2019). *Industrial Sensors and Controls in Communication Networks*. Computer Communications and Networks. Springer International Publishing, Cham.

[Kim et Tong, 2013] Kim, J. et Tong, L. (2013). On topology attack of a smart grid : Undetectable attacks and countermeasures. *IEEE Journal on Selected Areas in Communications*, 31(7):1294–1305.

[Knezic *et al.*, 2010] Knezic, M., Dokic, B. et Ivanovic, Z. (2010). Topology aspects in EtherCAT networks. *In Proceedings of 14th International Power Electronics and Motion Control Conference EPE-PEMC 2010*. IEEE.

[Kosut *et al.*, 2011] Kosut, O., Jia, L., Thomas, R. J. et Tong, L. (2011). Malicious data attacks on the smart grid. *IEEE Transactions on Smart Grid*, 2(4):645–658.

[Kratz et Aubry, 2003] Kratz, F. et Aubry, D. (2003). Finite memory observer for state estimation of hybrid system. *IFAC Proceedings Volumes (IFAC-PapersOnline)*, 36(5):639–643.

[Kratz *et al.*, 1993] Kratz, F., Bousghiri, S. et Mourot, G. (1993). Finite memory observer structure for robust residual generation. *In Proceedings of the IEEE Conference on Decision and Control*, volume 2, pages 1247–1249. IEEE.

[Kratz-Bousghiri *et al.*, 1996] Kratz-Bousghiri, S., Nuninger, W. et Kratz, F. (1996). Fault detection in stochastic dynamic systems by data reconciliation. *Engineering Simulation*, 13(5):837–852.

[Kubo *et al.*, 2008] Kubo, R., Kani, J. et Fujimoto, Y. (2008). Advanced internet congestion control using a disturbance observer. *In GLOBECOM - IEEE Global Telecommunications Conference*, pages 1370–1374.

[Kundur *et al.*, 2010] Kundur, D., Feng, X., Liu, S., Zourntos, T. et Butler-Purry, K. L. (2010). Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid. pages 244–249.

[Kyriakides et Polycarpou, 2015] Kyriakides, E. et Polycarpou, M. (2015). *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems Conclusions*, volume 565 de *Studies in Computational Intelligence*. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Kyung *et al.*, 2016] Kyung, C. M., Yasuura, H., Liu, Y. et Lin, Y. L. (2016). *Smart sensors and systems : Innovations for medical, environmental, and IoT applications*. Springer International Publishing, Cham.

[Langner, 2011] Langner, R. (2011). Stuxnet : Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, 9(3):49–51.

[Lele, 2019] Lele, A. (2019). *Industry 4.0*, volume 132. Apress, Berkeley, CA.

[Li *et al.*, 2010] Li, J. G., Yuan, J. Q. et Lu, J. G. (2010). Observer-based $H\infty$ control for networked nonlinear systems with random packet losses.

[Lin *et al.*, 2003] Lin, H., Zhai, G. et Antsaklis, P. J. (2003). Robust Stability and Disturbance Attenuation Analysis of a Class of Networked Control Systems. *In Proceedings of the IEEE Conference on Decision and Control*.

[Liu *et al.*, 2012] Liu, A., Yu, L. et Zhang, W. A. (2012). Moving horizon estimation for networked systems with packet dropouts. *In Proceedings of the IEEE Conference on Decision and Control*, pages 763–768. IEEE.

[Liu *et al.*, 2013] Liu, A., Yu, L., Zhang, W. A. et Chen, M. Z. (2013). Moving horizon estimation for networked systems with quantized measurements and packet dropouts. *IEEE Transactions on Circuits and Systems I : Regular Papers*, 60(7):1823–1834.

[Liu *et al.*, 2018] Liu, B., Liu, Y., Li, W., Ma, Y. et Jiang, Z. (2018). Modeling and control of networked control systems with random network-induced delay and packet-dropout. *In Proceedings of the 2017 12th IEEE Conference on Industrial Electronics and Applications, ICIEA 2017*.

[Liu *et al.*, 2009] Liu, Y., Ning, P. et Reiter, M. K. (2009). False data injection attacks against state estimation in electric power grids. *Proceedings of the ACM Conference on Computer and Communications Security*, 14(1):21–32.

[Lu *et al.*, 2015] Lu, J., Gao, C., Zhao, G. et Liu, S. (2015). Decentralized State Estimation for Networked Navigation Systems with Communication Delay and Packet Loss : The Receding Horizon Case. *IFAC-PapersOnLine*, 48(28):1094–1099.

[Mambou Kuipou, 2016] Mambou Kuipou, U. (2016). *Filtrage de Kalman a bruits correles pour le positionnement precis*. Thèse de doctorat, Universite de Nantes.

[Mansfield-Devine, 2018] Mansfield-Devine, S. (2018). Critical infrastructure : understanding the threat. *Computer Fraud and Security*, 2018(7):16–20.

[Maxon, 2020] Maxon (2020). https ://www.maxongroup.com/maxon/view/product/motor/dcmotor/DC-Sonderprogramm/2260.885.

[Mazenc et Bernard, 2011] Mazenc, F. et Bernard, O. (2011). Interval observers for linear time-invariant systems with disturbances. *Automatica*, 47(1):140–147.

[Medvedev, 1996] Medvedev, A. (1996). Fault detection and isolation by functional continuous deadbeat observers. *International Journal of Control*, 64(3):425–439.

[Medvedev, 1998] Medvedev, A. (1998). State estimation and fault detection by a bank of continuous finite-memory filters. *International Journal of Control*, 69(4):499–517.

[Medvedev et Toivonen, 1992] Medvedev, A. V. et Toivonen, H. T. (1992). A Continuous Finite-Memory Deadbeat Observer. *In 1992 American Control Conference*, pages 1800–1804. IEEE.

[Meseguer *et al.*, 2007] Meseguer, J., Puig, V. et Escobet, T. (2007). Observer gain effect in linear interval observer-based fault detection. *Fault Detection, Supervision and Safety of Technical Processes 2006*, 1(8):540–545.

[Milanese *et al.*, 1996] Milanese, M., Norton, J., Piet-Lahanier, H. et Walter, É., éditeurs (1996). *Bounding Approaches to System Identification*. Springer US, Boston, MA.

[Mo *et al.*, 2010] Mo, Y., Garone, E., Casavola, A. et Sinopoli, B. (2010). False data injection attacks against state estimation in wireless sensor networks. *In Proceedings of the IEEE Conference on Decision and Control*.

[Mo *et al.*, 2012] Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A. et Sinopoli, B. (2012). Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209.

[Montes De Oca *et al.*, 2012] Montes De Oca, S., Puig, V. et Blesa, J. (2012). Robust fault detection based on adaptive threshold generation using interval LPV observers. *International Journal of Adaptive Control and Signal Processing*, 26(3):258–283.

[Moore, 1979] Moore, R. E. (1979). *Methods and Applications of Interval Analysis*.

[Moore *et al.*, 2009] Moore, R. E., Kearfortt, R. B. et Cloud, M. J. (2009). *Introduction to interval analysis*. SIAM, siam édition.

[Morel *et al.*, 2007] Morel, G., Valckenaers, P., Faure, J.-M., Pereira, C. E. et Diedrich, C. (2007). Manufacturing plant control challenges and issues. *Control Engineering Practice*, 15(11):1321–1331.

[Mukhopadhyay, 2014] Mukhopadhyay, S. C., éditeur (2014). *Internet of Things*, volume 9 de *Smart Sensors, Measurement and Instrumentation*. Springer International Publishing, Cham.

[Naghshtabrizi et Hespanha, 2005] Naghshtabrizi, P. et Hespanha, J. P. (2005). Designing an observer-based controller for a network control system. *In Proceedings of the 44th IEEE Conference on Decision and Control, and the European Control Conference, CDC-ECC '05*, volume 2005, pages 848–853.

[Neumaier et Hansen, 1994] Neumaier, A. et Hansen, E. (1994). Global Optimization Using Interval Analysis. *Mathematics of Computation*.

[Neumann, 2007] Neumann, P. (2007). Communication in industrial automation—What is going on ? *Control Engineering Practice*, 15(11):1332–1347.

[Nuninger *et al.*, 1998] Nuninger, W., Kratz, F. et Ragot, J. (1998). Finite memory generalized state observer for failure detection in dynamic systems. *In Proceedings of the IEEE Conference on Decision and Control*, volume 1, pages 581–585. IEEE.

[Oppenheimer et Michel, 1988] Oppenheimer, E. P. et Michel, A. N. (1988). Application of Interval Analysis Techniques to Linear Systems : Part II—The Interval Matrix Exponential Function. *IEEE Transactions on Circuits and Systems*.

[Pasqualetti *et al.*, 2013] Pasqualetti, F., Dorfler, F. et Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*.

[Patton *et al.*, 1989] Patton, R., Clark, R. et Frank, P. (1989). Fault Diagnosis in Dynamic Systems : Theory and Application.

[Peijiang et Xuehua, 2008] Peijiang, C. et Xuehua, J. (2008). Design and implementation of remote monitoring system based on GSM. *In Proceedings - 2008 Pacific-Asia Workshop on Computational Intelligence and Industrial Application, PACIIA 2008*, volume 1, pages 678–681. IEEE.

[Peng *et al.*, 2015] Peng, C., Yue, D. et Han, Q. L. (2015). *Communication and control for networked complex systems*. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Pietrabissa et Priscoli, 2009] Pietrabissa, A. et Priscoli, F. D. (2009). *Modelling, Estimation and Control of Networked Complex Systems*, volume 2009 de *Understanding Complex Systems*. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Prytz, 2008] Prytz, G. (2008). A performance analysis of EtherCAT and PROFINET IRT. *In IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, pages 408–415. IEEE.

[Raïssi *et al.*, 2010] Raïssi, T., Videau, G. et Zolghadri, A. (2010). Interval observer design for consistency checks of nonlinear continuous-time systems. *Automatica*, 46(3):518–527.

[Richter, 2012] Richter, H. (2012). *Advanced Control of Turbofan Engines*. Springer New York, New York, NY.

[Schenato, 2008] Schenato, L. (2008). Optimal estimation in networked control systems subject to random delay and packet drop. *IEEE Transactions on Automatic Control*.

[Security, 2018] Security, D. o. H. (2018). Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure.

[Shi *et al.*, 2009] Shi, L., Xie, L. et Murray, R. M. (2009). Kalman filtering over a packet-delaying network : A probabilistic approach. *Automatica*, 45(9):2134–2140.

[Shmaliy, 2006] Shmaliy, Y. (2006). *Continuous-time signals*. Springer Netherlands.

[Simon, 2006] Simon, D. (2006). *Optimal State Estimation : Kalman, H∞, and Nonlinear Approaches*. John Wiley & Sons, Inc., Hoboken, NJ, USA.

[Smets, 2005] Smets, P. (2005). Belief functions on real numbers. *International Journal of Approximate Reasoning*.

[Smith et Shafer, 1976] Smith, A. F. M. et Shafer, G. (1976). A Mathematical Theory of Evidence. *Biometrics*.

[Smith, 1961] Smith, C. A. B. (1961). Consistency in Statistical Inference and Decision. *Journal of the Royal Statistical Society : Series B (Methodological)*, 23(1):1–25.

[Sugeno et Yasukawa, 1993] Sugeno, M. et Yasukawa, T. (1993). A Fuzzy-Logic-Based Approach to Qualitative Modeling. *IEEE Transactions on Fuzzy Systems*.

[Symantec Corporation, 2002] Symantec Corporation (2002). Internet Security Threat Report. *Network Security*.

[Symantec Corporation, 2010] Symantec Corporation (2010). Internet Security Threat Report trends for 2010.

[Tanwani *et al.*, 2019] Tanwani, A., Jungers, R. et Maurice Heemels, W. P. (2019). Observability of Discrete-Time Linear Systems with Communication Protocols and Dropouts. *In Proceedings of the IEEE Conference on Decision and Control*, volume 2018-Decem, pages 4194–4199. IEEE.

[Teixeira *et al.*, 2015] Teixeira, A., Sou, K. C., Sandberg, H. et Johansson, K. H. (2015). Secure control systems : A quantitative risk management approach. *IEEE Control Systems*.

[Thomesse, 2005] Thomesse, J.-P. (2005). Fieldbus Technology and Industrial Automation. *In 2005 IEEE Conference on Emerging Technologies and Factory Automation*, volume 1, pages 651–653. IEEE.

[Tovar et Vasques, 1999] Tovar, E. et Vasques, F. (1999). Real-time fieldbus communications using Profibus networks. *IEEE Transactions on Industrial Electronics*, 46(6):1241–1251.

[Trinquet et Elloy, 2010] Trinquet, Y. et Elloy, J.-P. (2010). *Systèmes d'exploitation temps réel-Exemples d'exécutifs industriels*. Ed. Techniques Ingénieur.

[Vasiliadis *et al.*, 2015] Vasiliadis, G., Polychronakis, M. et Ioannidis, S. (2015). GPU-assisted malware. *International Journal of Information Security*, 14(3):289–297.

[Von Solms et Van Niekerk, 2013] Von Solms, R. et Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*.

[Wan *et al.*, 2012] Wan, X., Fang, H. et Fu, S. (2012). Observer-based fault detection for networked discrete-time infinite-distributed delay systems with packet dropouts. *Applied Mathematical Modelling*, 36(1):270–278.

[Wang et Liu, 2008] Wang, F. Y. et Liu, D. (2008). *Networked control systems : Theory and applications*. Springer London, London.

[Wang *et al.*, 2010] Wang, H., Yu, C. et Jing, Y. (2010). Observer-based sliding mode control for internet network congestion control. *In 2010 Chinese Control and Decision Conference, CCDC 2010*, pages 3258–3262.

[Wang *et al.*, 2007] Wang, Z., Yang, F., Ho, D. W. et Liu, X. (2007). Robust $H\infty$ control for networked systems with random packet losses. *IEEE Transactions on Systems, Man, and Cybernetics, Part B : Cybernetics*, 37(4):916–924.

[Wedding, 1997] Wedding, D. K. (1997). Fuzzy sets and fuzzy logic : Theory and applications. *Neurocomputing*.

[Weinmann, 1991] Weinmann, A. (1991). *Uncertain Models and Robust Control*, volume 29. Springer Vienna, Vienna.

[Wu *et al.*, 2012] Wu, L., Hao, X. et Yang, Q. (2012). Observer-based $H\infty$ control for industrial ethernet control systems with time delay and packet dropout. *In Proceedings of the 2012 4th International Conference on Intelligent Human-Machine Systems and Cybernetics, IHMSC 2012*, volume 1, pages 130–133.

[Xia *et al.*, 2011] Xia, Y., Fu, M. et Liu, G. P. (2011). *Analysis and synthesis of networked control systems*, volume 409 de *Lecture Notes in Control and Information Sciences*. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Xue *et al.*, 2012] Xue, B., Li, S. et Zhu, Q. (2012). Moving horizon state estimation for networked control systems with multiple packet dropouts. *IEEE Transactions on Automatic Control*, 57(9):2360–2366.

[Yao, 2016] Yao, K. (2016). *Uncertain Differential Equations*. Springer Uncertainty Research. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Yasuura *et al.*, 2017] Yasuura, H., Kyung, C. M., Liu, Y. et Lin, Y. L. (2017). *Smart sensors at the IoT frontier*. Springer International Publishing, Cham.

[Yi *et al.*, 2011] Yi, P., Iwayemi, A. et Zhou, C. (2011). Developing ZigBee deployment guideline under WiFi interference for smart grid applications. *IEEE Transactions on Smart Grid*, 2(1):98–108.

[Zervakis, 2019] Zervakis, G. (2019). *IoT for Smart Grids*. Power Systems. Springer International Publishing, Cham.

[Zhang *et al.*, 2013] Zhang, L., Gao, H. et Kaynak, O. (2013). Network-induced constraints in networked control systems-A survey. *IEEE Transactions on Industrial Informatics*.

[Zhang *et al.*, 2001] Zhang, W., Phillips, M. et Branicky, S. (2001). Stability of networked control systems. *IEEE Control Systems*, 21(1):84–99.

[Zhao, 2017] Zhao, J. (2017). Dynamic State Estimation With Model Uncertainties Using $H\infty$ Extended Kalman Filter. *IEEE Transactions on Power Systems*, 33(1):1099–1100.

[Zhou *et al.*, 2008] Zhou, Y., Wang, H., Jing, Y. et Liu, X. (2008). Observer-based robust controller design for active queue management. *In IFAC Proceedings Volumes (IFAC-PapersOnline)*, volume 17.

Annexe A

Propriétés du résidu $r_1(t) = y^*(t) - C\hat{x}_{L_{D_1}}(t|T_t)$:

Espérance : $\mathbb{E}[r_1(t)]$

sans attaque	avec attaque
$= \mathbb{E}[y^*(t) - C\hat{x}_{L_{D_1}}(t\|T_t)]$ $= \mathbb{E}[Cx(t) + v(t) - C\hat{x}_{L_{D_1}}(t\|T_t)]$ $= \mathbb{E}[C\tilde{x}(t) + v(t)]$, où $\tilde{x}(t) = x(t) - \hat{x}_{L_{D_1}}(t\|T_t)$ $= C\mathbb{E}[\tilde{x}(t)]) + \mathbb{E}[v(t)]$ $= 0$	$= \mathbb{E}[Cx(t) + v(t) + \sigma(t) - C\hat{x}^+_{L_{D_1}}(t\|T_t)]$ où $C\hat{x}^+_{L_{D_1}}(t\|T_t) = \Omega^{-1}_{L_{D_1}}(A + (y + \sigma))$ $C\hat{x}^+_{L_{D_1}}(t\|T_t) = \Omega^{-1}_{L_{D_1}}(A + y) + \Omega^{-1}_{L_{D_1}}\sigma$ $C\hat{x}^+_{L_{D_1}}(t\|T_t) = C\hat{x}_{L_{D_1}}(t\|T_t) + C\Omega^{-1}_{L_{D_1}}\sigma$ $= \sigma - C\Omega^{-1}_{L_{D_1}}\sigma$ $= (I - C\Omega^{-1}_{L_{D_1}})\sigma$

Variance : $\mathbb{V}ar(r_1(t))$

sans attaque	avec attaque
$= \mathbb{E}[r_1(t)r_1^T(t)]$ $= \mathbb{E}\left[(C\tilde{x}(t) + v(t))(C\tilde{x}(t) + v(t))^T\right]$ où $\tilde{x}(t) = x(t) - \hat{x}_{L_{D_1}}(t\|T_t)$ $= \mathbb{E}[(C\tilde{x}(t)\tilde{x}(t)^T C^T + C\tilde{x}(t)v(t)^T + v(t)\tilde{x}(t)^T C^T$ $+ v(t)v(t)^T]$ $= C\mathbb{E}(\tilde{x}(t)\tilde{x}(t)^T)C^T + \mathbb{E}(v(t)v(t)^T)$ $= C\Omega^{-1}_{L_{D_1}}C^T + R$	$= \mathbb{E}[(r_1(t) - \mathbb{E}(r_1(t)))((r_1(t) - \mathbb{E}(r_1(t))))^T]$ $= \mathbb{E}[(C\tilde{x}(t) + v(t) + \sigma(t) - C\hat{x}^+_{L_{D_1}}(t\|T_t) - (I - C\Omega^{-1}_{L_{D_1}})\sigma)$ $\times ((C\tilde{x}(t) + v(t) + \sigma(t) - C\hat{x}^+_{L_{D_1}}(t\|T_t) - (I - C\Omega^{-1}_{L_{D_1}})\sigma))^T]$ où $\tilde{x}(t) = x(t) - \hat{x}_{L_{D_1}}(t\|T_t)$ et $C\hat{x}^+_{L_{D_1}}(t\|T_t) = C\hat{x}_{L_{D_1}}(t\|T_t) + C\Omega^{-1}_{L_{D_1}}\sigma$ $= \mathbb{E}[(C\tilde{x}(t) + v(t) + \sigma(t) - C\hat{x}_{L_{D_1}}(t) - C\Omega^{-1}_{L_{D_1}} - (I - C\Omega^{-1}_{L_{D_1}})\sigma)$ $\times (C\tilde{x}(t) + v(t) + \sigma(t) - C\hat{x}_{L_{D_1}}(t) - C\Omega^{-1}_{L_{D_1}} - (I - C\Omega^{-1}_{L_{D_1}})\sigma)^T$ $= \mathbb{E}\left[(C\tilde{x}(t) + v(t))(C\tilde{x}(t) + v(t))^T\right]$ $= C\Omega^{-1}_{L_{D_1}}C^T + R$

Propriétés du résidu $r_2(t) = y^*(t) - C\hat{x}_{L_{D_2}}(t|T_{t'})$

Espérance : $\mathbb{E}[r_2(t)]$

sans attaque	avec attaque
$= \mathbb{E}[y^*(t) - C\hat{x}_{L_{D_2}}(t\|T_{t'})]$ $= \mathbb{E}[Cx(t) + v(t) - C\hat{x}_{L_{D_2}}(t\|T_{t'})]$ $= \mathbb{E}[C\tilde{x}(t) + v(t)]$ où $\tilde{x}(t) = x(t) - \hat{x}_{L_{D_2}}(t\|T_{t'})$ $= C\mathbb{E}[\tilde{x}(t)] + \mathbb{E}[v(t)]$ $= 0$	$= \mathbb{E}[Cx(t) + v(t) + \sigma(t) - C\hat{x}^+_{L_{D_2}}(t\|T_{t'})]$ ou $C\hat{x}^+_{L_{D_2}}(t\|T_{t'}) = C\hat{x}_{L_{D_2}}(t\|T_{t'}) + C\Omega^{-1}_{L_{D_2}}\sigma$ $= \mathbb{E}[C\tilde{x}(t) + v(t) + \sigma(t)]$ où $\tilde{x}(t) = x(t) - \hat{x}^+_{L_{D_2}}(t\|T_{t'})$ $= C\mathbb{E}(\tilde{x}(t)) + \mathbb{E}(v(t)) + \mathbb{E}(\sigma(t))$ $= \sigma$

Variance : $\mathbb{V}ar(r_2(t))$

sans attaque	avec attaque
$= \mathbb{E}[r_1(t)r_1^T(t)]$ $= \mathbb{E}\left[(C\tilde{x}(t) + v(t))(C\tilde{x}(t) + v(t))^T\right]$ où $\tilde{x}(t) = x(t) - \hat{x}_{L_{D_2}}(t\|T_t)$ $= \mathbb{E}[(C\tilde{x}(t)\tilde{x}(t)^T C^T + C\tilde{x}(t)v(t)^T$ $+ v(t)\tilde{x}(t)^T C^T + v(t)v(t)^T]$ $= C\mathbb{E}(\tilde{x}(t)\tilde{x}(t)^T)C^T + \mathbb{E}(v(t)v(t)^T)$ $= C\Omega^{-1}_{L_{D_2}}C^T + R$	$= \mathbb{E}[(r_1(t) - \mathbb{E}(r_1(t)))((r_1(t) - \mathbb{E}(r_1(t))))^T]$ $= \mathbb{E}[(C\tilde{x}(t) + v(t) + \sigma(t) - C\hat{x}^+_{L_{D_2}} - (I - C\Omega^{-1}_{L_{D_2}})\sigma)$ $\times ((C\tilde{x}(t) + v(t) + \sigma(t) - C\hat{x}^+_{L_{D_2}} - (I - C\Omega^{-1}_{L_{D_2}})\sigma))^T]$ où $\tilde{x}(t) = x(t) - \hat{x}_{L_{D_2}}(t\|T_t)$ et $C\hat{x}^+_{L_{D_2}}(t\|T_{t'}) = C\hat{x}_{L_{D_2}}(t\|T_{t'}) + C\Omega^{-1}_{L_{D_2}}\sigma$ $= \mathbb{E}[(C\tilde{x}(t) + v(t) + \sigma(t) - C\hat{x}_{L_{D_2}} - C\Omega^{-1}_{L_{D_2}} - (I - C\Omega^{-1}_{L_{D_2}})\sigma)$ $\times ((C\tilde{x}(t) + v(t) + \sigma(t) - C\hat{x}_{L_{D_2}} - C\Omega^{-1}_{L_{D_2}} - (I - C\Omega^{-1}_{L_{D_2}})\sigma))^T]$ $= \mathbb{E}\left[(C\tilde{x} + v(t))(C\tilde{x} + v(t))^T\right]$ $= C\Omega^{-1}_{L_{D_2}}C^T + R$

Relations entre $\hat{x}_{L_{D_1}}(t|T_t)$ et $\hat{x}_{L_{D_2}}(t|T_{t'})$

Soit l'équation d'estimation du FMO : $\hat{x}_L(t|T_t) = \Omega^{-1}_{L_{D_1}}(T_t)W_L(T_t)P_L^{-1}Z_L(t,T_t)$
avec P_L la matrice des variances des bruits de mesures de $Z_L(t,T_t)$ tels que :

$$P_L = \begin{pmatrix} R & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & R \end{pmatrix}$$

— l'estimation $\hat{x}_L(t|T_t)$ est calculé à partir de mesure prise aux L instants précédents, alors $T = [\tau_0, \tau_1, ..., \tau_{L-1}]$ avec $i = 0, 1, .., L-1$,
— l'estimation $\hat{x}_{L-1}(t|T'_t)$ est calculé à partir de mesure prise aux $L-1$ instants précédents, alors $T' = [\tau_1, ..., \tau_{L-1}]$ avec $i = 1, .., L-1$.

Exprimons $\Omega^{-1}_{L_{D_1}}(T_{t'})$ en fonction de $\Omega^{-1}_{L_{D_2}}(T_t)$:

$$\begin{aligned}
\Omega^{-1}_{L_{D_1}}(T_t) &= \sum_{i=0}^{L_{D_2}} e^{-A^T T(i)} C^T C e^{-AT(i)} \\
&= \sum_{i=1}^{L_{D_2}} e^{-A^T T(i)} C^T R^{-1}(t - T(i)) C e^{-AT(i)} + e^{-A^T T(0)} C^T R^{-1}(t - T(0)) C e^{-AT(0)} \\
&= \Omega^{-1}_{L_{D_2}}(T'_t) + e^{-A^T T(0)} C^T R^{-1}(t - T(0)) C e^{-AT(0)}
\end{aligned}$$

D'après le lemme d'inversion matriciel :

$$(A + BCD)^{-1} = A^{-1} - A^{-1}BC(I + DA^{-1}BC)^{-1}DA^{-1}$$

$\Omega^{-1}_{L_{D_1}}(T_t)$ peut alors s'écrire

$$\begin{aligned}
\Omega^{-1}_{L_{D_1}}(T_t) = \Omega^{-1}_{L_{D_2}}(T'_t) - \Omega^{-1}_{L_{D_2}}(T'_t) e^{-A^T T(0)} C^T R^{-1}(t - T(0)) C \left(I + e^{-AT(0)} \Omega^{-1}_{L_{D_2}}(T'_t) e^{-A^T T(0)} C^T R^{-1}(t - T(0)) C \right)^{-1} \\
\times e^{-AT(0)} \Omega^{-1}_{L_{D_2}}(T'_t)
\end{aligned}$$

Posons $K = \left(I + e^{-AT(0)} \Omega^{-1}_{L_{D_2}}(T'_t) e^{-A^T T(0)} C^T R^{-1}(t - T(0)) C \right)$,

$$\Omega^{-1}_{L_{D_1}}(T_t) = \Omega^{-1}_{L_{D_2}}(T'_t) - \Omega^{-1}_{L_{D_2}}(T'_t) e^{-A^T T(0)} C^T R^{-1}(t - T(0)) C K^{-1} e^{-AT(0)} \Omega^{-1}_{L_{D_2}}(T'_t)$$

Sachant

$$\hat{x}_{L_{D_1}}(t|T_t) = \Omega^{-1}_{L_{D_1}}(T_t) \sum_{i=0}^{k} e^{A^{-T} T(i)} C^T R^{-1}(t - T(i)) \left(y(t - T(i)) + \int_{t-T(i)}^{t} e^{A(t - T(i) - \theta)} B u(\theta) d\theta \right)$$

en injectant 5 dans 6 :

$$\begin{aligned}\hat{x}(t|T_t)_{L_{D_1}} &= \Omega^{-1}_{L_{D_2}}(T'_t) - \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))CK^{-1}e^{-AT(0)}\Omega^{-1}_{L_{D_2}}(T'_t) \\ &\quad \times \sum_{i=0}^{k} e^{-A^T T(i)}C^T R^{-1}(t-T(i))\left(y(t-T(i)) + \int_{t-T(i)}^{t} e^{A(t-T(i)-\theta)}Bu(\theta)d\theta\right)\end{aligned} \tag{6}$$

$$\begin{aligned}\hat{x}(t|T_t)_{L_{D_1}} &= \Omega^{-1}_{L_{D_2}}(T'_t)\sum_{i=1}^{k} e^{-A^T T(i)}C^T R^{-1}(t-T(i))\left(y(t-T(i)) + \int_{t-T(i)}^{t} e^{A(t-T(i)-\theta)}Bu(\theta)d\theta\right) \\ &\quad + \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))\left(y(t-T(0)) + \int_{t-T(0)}^{t} e^{A(t-T(0)-\theta)}Bu(\theta)d\theta\right) \\ &\quad - \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))CK^{-1}e^{-AT(0)}\Omega^{-1}_{L_{D_2}}(T'_t)\sum_{i=1}^{k} e^{A-^T T(i)}C^T R^{-1}(t-T(i)) \\ &\quad \times \left(y(t-T(i)) + \int_{t-T(i)}^{t} e^{A(t-T(i)-\theta)}Bu(\theta)d\theta\right) \\ &\quad - \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))CK^{-1}e^{-AT(0)}\Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0)) \\ &\quad \times \left(y(t-T(0)) + \int_{t-T(0)}^{t} e^{A(t-T(0)-\theta)}Bu(\theta)d\theta\right)\end{aligned} \tag{7}$$

$$\begin{aligned}\hat{x}(t|T_t)_{L_{D_1}} &= \hat{x}_{L-1}(t|T'_t) \\ &\quad + \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))\left(y(t-T(0)) + \int_{t-T(0)}^{t} e^{A(t-T(0)-\theta)}Bu(\theta)d\theta\right) \\ &\quad - \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))CK^{-1}e^{-AT(0)}\hat{x}_{L-1}(t|T'_t) \\ &\quad - \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))CK^{-1}e^{-AT(0)}\Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0)) \\ &\quad \times \left(y(t-T(0)) + \int_{t-T(0)}^{t} e^{A(t-T(0)-\theta)}Bu(\theta)d\theta\right)\end{aligned} \tag{8}$$

$$\begin{aligned}\hat{x}(t|T_t)_{L_{D_1}} &= \left[I - \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))CK^{-1}e^{-AT(0)}\right]\hat{x}_{L-1}(t|T'_t) \\ &\quad + \left[I - \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))CK^{-1}e^{-AT(0)}\right]\Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0)) \\ &\quad \times \left(y(t-T(0)) + \int_{t-T(0)}^{t} e^{A(t-T(0)-\theta)}Bu(\theta)d\theta\right)\end{aligned} \tag{9}$$

$$\hat{x}(t|T_t)_{L_{D_1}} = J\hat{x}_{L-1}(t|T'_t) + F\left(y(t-T(0)) + \int_{t-T(0)}^{t} e^{A(t-T(0)-\theta)}Bu(\theta)d\theta\right) \tag{10}$$

avec,

$$\begin{aligned}J &= \left[I - \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))CK^{-1}e^{-AT(0)}\right] \\ F &= \left[I - \Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))CK^{-1}e^{-AT(0)}\right]\Omega^{-1}_{L_{D_2}}(T'_t)e^{-A^T T(0)}C^T R^{-1}(t-T(0))\end{aligned} \tag{11}$$

$\diamond$

Génération du résidu :

Soit le résidu $r(t) = \hat{x}(t|T_t)_{L_{D_1}} - \hat{x}_{L_{D_2}}(t|T'_t)$

$$\begin{aligned} r(t) &= J\hat{x}_{L_{D_2}}(t|T'_t) + F\left(y(t-T(0)) + \int_{t-T(0)}^{t} e^{A(t-T(0)-\theta)}Bu(\theta)d\theta\right) - \hat{x}_{L_{D_2}}(t|T'_t) \\ &= (J-I)\hat{x}_{L_{D_2}}(t|T'_t) + F\left(y(t-T(0)) + \int_{t-T(0)}^{t} e^{A(t-T(0)-\theta)}Bu(\theta)d\theta\right) \end{aligned} \tag{12}$$

si $T(0) = 0$:

$$r(t) = (J-I)\hat{x}_{L_{D_2}}(t|T'_t) + F\left[y(t-T(0))\right] \tag{13}$$

$$r(t) = (J-I)\hat{x}_{L_{D_2}}(t|T'_t) + F\left[y(t)\right] \tag{14}$$

Propriétés du résidu $r_3(t) = \hat{x}_{L_{D_1}}(t|T_t) - \hat{x}_{L_{D_2}}(t|T_{t'})$

Espérance $\mathbb{E}[r_3(t)]$

sans attaque	avec attaque
$= (J-I)\mathbb{E}[\hat{x}_{L-1}(t\|T'_t)] + F\mathbb{E}[y(t)]$	
$=(J-I)\mathbb{E}[\hat{x}_{L-1}(t\|T'_t)] + FCx(t)$	
$=Jx_(t) - x(t) + J\Omega_{L_{D_2}}(T'_t)e^{-A^T T_0}C^T R^{-1}Cx(t)$	
$=[J-I] + J\Omega^{-1}_{L_{D_2}}(T'_t)C^T R^{-1}Cx(t)$	
Posons	
$G = [J-I] + J\Omega_{L_{D_2}}(T'_t)C^T R^{-1}C$	
$= I - \Omega^{-1}_{L_{D_2}}C^T R^{-1}CK^{-1} - I$	$= [\tilde{x}^+_{L_{D_1}} - \tilde{x}_{L_{D_2}}]$
$+ (I - \Omega^{-1}_{L_{D_2}}C^T R^{-1}CK^{-1})\Omega^{-1}_{L_{D_2}}C^T R^{-1}C$	$\times [\tilde{x}_{L_{D_1}} + \Omega^{-1}_{L_{D_1}}\sigma(t) - \tilde{x}^+_{L_{D_2}}]$
$= \Omega^{-1}_{L_{D_2}}C^T R^{-1}C - \Omega^{-1}_{L_{D_2}}C^T R^{-1}CK^{-1}$	$= \Omega^{-1}_{L_{D_1}}\sigma(t)$
$- \Omega^{-1}_{L_{D_2}}C^T R^{-1}CK^{-1}\Omega^{-1}_{L_{D_2}}C^T R^{-1}C$	
$= \Omega^{-1}_{L_{D_2}}C^T R^{-1}C - \Omega^{-1}_{L_{D_2}}C^T R^{-1}CK^{-1}$	
$\times (I + \Omega^{-1}_{L_{D_2}}C^T R^{-1}C)$	
or, $K = I + \Omega^{-1}_{L_{D_2}}C^T R^{-1}C$	
donc	
$= \Omega^{-1}_{L_{D_2}}C^T R^{-1}C - \Omega^{-1}_{L_{D_2}}C^T R^{-1}C = 0$	
nous obtenons, $\mathbb{E}(r_3(t)) = 0$	

Variance $\mathbb{V}ar(r_3(t))$

sans attaque	avec attaque
$= \mathbb{V}ar\{(J-I)\hat{x}_{L-1}(t\|T'_t) + Fy(t)\}$	$= \mathbb{E}[(\tilde{x}^+_{L_{D_1}} - \tilde{x}_{L_{D_2}} - \Omega^{-1}_{L_{D_1}}\sigma(t))$
Puisque $\hat{x}_{L-1}(t\|T'_t)$ est indépendant de $y(t)$	$\times (\tilde{x}^+_{L_{D_1}} - \tilde{x}_{L_{D_2}} - \Omega^{-1}_{L_{D_1}}\sigma(t))^T]$
$= (J-I)\mathbb{V}ar(\hat{x}_{L-1}(t\|T'_t))(J-I)^T + F\mathbb{V}ar(y(t))F^T$	$= \mathbb{E}[(\tilde{x}_{L_{D_1}} - \tilde{x}_{L_{D_2}})(\tilde{x}_{L_{D_1}} - \tilde{x}_{L_{D_2}})^T]$
$= (J-I)\Omega^{-1}_{L_{D_2}}(J-I)^T + FRF^T$	$= (J-I)\Omega^{-1}_{L_{D_1}}(J-I)^T + FRF^T$

Annexe B

Test d'hypothèses

Afin de compléter la prise de décision, il est possible d'utiliser le test statistique de Fisher. Ce test permettra de prendre en compte statistiquement les phénomènes aléatoires dans les résidus obtenus à l'aide de l'observateur à mémoire finie.

Une hypothèse de départ notée H_0 respecte les conditions statistiques de la variable observée de caractéristique notée A (cas de fonctionement normal). Une autre hypothèse notée H_1, représente un scénario alternatif (cas avec attaque), opposée à H_0 et vérifiant la caractéristique notée B.

Une régle de décision utilisant la probabilité d'être sous l'hypothèse H_0, quantifiera une variable appelée probabilité critique du test et notée P_c.

La faible probabilité que l'hypothèse H_0 ne se réalise pas est notée α. Cette faible probabilité correspond à la détection d'une attaque dans le cas sans attaque, également appelé faux-positif. La probabilités que l'hypothèse H_1 ne se réalise pas est notée β. Celle-ci correspond à la non-détection d'une attaque dans le cas avec attaque, également appelé faux-négatif.

A l'aide de l'établissement d'un seuil de confiance en regard de la probabilité P_c, la procédure de décision est réalisée à l'aide du rejet, de l'une ou de l'autre hyposthèse, respectivement H_0 et H_1 et cela suivant les probabilités associées.

Annexe C

Propriétés du résidu (sans attaque) $r_1(t) = y^*(t) - C\hat{x}_{L_{D_1}}(t)$ **:**

Espérance : $\mathbb{E}[r_1(t)]$
$= \mathbb{E}[y^*(t) - C\hat{x}_{L_{D_1}}(t\|T_t)]$ $= \mathbb{E}[Cx(t) + v(t) + Hw(t) - C\hat{x}_{L_{D_1}}(t)]$ $= \mathbb{E}[C\tilde{x}(t) + v(t) + Hw(t)],$ où $\tilde{x}(t) = x(t) - \hat{x}_{L_{D_1}}(t)$ $= C\mathbb{E}[\tilde{x}(t)]) + \mathbb{E}[v(t)] + H\mathbb{E}[w(t)]$ $= 0$

Variance : $\mathbb{V}ar(r_1(t))$
$= \mathbb{E}[r_1(t)r_1^T(t)]$ $= \mathbb{E}\left[(C\tilde{x}(t) + v(t) + Hw(t))(C\tilde{x}(t) + v(t) + Hw(t))^T\right]$ où $\tilde{x}(t) = x(t) - \hat{x}_{L_{D_1}}(t)$ $= \mathbb{E}[C\tilde{x}(t)\tilde{x}(t)^T C^T + C\tilde{x}(t)v(t)^T + C\tilde{x}H^T w(t)^T + v(t)C^T\tilde{x}^T + v(t)v(t)^T$ $+ v(t)w(t)^T H^T + Hw(t)C^T\tilde{x}^T + Hw(t)v(t)^T + Hw(t)w(t)^T H^T]$ $= C\Omega_{L_{D_1}}^{-1} C^T + \mathbb{E}[C\tilde{x}(t)v(t)^T] + \mathbb{E}[C\tilde{x}H^T w(t)^T] + \mathbb{E}[v(t)C^T\tilde{x}^T] + R$ $+ JH^T + \mathbb{E}[Hw(t)C^T\tilde{x}^T] + HJ + HQH^T]$ $= C\Omega_{L_{D_1}}^{-1} C^T + R + JH^T + HJ + HQH^T$

Annexe D

Erreur d'estimation pour k pertes de données consécutives :

Comme précèdement explicité dans le chapitre 2, la covariance de l'erreur d'estimation est donnée par les valeurs propres de la matrice Ω_L^{-1} :

$$\Omega_L^{-1} = \left(W_L^T P_L^{-1} W_L\right)^{-1} \tag{15}$$

avec P_L^{-1} la matrice de variance des bruits de mesure et $W_L = \begin{pmatrix} Ce^{-A\tau_0} \\ \vdots \\ Ce^{-A\tau_{L-1}} \end{pmatrix}$.

La matrice de covariance pour k pertes de mesure notée $\Omega_{L,k}^{-1}$ peut être exprimée en fonction de la matrice de covariance du cas classique Ω_L^{-1} tel que :

$$\begin{aligned}
\Omega_{L,k}^{-1} &= \left((e^{-A^T kTe}) W_L^T P_L^{-1} W_L (e^{-AkTe})\right)^{-1} \\
\Omega_{L,k}^{-1} &= (e^{-AkTe})^{-1} (W_L^T P_L^{-1} W_L)^{-1} (e^{-A^T kTe})^{-1} \\
\Omega_{L,k}^{-1} &= (e^{-AkTe})^{-1} \Omega_L^{-1} (e^{-A^T kTe})^{-1} \\
\Omega_{L,k}^{-1} &= (e^{-A^T Te})^k \Omega_L^{-1} (e^{-ATe})^k
\end{aligned}$$

Julien THUILLIER

Fiabilité de l'intégrité des informations par observateur à mémoire finie pour un système commandé en réseau

Résumé : Les travaux décrits dans cette thèse concernent l'intégrité et la disponibilité des informations de systèmes commandés en réseau. L'importance de celles-ci a été mise en exergue face au nombre de plus en plus important de cyber-attaques. Nous proposons comme outil pour répondre à cette problématique un observateur à mémoire finie. Cet outil apporte une réponse aux problèmes de pertes de paquets sur le réseau ainsi qu'aux cyber-attaques statiques et dynamiques par injection de biais. Associé à une stratégie de détection-décision-correction, la fiabilité des informations de systèmes lors de cyber-attaques est assurée. Les incertitudes du modèle pour certains systèmes sont également prises en compte dans le développement de l'observateur à mémoire finie. Plus particulièrement, deux catégories d'incertitudes sont traitées (systèmes incertains et systèmes à bruits corrélés). Tous les cas d'études sont illustrés par des simulations numériques confirmant les qualités de cet outil. Enfin, nous appliquerons cet outil aux systèmes télé-opérés soumis à de nouveaux types d'attaques appelés attaques intelligentes".

Mots-clés : systèmes commandés en réseau, intégrité et disponibilité de l'information, cyber-attaques, observateurs à mémoire finie, systèmes incertains, bruits corrélés.

Reliability of information integrity by finite memory observer to a networked control system

Summary : The works described in this thesis deal with the integrity and availability of networked control systems information. The importance of this has been highlighted by the growing number of cyber-attacks. A finite memory observer is proposed as a tool to answer this problem. This tool provides an answer to the problems of packet loss on the network as well as to static and dynamic cyber-attacks using bias injection. Combined with a detection-decision-correction strategy, the reliability of system information during cyber-attacks is ensured. The uncertainties of the models of some systems are also taken into account in the development of the finite memory observer. More specifically, two categories of uncertainties are addressed (uncertain systems and correlated noise systems). All case studies are illustrated by numerical simulations confirming the qualities of this tool. Finally, we will apply this tool to teleoperated systems subjected to new types of attacks called "smart attacks".

Keywords : networked control systems, integrity and availability of information, cyber-attacks, finite memory observer, uncertain systems, correlated noises.

Laboratoire PRISME
INSA Centre Val de Loire
88, Boulevard Lahitolle
18000 Bourges