RESILIENT ESTIMATION AND CONTROL FOR DISTRIBUTED DYNAMIC SYSTEMS

A thesis submitted to the University of Manchester
for the degree of Doctor of Philosophy
in the Faculty of Science and Engineering

2023

Xiaoyu Guo
Department of Electrical and Electronic Engineering
School of Engineering

Contents

List of Figures

The University of Manchester

Xiaoyu Guo
Doctor of Philosophy
Resilient estimation and control for distributed dynamic systems
May 9, 2023

Increasing research attention has been placed towards distributed dynamic systems that integrate sensing, computation, communication and physical processes. A prominent feature of such systems is communication among subsystems via network mediums, and distributed estimation and control schemes can enable distributed dynamic systems to carry out complicated tasks in a cooperative manner. Utilization of networks and exposure to the physical environment means that distributed systems are more vulnerable to adversaries that include attacks, faults, and disturbances. In practical distributed systems, a wide range of adversaries exist in various forms (such as deception attack and denial-of-service attack) that affect various channels (such as the sensor channel, communication channel and actuator channel). This thesis focuses on the important topic of developing resilient estimation and control schemes for distributed dynamic systems to improve the safety and performance in the presence of adversaries.

Firstly, the simultaneous presence of disturbances and attacks on distributed systems is tackled by a novel three-stage estimation approach which includes anti-disturbance estimation, optimal attack detection and detection-triggered attack-resilient estimation. This approach effectively decouples the influence of multiple disturbances and false data injection attacks existing on the same channel.

In some cases, heterogeneous attacks on different channels can be simultaneously injected to have a joint effect on distributed systems. Utilizing a novel event-based update scheme, an adaptive term and a distributed disturbance observer, an event-based distributed estimation approach is introduced to deal with the joint effects of aperiodic denial-of-service attacks on the communication channel and unknown deception attacks on the sensor channel.

While the previous works deal with disturbances and attacks through compensation and attenuation, some attacks, namely the sparse injection attacks on sensors are potentially unbounded and cannot be dealt with the observer-based compensation approach. In such cases, it is more desirable to isolate and remove the sensor channels that are under attack. In the third section, a switching sparse attack detector based on a monitoring function utilizes the sensing redundancy to identify and remove the attacked sensor channels, and a backstepping control scheme is designed for the practical implementation of the proposed algorithm on a robotic manipulator.

In the final section, adversaries on the actuator channel are studied, where the challenging topic of unknown direction faults on multi-input-multi-output distributed systems is dealt with novel Nussbaum functions, and a distributed containment control

scheme is proposed for a network of uncertain nonlinear agents. Moreover, an event-triggering mechanism is introduced to avoid continuous communication among agents.

The main contribution of this thesis is presenting a framework for the resilient estimation and control of distributed network systems against a wide range of adversaries, including but not limited to injection attacks, denial of service attacks, actuator faults and disturbances. The approaches introduced in each chapter of this thesis have compelling features that can be either implemented on their own, or integrated with other existing control and estimation schemes to enhance the resilience of distributed systems.

Declaration

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

Copyright Statement

Publications

1. **Xiaoyu Guo**, Songyin Cao and Zhengtao Ding, "Enhanced distributed state estimation with resilience to multiple disturbances and false data injection attacks," *International Journal of Robust and Nonlinear Control*, vol.32, no.2, pp. 1075-1092, 2022.

2. **Xiaoyu Guo**, Zhen Dong, Chenliang Wang and Zhengtao Ding, "Event-based resilient distributed estimation under multiple heterogeneous cyber-attacks," *IEEE Transactions on Control of Network Systems*, Published Online, DOI: 10.1109/TCNS.2022.3203903.

3. **Xiaoyu Guo**, Chenliang Wang, Zhen Dong and Zhengtao Ding, "Secure state estimation for nonlinear systems under sparse attacks with application to robotic manipulators," *IEEE Transactions on Industrial Electronics*, Published Online, DOI: 10.1109/TIE.2022.3208581.

4. **Xiaoyu Guo**, Chenliang Wang, Zhen Dong and Zhengtao Ding, "Adaptive containment control for heterogeneous MIMO nonlinear multi-agent systems with unknown direction actuator faults," *IEEE Transactions on Automatic Control*, Published Online, DOI: 10.1109/TAC.2022.3228858.

5. **Xiaoyu Guo**, Zhen Dong, Jiabin Shen, Yiqiao Xu, Qiaohui He, Xiaowei Zhao and Zhengtao Ding, "Towards intelligent and integrated architecture for hydrogen fuel cell system: challenges and approaches," *National Science Open*, Published Online, DOI: 10.1360/NSO/20220038.

6. Zhen Dong, Zhongguo Li, Yiqiao Xu, **Xiaoyu Guo** and Zhengtao Ding, "Surrogate-assisted cooperation control of network-connected doubly fed induction generator wind farm with maximized reactive power capacity," *IEEE Transactions on Industrial Informatics*, vol.18, no.1, pp.197-206, 2021.

Acknowledgements

First and foremost, I would like to express my deepest thanks to Professor Zhengtao Ding for his invaluable guidance over the past three years. His dedication and enthusiasm towards science, and his insightful and rigorous approach towards research continue to inspire me. Without his encouragement, this dissertation would not be possible, and I will forever cherish the privilege of working under his supervision.

I am also grateful towards my collaborators, in particular Dr. Chenliang Wang and Dr. Zhen Dong, for their guidance and assistance. It is an understatement to say that the discussions we've had greatly improved the quality of my research. I would also like to thank my friends, my partner and the PhD students in Prof. Ding's research group for their friendship and valuable advice.

Last but not least, I would like to acknowledge my parents for their unconditional love and support. Their guidance and encouragement made my PhD experience both enjoyable and rewarding, and I would like to dedicate this thesis as a token of my appreciation.

Abbreviations

MAS	**M**ulti-**A**gent **S**ystem
CPS	**C**yber **P**hysical **S**ystem
FDI	**F**alse **D**ata **I**njection
DoS	**D**enial-**o**f-**S**ervice
LMI	**L**inear **M**atrix **I**nequality
CGM	**C**ontrol **G**ain **M**atrix
SISO	**S**ingle-**I**nput **S**ingle-**O**utput
MIMO	**M**ulti-**I**nput **M**ulti-**O**utput
DOBC	**D**isturbance **O**bserver-**B**ased **C**ontrol
CHADC	**C**omposite **H**ierarchical **A**nti-**D**isturbance **C**ontrol

Notations

$\mathbb{R}$	The set of real numbers
$\mathbb{R}^n$	The n-dimensional Euclidean space
$\mathbb{R}^{n\times m}$	The set of $n \times m$ real matrices
$\mathbb{R}_{\geq 0}$	The set of nonnegative real numbers
1_n	A size n column vector with all elements equal to 1
$\mathcal{A}$	The adjacency matrix of a graph
$\mathcal{L}$	The Laplacian matrix of a graph
$\mathcal{G}$	A graph
$\mathcal{N}_i$	The set of neighbours of agent i
$\mathcal{E}$	The set of edges in a graph
$\otimes$	The Kronecker product
$\mathrm{diag}_n^i\{Z_i\}$	Block-diagonal matrix with n blocks $Z_1, \ldots, Z_n$
$\mathrm{col}_n\{Z\}$	n-block column vector $[\ Z^{\mathrm{T}} \quad \ldots \quad Z^{\mathrm{T}}\ ]^{\mathrm{T}}$
$\mathrm{col}_n^i\{Z_i\}$	n-block column vector $[\ Z_1^{\mathrm{T}} \quad \ldots \quad Z_n^{\mathrm{T}}\ ]^{\mathrm{T}}$
I_n	The $n \times n$ identity matrix
$\|x\|$	The Euclidean norm of a vector
A^{T}	The transpose of matrix A

Chapter 1

Introduction

1.1 Background

Recent years have witnessed rapid development of distributed control systems, which features communication between sensors, actuators, and controllers across a communication network [2, 3, 4, 5, 6]. Advantages of distributed systems over their centralised counterparts include scalability, reduced communication burden, increased area of coverage and ease of maintenance and diagnosis. Distributed control systems have been applied in a wide range of fields including smart grids, remote monitoring, robotics, transportation and telecommunications. Through the tight integration of computing, communication and control technologies, distributed techniques have been utilised to form cyber-physical systems [7, 8]. From an algorithmic perspective, the main tasks to be carried out by a distributed control system include distributed estimation, which involves combination of local information from agents in a distributed manner to obtain the estimation of global information; and distributed control (also known as cooperative control), which is the coordination of agents' behavior by transmission/reception of information to/from other controllers.

On the other hand, several factors, including utilization of wireless connection, exposure to the physical environment and wide area of coverage means that distributed control systems are more vulnerable to various types of adversaries, including but

not limited to disturbances, faults, and cyber-attacks [8, 9]. Such adversaries can be applied to various channels (sensor channel, communication channel, actuator channel, etc.) of the distributed control system in various forms (deceptive signal, false data, denial-of-service, etc.). The typical adversaries faced by the distributed dynamic system are depicted in Figure 1.1. It is of great significance to place security and resilience against adversaries into consideration in the design of distributed estimation and control methods. Resilient estimation and control aim to enhance the resilience of distributed dynamic systems against adversaries through approaches such as detection, estimation, compensation, isolation, and tolerance. The topic of resilient estimation and control have garnered considerable research interest in recent years. However, in spite of the progress, it has been noted that some gaps are still withstanding in research of resilient estimation and control for distributed dynamic systems.

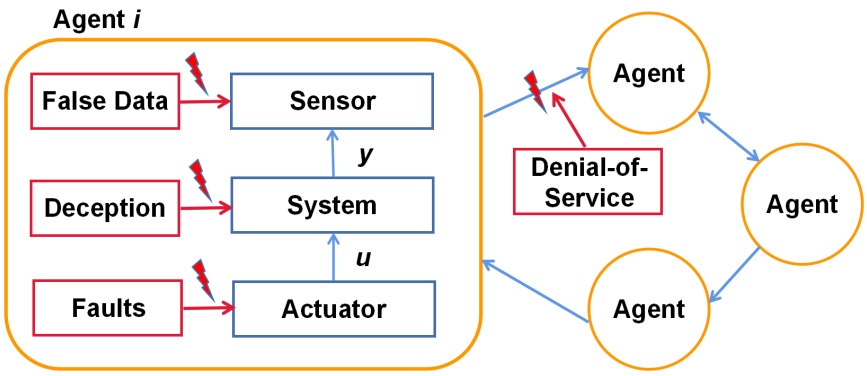

Figure 1.1: Adversaries in distributed dynamic systems.

The key objective of distributed estimation is for all agents in the distributed system to acquire full knowledge of the state for the controller to make informed decisions. In a distributed dynamic system, the complete state of the system is not always accessible to all agents, which makes the distributed estimation problem challenging. Here, we provide a general formulation of the distributed estimation problem for linear systems. Consider a linear dynamic system of the following form:

$$\dot{x}(t) = Ax(t) + Bd(t), \tag{1.1}$$

where $x(t) \in \mathbb{R}^{n_x}$ denotes the state of the system, $d(t) \in \mathbb{R}^{n_d}$ is the system disturbance or process noise, and A and B are matrices with appropriate dimensions. Assume that

the state x is monitored by N sensors, and the N sensors form a cooperative network whose topology can be described by a digraph $\mathcal{G}$. The measurement model of the ith sensor can be given by

$$y_i(t) = C_i x(t) + D_i v_i(t), \quad \forall i = 1, \ldots, N, \tag{1.2}$$

where $y_i(t) \in \mathbb{R}^{n_y}$ denotes the measurement from the ith sensor, $v_i(t) \in \mathbb{R}^{n_v}$ is the sensor disturbance or communication noise, and C_i and D_i are matrices with appropriate dimensions. It should be noted that since sensors in a spatially dispersed network sometimes only have partial measurements of the state to be estimated, the measurement matrix C_i may not always be of full rank. Denote by $\hat{x}_i(t)$ the estimate transmitted by the ith sensor, and a typical distributed estimator structure can be presented as [10, 11, 12, 13]

$$\dot{\hat{x}}_i(t) = A\hat{x}_i(t) + K_i(y_i - C_i\hat{x}_i) + \sum_{j \in \mathcal{N}_i} a_{ij} L_{ij}(\hat{x}_i - \hat{x}_j), \tag{1.3}$$

where K_i and L_{ij} are the gain matrices on the ith agent. Depending on the performance requirements and system restrictions, the estimator gain matrices can be selected by the user to follow some conditions, or solved with linear matrix inequalities. It is shown in (1.3) that the estimation $\hat{x}_i$ is updated by both its own measurement (referred to as local innovation) and the estimation from neighbouring agents (referred to as global innovation).

In this thesis, some open research problems will be addressed, including detection and compensation of false data injection attacks in the presence of multiple disturbances, resilient estimation for systems under multiple heterogeneous attacks, detection and isolation of sparse injection attacks for nonlinear systems, and tolerance of unknown direction actuator faults for uncertain MIMO agents performing containment control. In the following section, a systematic overview of the state-of-the-art in resilient estimation and control for distributed dynamic systems will be given. The estimation and control approaches will be categorised by the type of adversary (false data injection, denial-of-service, sparse injection, disturbances and faults) in consideration.

1.2 Overview of Related Work

1.2.1 Resilient Estimation

1) False Data Injection Attacks

False data injection (FDI) attack, also referred to as deception attack, is a malicious signal sent by the attacker with the intent of corrupting the integrity of information. Replay attack is another widely studied type of adversary that can be considered as a special case of false data injection attack. FDI attacks are typically sent through the measurement channel of distributed dynamic systems, such as through the sensors in a monitoring network. As shown in [14], FDI attacks do not require prior knowledge of the internal model or the network topology. Therefore, false signals could easily be mixed with the actual sensor measurement and degrade the accuracy of the estimation or even destabilise the state estimator. FDI attacks are shown to be able to disrupt the integrity of practical distributed systems and cause severe security loss in numerous real-life incidents [15, 16]. Motivated by information security concerns, it is of great importance to investigate secure distributed state estimation methods with enhanced resilience to FDI attacks. In [17], a χ^2 failure detector towards FDI attacks on cyber-physical systems was proposed. In [18], Wang et al. proposed a FDI attack detection and isolation scheme based on unknown input observers. The authors of [19] investigated secure state estimation based on satisfiability modulo theory; and a joint state and deception attack estimator via sliding mode was introduced in [20]. [21] adopts a detector to partition the agents into sets of attacked/attack-free and designs a saturation-based innovation to limit the effect of attack signals. Many other effective methods have been given for FDI attack detection and distributed estimation in recent literature [22, 23, 24, 25, 26, 27, 28]. In existing works, the attacks are often modelled as an unknown signal that follows some type of boundedness assumption.

It is well known that disturbances from both internal and external sources exist in distributed control systems. The phenomenon of disturbances being coupled with attack signals poses a major challenge to the detection and rejection of attacks. Attack-resilient estimation in the presence of a single disturbance has been studied in

recent literature. In [29], Guan et al. proposed a resilient attack detection estimator to deal with the simultaneous effects of FDI attacks, jamming attacks and norm-bounded disturbances. In [30], distributed estimation in the presence of FDI attacks on sensor communication edges and Gaussian disturbances was studied. In [1], Ugrinovskii proposed a novel distributed observer structure that is resilient to biasing attacks in the presence of norm-bounded disturbances via active feedback control.

2) Denial-of-Service Attacks

Denial-of-service (DoS) attacks are a type of adversary with the intent of blocking the data transmission in distributed systems. DoS could either be inflicted on the communication or sensor channel of the distributed control system. From a modeling perspective, the intervals of DoS attack can be modelled by a time sequence $\mathcal{H}_j = [h_j, h_j + \eta_j)$, where h_j represents the beginning instant of the attack, and $\eta_j > 0$ the duration of the attack. The length of the attack can either be described by a probability distribution, or an aperiodic set of intervals that is restricted through some boundedness constraints. It should be noted that the effect of DoS attacks is completely heterogeneous to the effect of deception attacks and cannot be dealt with a uniform approach. Existing work on resilient estimation against DoS attacks can be divided into several lines of work. To highlight a few, [31] proposed a game theoretic approach to model the decision-making of sensors under DoS attacks with energy constraint; in [32], based on a unified compensation model for DoS attacks obeying the Bernoulli distribution, the distributed secure state estimation problem was solved by using Kalman filters; an estimator with resilience towards DoS attacks was designed by solving a dynamic game with the reinforcement learning method in [33]. In [34], the performance of a discrete-time distributed system subject to network-induced delays and DoS attacks was analysed by placing an upper bound on the number of consecutive transmissions that are affected by the DoS.

It is noted that most of the works introduced above assume that the DoS attacks follow a probability distribution, and require continuous data transmission among the agents. Inspired by distributed estimation approaches using event-based updates [35, 36, 37], more recently, some works have designed event-based update schemes

to deal with aperiodic DoS attacks. The covariance intersection method and the collectively observable condition were utilised in [38] to design resilient distributed Kalman filters. In [39], a multi-mode switching estimator and a dynamic trigger threshold were introduced for DoS resilient estimation for nonlinear systems. In [40], a distributed interval estimator was developed based on an adaptive event-triggered protocol that is based on the latest update.

3) Sparse Attacks

From the previous sections, it can be concluded that both false data injection and denial-of-service attacks are required to follow some boundedness constraints. On the contrary, sparse attacks, also referred to as Byzantine attacks or simply sensor attacks in some literature, assume that the state/measurement of the attacked agents are arbitrary, under the condition that the adversary can only target a part of sensors. In the presence of sparse attacks, it is natural to consider approaches that identify and isolate the attacked sensors, and reconstruction of the correct state under sparse attacks is intrinsically a combinatorial problem.

Resilient estimation against sparse attacks has been widely investigated in recent years. The observability of systems under sparse attacks was analysed in [41], and a definition called strong observability was further defined in [42]. For discrete-time linear time-invariant systems, the secure state estimation can be performed by collecting the past τ consecutive measurements and performing static batch optimization [43, 44, 45, 46]. In addition to the static batch optimization, many effective methods have been proposed, including the set cover approach [47], satisfiability modulo theory [48], and optimal graph searching [49]. However, the aforementioned results are computationally demanding, and cannot achieve real time estimation.

For continuous-time linear time-invariant systems, secure state estimation under sparse attacks has also been studied. To identify sparse attacks, multi-model observers were designed in [22] and [50]. But the schemes proposed in [22] and [50] suffer from heavy computational burden because multiple observers are required to run in parallel. With the assumption that the attack signals are bounded, an adaptive switching mechanism was introduced in [51] to search for the attack mode. In a similar vein,

a descriptor form sliding mode observer was designed for secure state estimation under sparse attacks, under the conditions that both the attack and its derivative are bounded [52]. However, for sparse attacks, the boundedness assumptions in [51] and [52] are unfavorable. In [53], a monitored state observer was introduced for linear systems under location-varying attacks. The same as in [52], only some sufficient conditions were given in [53] for the existence of estimators in the form of multiple LMIs, and such LMIs may even have no solutions in some cases.

1.2.2 Resilient Control

Another widely-researched topic in distributed dynamic systems is performing coordination tasks by designing suitable distributed control strategies. Typical applications of distributed control include cooperative control of industrial systems such as manipulators [54, 55, 56], formation control for robots [57, 58] and scheduling of smart grids [59, 60].

In some aspects, the distributed control problem is analogous to that of distributed estimation. However, some distinctions between distributed estimation and control can be found in the problem and system formulation. Firstly, the distributed control task can be categorised based on the number of leaders into leaderless consensus, leader-following and containment control. Leaderless consensus is the control problem for all agents in the distributed system to reach an agreement as a whole. Leader-following control involves all follower agents to track the state of the single leader agent, and the objective of containment control is to drive all followers into the convex hull spanned by multiple leaders. Secondly, obtaining accurate models of practical industrial systems is a challenging task, and cooperative control for uncertain distributed systems has received an increasing amount of attention [61, 62, 63, 64, 65, 66, 67]. Finally, the actuator channel is also subject to security and reliability challenges, which is motivation to consider resilient distributed control approaches.

During the practical operation of distributed control systems, the actuators of agents may suffer from unknown faults, which could lead to performance degradation or even accidents. Ensuring the stability and performance of distributed control systems

under faults is a topic of both theoretical and practical importance. It is noted that though the distributed control problem could also be faced with the aforementioned false data injection, denial-of-service and sparse attacks, faults on the actuators are the main type of adversary that is relatively unique to the distributed control problem, and will be the focus of this section.

1) Known Direction Actuator Faults

A wealth of research has been carried out for resilient distributed control with actuator faults. Authors of [62] developed an adaptive distributed fault-tolerant control scheme for actuator faults that can be modelled as a constant. A more practical and challenging type of faults is where the effectiveness of the actuator and the additive fault signal are time-varying. In these cases, the actuator signal of the ith agent can be modelled as

$$u_i(t) = b_i(t)v_i(t) + \delta_i(t), i = 1, \ldots, N, \tag{1.4}$$

where $v_i(t) \in \mathbb{R}^{n_i}$ is the control signal to be designed, and $b_i(t) \in \mathbb{R}^{n_i \times n_i}$ and $\delta_i(t) \in \mathbb{R}^{n_i}$ are unknown. Aiming at time-varying additive faults and partial loss of effectiveness faults, many effective adaptive fault-tolerant control schemes have been proposed [65, 68, 69, 70, 71]. To name a few, [72] investigated fault-tolerant leader-following for leaders with uncertain dynamics via a data-driven approach. A reinforcement learning method was introduced in [73] for the containment control problem. Both sensor and actuator faults were considered in [74], where adaptive and H_∞ controllers were introduced and compared. On the other hand, many engineering systems are multi-input multi-output (MIMO) systems, where n_i in (1.4) is larger than 1, which makes the resilient control problem more challenging. A number of works have dealt with the fault-resilient control problem for distributed MIMO systems [68, 75, 76].

2) Unknown Direction Actuator Faults

It has been noted that the aforementioned work are carried out under the assumption that the control directions and fault directions are known, that is, $b_i(t) > 0$. However, in many cases, the control/fault directions may be unknown in the controller design process, where practical examples of unknown control direction include un-calibrated visual servoing and autopilot design of ships [77]. A typical approach to

deal with unknown control directions is to introduce a Nussbaum function, and this approach was only recently extended to distributed systems whose control directions are unknown [78, 79, 80]. However, the application of the Nussbaum function approach for distributed systems means that additions involving multiple Nussbaum functions exist for multiple agents in the distributed system, and their effects may counteract each other, therefore [78, 79, 80] assumed that all unknown control directions in the distributed system are identical. In another line of work, [81, 82, 83] applied a compensator network to tackle unknown nonidentical control directions, with the trade-off being increased order of the closed-loop system. The control for MIMO systems with unknown control direction is a more challenging problem. Some novel Nussbaum functions which ensure that the effects of the multiple Nussbaum functions reinforce rather than counteract each other were introduced in [84]. In [85], a multiple-model adaptive control scheme was proposed, where for a q-input q-output system, 2^q controllers were required to run in parallel, and 2^q estimators were required for each unknown nominal controller parameter, resulting in considerable computation burden.

In spite of the progress, all the aforementioned research make the assumption that the unknown control directions are constant and do not experience jumps. Unknown direction actuator faults, which introduce jumps to the actuation directions are a type of actuator faults that exists on practical engineering systems such as, spacecraft [86], power systems [87] and vehicles [88]. The jumps in actuator directions introduced by the unknown direction faults make the existing Nussbaum function based approaches no longer valid. Resilient control for distributed systems with time-varying unknown control direction faults is a challenging problem that has yet to be addressed.

1.3 Contributions and Organization

This thesis aims to address the gaps in current research on resilient estimation and control. The main contributions of this thesis can be summarised as follows.

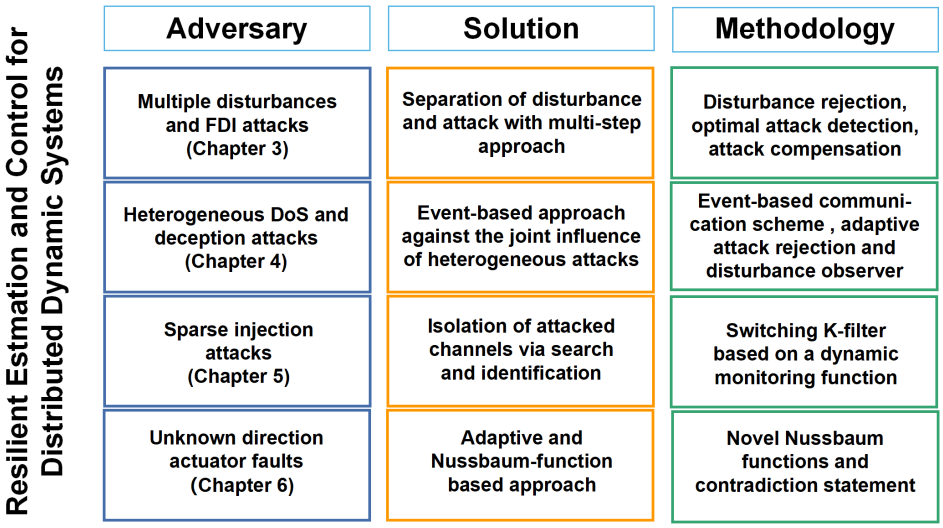

Figure 1.2: Organization and contents of this thesis.

- For distributed systems with multiple disturbances and false data injection attacks, a multi-step resilient estimation approach consisting of a composite hierarchical anti-disturbance observer, an attack detector and a detection-triggered attack observer is introduced. Compared with existing results, the proposed approach separates the influence of disturbances and attacks to enhance the resilience of distributed systems.

- For distributed systems under both deception and denial-of-service attacks, a novel event-based distributed estimator is designed. A novel event-based communication scheme, an adaptive term and a distributed disturbance observer are introduced, which reduces the communication burden and guarantees the estimation performance under the joint influence of heterogeneous attacks and disturbances.

- For nonlinear systems under sparse injection attacks, a monitoring function and a switching estimator are proposed. By utilizing redundancy of measurements, the sparse attack channels can be identified and subsequently removed to guarantee the correctness of estimation. This is the first research to consider sparse attack-resilient estimation for nonlinear systems.

- An adaptive resilient containment control scheme is designed for a class of heterogeneous distributed MIMO systems with unknown direction faults. Through introduction of novel Nussbaum function-based controllers and a novel contradiction statement, the unknown system parameters and unknown direction jumps in the actuators are dealt with successfully. Compared with existing research, the proposed resilient control scheme allows the fault directions to be unknown and time-varying and only requires the leading principle minors of the control gain matrices to be nonzero, which relaxes the restrictions on the CGMs and enhances system reliability.

As shown in Figure 1.2, this thesis consists of six chapters, and a brief introduction of each chapter is presented as follows.

In Chapter 1, the background and motivation of the estimation and control problem for distributed dynamic systems are introduced. Then, we review the current research progress related to resilient estimation and control. The main contributions of this thesis are also given.

In Chapter 2, related preliminaries including mathematical notations, stability theory and basic algebraic graph theory are introduced.

In Chapter 3, the resilient estimation problem for distributed systems under multiple disturbances and false data injection attacks is considered. Disturbances and attacks co-exist widely in practical systems and distributed state estimation of distributed systems in the simultaneous presence of disturbances and attacks has been widely recognised as a challenging issue. In this chapter, an enhanced three-stage approach for the detection and rejection of attacks is established. First, a multi-layer distributed estimator with a disturbance observer layer is proposed. Then, an optimal observer-based attack detection scheme is designed to specify an attack detection logic. After disturbance rejection and attack detection, an attack-resilient estimator with a dynamic detection-triggered structure is proposed to actively reject FDI attacks online. This three-stage approach effectively separates the influence of disturbances and attacks in the distributed estimation process, enabling multiple heterogeneous disturbances and attacks across the sensor network to be rejected. A numeric example and

comparisons are provided to illustrate the effectiveness of the proposed approach.

In Chapter 4, we investigate the resilient estimation problem for distributed system under heterogeneous attacks. Distributed control systems, particularly networked cyber-physical systems are prone to various types of cyber-attacks and disturbances. An event-based distributed estimation approach is introduced to deal with the joint influence of DoS and deception attacks under disturbances. A distributed event-based communication scheme is proposed to guarantee estimation performance in the presence of aperiodic DoS attacks and simultaneously reduce the data transmission burden. A novel adaptive observer is constructed to compensate for deception attacks. Moreover, a distributed disturbance observer is proposed for disturbance rejection. Sufficient conditions for the estimator design are given, which take the joint effects of DoS attacks and deception attacks into account. The proposed estimation approach is capable of attack-resilient state estimation subject to both DoS and deception attacks under disturbances and precludes Zeno phenomenon. Finally, a simulation example on an IEEE 4-bus power grid demonstrates the feasibility and effectiveness of the proposed approach.

In Chapter 5, resilient estimation for nonlinear engineering systems under sparse attacks is addressed. Secure state estimation against sparse injection attacks and disturbances is a challenging problem of both theoretical and practical importance, and existing results mainly focus on linear systems despite many practical systems being nonlinear. In this chapter, a novel secure state estimation scheme is proposed for a class of nonlinear systems with application to robotic manipulators. A kind of high-gain K-filters is constructed to estimate the unmeasured states, which can attenuate the disturbances to an arbitrary level. Moreover, a monitoring function and a switching scheme are introduced, which successfully preclude attacked measurements after a finite number of switching. With these efforts, the proposed estimation scheme steers the estimation error into a residual set which can be made arbitrarily small by properly choosing some design parameters, regardless of the disturbances and possibly unbounded attacks. Both simulation and experimental results on a robotic manipulator demonstrate the effectiveness of the proposed method.

In Chapter 6, a novel output-feedback adaptive containment control scheme is proposed for a class of heterogeneous multi-agent systems, where the agents are nonlinear multi-input multi-output (MIMO) systems whose relative degrees are allowed to be different. Unlike existing results, we only require the leading principal minors of agents' control gain matrices (CGMs) to be nonzero and take into account unknown direction actuator faults, which relaxes the restrictions on CGMs and enhances system reliability. The difficulties jointly caused by the unknown CGMs, unknown parameters, and unknown jumps introduced by the actuator faults are successfully overcome by a novel recursive contradiction argument based on some Nussbaum functions and a matrix similarity transformation. Moreover, an event-triggering mechanism is introduced to avoid continuous communication among agents and reduce the communication burden. It is shown that all closed-loop signals are globally uniformly bounded and the containment errors converge to a residual set that can be made arbitrarily small. Simulation results illustrate the effectiveness of the proposed scheme.

In Chapter 7, the thesis is summarised, and potential directions for future research are pointed out.

Chapter 2

Preliminaries

2.1 Notations

In this section, some notations and definitions used throughout this thesis are given. For a vector $v(t)$, its Euclidean norm is denoted as $\|v(t)\| = \sqrt{v^{\mathrm{T}}(t)v(t)}$. $C_n^m = \frac{n!}{m!(n-m)!}$, where ! is the factorial operator. $\mathrm{supp}(a(t))$ denotes the set consisting of indices corresponding to the non-zero elements of $a(t)$. For a set S, $|S|$ denotes its number of nonzero elements. 1_n denotes a column vector of dimension n with all elements equal to 1, and I_n denotes the $n \times n$ identity matrix. P^{T} represents the transpose of the matrix P. $P > 0$ and $P < 0$ denote positive definiteness and negative definiteness, respectively. $\lambda_{\max}(A)$ denotes the largest eigenvalue of matrix A and $\lambda_{\min}(A)$ denotes the smallest eigenvalue of matrix A. For a real matrix M, we define the operation $\mathbb{H}\{M\}$ as $\mathbb{H}\{M\} = M + M^{\mathrm{T}}$.

Definition 2.1.1. The Kronecker product of a $m \times n$ matrix A and a $p \times q$ matrix B is a $mp \times nq$ matrix denoted as $A \otimes B$ defined as

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}.$$

Definition 2.1.2. The function f is globally Lipschitz on $\mathbb{R}$ if there exists $K \in \mathbb{R}_{\geq 0}$

such that $|f(x) - f(y)| \leq K\|x - y\|, \ \forall x, y \in \mathbb{R}^n$.

Lemma 2.1.1. (Young's inequality, [89]). For $a, b \geq 0$ and $p, q \geq 1$ such that $\frac{1}{p} + \frac{1}{q} = 1$ one has

$$ab \leq \frac{1}{p}a^p + \frac{1}{q}b^q.$$

2.2 Basic Graph Theory

The topological features of a distributed system can be modelled using graphs. In this section, we introduce some graph theory basics that are essential to distributed estimation and control.

A graph denoted by $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ with the index set $\mathcal{V} = \{1, 2, \ldots, \mathcal{N}\}$ represents a networked system with $\mathcal{N}$ agents. $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ denotes the set of edges. An edge of the directed graph $\mathcal{G}$ is denoted by (i, j). An edge $(j, i) \in \mathcal{E}$ implies that information can be transferred from agent j to agent i but not vice versa. In this case, agent j is an in-neighbour of agent i, and agent i is an out-neighbour of agent j. If for any edge on the graph, $(i, j) \in \mathcal{E}$ implies $(i, j) \in \mathcal{E}$, then the graph is undirected. $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{\mathcal{N}\times\mathcal{N}}$ denotes the adjacency matrix. Elements of the adjacency matrix $a_{ij} > 0 \Leftrightarrow (j, i) \in \mathcal{E}$ are positive elements representing the directed information transmission, whereas the adjacency element $a_{ij} = 0$ if no directed link exists from sensor j to sensor i. The set of neighbors of node i is denoted by $\mathcal{N}_i = \{j \in \mathcal{V} : (j, i) \in \mathcal{E}\}$. The Laplacian matrix of the graph $\mathcal{G}$ is defined as

$$\mathcal{L} = \mathcal{W} - \mathcal{A},$$

where $\mathcal{W} = \mathrm{diag}^i_{\mathcal{N}}\{w_i\}$ with the diagonal elements $w_i = \sum_{j\in\mathcal{N}_i} a_{ij}$ represents the degree of the sensor node, and $\mathcal{A}$ is the adjacency matrix. It is clear that since $\mathcal{L}$ has zero row sums, 0 is an eigenvalue of $\mathcal{L}$ associated with the eigenvector $1_{\mathcal{N}}$.

A directed graph is strongly connected if there exist a directed path from every agent to every other agent. A directed graph is complete if there is an edge from every node to every other node. A directed tree is a directed graph, where every node has exact one parent except for one node, called the root, and the root has directed paths

to every other node. A spanning tree is a subset of the Graph $\mathcal{G}$, which has all the vertices covered with minimum possible number of edges. The existence of a spanning tree in a undirected graph is equivalent to the undirected graph being connected. A strongly connected graph contains at least one directed spanning tree, therefore the existence of a spanning tree is a weaker condition than being strongly connected. The Laplacian matrix $\mathcal{L}$ of a strongly connected graph has 0 as a simple eigenvalue, and all nonzero eigenvalues have positive real parts.

Depending on the number of leaders, the topology of distributed systems can be categorised as leaderless, leader-follower, and multiple leaders. For distributed systems with multiple leaders, containment control can be carried out with the objective to drive all followers into the convex hull spanned by multiple leaders. Assuming that the leaders have no in-neighbors, the Laplacian matrix associated with a distributed system with n leaders and m followers can be written as

$$\mathcal{L} = \begin{bmatrix} \mathcal{L}_1 & \mathcal{L}_2 \\ 0_{m\times n} & 0_{m\times m} \end{bmatrix} \tag{2.1}$$

where $\mathcal{L}_1 \in \mathbb{R}^{n\times n}$ contains the topology of the leaders and $\mathcal{L}_2 \in \mathbb{R}^{n\times m}$ contains the topology of followers.

Definition 2.2.1 ([90]). A square matrix $A \in \mathbb{R}^{n\times n}$ is called a nonsingular M-matrix if all its off-diagonal elements are non-positive, and all eigenvalues of A have positive real parts.

Lemma 2.2.1. ([91]) Assume that for each of the followers, there exists at least one leader that has a directed path to the follower. Then, each entry of $-\mathcal{L}_1^{-1}\mathcal{L}_2$ is non-negative, and all row sums of $-\mathcal{L}_1^{-1}\mathcal{L}_2$ is equal to one.

Proof. Noting that $\mathcal{L}_1$ is a nonsingular M-matrix, the eigenvalues of $\mathcal{L}_1$ have non-negative real parts. Noting that $\mathcal{L}$ contains a spanning tree, $\mathcal{L}_1$ is non-singular, and all eigenvalues of $\mathcal{L}_1$ have non-negative real parts. Since each entry of $\mathcal{L}_2$ is non-positive, it can be concluded that each entry of $-\mathcal{L}_1^{-1}\mathcal{L}_2$ is non-negative. It can also be obtained that $\begin{bmatrix} \mathcal{L}_1 & \mathcal{L}_2 \end{bmatrix} \begin{bmatrix} 1_n \\ 1_m \end{bmatrix} = 0$, and it follows that $\mathcal{L}_1 1_n = -\mathcal{L}_2 1_m$, which implies that $-\mathcal{L}_1^{-1}\mathcal{L}_2 1_m = 1_n$. Thus, each row sum of $-\mathcal{L}_1^{-1}\mathcal{L}_2$ equals one.

2.3 Basic Stability Theory

Consider the system

$$\dot{x} = f(x,t), \quad x(t_0) = x_0, \quad x \in \mathbb{R}^n. \tag{2.2}$$

The point $x^* \in \mathbb{R}^n$ is called a equilibrium point of (2.2) if $f(x^*, t) \equiv 0$.

Definition 2.3.1. (Lyapunov Stability) The equilibrium point $x^* = 0$ of (2.2) is Lyapunov stable at $t = t_0$ if for any constant $\epsilon > 0$, there exists a $\delta(t_0, \epsilon) > 0$ such that

$$\|x(t_0)\| < \delta \quad \Longrightarrow \quad \|x(t)\| < \epsilon, \quad \forall t \geq t_0.$$

Definition 2.3.2. (Asymptotic Stability) For the system (2.2), the equilibrium point $x^* = 0$ is asymptotically stable if it is Lyapunov stable, and $\lim_{t\to\infty} x(t) = 0$. If $\lim_{t\to\infty} x(t) = 0$ holds for any initial state in $\mathbb{R}^n$, the equilibrium point is globally asymptotically stable.

Definition 2.3.3. (Exponential Stability) For the system (2.2), the equilibrium point $x^* = 0$ is exponentially stable if there exist $\alpha > 0$ and $\beta > 0$ such that

$$\|x(t)\| < \alpha \|x(0)\| e^{-\beta t}$$

holds. If this inequality holds for any initial state in $\mathbb{R}^n$, the equilibrium point is globally exponentially stable.

Definition 2.3.4. (Positive Definite Function), A scalar function $V(x)$ is locally positive definite if $V(0) = 0$ and $x \neq 0$ implies $V(x) > 0$ in a ball around the origin. If the above properties hold for the entire space, the $V(x)$ is said to be globally positive definite.

Definition 2.3.5. (Lyapunov function) If the function $V(x)$ is positive definite, has continuous partial derivatives, and its time derivative $\dot{V}(x)$ satisfies $\dot{V}(x) \leq 0$, then $V(x)$ is a Lyapunov function.

Lemma 2.3.1. (Barbalat's Lemma) If a function $f(t)$ is uniformly continuous for $t \in [0, \infty)$, and $\int_0^\infty f(t)dt$ exists, then $\lim_{t\to\infty} f(t) = 0$.

Lemma 2.3.2. Let $V : [0, \infty) \mapsto \mathbb{R}$ and f be a constant. Then

$$\dot{V} \leq -\alpha V + f, \quad \forall t \geq t_0 \geq 0 \tag{2.3}$$

implies that

$$V(t) \leq e^{-\alpha(t-t_0)} V(t_0) + \frac{f}{\alpha} - \frac{f e^{(\alpha(t_0-t))}}{\alpha}, \quad \forall t \geq t_0 \geq 0 \tag{2.4}$$

for any positive constant α.

Proof. First, multiply both sides of (2.3) with $e^{\alpha t}$, and we have

$$e^{\alpha t}\dot{V} + e^{\alpha t}\alpha V \leq e^{\alpha t} f. \tag{2.5}$$

Noting that f is a constant, we can integrate both sides of (2.5) over $[t_0, t]$ and obtain

$$e^{\alpha t} V(t) \leq e^{\alpha t_0} V(t_0) + \frac{f e^{\alpha t}}{\alpha} - \frac{f e^{\alpha t_0}}{\alpha}, \tag{2.6}$$

Dividing both sides of (2.6) with $e^{\alpha t}$, we obtain (2.4) and the proof is complete. ■

Definition 2.3.6. (Nussbaum function, [92]) A continuously differentiable function $h(x) : [0, \infty) \mapsto (-\infty, \infty)$ is called a Nussbaum function if it satisfies

$$\limsup_{y \to \infty} \frac{1}{y} \int_0^y h(x) dx = \infty$$

$$\liminf_{y \to \infty} \frac{1}{y} \int_0^y h(x) dx = -\infty.$$

Chapter 3

Resilient Distributed Estimation Under Multiple Disturbances and Injection Attacks

3.1 Introduction

False data injection (FDI) attacks do not require prior knowledge of the internal model or the network topology, and false signals could easily be mixed with the actual sensor measurement to destabilise the state estimator [14]. FDI attacks can disrupt the integrity of information in networked systems, and lead to severe security loss, as is evident in numerous real-life incidents [15, 16]. It is of great importance to investigate secure distributed state estimation schemes with enhanced resilience towards FDI attacks.

On the other hand, it is well known that disturbances from both internal and external sources exist in networked systems. The coupling of disturbance and attack signals poses a major challenge to the detection and rejection of attacks. It is noted that only a single source of disturbance was considered in existing works, which can be described by either Gaussian [30] or norm-bounded variables [1, 29] and can be separated from the attacks. However, in practical scenarios, multiple types of disturbances

co-exist. When multiple sources of disturbances appear in the sensor measurements, it is difficult to distinguish attack signals from disturbances. Detection and rejection of FDI attacks for a network subject to multiple disturbances remains a challenging and open problem.

In this chapter, an enhanced distributed state estimation approach with resilience to multiple disturbances and FDI attacks is proposed. In many practical cases, a distinction between disturbances and attacks is that while most disturbances are persistent, the occurrence of FDI attacks is intermittent and irregular. This suggests that it is possible to estimate and reject some disturbances in prior to the occurrence of FDI attacks. Inspired by this phenomenon, a novel three-stage approach is proposed to reject both multiple disturbances and FDI attacks. In the initial stages of estimation, a multi-layer anti-disturbance estimator integrated with a disturbance observer is proposed for simultaneous attenuation and compensation of multiple disturbances. This stage can be considered as the calibration/initialization of the system. Subsequently, an optimal observer-based FDI attack detection algorithm in the presence of disturbances is developed and adopted as a trigger to activate the attack estimator. Finally, a detection-triggered attack-resilient estimator is introduced to actively reject the effect of attacks. The considered adversaries do not require knowledge of the system, measurements or the topology of the network. The main contributions of this chapter are as follows:

1) For a networked system under multiple disturbances, an anti-disturbance estimator with a novel multi-layer architecture is presented to achieve simultaneous state estimation and disturbance rejection for a distributed system. Specifically, a disturbance observer is constructed in the inner layer to estimate and compensate for the disturbances with partially known dynamics, and a robust H_∞ filtering scheme is employed in the outer layer to attenuate the remaining norm-bounded disturbances. With the proposed disturbance rejection scheme, multiple sources of disturbances can be dealt with simultaneously. Moreover, with the rejection of disturbances, the false alarm rate of the subsequent attack detection strategy is significantly reduced.

2) A three-stage resilient distributed estimation approach consisting of anti-disturbance

estimation, attack detection and attack-resilient estimation is proposed to simultaneously reject and attenuate multiple disturbances and FDI attacks in networked systems. The considered attack model is not assumed to have knowledge of the system, and the number of considered attacks is not limited. Compared with existing methods that aim to mitigate or isolate the effects of FDI attacks, the proposed estimation scheme estimates and compensates for FDI attacks to actively reject their effects whilst the system remains online.

3.2 Problem Formulation

In this chapter, a sensor network with $\mathcal{N}$ sensor subsystems is considered. The topology of the interacting sensor network is represented with a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$. The dynamics of the sensor systems and measurements are given by

$$\dot{x} = Ax + Gg(x,t) + Bw, \tag{3.1}$$

$$y_i = C_i x + H_i h(x,t) + D_i v_i + D_1^i d_i + D_2^i f_i, \qquad \forall i \in 1, ..., \mathcal{N}, \tag{3.2}$$

where $x \in \mathbb{R}^n$ and $y_i \in \mathbb{R}^m$ are the state and the sensor measurement, respectively. A, B, C_i, D_i, D_1^i, D_2^i, G and H_i are known constant matrices with compatible dimensions. $g(x,t)$ and $h(x,t)$ are known nonlinear functions. d_i are external disturbances. f_i are the FDI attacks satisfying $|f_i| \leq \bar{f}, \forall t \geq 0$, where $\bar{f}$ is an unknown constant. The modelling of the FDIs is based on the principle that typically no prior knowledge of FDIs should be known, and a similar attack model has been studied in [1, 93] and [94]. In this case, the attacks are assumed to be absent in the initial stages of estimation. w and v_i are the norm-bounded disturbances in the system and measurements, respectively.

Assumption 3.2.1. w and v_i satisfy

$$\|w\| \leq \beta_1, \|v_i\| \leq \beta_2, \tag{3.3}$$

where β_1 and β_2 are known positive constants.

Assumption 3.2.2. For any x_1 and $x_2 \in \mathbb{R}^n$, the nonlinear functions $g(x,t)$ and

$h(x,t)$ satisfy

$$g(0,t)=0, \|g(x_1,t)-g(x_2,t)\| \leq \|U_1(x_1-x_2)\|,$$
$$h(0,t)=0, \|h(x_1,t)-h(x_2,t)\| \leq \|U_2(x_1-x_2)\|, \tag{3.4}$$

where U_i $(i=1,2)$ are known constant matrices.

The external disturbances d_i can be described by the following exogenous systems:

$$\dot{d}_i = S_i d_i, \qquad \forall i \in 1,...,\mathcal{N}, \tag{3.5}$$

where S_i are known constant matrices. The model in (3.5) can describe many disturbances in practical engineering systems including Markov stochastic processes in inertial sensors, wind gust in the environment, jitters and vibrations in various sensor systems, and rotating mechanisms with eccentricity [95, 96].

Remark 3.2.1. The system model is a nonlinear model with norm-bounded disturbances and nonlinear items. The nonlinear items $g(x,t)$ and $h(x,t)$ are assumed to be Lipschitz. In addition to the norm-bounded disturbances w and v_i, which have been considered in works such as [1, 27, 97] and [98], unknown external disturbances d_i on the sensor measurements are considered in this chapter.

Remark 3.2.2. In this chapter, an assumption on the boundedness of the attack is made. It is noted that some works do not prescribe the attack signals to follow any particular structure or to be bounded. Examples include Byzantine attacks [99] and unbounded sparse attacks [53]. However, for the Byzantine model, the attacker is assumed to possess knowledge of the graph topology and the system dynamics, which is not required in our model. Moreover, both the Byzantine and unbounded sparse model limit the number of attacked sensors. Attack resilience cannot be guaranteed for those cases if this limit is exceeded, while our model allows for the 'worst case' situation where all sensors are corrupted with FDI attacks.

It is clear from the measurement model that the external disturbances d_i and attacks f_i are coupled on the measurement information, which is the main focal point of this chapter. The coupling of disturbances and attacks would cause great difficulties in the detection and rejection of these signals. Moreover, in a distributed estimator structure, the detrimental effects of d_i and f_i will propagate across the network.

3.3 Distributed Robust Anti-disturbance Estimation

In this section, a novel distributed multi-layer estimator with disturbance rejection capability is presented. The estimator comprises of two layers: 1) disturbance observer layer, which estimates and compensates for the effect of external disturbances across the network; 2) a robust H_∞ estimator layer, which attenuates the effects of additional norm-bounded disturbances and uncertainties to a predefined level. This multi-layer architecture enables simultaneous compensation and attenuation for multiple disturbances, which is akin to the approach taken in CHADC [95, 100]. The main objective of this estimator is to mitigate the influence of multiple disturbances on the following attack detection and rejection efforts. This estimation approach is designed to be performed in the initial stages of sensor network state estimation, in attack-free environments where FDI attacks f_i are absent.

For this purpose, the following multi-layer estimator structure is proposed:

$$\begin{cases} \dot{\hat{x}}_i = A\hat{x}_i + K_i\delta_i + M_i \sum_{j\in\mathcal{N}_i} a_{ij}\eta_{ij} + Gg(\hat{x}_i, t), \\ \dot{\hat{d}}_i = S_i\hat{d}_i + L_i\delta_i, \qquad \forall i \in \mathcal{V}, \end{cases} \tag{3.6}$$

where δ_i and η_{ij} are the local and distributed innovations, respectively. The estimator innovations utilise the state estimations from the local node i and its neighbouring nodes j. The measurements and state estimates are processed at each sensor subsystem rather than a fusion center. The local innovation δ_i and the distributed innovation η_{ij} are defined as

$$\begin{cases} \delta_i = y_i - C_i\hat{x}_i - D_1^i\hat{d}_i - H_i h(\hat{x}_i, t), \\ \eta_{ij} = \hat{x}_i - \hat{x}_j, \qquad \forall i \in \mathcal{V}. \end{cases} \tag{3.7}$$

The first equation of (3.6), which comprises the state estimation layer of the estimator, is updated by both the local innovation and the distributed innovation. The second equation, which is the estimator for external disturbances $\hat{d}_i$, has a similar form to a full order disturbance observer utilizing only the local innovations. K_i, M_i and L_i are the estimator gains to be computed. Note that the local innovations δ_i utilise not

only the local measurement y_i and the local estimated state x_i, but also the estimated value of disturbance d_i from the disturbance estimator to compensate for the effect of external disturbances in the state estimation. Estimated state information is shared between sensor subsystem i and their neighbours j through the distributed innovation η_{ij}. The distributed innovation enables co-operation between neighbouring nodes, and can be considered as a dynamic consensus protocol. The main distinctions between the proposed distributed estimator and the distributed estimators presented in [97] and [98] are that: 1) the proposed estimator adopts a multi-layer structure to perform disturbance estimation and rejection, where the disturbance estimations $\hat{d}_i$ are included in the local innovations δ_i as additional control inputs to counter the effect of external disturbances; 2) the proposed estimator takes additional consideration for system nonlinearities.

Remark 3.3.1. The proposed estimator (3.6) implements a multi-layer architecture, where the first layer comprises of a distributed state estimator and the second layer includes a disturbance observer. It should be noted that the proposed estimator does not pose a limit to the number of disturbances applied onto the sensor network. Also, since the disturbance observer layer only utilises local innovations, heterogeneous disturbances with different characteristics across the network can be dealt with simultaneously.

Defining the estimation errors as $e_{xi} = x - \hat{x}_i$ and $e_{di} = d_i - \hat{d}_i$, the error dynamic of the proposed estimator can be obtained as follows:

$$\begin{cases} \dot{e}_{xi} =(A - K_iC_i)e_{xi} + G\tilde{g}_i(t) + Bw - K_iD_1^ie_{di} - K_iD_iv_i - K_iH_i\tilde{h}_i(t) \\ \qquad\quad + M_i\sum\limits_{j\in\mathcal{N}_i} a_{ij}(e_{xi} - e_{xj}), \\ \dot{e}_{di} =(S_i - L_iD_1^i)e_{di} - L_iC_ie_{xi} - L_iD_iv_i - L_iH_i\tilde{h}_i(t), \end{cases} \tag{3.8}$$

where $\tilde{g}_i(t) = g(x(t), t) - g(\hat{x}_i(t), t)$ and $\tilde{h}_i(t) = h(x(t), t) - h(\hat{x}_i(t), t)$.

In order to simplify the notations for the information across the entire sensor network and facilitate the discussions, we denote $\bar{A} = I_{\mathcal{N}} \otimes A$, $\bar{B} = I_{\mathcal{N}} \otimes B$, $\bar{C} = \mathrm{diag}^i_{\mathcal{N}}\{C_i\}$, $\bar{D} = \mathrm{diag}^i_{\mathcal{N}}\{D_i\}$, $\bar{D}_1 = \mathrm{diag}^i_{\mathcal{N}}\{D_1^i\}$, $\bar{D}_2 = \mathrm{diag}^i_{\mathcal{N}}\{D_2^i\}$, $\bar{S} = \mathrm{diag}^i_{\mathcal{N}}\{S_i\}$, $\bar{K} = \mathrm{diag}^i_{\mathcal{N}}\{K_i\}$, $\bar{L} = \mathrm{diag}^i_{\mathcal{N}}\{L_i\}$, $\bar{M} = \mathrm{diag}^i_{\mathcal{N}}\{M_i\}$, $\bar{G} = \mathrm{col}_{\mathcal{N}}\{G\}$, $\bar{H} = \mathrm{col}^i_{\mathcal{N}}\{H_i\}$,

$\bar{e}_x = \mathrm{col}^i_{\mathcal{N}}\{e_{xi}\}$, $\bar{e}_d = \mathrm{col}^i_{\mathcal{N}}\{e_{di}\}$, $\bar{w} = \mathrm{col}_{\mathcal{N}}\{w\}$, $\bar{v} = \mathrm{col}^i_{\mathcal{N}}\{v_i\}$, $\bar{U}_1 = \mathrm{col}_{\mathcal{N}}\{U_1\}$, $\bar{U}_2 = \mathrm{col}_{\mathcal{N}}\{U_2\}$, $\bar{g}(t) = \mathrm{col}^i_{\mathcal{N}}\{\tilde{g}_i(t)\}$, $\bar{h}(t) = \mathrm{col}^i_{\mathcal{N}}\left\{\tilde{h}_i(t)\right\}$, and $\tilde{\mathcal{L}} = I_n \otimes \mathcal{L}$.

According the definition of the Laplacian matrix $\mathcal{L} = \mathcal{W} - \mathcal{A}$ and its elements l_{ij}, it is obvious that $\sum_{j=1}^{\mathcal{N}} a_{ij}(x_i - x_j) = \sum_{j=1}^{\mathcal{N}} l_{ij}x_j$. Taking the estimator gain M_i and previously denoted notations into consideration, it can be further obtained that

$$\sum_{i=1}^{\mathcal{N}} M_i \sum_{j=1}^{\mathcal{N}} a_{ij}(e_{xi} - e_{xj}) = \sum_{i=1}^{\mathcal{N}} M_i \sum_{j=1}^{N} l_{ij}e_{xj} = \bar{M}\tilde{\mathcal{L}}\bar{e}_x.$$

With the congregate notations and the relation obtained above, defining an extended error state as $\bar{e} = \left[\bar{e}_x^{\mathrm{T}}, \bar{e}_d^{\mathrm{T}}\right]^{\mathrm{T}}$ and $\bar{d} = \left[\bar{w}^{\mathrm{T}}, \bar{v}^{\mathrm{T}}\right]^{\mathrm{T}}$, the error dynamic across the entire sensor network can be rewritten as

$$\dot{\bar{e}} = \tilde{\mathcal{A}}\bar{e} + \tilde{\mathcal{B}}\bar{d} + \tilde{\mathcal{G}}\bar{g}(t) + \tilde{\mathcal{H}}\bar{h}(t), \tag{3.9}$$

where

$$\begin{aligned}
\tilde{\mathcal{A}} &= \begin{bmatrix} \bar{A} - \bar{K}\bar{C} + \bar{M}\tilde{\mathcal{L}} & -\bar{K}\bar{D}_1 \\ -\bar{L}\bar{C} & \bar{S} - \bar{L}\bar{D}_1 \end{bmatrix}, \tilde{\mathcal{B}} = \begin{bmatrix} \bar{B} & -\bar{K}\bar{D} \\ 0 & -\bar{L}\bar{D} \end{bmatrix}, \\
\tilde{\mathcal{G}} &= \begin{bmatrix} \bar{G} \\ 0 \end{bmatrix}, \tilde{\mathcal{H}} = \begin{bmatrix} -\bar{K}\bar{H} \\ -\bar{L}\bar{H} \end{bmatrix}.
\end{aligned} \tag{3.10}$$

To facilitate further discussions, the congregate form of the matrices can be divided into known system matrices and the estimator gains to be solved as

$$\tilde{\mathcal{A}} = \bar{\mathcal{A}} - \mathcal{K}\mathcal{C} + \mathcal{M}\bar{\mathcal{L}}, \quad \tilde{\mathcal{B}} = \mathcal{B} - \mathcal{K}\mathcal{D}, \quad \tilde{\mathcal{H}} = -\mathcal{K}\mathcal{H}, \tag{3.11}$$

where

$$\begin{aligned}
\bar{\mathcal{A}} &= \begin{bmatrix} \bar{A} & 0 \\ 0 & \bar{S} \end{bmatrix}, \mathcal{B} = \begin{bmatrix} \bar{B} & 0 \\ 0 & 0 \end{bmatrix}, \mathcal{K} = \begin{bmatrix} \bar{K} \\ \bar{L} \end{bmatrix}, \mathcal{M} = \begin{bmatrix} \bar{M} \\ 0 \end{bmatrix}, \\
\mathcal{C} &= \begin{bmatrix} \bar{C} & \bar{D}_1 \end{bmatrix}, \mathcal{D} = \begin{bmatrix} 0 & \bar{D} \end{bmatrix}, \bar{\mathcal{L}} = \begin{bmatrix} \tilde{\mathcal{L}} & 0 \end{bmatrix}.
\end{aligned} \tag{3.12}$$

Assumption 3.3.1. The matrix pair $\left(\bar{\mathcal{A}}, \left[\mathcal{C}^{\mathrm{T}}, \bar{\mathcal{L}}^{\mathrm{T}}\right]^{\mathrm{T}}\right)$ is detectable.

Remark 3.3.2. Assumption 3.3.1 is a necessary condition for the distributed estimator (3.6) to be asymptotically stable. For the state estimation layer of the distributed

estimator, we do not require the detectability of each individual matrix pair (A, C_i). Since the distributed structure allows for a certain level of co-operation between the sub-estimators, the conditions of detectability for the first equation of (3.6) can be relaxed to the detectability of the congregate matrix pair $\left(\bar{A}, \left[\bar{C}^{\mathrm{T}}, \tilde{\mathcal{L}}^{\mathrm{T}}\right]^{\mathrm{T}}\right)$, as stated in [101].

Extending these results, a similar conclusion for the error dynamics (3.9) can be reached as in Assumption 3.3.1. Breaking up the composite matrices, the detectability of the augmented networked system is a result of a number of factors: 1) each matrix pair (A, C_i); 2) the parameter matrices S_i and D_i^i; 3) the topology of the sensor network, which in this case is represented by the Laplacian matrix $\mathcal{L}$. The matrices from the detectability condition in Assumption 3.3.1, A, C_i, S_i, D_i^i and $\mathcal{L}$ are all known to the user of the system. The verification for detectability is a static process which can be performed off-line, before the estimation.

The objective of the proposed estimation method is to simultaneously estimate the state and the disturbance of each sensor subsystem, and utilise the estimated value of the disturbance to compensate for its effects. In this situation, accurate estimation performance is equivalent to the convergence of the error system (3.9). In addition, an H_∞ performance index is introduced to guarantee that the norm-bounded disturbances are attenuated. For a predefined level of disturbance attenuation performance $\gamma > 0$, the objective of the distributed estimator is to compute appropriate gains K_i, M_i and L_i to ensure that the following conditions are met:

(P1) The estimation error dynamic (3.9) in the absence of $\bar{d}$ is asymptotically stable, and

(P2) For nonzero $\bar{d}$, a given disturbance attenuation index γ and a predefined matrix M_∞, a reference output $Z = M_\infty \bar{e}$ under zero initial condition satisfies

$$\int_0^t Z^{\mathrm{T}}(\tau) Z(\tau) \mathrm{d}\tau < \gamma^2 \int_0^t (\bar{d}^{\mathrm{T}}(\tau)\bar{d}(\tau)) \mathrm{d}\tau. \tag{3.13}$$

In the following theorem, the design of the desired resilient estimator with appropriate estimator gains $\bar{K}$, $\bar{L}$ and $\bar{M}$ that satisfy conditions (P1) and (P2) is presented.

The first condition ensures that both the state and disturbance estimation asymptotically converge to their true values, while the second condition ensures that the norm-bounded disturbances are attenuated to a predefined H_∞ performance index.

Theorem 3.3.1. For the sensor network estimation with error dynamics (3.9) satisfying Assumptions 3.2.1, 3.2.2 and 3.3.1, for a predefined parameter $\gamma > 0$ and matrix M_∞, suppose that there exist matrices $P > 0$ and any Q, R satisfying $\Omega < 0$, where

$$\Omega = \begin{bmatrix} \Phi_1 & \Phi_2 & P\tilde{\mathcal{G}} & P\tilde{\mathcal{H}} & U_1^{\mathrm{T}} & U_2^{\mathrm{T}} & M_\infty^{\mathrm{T}} \\ * & -\gamma^2 I & 0 & 0 & 0 & 0 & 0 \\ * & * & -\frac{1}{\lambda_1^2} I & 0 & 0 & 0 & 0 \\ * & * & * & -\frac{1}{\lambda_2^2} I & 0 & 0 & 0 \\ * & * & * & * & -\lambda_1^2 I & 0 & 0 \\ * & * & * & * & * & -\lambda_2^2 I & 0 \\ * & * & * & * & * & * & -I \end{bmatrix}, \tag{3.14}$$

and

$$\Phi_1 = P\bar{\mathcal{A}} + \bar{\mathcal{A}}^{\mathrm{T}} P - Q\mathcal{C} - \mathcal{C}^{\mathrm{T}} Q^{\mathrm{T}} + R\bar{\mathcal{L}} + \bar{\mathcal{L}}^{\mathrm{T}} R^{\mathrm{T}},$$
$$\Phi_2 = P\mathcal{B} + \mathcal{B}^{\mathrm{T}} P - Q\mathcal{D} - \mathcal{D}^{\mathrm{T}} Q^{\mathrm{T}},$$

with $*$ representing the corresponding elements in the symmetric matrix. Then, by defining $\mathcal{K} = P^{-1}Q$ and $\mathcal{M} = P^{-1}R$, the estimator gains can be obtained and the error system (3.9) satisfies objective in (P1) and (P2).

Proof. In order to analyse the asymptotic stability of the estimator error dynamics, consider the Lyapunov candidate

$$V(t) = \bar{e}^{\mathrm{T}}(t) P \bar{e}(t) + \frac{1}{\lambda_1^2} \int_0^t \left[\|U_1 \bar{e}(\tau)\|^2 - \|\bar{g}(\tau)\|^2 \right] \mathrm{d}\tau + \frac{1}{\lambda_2^2} \int_0^t \left[\|U_2 \bar{e}(\tau)\|^2 - \left\|\bar{h}(\tau)\right\|^2 \right] \mathrm{d}\tau. \tag{3.15}$$

From the definitions of Assumption 3.2.2, we have $\|\bar{g}(\tau)\| \leq \|U_1 \bar{e}(\tau)\|$ and $\left\|\bar{h}(\tau)\right\| \leq \|U_2 \bar{e}(\tau)\|$, which ensures that $V \geq 0$ holds for all arguments. In the absence of $\bar{d}$, it

can obtained that

$$\begin{aligned}\dot{V} =& \bar{e}^{\mathrm{T}}\left(P\tilde{\mathcal{A}}+\tilde{\mathcal{A}}^{\mathrm{T}}P\right)\bar{e}+2\bar{e}^{\mathrm{T}}P\tilde{\mathcal{G}}\bar{g}(t)+2\bar{e}^{\mathrm{T}}P\tilde{\mathcal{H}}\bar{h}(t)+\lambda_1^2[\|U_1\bar{e}\|^2-\|\bar{g}(\tau)\|^2]\\ &+\lambda_2^2[\|U_2\bar{e}\|^2-\|\bar{f}(\tau)\|^2]\\ \leq& \bar{e}^{\mathrm{T}}[P\tilde{\mathcal{A}}+\tilde{\mathcal{A}}^{\mathrm{T}}P+\frac{1}{\lambda_1^2}P\tilde{\mathcal{G}}\tilde{\mathcal{G}}^{\mathrm{T}}P+\frac{1}{\lambda_2^2}P\tilde{\mathcal{H}}\tilde{\mathcal{H}}^{\mathrm{T}}P+\lambda_1^2U_1^{\mathrm{T}}U_1+\lambda_2^2U_2^{\mathrm{T}}U_2]\bar{e}\\ =& \bar{e}^{\mathrm{T}}\Omega_{11}\bar{e},\end{aligned} \tag{3.16}$$

where

$$\Omega_{11}=P\tilde{\mathcal{A}}+\tilde{\mathcal{A}}^{\mathrm{T}}P+\frac{1}{\lambda_1^2}P\tilde{\mathcal{G}}\tilde{\mathcal{G}}^{\mathrm{T}}P+\frac{1}{\lambda_2^2}P\tilde{\mathcal{H}}\tilde{\mathcal{H}}^{\mathrm{T}}P+\lambda_1^2U_1^{\mathrm{T}}U_1+\lambda_2^2U_2^{\mathrm{T}}U_2. \tag{3.17}$$

Based on Lyapunov theory, it is shown that the error dynamics in (3.9) is asymptotically stable in the absence of $\bar{d}$ if $\Omega_{11}<0$ holds.

Then, we focus on the condition (P2) for disturbance attenuation. Let us define the following auxiliary function

$$J(t)=V(t)+\int_0^t\left[\|Z(\tau)\|^2-\gamma^2\|\bar{d}(\tau)\|^2\right]\mathrm{d}\tau, \tag{3.18}$$

which satisfies $J(t)=\int_0^t S(\tau)\mathrm{d}\tau$ under zero initial condition, where V is denoted as in (3.15). We have

$$\begin{aligned}S(t)=&Z^{\mathrm{T}}(t)Z(t)-\gamma^2\bar{d}^{\mathrm{T}}(t)\bar{d}(t)+\dot{V}(t)\\ =&\bar{e}^{\mathrm{T}}(t)(\Omega_{11}+M_\infty^{\mathrm{T}}M_\infty)\bar{e}(t)+2e^{\mathrm{T}}(t)P\tilde{B}\bar{d}(t)-\gamma^2\bar{d}^{\mathrm{T}}(t)\bar{d}(t)\\ =&\begin{bmatrix}\bar{e}^{\mathrm{T}}(t) & \bar{d}^{\mathrm{T}}(t)\end{bmatrix}\Omega_{22}\begin{bmatrix}\bar{e}(t)\\ \bar{d}(t)\end{bmatrix},\end{aligned}$$

where

$$\Omega_{22}=\begin{bmatrix}\Omega_{11}+M_\infty^{\mathrm{T}}M_\infty & P\tilde{B}\\ \tilde{B}^{\mathrm{T}}P & -\gamma^2I\end{bmatrix}.$$

It can be seen that $\Omega<0$ if and only if $\Omega_{22}<0$ according to the Schur complement lemma, and it is obvious that Ω_{11} is a submatrix of Ω. Hence, it implies that $\Omega<0$ is equivalent to $S(t)\leq 0$. It is clear that $J(t)\leq 0$ when $S(t)\leq 0$ holds, and thus the condition (P2) is satisfied. The proof is complete. ■

In the estimators proposed in the following sections, the disturbance estimation is no longer updated by the innovation information, but rather updated using the previous estimation and the known dynamics of the disturbances. $\|\bar{e}\| \leq \varepsilon$ is proposed as the condition for the convergence of the estimator (3.6), and the moment that this condition is satisfied is denoted as t_n.

3.4 Optimal Observer-based Attack Detection

In this section, an optimal observer-based distributed attack detection method is introduced. The detector generates an optimal threshold to determine the presence of attacks. An attack detection logic is then established to enable the sensor network to make informed decisions. Using a guaranteed cost performance index as the objective function, an optimization algorithm with LMI constraints is applied to minimise the threshold value, improving the sensitivity to incoming FDI attacks.

The local innovations δ_i are selected as the residue signal of the detection due to its direct availability to the estimator system. Following the definition in the previous section, the set of local innovation values $\Delta = \mathrm{col}^i_{\mathcal{N}}\{\delta_i\}$ can be denoted as

$$\Delta = \bar{C}\bar{e}_x + \bar{D}_1\bar{e}_d + \bar{D}\bar{v} + \bar{H}\bar{h}(t) \leq (\bar{C} + \bar{H}\bar{U}_2)\bar{e}_x + \bar{D}_1\bar{e}_d + \bar{D}\bar{v}, \tag{3.19}$$

where $\bar{v} = \mathrm{col}^i_{\mathcal{N}}\{v_i\}$. Since attack detection takes place after the disturbance compensation, here $\bar{e}_d$ is considered as a norm-bounded residue error. A reference output is defined as

$$\begin{aligned} \varrho =& M_2\Delta = M_2\bar{C}\bar{e}_x + M_2\bar{D}_1\bar{e}_d + M_2\bar{D}\bar{v} + M_2\bar{H}\bar{h}(t) \\ \leq& M_2(\bar{C} + \bar{H}\bar{U}_2)\bar{e}_x + M_2\bar{D}_1\bar{e}_d + M_2\bar{D}\bar{v}. \end{aligned} \tag{3.20}$$

We consider the sub-optimal guaranteed cost for the H_2 performance index as

$$J_p = \int_0^\infty \varrho^{\mathrm{T}}(t)\varrho(t)\mathrm{d}t. \tag{3.21}$$

The design of observer based attack detection can be described as designing appropriate gains such that:

(Q1) The state estimation error dynamics $\dot{\bar{e}}_x = (\bar{A} - \bar{K}\bar{C} + \bar{M}\tilde{\mathcal{L}})\bar{e}_x + \bar{B}\bar{v}$ is asymptotically stable;

(Q2) The H_2 performance index J_p satisfies $J_p \leq J_b$, where the guaranteed performance index J_b of the proposed reference output is

$$J_b = V_x + \|\varrho\|^2 - \epsilon\|\bar{v}\|^2 - \epsilon\|\bar{e}_d\|^2,$$

where $V_x = \bar{e}_x^{\mathrm{T}} P \bar{e}_x$ and J_b is as small as possible. By minimising J_b, this attack detection approach aims to minimise the residue's sensitivity towards disturbances, so that its sensitivity towards incoming attacks is effectively maximised. The aforementioned conditions can be effectively represented by an LMI constraint. In the the following theorem, the design of an attack detection observer is provided such that conditions (Q1) and (Q2) are satisfied.

Theorem 3.4.1. For the reference output (3.20) and performance index (3.21), if there exist $P > 0$ and any Q, R such that

$$\Omega_1 = \begin{bmatrix} \Pi_{11} & \Pi_{12} & \Pi_{13} \\ * & \Pi_{22} & \Pi_{23} \\ * & * & \Pi_{33} \end{bmatrix} < 0,$$

where

$$\begin{aligned}
\Pi_{11} =& P\bar{A} + \bar{A}^{\mathrm{T}}P - Q\bar{C} - (Q\bar{C})^{\mathrm{T}} + R\tilde{\mathcal{L}} + (R\tilde{\mathcal{L}})^{\mathrm{T}} + (\bar{C} + \bar{H}\bar{U}_2)^{\mathrm{T}} M_2^{\mathrm{T}} M_2 (\bar{C} + \bar{H}\bar{U}_2), \\
\Pi_{12} =& (\bar{C} + \bar{H}\bar{U}_2)^{\mathrm{T}} M_2^{\mathrm{T}} M_2 \bar{D}_1, \quad \Pi_{13} = P\bar{B} + (\bar{C} + \bar{H}\bar{U}_2)^{\mathrm{T}} M_2^{\mathrm{T}} M_2 \bar{D}, \\
\Pi_{22} =& \bar{D}_1^{\mathrm{T}} M_2^{\mathrm{T}} M_2 \bar{D}_1 - \epsilon I, \quad \Pi_{23} = \bar{D}_1^{\mathrm{T}} M_2^{\mathrm{T}} M_2 \bar{D}, \quad \Pi_{33} = \bar{D}^{\mathrm{T}} M_2^{\mathrm{T}} M_2 \bar{D} - \epsilon I,
\end{aligned}$$

and $*$ represents the corresponding elements in the symmetric matrix, then condition (Q1) is met and the performance index satisfies

$$J_p = \|\varrho\|^2 \leq \bar{e}_x^{\mathrm{T}}(0) P \bar{e}_x(0) + \epsilon\|\bar{e}_d\|^2 + \epsilon\|\bar{v}\|^2, \tag{3.22}$$

with ϵ the infimum of the feasibility of $\Omega_1 < 0$.

Proof. A Lyapunov candidate is defined as

$$V_x = \bar{e}_x^{\mathrm{T}} P \bar{e}_x.$$

According to the error dynamics of $\bar{e}_x$ the derivative of V can be obtained as

$$\dot{V}_x = \bar{e}_x^{\mathrm{T}}(P\bar{A} + \bar{A}^{\mathrm{T}}P - Q\bar{C} - (Q\bar{C})^{\mathrm{T}} + R\tilde{\mathcal{L}} + (R\tilde{\mathcal{L}})^{\mathrm{T}})\bar{e}_x + 2\bar{e}_x^{\mathrm{T}} P \bar{B}\bar{v}.$$

Taking the derivative of J_b, we have

$$\dot{J}_b = \dot{V} + \|\varrho\| - \epsilon\|\bar{v}\| - \epsilon\|\bar{e}_d\| = \begin{bmatrix} \bar{e}_x^{\mathrm{T}}(t) & \bar{e}_d^{\mathrm{T}}(t) & \bar{v}^{\mathrm{T}} \end{bmatrix} \Omega_1 \begin{bmatrix} \bar{e}_x \\ \bar{e}_d \\ \bar{v} \end{bmatrix},$$

where the condition $\Omega_1 < 0$ ensures that condition (Q1) is met. The performance index J_b in (Q2) is minimised by calculating the infimum of the parameter ϵ of the feasibility of $\Omega_1 < 0$. The proof is complete. ■

After the design of the attack detection observer, an attack detection threshold can be specified and a decision logic based on value of the residue signals can be obtained. In this case, following the previous assumptions on the upper bound of the norm of estimation errors $\|\bar{e}_x\|^2$, $\|\bar{e}_d\|^2$ and the disturbances $\|\bar{v}\|^2$, we have a reference in $\|\varrho\|$ and a threshold value

$$\beta = \sqrt{\bar{e}_x^{\mathrm{T}}(0)P\bar{e}_x(0) + \epsilon\|\bar{e}_d\|^2 + \epsilon\|\bar{v}\|^2} = \sqrt{(\lambda_{\max}(P) + \epsilon)\varepsilon + \epsilon\beta_2}. \tag{3.23}$$

This attack detection threshold represents the practical upper bound of the effects of the estimation error residues and norm-bounded disturbances on the reference signal ϱ. Defining the residue indicator as $\rho(t) = \|\varrho(t)\|$, when the residue indicator does not exceed the threshold, it can be concluded that there are no attacks on the estimator system. The following logic for attack detection is proposed:

$$\rho \leq \beta \rightarrow \text{No attack},$$
$$\rho > \beta \rightarrow \text{attack} \rightarrow \text{alarm}.$$

Remark 3.4.1. It should be noted that the proposed attack detector is effectively a minimax detector, where the residue's sensitivity towards attack is maximised by minimizing its sensitivity towards disturbances. In this case, the attack detector is proposed as part of the multi-stage framework to facilitate the consequent resilient estimation efforts. Once an attack is detected and an alarm is raised, our attack detection logic leads to the activation of the attack-resilient estimator in the next section. In contrast to the anti-disturbance estimator proposed in Section 3.3, where a disturbance observer layer is constantly being updated, the attack observer layer to be

introduced in the next section is only activated when an attack is detected, effectively reducing the computation load.

3.5 Distributed Attack-Resilient Estimator

In the third and final stage of the proposed method, we focus on developing a detection-triggered distributed attack-resilient estimator. Resilience to FDI attacks on the sensor measurements is guaranteed via active attack estimation and compensation. An attack observer layer provides the estimator with the ability to recover from the effects of FDI attacks online. In addition, the proposed estimator is equipped with a dynamic detection-triggered structure, in which the attack estimator layer is only activated in the event of a detected attack.

Instead of isolating or re-initializing the sensor subsystems that are being attacked, the proposed distributed state estimator deals with the effect of the FDI attack via real-time online attack compensation, thereby enabling the sensor network to recover from FDI attacks without re-initialization. Unlike the research towards the Byzantine model [99] of attacks, our approach does not impose an upper bound on the number of compromised sensors. Also, since only the local innovation is utilised in the attack estimator, our method can deal with heterogeneous attacks across the sensor network.

The initial value of the attack-resilient estimator can be inherited from the estimation of the previous anti-disturbance estimator at the moment t_n:

$$\chi(0) = \hat{x}(t_n), \quad d^n(0) = \hat{d}(t_n). \tag{3.24}$$

We recall the measurement model from (3.2). At this stage of estimation, FDI attacks f_i are introduced. The FDI attacks are estimated and compensated for by a full-order attack observer in the event of a detected attack. The following estimator

structure is introduced:

$$\begin{cases} \dot{\chi}_i = A\chi_i + K_i^n \delta_i^n + M_i^n \sum_{j\in\mathcal{N}_i} a_{ij}\eta_{ij}^n + Gg(\chi_i, t), \\ \dot{\hat{f}}_i = \{ \begin{array}{l} J_i\delta_i^n, \text{ if attack detected,} \\ 0, \text{ otherwise,} \end{array} \end{cases} \tag{3.25}$$

where the local innovations δ_i^n and distributed innovations η_{ij}^n are defined as

$$\begin{cases} \delta_i^n = y_i - C_i\chi_i - D_1^i d_i^n - H_i h(\chi_i, t) - \hat{f}_i, \\ \eta_{ij}^n = \chi_i - \chi_j, \qquad \forall i \in \mathcal{V}. \end{cases} \tag{3.26}$$

It should also be noted that the external disturbances d_i are assumed to be still prevailing at this stage. Based on the known model of the disturbances and the previous estimation of the disturbances, the disturbances can be actively updated as $\dot{d}^n = Sd^n$.

Defining the estimation errors as $e_{\chi i} = \chi_i - \hat{\chi}_i$ and $e_{fi} = f_i - \hat{f}_i$, the error dynamic of the proposed estimator can be obtained as follows:

$$\begin{cases} \dot{e}_{\chi i} =(A - K_i^n C_i)e_{\chi i} + G\tilde{g}(t) + Bw - K_i^n D_2^i e_{fi} - K_i^n D_i v_i - K_i^n H_i \tilde{h}(t) \\ \qquad + M_i^n \sum_{j\in\mathcal{N}_i} a_{ij}(e_{\chi i} - e_{\chi j}), \\ \dot{e}_{fi} = - J_i D_2^i e_{fi} - J_i C_i e_{fi} - J_i D_i v_i - J_i H_i \tilde{h}(t). \end{cases} \tag{3.27}$$

According to congregate notations similar to that in Section 3.3, defining an extended error state as $\bar{e}_n = \left[\bar{e}_\chi^{\mathrm{T}}, \bar{e}_f^{\mathrm{T}}\right]^{\mathrm{T}}$ and $\bar{d} = \left[\bar{w}^{\mathrm{T}}, \bar{v}^{\mathrm{T}}\right]^{\mathrm{T}}$, the error dynamic across the entire sensor network can be rewritten as

$$\dot{\bar{e}}_n = \tilde{\mathcal{A}}_n \bar{e}_n + \tilde{B}_n \bar{d} + \tilde{\mathcal{G}}_n \bar{g}(t) + \tilde{\mathcal{H}}_n \bar{h}(t), \tag{3.28}$$

where

$$\tilde{\mathcal{A}}_n = \begin{bmatrix} \bar{A} - \bar{K}_n\bar{C} + \bar{M}_n\tilde{\mathcal{L}} & -\bar{K}_n\bar{D}_2 \\ -\bar{J}\bar{C} & -\bar{J}\bar{D}_2 \end{bmatrix}, \tilde{B}_n = \begin{bmatrix} \bar{B} & -\bar{K}_n\bar{D} \\ 0 & -\bar{J}\bar{D} \end{bmatrix},$$

$$\tilde{\mathcal{G}}_n = \begin{bmatrix} \bar{G} \\ 0 \end{bmatrix}, \tilde{\mathcal{H}}_n = \begin{bmatrix} -\bar{K}_n\bar{H} \\ -\bar{J}\bar{H} \end{bmatrix}.$$

The congregate form of the matrices can be divided into known system matrices and the estimator gains to be solved as

$$\tilde{\mathcal{A}} = \mathcal{A}_n - \mathcal{K}_n\mathcal{C}_n + \mathcal{M}_n\bar{\mathcal{L}}, \quad \tilde{B} = \mathcal{B} - \mathcal{K}_n\mathcal{D}, \quad \tilde{\mathcal{H}}_n = -\mathcal{K}_n\bar{H}_n, \tag{3.29}$$

where $\mathcal{C}_n = \begin{bmatrix} \bar{C} & \bar{D}_2 \end{bmatrix}$ and

$$\mathcal{A}_n = \begin{bmatrix} \bar{A} & \bar{B}_1 \\ 0 & 0 \end{bmatrix}, \mathcal{K}_n = \begin{bmatrix} \bar{K}_n \\ \bar{J} \end{bmatrix}, \mathcal{M}_n = \begin{bmatrix} \bar{M}_n \\ 0 \end{bmatrix}.$$

Assumption 3.5.1. The matrix pair $\left(\mathcal{A}_n, \left[\mathcal{C}_n^{\mathrm{T}}, \bar{\mathcal{L}}^{\mathrm{T}}\right]^{\mathrm{T}}\right)$ is detectable.

Remark 3.5.1. As discussed in Remark 3.3.2, the detectability conditions for the estimator in Assumption 3.5.1 should be regarded as an extension to the detectability condition proposed in Reference [101]. However, since the estimator proposed in this section takes a dynamic detection-triggered structure, when no attacks are detected, the estimator is reduced to a distributed H_∞ state estimator and correspondingly, the conditions for the stability of the error dynamics of the estimator would be reduced to the detectability of the matrix pair $\left(\bar{A}, \left[\bar{C}^{\mathrm{T}}, \tilde{L}^{\mathrm{T}}\right]^{\mathrm{T}}\right)$. For the sake of simplicity, we will focus on the stability of the expanded form of the attack-resilient estimator in the following theorem.

The objective of the distributed attack-resilient estimator is to ensure that the following conditions are met:

(R1) The estimation error dynamics (3.28) in the absence of $\bar{d}$ is asymptotically stable, and

(R2) For nonzero $\bar{d}$, a given disturbance attenuation index γ_n and a predefined matrix M_n, the reference output $Z = M_n\bar{e}_n$ under zero initial condition satisfies

$$\int_0^t Z^{\mathrm{T}}(\tau)Z(\tau)\mathrm{d}\tau < \gamma_n^2 \int_0^t (\bar{d}^{\mathrm{T}}(\tau)\bar{d}(\tau))\mathrm{d}\tau. \tag{3.30}$$

In the following theorem, we present a criteria of the existence of the proposed attack-resilient estimator with corresponding estimator gains $\bar{K}_n$, $\bar{J}$ and $\bar{M}_n$, where

for a predefined level of disturbance attenuation, asymptotic stability of the error dynamic (3.28) is ensured in the absence of $\bar{d}$ and the disturbances in $\bar{d}$ are attenuated to a level according to the H_∞ performance index.

Theorem 3.5.1. For the sensor network estimation with error dynamics (3.28) satisfying Assumptions 3.2.1, 3.3.1 and 3.5.1, for a predefined parameter $\gamma_n > 0$ and a matrix M_n, if there exist $P > 0$ and Q, R satisfying $\Omega_2 < 0$, where

$$\Omega_2 = \begin{bmatrix} N_1 & N_2 & P\tilde{\mathcal{G}} & P\tilde{\mathcal{H}} & U_1^{\mathrm{T}} & U_2^{\mathrm{T}} & M_n^{\mathrm{T}} \\ * & -\gamma_n^2 I & 0 & 0 & 0 & 0 & 0 \\ * & * & -\frac{1}{\lambda_1^2} I & 0 & 0 & 0 & 0 \\ * & * & * & -\frac{1}{\lambda_2^2} I & 0 & 0 & 0 \\ * & * & * & * & -\lambda_1^2 I & 0 & 0 \\ * & * & * & * & * & -\lambda_2^2 I & 0 \\ * & * & * & * & * & * & -I \end{bmatrix}, \tag{3.31}$$

and

$$N_1 = P\mathcal{A}_n + \mathcal{A}_n^{\mathrm{T}} P - Q\mathcal{C}_n - \mathcal{C}_n^{\mathrm{T}} Q^{\mathrm{T}} + R\bar{\mathcal{L}} + \bar{\mathcal{L}}^{\mathrm{T}} R^{\mathrm{T}},$$
$$N_2 = P\mathcal{B}_n + \mathcal{B}_n^{\mathrm{T}} P - Q\mathcal{D} - \mathcal{D}^{\mathrm{T}} Q^{\mathrm{T}},$$

with $*$ representing the corresponding elements in the symmetric matrix, then by defining $\mathcal{K}_n = P^{-1}Q$, $\mathcal{M}_n = P^{-1}R$, the estimator gains can be solved such that the conditions (R1) and (R2) are satisfied.

Proof. Noting the difference between $\mathcal{A}/\mathcal{A}_n, \mathcal{B}/\mathcal{B}_n$, $\mathcal{K}/\mathcal{K}_n, \mathcal{M}/\mathcal{M}_n$ and $\mathcal{C}/\mathcal{C}_n$, the proof can be given similarly to that of Theorem 3.3.1.

Remark 3.5.2. The main differences between the attack-resilient estimator proposed in (3.25) and the anti-disturbance estimator (3.6) are that: 1) The estimator (3.25) has a detection-triggered dynamic structure, which would significantly reduce the computation load of the estimator when no attacks are detected, whereas the estimator (3.6) has a fixed expanded multi-layer structure and higher computational load, but is only designed to be updated for the initial stages of estimation; 2) The model of the external disturbance d_i is supposed to be known, whereas no prior knowledge on the attack

is required. In many existing literature [1, 93], the attack on sensor measurements is assumed to be an injection of constant bias, a type of model which the proposed method is proven to be able to reject with sufficiency.

The proposed enhanced distributed state estimation algorithm is summarised in Figure 3.1 and Algorithm 1.

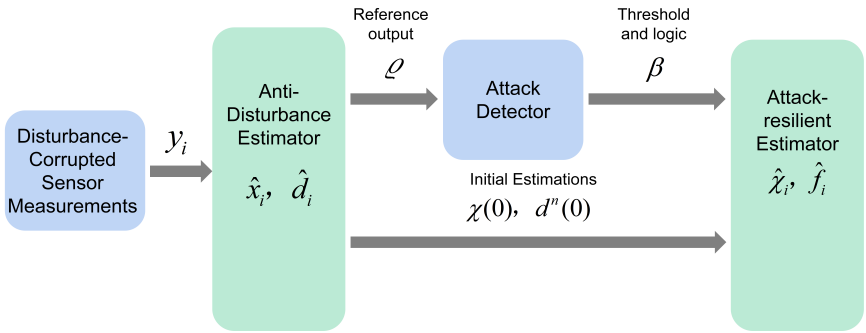

Figure 3.1: Schematic of enhanced approach to disturbance and attack rejection in distributed estimation.

Algorithm 1 Enhanced Distributed State Estimation

for Each sensor $i \in \mathcal{N}$ **do**
  Initialise and design a bank of estimators (3.6) for the sensor network (3.2);
  Update set of local and consensus innovations δ_i, η_{ij}; solve LMI Ω, compute estimator gains K_i, M_i, L_i;
  Output state estimation $\hat{x}_i$, disturbance estimation $\hat{d}_i$
  if $\|\bar{e}\| \leq \varepsilon$ **then**
    Solve LMI Ω_1, compute ϵ;
    Generate the attack detection threshold β in (3.23);
    Design new bank of estimators (3.25) for sensor network (3.2), initialise estimation values $\chi(0), d^n(0)$ as in (3.24);
    Update set of local and consensus innovations δ_i^n, η_{ij}^n; solve LMI Ω_2, compute new set of estimator gains K_i^n, M_i^n, J_i, output state estimation $\hat{\chi}_i$
  else Continue with estimator (3.6)
  end if
end for

3.6 Numerical Examples

Now, a simulation example is presented to demonstrate the effectiveness of the proposed method. A sensor network consisting of four sensor subsystems is constructed

where the target state evolves according to (3.1) and the sensing mechanism is given in (3.2).

In the following simulations, the system parameters are given as $A = \begin{bmatrix} -0.98 & 0.40 \\ 0.15 & -0.75 \end{bmatrix}$, $B = \begin{bmatrix} 0.16 & 0.18 \end{bmatrix}^{\mathrm{T}}$, $C_1 = \begin{bmatrix} 0.82 & 0.62 \end{bmatrix}$, $C_2 = \begin{bmatrix} 0.75 & 0.60 \end{bmatrix}$, $C_3 = \begin{bmatrix} 0.74 & 0.75 \end{bmatrix}$, $C_4 = \begin{bmatrix} 0.75 & 0.65 \end{bmatrix}$, $D_1 = 0.18$, $D_2 = 0.12$, $D_3 = 0.16$, $D_4 = 0.14$, $D_{11} = \begin{bmatrix} 0.22 & 0.24 \end{bmatrix}$, $D_{12} = \begin{bmatrix} 0.20 & 0.20 \end{bmatrix}$, $D_{13} = \begin{bmatrix} 0.10 & 0.10 \end{bmatrix}$, $D_{14} = \begin{bmatrix} 0.16 & 0.16 \end{bmatrix}$, $D_{21} = 0.24$, $D_{22} = 0.20$, $D_{23} = 0.10$, $D_{24} = 0.10$, $\beta_1 = \beta_2 = 1$, $G_i = H_i = 1$ $(i = 1, ..., 4)$, and the nonlinear items are defined as $g(x,t) = \sin(10\pi t)x(t)$, $h(x,t) = 0.5\sin(10\pi t)x(t)$, which satsify Assumption 3.2.2 with $U_1 = I_2$ and $U_2 = 0.5I_2$. In the following results, the first and second states of the system are denoted as $x^{(1)}$ and $x^{(2)}$ respectively. The Laplacian matrix representing the topology of the connected sensor network is given below, where it can be verified that the detectability conditions in Assumptions 3.3.1 and 3.5.1 are satisfied for this set of parameters:

$$\mathcal{L} = \begin{bmatrix} 2 & -1 & 0 & -1 \\ -1 & 2 & 0 & -1 \\ -1 & -1 & 3 & -1 \\ -1 & 0 & -1 & 2 \end{bmatrix}.$$

In this simulation, the exogenous disturbances are constructed in the form of (3.5), and defined as $S_1 = S_2 = S_4 = \begin{bmatrix} 0 & -0.1 \\ 0.1 & 0 \end{bmatrix}$, $S_3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, representing harmonic disturbances with different frequencies. The initial value of the state is given as $x_0 = 5$ and the initial values of the disturbances are given as $\begin{bmatrix} 4 & 4 \end{bmatrix}^{\mathrm{T}}$.

First, the performance of the anti-disturbance estimator is assessed. The LMI Ω is solved by the LMI toolbox in Matlab, where the reference output is defined as in (3.13) with $M_\infty = \begin{bmatrix} 1 & 1 \end{bmatrix}$ and $\gamma = 0.3$. Comparing the estimation performance of a generic distributed H_∞ filter (Figure 3.2) without disturbance rejection with the proposed anti-disturbance estimator (3.6) (Figure 3.3), it is clear that the measurement of the generic filter is severely affected by the disturbance, whereas the proposed estimator (3.6) effectively rejects the effects of disturbance through disturbance estimation and compensation.

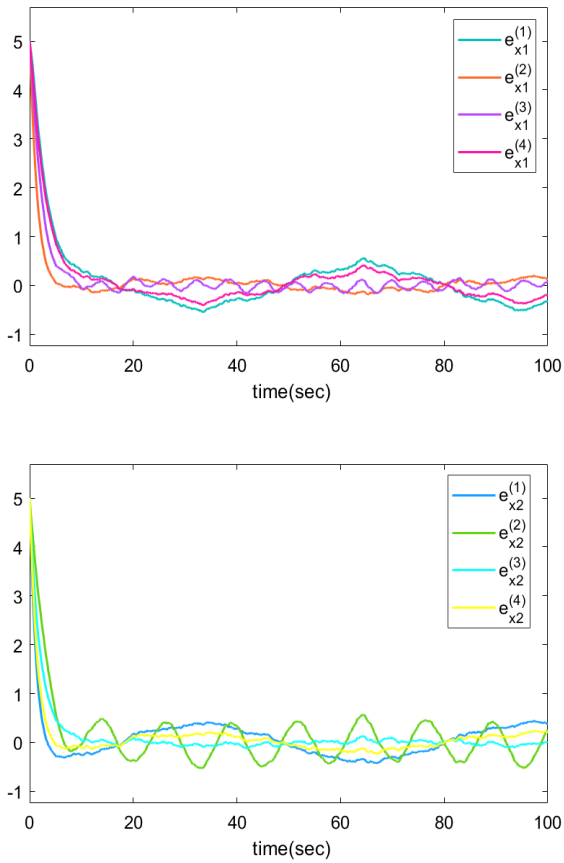

Figure 3.2: State estimation error e_x of an H_∞ estimator under disturbances.

In the case of Figure 3.3, defining $\varepsilon = 0.05$, it can be obtained that $t_n = 18s$. According to the proposed multi-stage approach, the system carries on to the attack-resilient estimator in (3.25) and an attack detection criterion is simultaneously computed by solving the LMI constraint Ω_1 to obtain the optimal detection threshold. The infimum of ϵ for the feasibility of Ω_1 is solved as $\epsilon = 0.5681$, the corresponding optimal threshold is obtained as $\beta = 0.748$ and an attack detection logic is developed based on this threshold.

The FDI attack signals on the sensors are set as constant biasing signals. A signal of the amplitude of 5 is applied on sensor subsystems 2, 3 and 4 at $t = 25s$, and a signal of the amplitude of 10 is applied on the 1st sensor subsystem at $t = 50s$. As displayed in Figure 3.4, the FDI attacks are confirmed to have taken the local innovation δ_i above the threshold and activated the attack estimation. In the event of attacks, the constraint Ω_2 is solved to obtain the corresponding estimator gains across the network. Again, a generic distributed H_∞ filter (Figure 3.5) is compared with the

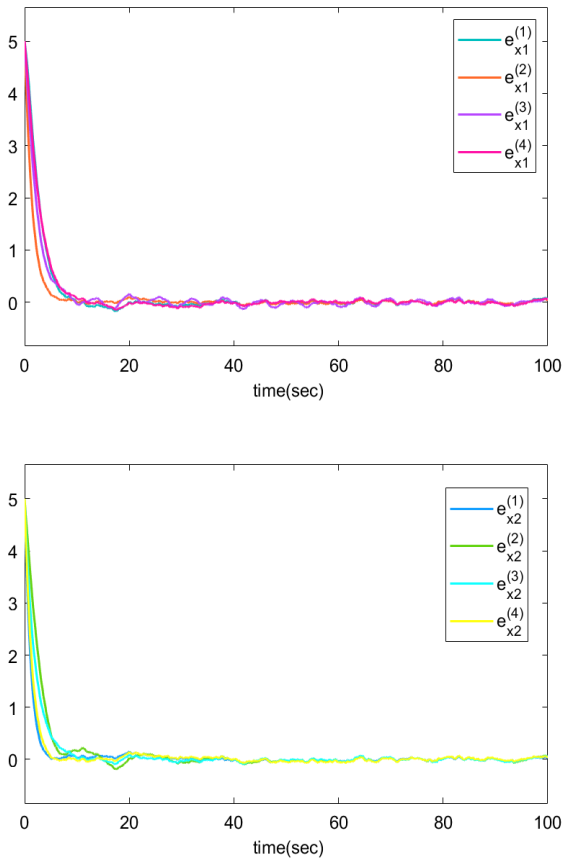

Figure 3.3: State estimation error e_x of the anti-disturbance estimator (3.6) under disturbances.

attack-resilient estimator (3.25) (Figure 3.6). From Figure 3.5, it is shown that not only the attacked sensor subsystems, but all sensor measurements in the network have been heavily biased by the FDI attacks. Comparing Figure 3.5 and Figure 3.6, it can be seen that the proposed attack-resilient estimator can successfully detect and track the value of the attack and simultaneously reject the attack via compensation in the estimator structure, enabling the sensor measurements to actively recover from the attack via online attack compensation.

It should be noted that the model of attack in this simulation study is similar to the biasing attack in References [1] and [93]. However, different from the approach taken in References [1] and [93], our proposed approach considers and effectively deals with the coupling of multiple disturbances and attacks.

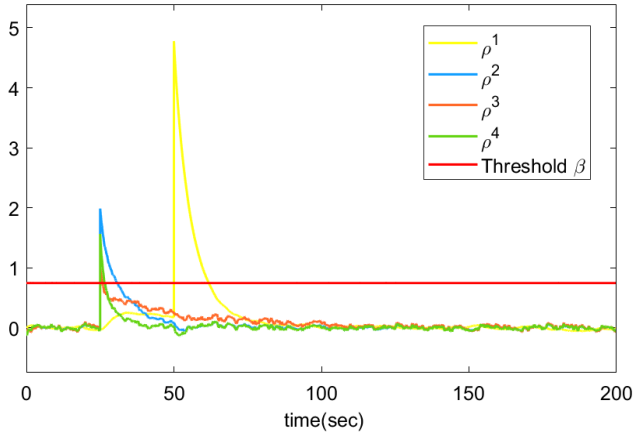

Figure 3.4: Response of residue ρ and threshold β.

For the purpose of further highlighting the the advantages of the proposed estimation methods, comparisons with existing methods are carried out in the following. We suppose that the sensor network is subject to the same multiple sources of disturbances and FDI attacks as described above. Figure 3.7 displays the comparison between the multi-stage estimation approach proposed in this chapter and the method presented in Reference [1]. From Figure 3.7, we can see that the estimation strategy proposed by Reference [1] can not estimates the states accurately due to the presence of multiple disturbances, while the method proposed in this chapter can achieve better performance due to the introduction of a robust anti-disturbance estimation scheme in addition to the attack-resilient estimator.

3.7 Conclusions

In this chapter, an enhanced resilient distributed estimation approach has been proposed for sensor networks subject to multiple disturbances and FDI attacks. The proposed approach consists of three stages. In the initial stages of estimation, an anti-disturbance estimator with a multi-layer architecture is introduced to simultaneously compensate and attenuate the effects of multiple disturbances in the sensor measurements. Then, an observer-based attack detection scheme is introduced, where local residue signals are compared to an optimal threshold to determine whether an

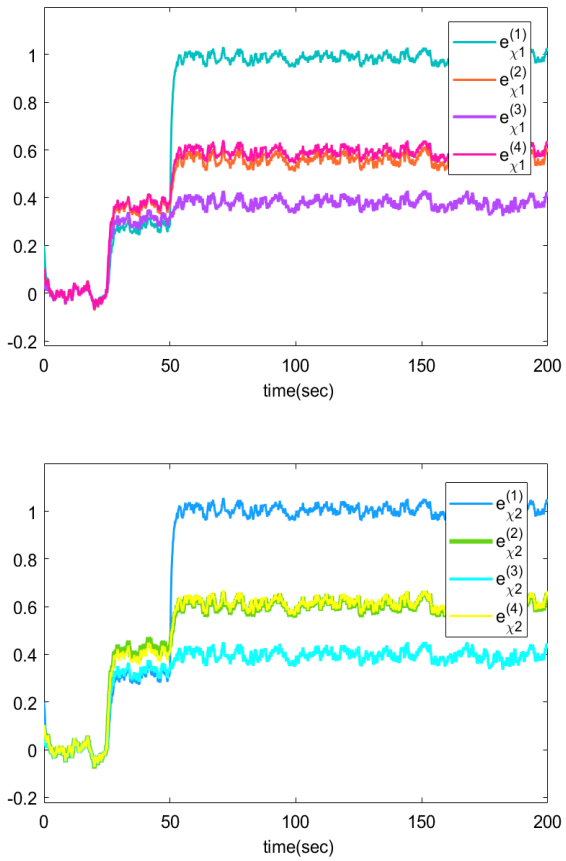

Figure 3.5: State estimation error e_χ of an H_∞ estimator under FDI attacks.

FDI attack is present. Finally, an attack-resilient estimator with a dynamic detection-triggered structure is introduced to develop resilience towards FDI attacks.

The proposed enhanced three-stage approach effectively deals with the coupling between FDI attacks and multiple disturbances. Compared with existing resilient estimation results, which only consider a single source of disturbance, our approach is shown to be able to actively reject FDI attacks in the presence of multiple disturbances. Another feature of the proposed scheme is that it can deal with arbitrary number of heterogeneous disturbances and attacks across the sensor network. Furthermore, a novel detection-trigger architecture reduces the computational load of the attack-resilient estimator.

On the other hand, in addition to false data injection attacks, denial-of-service (DoS) attacks is another typical type of cyber attacks that is likely to simultaneously exist on distributed systems once the cyber defence is compromised. DoS attack

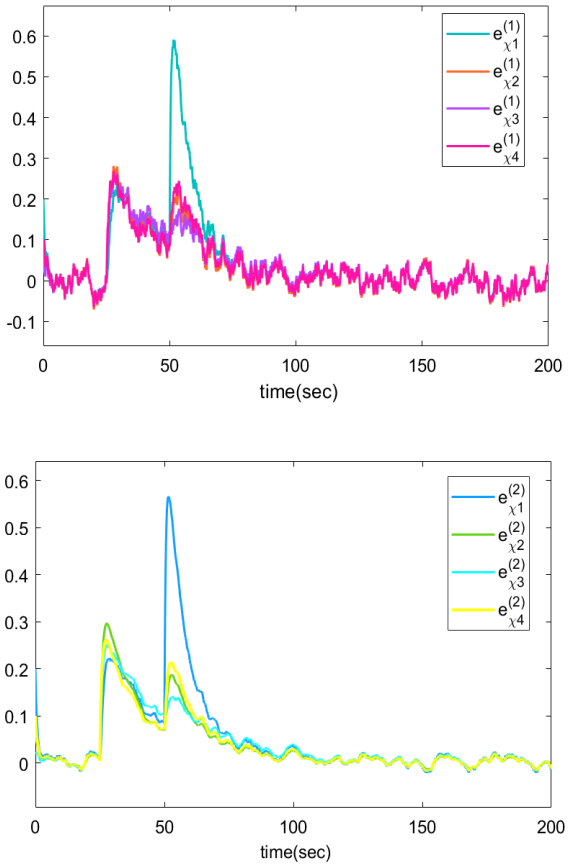

Figure 3.6: State estimation error e_χ of the attack-resilient estimator (3.25) under FDI attacks.

signals are completely heterogeneous to the attack and disturbance signals considered in this chapter. This motivates us to consider resilient distributed estimation towards heterogeneous attacks. In the next chapter, an event-based communication scheme will be designed to mitigate the effect of DoS attacks.

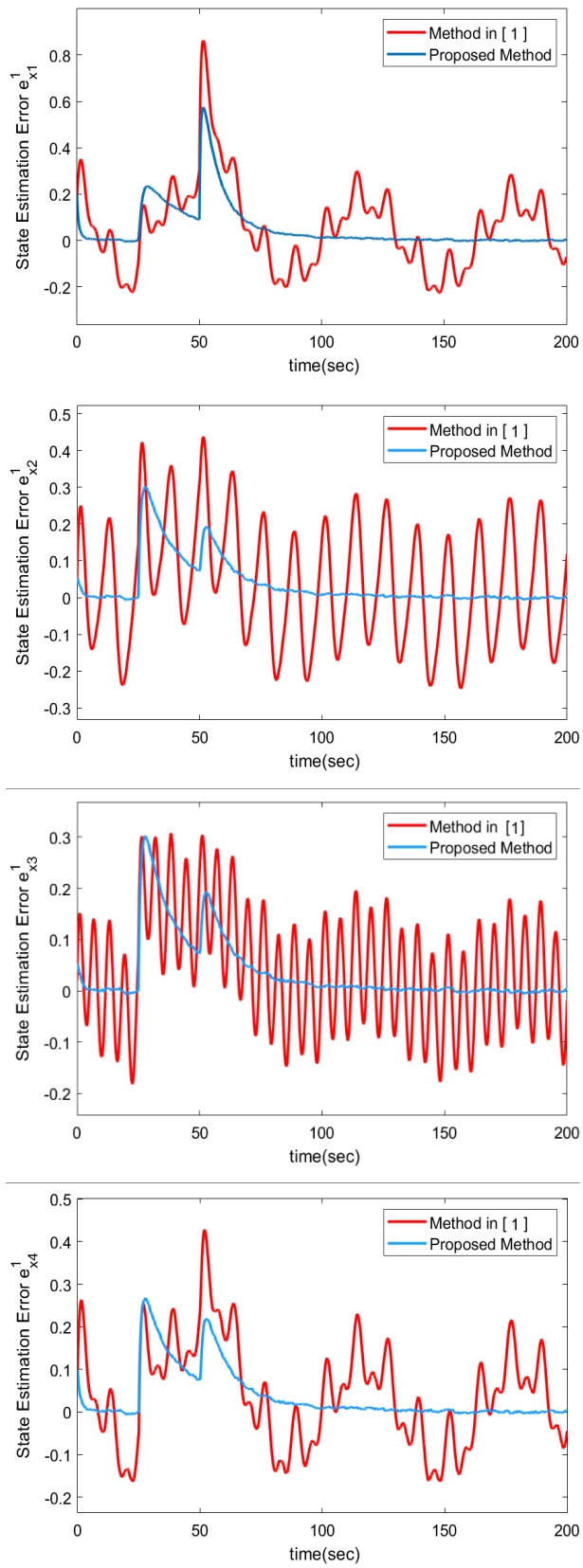

Figure 3.7: Comparison between proposed resilient estimation scheme and the method in Reference [1].

Chapter 4

Event-Based Resilient Distributed Estimation Under Multiple Heterogeneous Cyber-Attacks

4.1 Introduction

Typical cyber-attacks on networked systems include denial-of-service (DoS) attacks [102], which block the communication channels in the network to prevent data transmission, and deception attacks [103, 104], which corrupt the integrity of the system to alter the state or maliciously tamper measurement data. For systems under a single type of attacks, many effective estimation approaches have been proposed. However, despite the research progress, it has been noted that in most existing work, only a single type of attacks was considered. However, in practice, networked CPSs are prone to multiple heterogeneous types of attacks and disturbances, as once the cyber-layer defense is compromised, the attacker is likely to simultaneously launch DoS and deception attacks to maliciously modify system's states and block signal transmission. The presence of multiple heterogeneous cyber-attacks poses additional difficulties for the distributed state estimation problem, since attacks of different nature cannot be

dealt with a uniform approach. Recently, some research [29, 105, 106] investigated distributed state estimation for systems under both DoS and deception attacks. However, some notable gaps still exist in the research on this topic. Firstly, the works mentioned above assume that the presence of DoS attacks follows a probability distribution, which is often a strict assumption in practical applications. Secondly, the existing works are based on the assumption of continuous data transmission in the network, leading to significantly higher consumption of network resources compared with the event-based approach. Thirdly, in the aforementioned work, reconstruction and compensation of deception attacks is not considered, which limits their attack-rejection capabilities.

In the mean time, multiple sources of disturbances may also seriously influence the performance of CPSs. In the simultaneous presence of both attacks and disturbances, disturbances could be mixed and become indistinguishable with the attack signals if the disturbances are not rejected properly. Therefore, the disturbance estimation and compensation is a critical problem for the performance of attack-resilient state estimation. All of the aforementioned estimation approaches deal with disturbances via either disturbance attenuation under an H_2/H_∞ framework or filtering under a stochastic framework, instead of active disturbance estimation and compensation.

Moreover, though event-based transmission schemes have been proposed to reduce network transmission burden whilst maintaining a desired level of estimation performance [35, 36, 37], the balance between the event-based mechanisms and the estimation performance requires significant reconsideration when a number of data transmissions are blocked by DoS attacks. There is a demand for novel event-based communication schemes to cope with the adverse effects of DoS attacks on the network transmission.

To address the above challenges, this chapter presents an event-based distributed state estimation method for systems under multiple heterogeneous cyber-attacks and disturbances, where the attacker simultaneously launches DoS attacks on the measurement transmission channels and deception attacks on the agents, as shown in Figure 4.1. The main contributions of this chapter include the following.

1) Considering that practical CPSs are prone to multiple heterogeneous types of

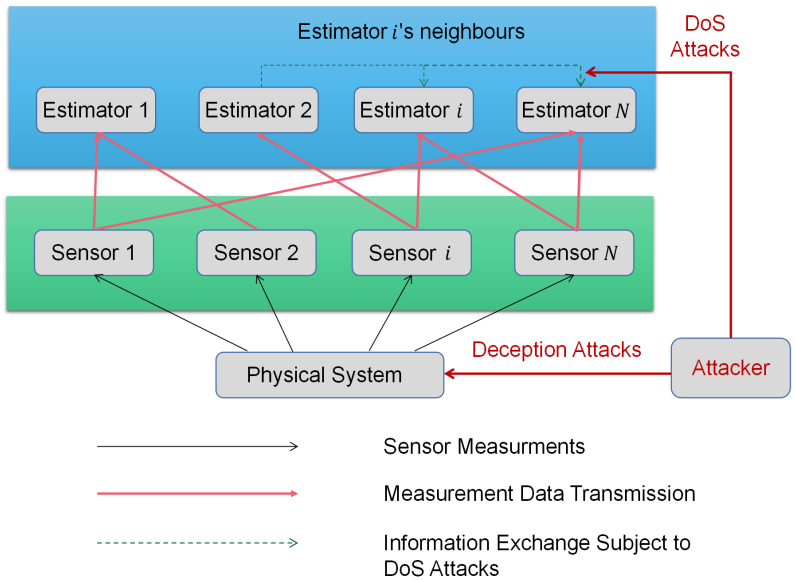

Figure 4.1: Schematic of the distributed state estimation of a networked system under DoS and deception attacks.

cyber-attacks, non-periodic DoS attacks and time-varying deception attacks are considered simultaneously. A novel event-based distributed state estimation approach is proposed to provide resilience towards the joint influence of DoS and deception attacks under disturbances.

2) A novel distributed event-based network communication scheme is introduced, which reduces the data transmission burden with consideration towards the adverse effect of DoS attacks. Meanwhile, Zeno behaviour is successfully precluded. An adaptive term is designed for reconstruction and compensation of unknown time-varying deception attacks, and a distributed disturbance observer is introduced for estimation and compensation of disturbances.

4.2 Problem Formulation

A networked system with N sensors is considered. The topology of the interacting sensor network is represented by a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$. The dynamics of the observed system can be described by

$$\dot{x} = Ax + Bd + Ff(t), \tag{4.1}$$

where $x \in \mathbb{R}^{n_x}$ is the state vector, $d \in \mathbb{R}^{n_d}$ represents the disturbance in the system, $f(t) \in \mathbb{R}$ is an unknown deception attack, and $A \in \mathbb{R}^{n_x \times n_x}$, $B \in \mathbb{R}^{n_x \times n_d}$ and $F \in \mathbb{R}^{n_x}$ are known constant matrices.

Define the sequence of DoS attacks as $h_0 < h_1 < h_2 < \cdots \leq +\infty$. The jth ($j = 0, 1, 2, \ldots$) DoS attack interval can be denoted as $\mathcal{H}_j = [h_j, h_j + \eta_j)$, where h_j represents the beginning instant of the attack, and $\eta_j > 0$ the duration of the attack. It is clear that $h_{j+1} > h_j + \eta_j$. We define $\Phi(t) = \bigcup_{h_j \in [t_0, t]} [h_j, h_j + \eta_j) \cap [t_0, t]$ as the time periods when the network is subject to DoS attacks, and $\Psi(t) = [t_0, t] \setminus \Phi(t)$ as the time periods when the network is free from DoS attacks during $[t_0, t)$. For convenience, it is assumed that the initial time instant $t_0 \in \Psi(t)$.

Assumption 4.2.1. There exist an unknown constant ε and a known non-negative function $\varphi(t)$ such that $|f(t)| \leq \varepsilon\varphi(t)$.

Remark 4.2.1. The above definition puts a time-varying deception cyber-attack into consideration, which maliciously alters the state of the system, similar to the definitions given in [94]. Together with the DoS attacks, attackers can design heterogeneous attacks that simultaneously block network communication and alter system states. From the defender's perspective, it is fair to assume that the attack has an energy constraint. Similar assumptions on the deception attacks are given in existing literature [1, 29, 94, 103, 104]. In practical scenarios, the defender can obtain some information of the attack signal by monitoring the target for a period of time. In this chapter, the presence of deception attacks, DoS attacks and disturbances will be considered and dealt with simultaneously.

The measurement model of the ith sensor is given as

$$y_i = C_i x + D_i d, \qquad \forall i \in \mathcal{V}, \tag{4.2}$$

where $y_i \in \mathbb{R}^{m_i}$ is the measurement from the ith sensor, and $C_i \in \mathbb{R}^{m_i \times n_x}$ and $D_i \in \mathbb{R}^{m_i \times n_d}$ are known constant matrices. A total of N sensors exist in the network following the topology defined by the graph $\mathcal{G}$. In this chapter, we consider a class of disturbances d in the following form:

$$\dot{d} = Sd + \gamma, \tag{4.3}$$

where $S \in \mathbb{R}^{n_d \times n_d}$ is a known matrix, and $\gamma \in \mathbb{R}^{n_d}$ is unknown and satisfies $\|\gamma\|^2 \leq \gamma_m$ with $\gamma_m \geq 0$ an unknown constant. We assume that x and d are bounded.

Remark 4.2.2. In this chapter, the disturbances under consideration are formulated by an exogeneous system (4.3). The parameter matrix S can be determined by parameter identification methods or even direct measurement. The potential limit for this assumption is that the modelled representation of disturbances will not always be accurate. For this purpose, the uncertainties in the disturbance dynamics are accounted for by the additional norm-bounded term γ to provide a more general description of the disturbance, making it more general than the disturbance model considered in (3.5).

4.3 Event-Based Communication Scheme

Event-based communication schemes have been demonstrated to be effective for improving the utilization of communication resources for networked systems by reducing the number of transmissions. In this section, a dynamic event-based communication scheme is proposed to reduce network resource consumption and provide the estimator with resilience towards non-periodic DoS attacks. With the proposed communication scheme, each estimator will generate its own event update sequence, and Zeno behaviour is strictly precluded for all estimators by deriving a positive minimum triggering interval.

First, we define the sequence of event time for estimator i ($i \in \mathcal{V}$) as $t_{i,0} < t_{i,1} < t_{i,2} < \cdots \leq +\infty$, where $t_{i,0} := t_0$. The event-based communication scheme dictates that the estimators shall only share their information to the neighboring estimators at these event instants. To generate a condition for event-based update, we define

$$s_i(t) = \hat{x}_i(t) + B\hat{d}_i(t), \quad i \in \mathcal{V}, \tag{4.4}$$

where $\hat{x}_i$ and $\hat{d}_i$ are the estimations of the state x and the disturbance d generated by the ith estimator to be designed in the next section. Moreover, define

$$\bar{s}_i(t) = \hat{x}_i(t_{i,k}) + B\hat{d}_i(t_{i,k}), \quad \forall t \in [t_{i,k}, t_{i,k+1}), \tag{4.5}$$

where $k = 0, 1, 2, \ldots$. Define the signal

$$\mu_i(t) = s_i(t) - \bar{s}_i(t), \quad \forall t \in [t_{i,k}, t_{i,k+1}). \tag{4.6}$$

It is clear that the presence of the DoS attacks will block updates of network transmission, and therefore the network should seek a stable rate of update when DoS attacks are detected. Here, a novel event-based communication scheme is proposed to determine the communication instants with consideration towards DoS attacks, given by

$$t_{i,k+1} = \begin{cases} \inf\{t > t_{i,k} \mid \|\mu_i(t)\|^2 \geq \varpi_i(t)\}, & \text{if} \quad t_{i,k} \in \Psi(t), \\ t_{i,k} + \sigma, & \text{if} \quad t_{i,k} \in \Phi(t), \end{cases} \tag{4.7}$$

where $\sigma > 0$ is a predefined constant, and $\varpi_i(t)$ is a dynamic threshold given by

$$\dot{\varpi}_i(t) = -\rho_i \varpi_i(t) - q_i \|\mu_i(t)\|^2 + \varsigma_i, \tag{4.8}$$

with $\rho_i > 0$, $q_i > 0$, $\varsigma_i > 0$ and $\varpi_i(t_0) > \frac{\varsigma_i}{\rho_i}$. This communication scheme follows a distributed event-triggered condition when the network is reliable, and switches to a fixed update interval when DoS attacks are detected in the network.

Define the latest triggering time instant of the ith estimator during the time interval $[t_0, t]$ as $g_i(t) = \max\{t_{i,k} | t_{i,k} \leq t\}$. Then, noting $t_0 \in \Psi(t)$, we iteratively define

$$t_{2j+1} = \min\{t_{i,k} > t_{2j} | g_i(t) \in \Phi(t) \text{ for at least one } i \in \mathcal{V}\}, \tag{4.9}$$

$$t_{2j+2} = \min\{t > t_{2j+1} | g_i(t) \in \Psi(t) \text{ for all } i \in \mathcal{V}\}, \tag{4.10}$$

where $j = 0, 1, 2, \ldots$. Here, t_{2j+1} denotes the earliest triggering instant after t_{2j} when at least one estimator is under DoS attack, and t_{2j+2} denotes the earliest triggering instant after t_{2j+1} when all estimators in the network are free from DoS attacks. The definitions above allow us to quantify the effect of DoS attacks with the event-based updates and facilitate the estimator design.

In consideration of the DoS attacks, we further define $\zeta_i(j)$ as the number of communication failures on the ith estimator caused by the jth attack, and let

$$\zeta(j) = \max\{\zeta_1(j), \ldots, \zeta_N(j)\}. \tag{4.11}$$

We can further define the frequency of blocked communications from DoS attacks as

$$\ell(j) = \frac{\zeta(j)}{t_{2j+3} - t_{2j+1}}. \tag{4.12}$$

Remark 4.3.1. A dynamic event-triggering condition is introduced in (4.7). Advantages of this event-triggered scheme include: 1) Each estimator has its own triggering sequence, which offers additional flexibility compared to the centralised triggering condition in literature such as [107], where the network shares a triggering sequence; 2) The value of the event-triggering threshold is state-dependent. Compared with static parameter-based conditions, it is easier to acquire an appropriate set of parameters; 3) Zeno behaviour can be strictly precluded by obtaining a positive inter-event interval.

Remark 4.3.2. The definition of DoS attack frequency in (4.12) provides an alternative to the definition based on probabilistic assumption in work such as [29, 105, 106] to accommodate non-periodic DoS attacks. This definition is more practical since attackers will likely launch their attacks without following any specific probability distributions or determined periodic features. The energy constraint of DoS attacks is described by the frequency $\ell(j)$. The design parameter σ determines the fixed interval in which the network updates when DoS attacks occur. The value of this interval allows us to quantify the effects of DoS attacks to the event-based update and facilitates the stability analysis. In practice, σ should be carefully selected by the user as a relatively small number.

4.4 Estimator Design

In this section, a distributed resilient estimator structure and a novel compensation term for deception attacks are introduced. With the communication instants defined in (4.7), we introduce the signal $s_i^*(t) \in \mathbb{R}^{n_x}$ for the ith estimator as follows:

$$s_i^*(t) = s_i^*(t_{i,k}),\ \forall t \in [t_{i,k}, t_{i,k+1}),$$

$$s_i^*(t_{i,k}) = \begin{cases} s_i(t_{i,k}),\ \text{if } t_{i,k} \in \Psi(t), \\ s_i(t_{i,k-1}),\ \text{if } t_{i,k} \in \Phi(t). \end{cases} \tag{4.13}$$

And define the distributed innovations as

$$\xi_i(t) = \sum_{j=1}^{N} a_{ij}(s_i(t) - s_j(t)), \tag{4.14}$$

$$\bar{\xi}_i(t) = \sum_{j=1}^{N} a_{ij}(\bar{s}_i(t) - \bar{s}_j(t)), \tag{4.15}$$

$$\xi_i^*(t) = \sum_{j=1}^{N} a_{ij}(s_i^*(t) - s_j^*(t)). \tag{4.16}$$

In addition, we can obtain $e_i(t) = \bar{\xi}_i - \xi_i = \sum_{j=1}^{N} a_{ij}(\mu_i - \mu_j)$. Then, the estimator associated with the ith sensor is designed as

$$\begin{cases} \dot{\hat{x}}_i = A\hat{x}_i + K_i\delta_i + M_i\xi_i^* + B\hat{d}_i + Fv_i(t), \\ \dot{\hat{d}}_i = S\hat{d}_i + G_i\delta_i + J_i\xi_i^*, \qquad\qquad \forall i \in \mathcal{V}, \end{cases} \tag{4.17}$$

where $\hat{x}_i$ and $\hat{d}_i$ are the estimations of the state x and the disturbance d generated by the ith estimator, respectively, v_i are the compensation terms for the deception attacks to be designed, $K_i \in \mathbb{R}^{n_x \times m_i}, M_i \in \mathbb{R}^{n_x \times n_x}, G_i \in \mathbb{R}^{n_d \times m_i}$ and $J_i \in \mathbb{R}^{n_d \times n_x}$ are estimator gains to be determined, and $\delta_i \in \mathbb{R}^{m_i}$ represents the local innovation, given by

$$\delta_i = y_i - C_i\hat{x}_i - D_i\hat{d}_i. \tag{4.18}$$

Denote the state and disturbance estimation errors as $\tilde{x}_i = x - \hat{x}_i$ and $\tilde{d}_i = d - \hat{d}_i$, respectively. In order to simplify notations and facilitate further discussions, we denote $\bar{A} = \mathrm{diag}_N\{A\}$, $\bar{B} = \mathrm{diag}_N\{B\}$, $\bar{F} = \mathrm{diag}_N\{F\}$, $C = \mathrm{diag}_N^i\{C_i\}$, $D = \mathrm{diag}_N^i\{D_i\}$, $\bar{S} = \mathrm{diag}_N\{S\}$, $K = \mathrm{diag}_N^i\{K_i\}$, $M = \mathrm{diag}_N^i\{M_i\}$, $G = \mathrm{diag}_N^i\{G_i\}$, $J = \mathrm{diag}_N^i\{J_i\}$, $\tilde{x} = \mathrm{col}_N^i\{\tilde{x}_i\}$, $\tilde{d} = \mathrm{col}_N^i\{\tilde{d}_i\}$, $e = \mathrm{col}_N^i\{e_i\}$, $\bar{\gamma} = \mathrm{col}_N\{\gamma\}$, $v = \mathrm{col}_N^i\{v_i\}$, $\bar{f} = \mathrm{col}_N\{f\}$, $\xi = \mathrm{col}_N^i\{\xi_i\}$, $\bar{\xi} = \mathrm{col}_N^i\{\bar{\xi}_i\}$, $\xi^* = \mathrm{col}_N^i\{\xi_i^*\}$, $\bar{I}_d = \mathrm{diag}_N\{I_d\}$, $\mathcal{L}_x = \mathcal{L} \otimes I_x$, $\mathcal{L}_d = \mathcal{L} \otimes B$, and $\tilde{\mathcal{L}} = [\mathcal{L}_x \ \mathcal{L}_d]$.

Define an extended estimation error across the sensor network as $\tilde{\chi} = [\tilde{x}^{\mathrm{T}}, \tilde{d}^{\mathrm{T}}]^{\mathrm{T}}$. It is clear that $\xi = \tilde{\mathcal{L}}\tilde{\chi}$. Then, we have

$$\dot{\tilde{\chi}} = (\tilde{\mathcal{A}} - \tilde{\mathcal{K}}\tilde{\mathcal{C}} - \tilde{\mathcal{M}}\tilde{\mathcal{L}})\tilde{\chi} + \tilde{\mathcal{F}}(\bar{f} - v) + \tilde{\mathcal{I}}\bar{\gamma} - \tilde{\mathcal{M}}(\xi^*(t) - \xi(t)),$$

where

$$\tilde{\mathcal{A}} = \begin{bmatrix} \bar{A} & \bar{B} \\ 0 & \bar{S} \end{bmatrix}, \tilde{\mathcal{K}} = \begin{bmatrix} K \\ G \end{bmatrix}, \tilde{\mathcal{M}} = \begin{bmatrix} M \\ J \end{bmatrix}, \tilde{\mathcal{F}} = \begin{bmatrix} \bar{F} \\ 0 \end{bmatrix},$$
$$\tilde{\mathcal{C}} = \begin{bmatrix} C & D \end{bmatrix}, \tilde{\mathcal{I}} = \begin{bmatrix} 0 \\ \bar{I}_d \end{bmatrix}. \tag{4.19}$$

It can be checked that when the network communication is reliable (in the absence of DoS attacks), $\xi^*(t) = \bar{\xi}(t)$, and the system error dynamics can be rewritten as

$$\dot{\tilde{\chi}} = (\tilde{\mathcal{A}} - \tilde{\mathcal{K}}\tilde{\mathcal{C}} - \tilde{\mathcal{M}}\tilde{\mathcal{L}})\tilde{\chi} + \tilde{\mathcal{F}}(\bar{f} - v) + \tilde{\mathcal{I}}\bar{\gamma} - \tilde{\mathcal{M}}e. \tag{4.20}$$

For the deception attacks with unknown upper bound, the following adaptive compensation term $v_i(t)$ is designed:

$$v_i(t) = -\frac{\hat{\varepsilon}_i^2\varphi^2(t)}{\sqrt{|W_i\delta_i|^2\hat{\varepsilon}_i^2\varphi^2(t) + \epsilon_i}}W_i\delta_i, \tag{4.21}$$

where ϵ_i are design parameters, and $\hat{\varepsilon}_i$ are the estimations of the upper bound ε updated according to

$$\dot{\hat{\varepsilon}}_i(t) = -\bar{a}_1\hat{\varepsilon}_i(t) + 2\bar{a}_2\varphi(t)|W_i\delta_i|, \tag{4.22}$$

with $W_i \in \mathbb{R}^{1\times m_i}$ gain matrices and $\bar{a}_1 > 0$ and $\bar{a}_2 > 0$ design parameters. Define $\tilde{\varepsilon}_i = \varepsilon - \hat{\varepsilon}_i$ and $W = \mathrm{diag}_N^i\{W_i\}$. The following assumption is made.

Assumption 4.4.1. The matrix pair $(\tilde{\mathcal{A}}, [\tilde{\mathcal{C}}^{\mathrm{T}}, \tilde{\mathcal{L}}^{\mathrm{T}}]^{\mathrm{T}})$ is detectable.

4.5 Performance Analysis

Now, we are ready to establish our main theorem of this chapter.

Theorem 4.5.1. Under Assumptions 4.3.1 and 4.4.1, consider the distributed estimation of the network system with error dynamics in (4.19), the adaptive compensation terms in (4.21) and the adaptive laws in (4.22). Suppose that there exist matrices $P_1 > 0, P_2 > 0$, Q and R, positive constants Θ, θ_1, θ_2 and θ_3, and a positive integer j^* such that

$$\mathbb{H}\{P\tilde{\mathcal{A}} - Q\tilde{\mathcal{C}} + R\tilde{\mathcal{L}}\} + \frac{1}{\theta_1}R^{\mathrm{T}}R + \theta_3\tilde{\mathcal{I}}^{\mathrm{T}}\tilde{\mathcal{I}} < -\Theta I, \tag{4.23}$$

$$P_1\bar{F} = C^{\mathrm{T}}W^{\mathrm{T}}, \tag{4.24}$$

$$\rho_i > \theta_1\|\mathcal{L}\|^2 - q_i, \tag{4.25}$$

$$\ell(j) \leq \frac{\varrho_1 - \varrho_0}{(\varrho_1 + \varrho_2)\,\sigma}, \qquad \forall j \geq j^*, \tag{4.26}$$

where $P = \mathrm{diag}\{P_1, P_2\}$, $\varrho_1 = \min\{\frac{\Theta}{\lambda_{\max}(P)}, \bar{a}_1, \sum_{i=1}^{N}(\rho_i + q_i - \theta_1\|\mathcal{L}\|^2)\}$, $\varrho_2 = \max\{\frac{\lambda_{\max}(H_1)}{\lambda_{\min}(P)}, \theta_1||\mathcal{L}||^2\Lambda, \bar{a}_1, 2\theta_1\}$ with $\Lambda = \max\{\frac{4}{\lambda_{\min}(P)}, \frac{4||B||^2}{\lambda_{\min}(P)}\}$, $0 < \varrho_0 < \varrho_1$, and

$$H_1 = \mathbb{H}\{P\tilde{\mathcal{A}} - Q\tilde{\mathcal{C}} + R\tilde{\mathcal{L}}\} + \frac{1}{\theta_1}R^{\mathrm{T}}R + \frac{1}{\theta_2}R^{\mathrm{T}}R + \theta_2\tilde{\mathcal{L}}^{\mathrm{T}}\tilde{\mathcal{L}} + \theta_3\tilde{\mathcal{I}}^{\mathrm{T}}\tilde{\mathcal{I}}. \tag{4.27}$$

Then, by defining $\tilde{\mathcal{K}} = P^{-1}Q$ and $\tilde{\mathcal{M}} = P^{-1}R$, the estimator gains can be obtained and the error system (4.19) is stable.

Proof. Define the following Lyapunov candidate:

$$V(t) = \bar{V}(t) + \sum_{i=1}^{N}\varpi_i(t), \tag{4.28}$$

where

$$\bar{V}(t) = \tilde{\chi}^{\mathrm{T}}(t)P\tilde{\chi}(t) + \sum_{i=1}^{N}\frac{1}{2\bar{a}_2}\tilde{\varepsilon}_i^2. \tag{4.29}$$

In view of the definitions in (4.9) and (4.10), two cases are considered when calculating $\dot{V}(t)$.

Case 1: $t \in [t_{2j}, t_{2j+1})$. In this case, $\xi^*(t) = \bar{\xi}(t)$ and (4.20) holds. In view of (4.20), noting $\tilde{\mathcal{K}} = P^{-1}Q$, $\tilde{\mathcal{M}} = P^{-1}R$, and

$$\frac{\mathrm{d}}{\mathrm{d}t}(\frac{1}{2\bar{a}_2}\tilde{\varepsilon}_i^2) = \frac{\bar{a}_1}{\bar{a}_2}\tilde{\varepsilon}_i\hat{\varepsilon}_i - 2|W_i\delta_i|\tilde{\varepsilon}_i\varphi(t), \tag{4.30}$$

we can obtain

$$\begin{aligned}\dot{\bar{V}}(t) =& \tilde{\chi}^{\mathrm{T}}(t)\mathbb{H}\{P\tilde{\mathcal{A}} - Q\tilde{\mathcal{C}} + R\tilde{\mathcal{L}}\}\tilde{\chi}(t) + 2\tilde{\chi}^{\mathrm{T}}(t)P\tilde{\mathcal{F}}(\bar{f} - v)\\ &+ 2\tilde{\chi}^{\mathrm{T}}(t)\tilde{\mathcal{I}}\bar{\gamma} - 2\tilde{\chi}^{\mathrm{T}}(t)Re(t) + \sum_{i=1}^{N}\frac{\bar{a}_1}{\bar{a}_2}\tilde{\varepsilon}_i\hat{\varepsilon}_i - 2\sum_{i=1}^{N}|W_i\delta_i|\tilde{\varepsilon}_i\varphi(t).\end{aligned} \tag{4.31}$$

Using Young's inequality, it can be readily checked that

$$\begin{aligned}-2\tilde{\chi}^{\mathrm{T}}(t)Re(t) \leq& \frac{1}{\theta_1}\tilde{\chi}^{\mathrm{T}}(t)R^{\mathrm{T}}R\tilde{\chi}(t) + \theta_1 e^{\mathrm{T}}(t)e(t)\\ \leq& \frac{1}{\theta_1}\tilde{\chi}^{\mathrm{T}}(t)R^{\mathrm{T}}R\tilde{\chi}(t) + \theta_1\|\mathcal{L}\|^2\sum_{i=1}^{N}\|\mu_i(t)\|^2.\end{aligned} \tag{4.32}$$

Taking (4.23), (4.24), (4.31) and (4.32) into consideration, and noting $\|\gamma\|^2 \leq \gamma_m$, the derivative of $\bar{V}(t)$ satisfies

$$
\begin{aligned}
\dot{\bar{V}}(t) \leq & -\Theta\|\tilde{\chi}(t)\|^2 + 2\tilde{\chi}^{\mathrm{T}}(t)P\tilde{\mathcal{F}}(\bar{f}-v) + \frac{1}{\theta_3}\|\bar{\gamma}\|^2 + \sum_{i=1}^{N}\frac{\bar{a}_1}{\bar{a}_2}\tilde{\varepsilon}_i\hat{\varepsilon}_i \\
& - 2\sum_{i=1}^{N}|W_i\delta_i|\tilde{\varepsilon}_i\varphi(t) + \theta_1 e^{\mathrm{T}}(t)e(t) \\
\leq & -\Theta\|\tilde{\chi}(t)\|^2 + 2\sum_{i=1}^{N}|W_i\delta_i|\varepsilon\varphi(t) - 2\sum_{i=1}^{N}|W_i\delta_i|\hat{\varepsilon}_i\varphi(t) + \frac{1}{\theta_3}\|\bar{\gamma}\|^2 + \\
& \sum_{i=1}^{N}\frac{\bar{a}_1}{\bar{a}_2}\tilde{\varepsilon}_i\hat{\varepsilon}_i - 2\sum_{i=1}^{N}|W_i\delta_i|\tilde{\varepsilon}_i\varphi(t) + \theta_1 e^{\mathrm{T}}(t)e(t) + \sum_{i=1}^{N}2\epsilon_i \\
\leq & -\Theta\|\tilde{\chi}(t)\|^2 + \frac{N}{\theta_3}\gamma_m + \theta_1 e^{\mathrm{T}}(t)e(t) - \sum_{i=1}^{N}\frac{\bar{a}_1}{2\bar{a}_2}\tilde{\varepsilon}_i^2(t) + \frac{\bar{a}_1 N}{2\bar{a}_2}\varepsilon^2 + \sum_{i=1}^{N}2\epsilon_i \\
\leq & -\Upsilon_1\bar{V}(t) + \frac{\bar{a}_1 N}{2\bar{a}_2}\varepsilon^2 + \frac{N}{\theta_3}\gamma_m + \theta_1\|\mathcal{L}\|^2\sum_{i=1}^{N}\|\mu_i(t)\|^2 + \sum_{i=1}^{N}2\epsilon_i \\
\leq & -\Upsilon_1\bar{V}(t) + \iota_1 + \theta_1\|\mathcal{L}\|^2\sum_{i=1}^{N}\|\mu_i(t)\|^2,
\end{aligned} \tag{4.33}
$$

where $\Upsilon_1 = \min\{\frac{\Theta}{\lambda_{\max}(P)}, \bar{a}_1\}$, and $\iota_1 = \frac{\bar{a}_1 N}{2\bar{a}_2}\varepsilon^2 + \frac{N}{\theta_3}\gamma_m + \sum_{i=1}^{N}2\epsilon_i$. It follows from (4.8) that

$$
\sum_{i=1}^{N}\dot{\varpi}_i(t) = \sum_{i=1}^{N}(-\rho_i\varpi_i(t) - q_i\|\mu_i(t)\|^2 + \varsigma_i). \tag{4.34}
$$

Combining (4.33) and (4.34), we can obtain

$$
\dot{V}(t) \leq -\Upsilon_1\bar{V}(t) + \sum_{i=1}^{N}(\theta_1\|\mathcal{L}\|^2 - q_i)\|\mu_i\|^2 - \sum_{i=1}^{N}\rho_i\varpi_i(t) + \sum_{i=1}^{N}\varsigma_i + \iota_1. \tag{4.35}
$$

In this case, we know from (4.7) that $\|\mu_i(t)\|^2 \leq \varpi_i(t)$. Thus,

$$
\begin{aligned}
\dot{V}(t) \leq & -\Upsilon_1\bar{V}(t) - \sum_{i=1}^{N}(\rho_i + q_i - \theta_1\|\mathcal{L}\|^2)\varpi_i(t) + \sum_{i=1}^{N}\varsigma_i + \iota_1 \\
\leq & -\varrho_1 V(t) + f_1^*,
\end{aligned} \tag{4.36}
$$

where $f_1^* = \frac{\bar{a}_1 N}{2\bar{a}_2}\varepsilon^2 + \frac{N}{\theta_3}\gamma_m + \sum_{i=1}^{N}\varsigma_i + \sum_{i=1}^{N}2\epsilon_i$.

For all $t \in [t_{2j}, t_{2j+1})$, it follows from (4.36) and Lemma 2.3.2 that

$$
V(t) \leq V(t_{2j})e^{(-\varrho_1(t-t_{2j}))} + \frac{f_1^*}{\varrho_1}(1 - e^{(-\varrho_1(t-t_{2j})}). \tag{4.37}
$$

Case 2: $t \in [t_{2j+1}, t_{2j+2})$. In this case, the system error dynamics satisfies

$$\dot{\tilde{\chi}}(t) =(\tilde{\mathcal{A}} - \tilde{\mathcal{K}}\tilde{\mathcal{C}} - \tilde{\mathcal{M}}\tilde{\mathcal{L}})\tilde{\chi}(t) + \tilde{\mathcal{F}}(\bar{f}(t) - v(t)) - \tilde{\mathcal{M}}(\xi^*(t) - \xi(t)) + \tilde{\mathcal{I}}\bar{\gamma}, \tag{4.38}$$

and the derivative of $\bar{V}(t)$ is given by

$$\begin{aligned}\dot{\bar{V}}(t) =&\tilde{\chi}^{\mathrm{T}}(t)\mathbb{H}\{P\tilde{\mathcal{A}} - Q\tilde{\mathcal{C}} + R\tilde{\mathcal{L}}\}\tilde{\chi}(t) + 2\tilde{\chi}^{\mathrm{T}}(t)\tilde{\mathcal{I}}\bar{\gamma} + 2\tilde{\chi}^{\mathrm{T}}(t)P\tilde{\mathcal{F}}(\bar{f}(t) - v(t))\\ &- 2\tilde{\chi}^{\mathrm{T}}(t)R(\xi^*(t) - \xi(t)) + \sum_{i=1}^{N}\frac{\bar{a}_1}{\bar{a}_2}\tilde{\varepsilon}_i\hat{\varepsilon}_i - 2\sum_{i=1}^{N}|W_i\delta_i|\tilde{\varepsilon}_i\varphi(t).\end{aligned} \tag{4.39}$$

Let $t_{i,s}$ be the latest time instant at which s_i^* successfully updates its value by receiving information of s_i. If $t_{i,s} < t_{2j+1}$, by (4.5), (4.7) and (4.13), we have

$$||s_i(t_{2j+1}) - s_i(t_{i,s})||^2 \leq \varpi_i(t_{2j+1}), \tag{4.40}$$

and

$$||s_i^*(t)||^2 = ||s_i(t_{i,s})||^2 \leq 2||s_i(t_{2j+1})||^2 + 2\varpi_i(t_{2j+1}). \tag{4.41}$$

On the other hand, if $t_{i,s} \geq t_{2j+1}$, then

$$||s_i(t) - s_i(t_{i,s})||^2 \leq \varpi_i(t), \tag{4.42}$$

$$||s_i^*(t)||^2 = ||s_i(t_{i,s})||^2 \leq 2||s_i(t)||^2 + 2\varpi_i(t). \tag{4.43}$$

Combining (4.41) and (4.43) gives

$$||s_i^*(t)||^2 \leq||s_i(t_{2j+1})||^2 + ||s_i(t)||^2 + 2\varpi_i(t_{2j+1}) + 2\varpi_i(t), \quad \forall i \in \mathcal{V}. \tag{4.44}$$

Letting $s(t) = \mathrm{col}_N^i\{s_i(t)\}$, we have

$$\begin{aligned}||s(t)||^2 =&\sum_{i=1}^{N}||\hat{x}_i(t) + B\hat{d}_i(t)||^2\\ \leq&2N\Xi + 2\sum_{i=1}^{N}||\tilde{x}_i(t) + B\tilde{d}_i(t)||^2\\ \leq&2N\Xi + 4\sum_{i=1}^{N}||\tilde{x}_i(t)||^2 + 4\sum_{i=1}^{N}||B||^2||\tilde{d}_i(t)||^2\\ \leq&2N\Xi + \Lambda\bar{V}(t).\end{aligned} \tag{4.45}$$

where $\Xi = \sup_{t\geq t_0} ||x(t) + Bd(t)||^2$. Define $s^*(t) = \mathrm{col}_N^i\{s_i^*(t)\}$ and recalling $\xi^*(t) = \mathrm{col}_N^i\{\xi_i^*(t)\}$, we have $\xi^*(t) = \mathcal{L}s^*(t)$. In view of (4.44) and (4.45), we can obtain

$$\begin{aligned}\xi^{*\mathrm{T}}(t)\xi^*(t) \leq& ||\mathcal{L}||^2||s^*(t)||^2\\ \leq& ||\mathcal{L}||^2(\Lambda\bar{V}(t) + \Lambda\bar{V}(t_{2j+1}) + 4N\Xi) + \sum_{i=1}^{N}(2\varpi_i(t_{2j+1}) + 2\varpi_i(t)). \end{aligned} \tag{4.46}$$

From (4.46) and Young's inequality, it can be checked that

$$\begin{aligned} & -2\tilde{\chi}^{\mathrm{T}}(t)R(\xi^*(t) - \xi(t))\\ \leq\ & \tilde{\chi}^{\mathrm{T}}(t)\left(\frac{1}{\theta_1}R^{\mathrm{T}}R + \frac{1}{\theta_2}R^{\mathrm{T}}R + \theta_2\tilde{\mathcal{L}}^{\mathrm{T}}\tilde{\mathcal{L}}\right)\tilde{\chi}(t) + \theta_1\xi^{*\mathrm{T}}(t)\xi^*(t)\\ \leq\ & \tilde{\chi}^{\mathrm{T}}(t)\left[\frac{1}{\theta_1}R^{\mathrm{T}}R + \frac{1}{\theta_2}R^{\mathrm{T}}R + \theta_2\tilde{\mathcal{L}}^{\mathrm{T}}\tilde{\mathcal{L}}\right]\tilde{\chi}(t) + \theta_1||\mathcal{L}||^2\Lambda\bar{V}(t_{2j+1})\\ & +\theta_1||\mathcal{L}||^2\Lambda\bar{V}(t) + 4\theta_1||\mathcal{L}||^2N\Xi + \theta_1\sum_{i=1}^{N}(2\varpi_i(t_{2j+1}) + 2\varpi_i(t)). \end{aligned} \tag{4.47}$$

Substituting (4.47) into (4.39), we have

$$\begin{aligned}\dot{\bar{V}}(t) \leq\ & \tilde{\chi}^{\mathrm{T}}(t)H_1\tilde{\chi}(t) + \theta_1||\mathcal{L}||^2\Lambda\bar{V}(t_{2j+1}) + \theta_1||\mathcal{L}||^2\Lambda\bar{V}(t) + \frac{N}{\theta_3}\gamma_m\\ & +\theta_1\sum_{i=1}^{N}(2\varpi_i(t_{2j+1}) + 2\varpi_i(t)) + \sum_{i=1}^{N}\frac{\bar{a}_1}{\bar{a}_2}\tilde{\varepsilon}_i\hat{\varepsilon}_i + \sum_{i=1}^{N}2\epsilon_i + 4\theta_1||\mathcal{L}||^2N\Xi\\ \leq\ & \frac{\lambda_{\max}(H_1)}{\lambda_{\min}(P)}\tilde{\chi}^{\mathrm{T}}(t)P\tilde{\chi}(t) + \theta_1||\mathcal{L}||^2\Lambda\bar{V}(t_{2j+1}) + \theta_1||\mathcal{L}||^2\Lambda\bar{V}(t) - \sum_{i=1}^{N}\frac{\bar{a}_1}{2\bar{a}_2}\tilde{\varepsilon}_i^2(t)\\ & +\frac{\bar{a}_1N}{2\bar{a}_2}\varepsilon^2\gamma_m + \theta_1\sum_{i=1}^{N}(2\varpi_i(t_{2j+1}) + 2\varpi_i(t)) + 4\theta_1||\mathcal{L}||^2N\Xi + \sum_{i=1}^{N}2\epsilon_i\\ \leq\ & \Upsilon_2\max(\bar{V}(t), \bar{V}(t_{2j+1})) + \iota_2 + \theta_1\sum_{i=1}^{N}(2\varpi_i(t_{2j+1}) + 2\varpi_i(t)), \end{aligned} \tag{4.48}$$

where $\Upsilon_2 = \max\{\frac{\lambda_{\max}(H_1)}{\lambda_{\min}(P)}, \theta_1||\mathcal{L}||^2\Lambda, \bar{a}_1\}$ and $\iota_2 = \frac{\bar{a}_1N}{2\bar{a}_2}\varepsilon^2 + \frac{N}{\theta_3}\gamma_m + \sum_{i=1}^{N}2\epsilon_i + 4\theta_1||\mathcal{L}||^2N\Xi$. Noting that (4.34) still stands, we can obtain

$$\begin{aligned}\dot{V}(t) \leq& \Upsilon_2\max(\bar{V}(t), \bar{V}(t_{2j+1})) + 2\theta_1\sum_{i=1}^{N}\varpi_i(t_{2j+1}) - 2(\rho_i + q_i - \theta_1)\sum_{i=1}^{N}\varpi_i(t) + \iota_2 + \sum_{i=1}^{N}\varsigma_i\\ \leq& \varrho_2\max(V(t), V(t_{2j+1})) + f_2^*, \end{aligned} \tag{4.49}$$

where $f_2^* = \frac{\bar{a}_1N}{2\bar{a}_2}\varepsilon^2 + \frac{N}{\theta_3}\gamma_m + \sum_{i=1}^{N}\varsigma_i + \sum_{i=1}^{N}2\epsilon_i + 4\theta_1||\mathcal{L}||^2N\Xi$.

It is clear that for all $t \in [t_{2j+1}, t_{2j+2})$, $V(t)$ satisfies

$$V(t) \leq V(t_{2j+1})e^{(\varrho_2(t-t_{2j+1}))} + \frac{f_2^*}{\varrho_2}(e^{(\varrho_2(t-t_{2j+1}))} - 1). \tag{4.50}$$

Combining Case 1 and Case 2, we can conclude that for all $j = 0, 1, 2, \ldots,$

$$\begin{aligned} V(t_{2j+3}) \leq & V(t_{2j+1})e^{(\varrho_2(t_{2j+2}-t_{2j+1})-\varrho_1(t_{2j+3}-t_{2j+2}))} \\ & + \frac{f_2^*}{\varrho_2}e^{(\varrho_2(t_{2j+2}-t_{2j+1})-\varrho_1(t_{2j+3}-t_{2j+2}))-1)} \\ & + \frac{f_1^*}{\varrho_1}(1 - e^{(-\varrho_1(t_{2j+3}-t_{2j+2}))}). \end{aligned} \tag{4.51}$$

Noting the definitions of σ in (4.7), t_{2j+1} and t_{2j+2} in (4.9) and (4.10), and $\zeta(j)$ and $\ell(j)$ in (4.11) and (4.12), we can obtain the relation $t_{2j+2} - t_{2j+1} \leq \sigma\zeta(j) \leq \sigma\ell(j)(t_{2j+3} - t_{2j+1})$. Further noting (4.27), it can be concluded that there exists a finite j^* such that for all $j \geq j^*$,

$$\varrho_2(t_{2j+2} - t_{2j+1}) - \varrho_1(t_{2j+3} - t_{2j+2}) < -\varrho_0(t_{2j+3} - t_{2j+1}), \tag{4.52}$$

where ϱ_0 is a positive constant. As a result, for all $j \geq j^*$, we have

$$\begin{aligned} V(t_{2j+3}) \leq & V(t_{2j+1})e^{(-\varrho_0(t_{2j+3}-t_{2j+1}))} + \frac{f_2^*}{\varrho_2}e^{(-\varrho_0(t_{2j+3}-t_{2j+1})-1)} \\ & + \frac{f_1^*}{\varrho_1}(1 - e^{(-\varrho_1(t_{2j+3}-t_{2j+2}))}). \end{aligned} \tag{4.53}$$

From (4.53), we can further obtain

$$\begin{aligned} V(t_{2j+3}) \leq & V(t_{2j^*+1})e^{(-\varrho_0(t_{2j+3}-t_{2j^*+1}))} + \frac{f_2^*}{\varrho_2}e^{(-\varrho_0(t_{2j+3}-t_{2j^*+1})-1)} \\ & + \frac{f_1^*}{\varrho_1}(1 - e^{(-\varrho_1\sum_{k=j^*}^{j}(t_{2j+3}-t_{2j+2}))}), \end{aligned} \tag{4.54}$$

which implies that $V(t_{2j+1})$ converges towards a constant bound $\frac{f_1^*}{\varrho_1}$ when $j \to \infty$. Further noting that for all $t \in [t_{2j+1}, t_{2j+3}]$, $V(t)$ is bounded by

$$V(t) \leq V(t_{2j+2}) \leq V(t_{2j+1})e^{(\varrho_2\zeta(j)\sigma)} + \frac{f_2^*}{\varrho_2}(e^{(\varrho_2\zeta(j)\sigma)} - 1), \tag{4.55}$$

where $\zeta(j)$ is finite. We can conclude that $V(t)$ converges to a bound as $t \to \infty$, and the error system is stable.

Now, we prove that Zeno behaviour is precluded under the event-based communication scheme. Obviously, for all $t_{i,k} \in \Phi(t)$, noting that $\sigma > 0$, Zeno behaviour is precluded. On the other hand, for all $t \in [t_{i,k}, t_{i,k+1})$ with $t_{i,k} \in \psi(t)$, it follows from

the triggering condition that $\|\mu_i(t)\|^2 \leq \varpi_i(t)$. Calculate the change rate of $\|\mu_i(t)\|^2$:

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}t}\|\mu_i(t)\|^2 =& 2\mu_i^{\mathrm{T}}(t)\dot{s}_i(t) = 2\mu_i^{\mathrm{T}}(t)(\dot{\hat{x}}_i(t) + B\dot{\hat{d}}_i(t)) \\ =& 2\mu_i^{\mathrm{T}}(t)(A\hat{x}_i(t) + (B+BS)\hat{d}_i(t) + (K_i + BG_i)\delta_i(t) \\ &+ (M_i + BJ_i)\xi_i^*(t) + Fv_i(t)) \\ :=& r_i(t), \qquad t \in (t_{i,k}, t_{i,k+1}].\end{aligned} \tag{4.56}$$

Noting the boundedness of $\mu_i(t)$, $\hat{x}_i(t)$, $\hat{d}_i(t)$, $\delta_i(t)$, $\xi_i^*(t)$ and $v_i(t)$, we can conclude that $|r_i(t)|$ is bounded by a constant $\bar{r}_i > 0$, which implies that $\frac{\mathrm{d}}{\mathrm{d}t}\|\mu_i(t)\|^2$ is upper bounded. On the other hand, according to (4.7), we have

$$\|\mu_i(t_{i,k})\|^2 = 0, \qquad \lim_{t \to t_{i,k+1}^-} \|\mu_i(t)\|^2 = \varpi_i(t). \tag{4.57}$$

In view of (4.7) and (4.8), we have

$$\dot{\varpi}_i(t) \geq -(\rho_i + q_i)\varpi_i(t) + \varsigma_i. \tag{4.58}$$

Thus, by induction, we can obtain

$$\begin{aligned}\varpi_i(t) \geq& (\varpi_i(t_{i,k}) - \frac{\varsigma_i}{\rho_i + q_i})e^{[-(\rho_i+q_i)(t-t_{i,k})]} + \frac{\varsigma_i}{\rho_i + q_i} \\ \geq& (\varpi_i(t_{i,k-1}) - \frac{\varsigma_i}{\rho_i + q_i})e^{[-(\rho_i+q_i)(t-t_{i,k-1})]} + \frac{\varsigma_i}{\rho_i + q_i} \\ \geq& \cdots \\ \geq& (\varpi_i(t_0) - \frac{\varsigma_i}{\rho_i + q_i})e^{[-(\rho_i+q_i)(t-t_0)]} + \frac{\varsigma_i}{\rho_i + q_i} \\ >& \frac{\varsigma_i}{\rho_i + q_i}, \qquad t \in (t_{i,k}, t_{i,k+1}],\end{aligned} \tag{4.59}$$

which confirms that the auxiliary variables $\varpi_i(t)$ are positive. By (4.56), (4.57) and (4.59), it can be checked that

$$t_{i,k+1} - t_{i,k} \geq \frac{\varsigma_i}{\bar{r}_i(\rho_i + q_i)}. \tag{4.60}$$

Noting that $(\varsigma_i/\rho_i + q_i)$ is positive, (4.60) confirms that a positive minimum triggering interval exists. As a result, Zeno behaviour is strictly precluded, which completes the proof. ■

Remark 4.5.1. Theorem 4.5.1 shows that estimation error stability can be achieved for an unreliable networked system with event-based updates under both aperiodic DoS

attacks and deception attacks with an unknown upper bound. In this case, an observer applying a technique similar to the adaptive sliding-mode observer is introduced to compensate for deception attacks. The adaptive sliding mode observer is selected in this work because it provides: 1) fast response and good transient performance; 2) an independent structure to the main state observer, which can be separated from the state estimator when necessary and 3) the ability to include an on-line adaptive parameter estimator to estimate the upper bound of deception attacks.

4.6 Simulation Results

In this section, we evaluate the effectiveness of the proposed method with a simulation study. We consider the distributed state estimation problem for an IEEE 4-bus distribution line power grid. The model for a network of interconnected distributed energy generators (DEGs) is taken from [108], as shown in Figure 4.2. Four DEGs are modeled as voltage sources whose input voltages can be denoted by $\{v_{ci}(s)\}_{i=1,\ldots,4}$. The DEGs are connected to the power network at the points of common coupling (PCCs), where the voltages at the PCC are denoted by $\{v_{ti}(s)\}_{i=1,\ldots,4}$. A coupling inductor exists between each DEG and the rest of the network, which is denoted as $\{L_{ci}(s)\}_{i=1,\ldots,4}$. We define $\mathbf{v}_t = [v_{t1}, \ldots, v_{t4}]^{\mathrm{T}}$ and $\mathbf{v}_c = [v_{c1}, \ldots, v_{c4}]^{\mathrm{T}}$. The purpose of voltage control is to keep the voltages at PCCs at a reference value $\mathbf{v}_{\mathrm{ref}}$. It is clear that the system reaches equilibrium $\mathbf{v}_t = \mathbf{v}_{\mathrm{ref}}$ given a proper $\mathbf{v}_c$. Defining the system state as the derivation of the voltages from their reference value $x = \mathbf{v}_f - \mathbf{v}_{\mathrm{ref}}$, the voltage dynamic equation of the power grid can be given in the form of (4.1). Note that in this chapter, we are not concerned with the voltage control of the power grid, but rather the estimation of its states when appropriate control efforts are carried out.

In this case, the system matrices are given as

$$A = \begin{bmatrix} -0.837 & 0.5427 & 0 & 0 \\ -0.5427 & -0.837 & 0 & 0 \\ 0 & 0 & -0.9851 & 0 \\ 0 & 0 & 0 & -0.9556 \end{bmatrix}, B = I_4, D_i = \begin{bmatrix} 0.24 & 0.22 \\ 0.42 & 0.4 \\ 0.16 & 0.16 \\ 0.18 & 0.16 \end{bmatrix}, F = I_4,$$

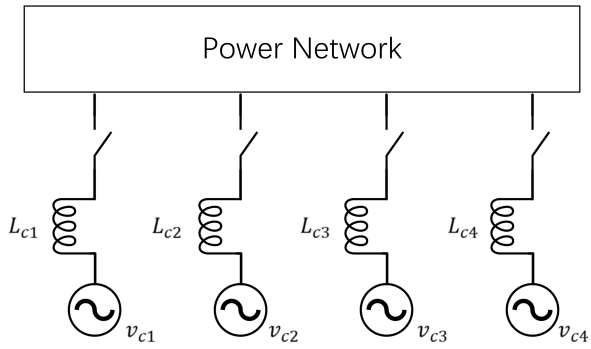

Figure 4.2: Model of DEGs connected to the power network.

and the model of disturbance is given as

$$S = \begin{bmatrix} 1.5 & 0 & -3 & 0 \\ 0 & -1.5 & 0 & 3 \\ 3 & 0 & -1.5 & 0 \\ -3 & 0 & 1.5 & 0 \end{bmatrix},$$

with $i = 1, \ldots, 4$, and $\gamma_m = 0.1$. The disturbance model represents a periodic disturbance with unknown amplitude and additional uncertainties, which commonly exists in practical power grids [109]. The network topology is given by the Laplacian matrix

$$\mathcal{L} = \begin{bmatrix} 2 & -1 & 0 & -1 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ -1 & 0 & -1 & 2 \end{bmatrix}.$$

In this distributed setting, each grid sub-estimator is assumed to have partial measurement of the system states. The 1st sensor measures the 1st and the 2nd coordinates of the state vector, the 2nd sensor measures the 2nd and the 3rd coordinates, the 3nd sensor measures the 3rd and the 4th coordinates, and the 4th sensor takes measurements of the 4th and the 1st coordinates. For instance, the 4th sensor has a measurement matrix of $C_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. This set of system matrices satisfies Assumption 4.4.1, while local detectability of pairs $(A, C_i), i = 1, \ldots, 4$, is not satisfied, meaning that the sub-estimators cannot successfully estimate the state of the system without assistance from their neighbors.

The deception attack is given as $f(t) = 2 + \sin(\pi t + 0.2)$ with upper bound $\varepsilon = 3$, and introduced to the system at $t = 20s$. The non-periodic DoS attack intervals are generated randomly as $\mathcal{H}_j = \{[1.54, 2.49], [4.97, 5.88], [6.69, 7.98], [8.05, 8.25], [8.58, 9.09], [10.48, 10.86], [11.16, 12.97], [14.51, 15.24], [15.38, 15.60], [17.20, 17.74], [19.16, 22.38], [23.69, 23.73], [24.59, 25.47], [25.59, 26.22], [26.65, 29.27]\}$. The parameters of the adaptive law are given as $\bar{a}_1 = 0.03$, $\bar{a}_2 = 0.25$, $\epsilon_i = 0.005$, $W_1 = [3.7\ 1.4]$, $W_2 = [3.09\ 1.56]$, $W_3 = [1.5\ 1.29]$, and $W_4 = [2.78\ 1.42]$. The function $\varphi(t)$ is designed as a hyperbolic function $\varphi(t) = \tanh(0.2t)$. The parameters for event based update are given as $\rho_i = 1.1$, $q_i = 0.2$, and $\varsigma_i = 0.005$, and the initial values are set as $x_i(0) = 5$, $d_i(0) = \begin{bmatrix} 0.3 & 0.3 & 0.3 & 0.3 \end{bmatrix}^{\mathrm{T}}$, where $i = 1, \ldots, 4$.

The system states and their estimates with the proposed algorithm are depicted in Figure 4.3. From these results, it is seen that the designed distributed state estimator can accurately estimate the system states in both cases, even in the presence of DoS and deception attacks. In comparison, simulations under the same conditions in the absence of disturbance rejection and attack compensation are carried out in Figure 4.4 and Figure 4.5, respectively, where the bound of the deception attack is unknown. It can be seen that the proposed algorithm has superior estimation performance and resilience.

To further assess the performance of the proposed algorithm, the adaptive estimation of the upper bound ε of the deception attack from each estimator is displayed in Figure 4.6. It can be seen that $\hat{\varepsilon}_i$ is bounded in each estimator. The mean square error $MSE = \frac{1}{N}\|\tilde{x}\|^2$ of estimation under various scenarios are shown in Figure 4.7. It can be observed that the proposed algorithm has considerably lower estimation error compared with estimators in the absence of disturbance rejection or attack compensation.

4.7 Conclusions

In this chapter, an event-based resilient distributed state estimation method has been proposed for systems under disturbances and multiple heterogeneous cyber-attacks. A

novel event-based communication scheme with resilience towards non-periodic DoS attacks is proposed to reduce unnecessary data transmissions within the network, while guaranteeing desired estimation performance. A novel adaptive deception attack rejection scheme is introduced to deal with deception attacks via compensation. Moreover, a distributed disturbance observer is proposed to compensate for disturbances in the system in a distributed manner. By means of the Lyapunov function approach, sufficient conditions for convergence of the estimator are obtained. A practical example with a 4-bus power grid is provided to demonstrate the effectiveness of the proposed estimation method, where the results show that the proposed method is capable of estimating the state of the system in the presence of both DoS and deception attacks.

While the approach proposed in this chapter addresses resilient distributed estimation against typical heterogeneous attacks, it is noted that some cyber attacks, namely sparse injection attacks, could be potentially unbounded and cannot be dealt with by the compensation approach. In these cases, a separation and isolation approach is required to remove the attack signal from the measurements. In the next chapter, a switching estimator based on a monitoring function will be introduced for the secure estimation for nonlinear systems against sparse attacks.

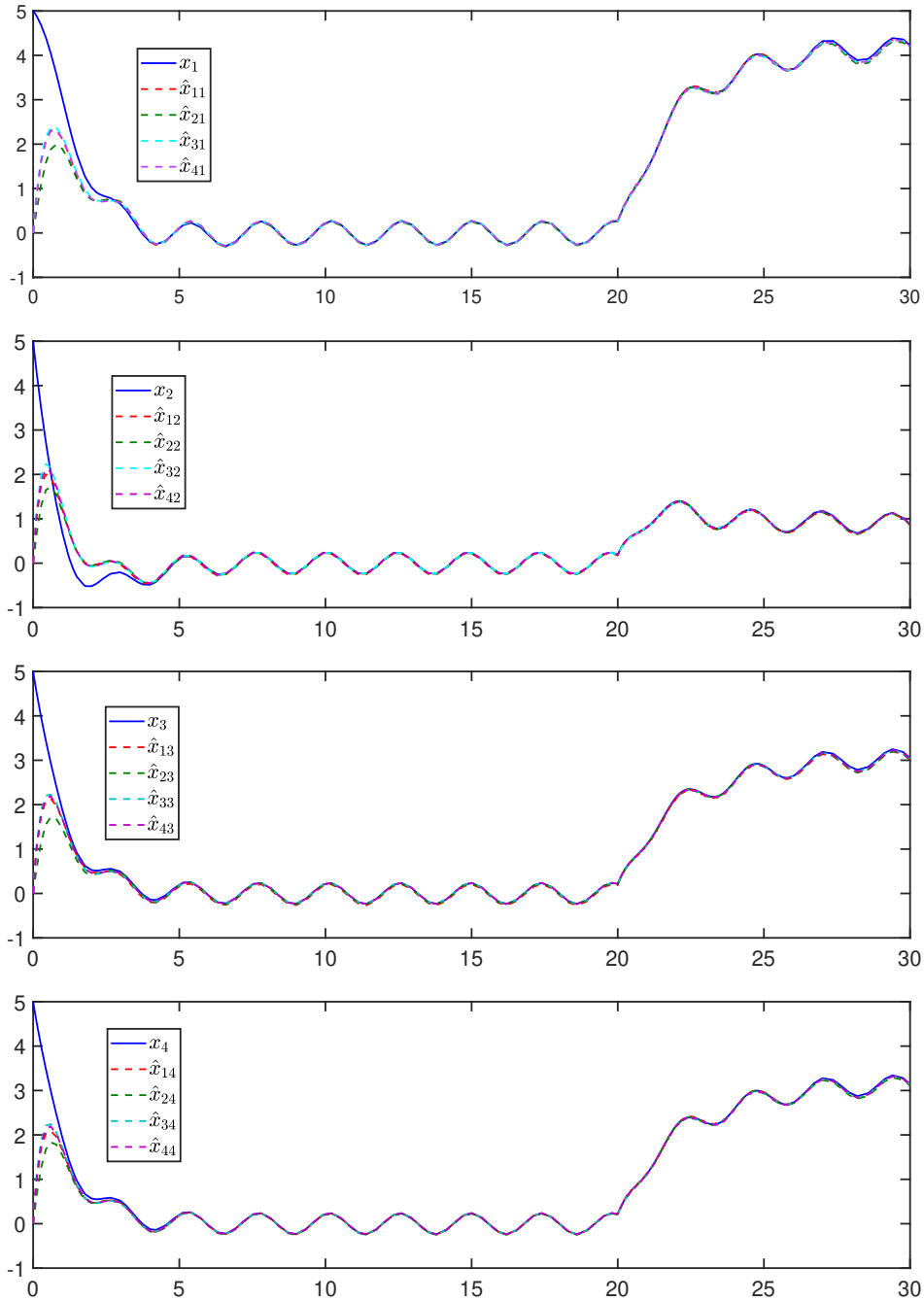

Figure 4.3: System states and estimates of the proposed algorithm.

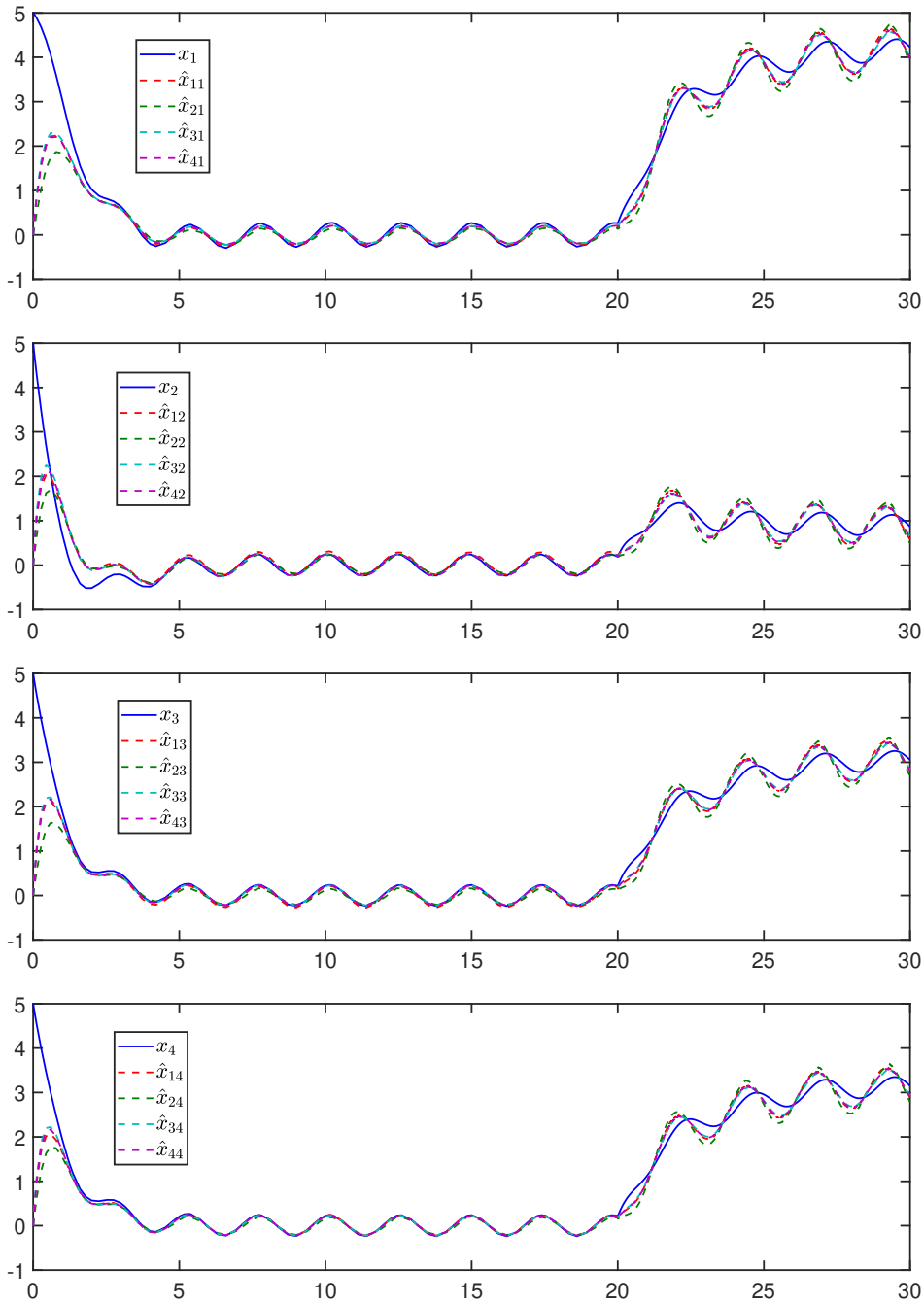

Figure 4.4: System states and estimates without disturbance rejection.

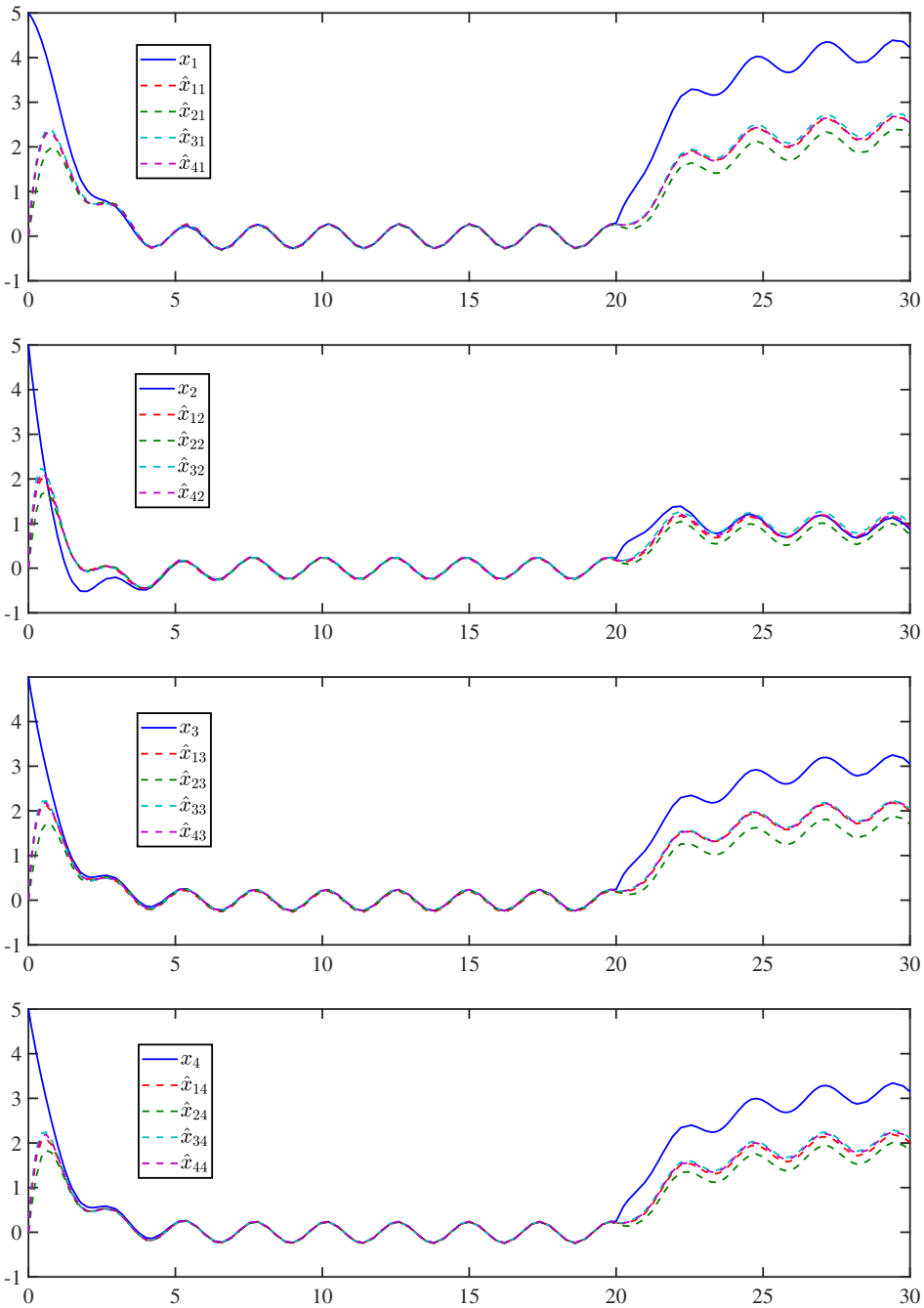

Figure 4.5: System states and estimates without attack compensation.

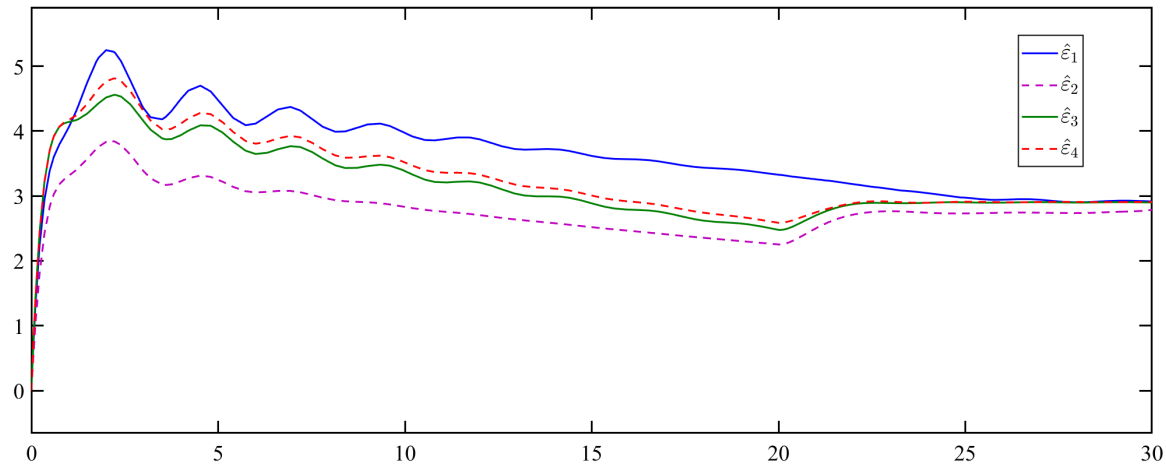

Figure 4.6: Estimation of attack upper bound ε.

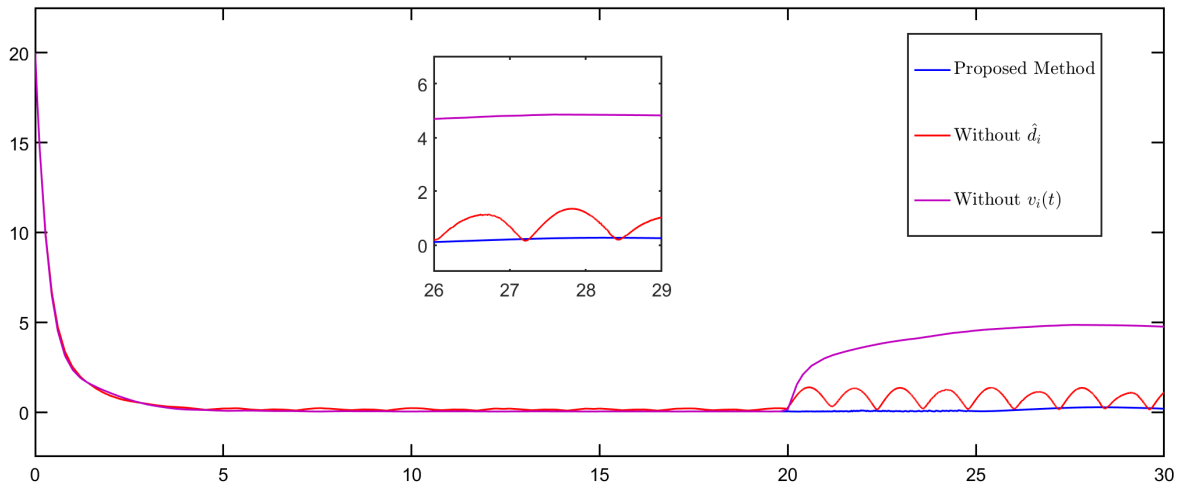

Figure 4.7: Comparison of mean square errors.

Chapter 5

Secure State Estimation for Nonlinear Systems Under Sparse Attacks

5.1 Introduction

Among the common types of cyber attacks, sparse injection attacks are particularly challenging to deal with, and have recently garnered the attention of researchers [41]. From a physical perspective, sparse attacks are a general class of unknown attacks that can be modelled as a sparse vector and that are maliciously injected to system measurements. As sparse attacks are potentially unbounded, in the presence of sparse attacks, the challenge of secure state estimation mainly lies in the identification of the attack mode.

Secure estimation against sparse attacks has been widely investigated in recent years for both discrete-time [43, 44, 49] and continuous-time [51, 52, 53] linear time-invariant systems. However it is noticed that while a wide range of practical systems, including robotic manipulators and unmanned aerial vehicles, are modelled as nonlinear systems, most existing estimation schemes against sparse attacks are limited to linear systems. In particular, modern robotic systems are often required to operate

under unstructured or even hostile environments, and are vulnerable to attacks. It is far from trivial to design suitable state observers for nonlinear systems, particularly in the presence of sparse attacks. Moreover, practical systems are subject to disturbances, and the disturbances may pollute the residue signals used to identify attacks, making it hard to preclude attacked sensors. Secure state estimation for nonlinear systems under the simultaneous presence of sparse attacks and disturbances remains an open problem.

Motivated by the above observations, in this chapter, a novel secure state estimation scheme is introduced for a class of continuous nonlinear systems under sparse attacks and disturbances, with application to robotic manipulators. The main contribution of this chapter is twofold.

1) A kind of high-gain K-filters is constructed to estimate unmeasured states of a class of high-order systems with strong nonlinearities. The high-gain K-filters can attenuate the disturbances to an arbitrary level and steer the estimation error into an arbitrarily small residual set when measurements from attacked sensors are precluded. It is also noted that contrary to the nonlinearities considered in Chapter 3, the nonlinear terms of the system considered in this chapter do not have to satisfy the Lipschitz assumption.

2) A monitoring function and a switching scheme are designed, which successfully preclude attacked sensors after a finite number of switchings. It is proved that with the switching scheme and high-gain K-filters, the estimation error can converge to a residual set which can be made arbitrarily small, regardless of the disturbances and possibly unbounded sparse attacks. The proposed estimation scheme removes the boundedness assumption on attack signals required in [51] and [52] and the LMI constraints on estimators required in [52] and [53]. Moreover, the application of the proposed method to a robotic manipulator illustrates its effectiveness.

5.2 Problem Formulation

Consider a class of nonlinear systems described by

$$\dot{x} = Ax + \varphi(x_1) + b(u + d), \tag{5.1}$$

where $x = [x_1, \ldots, x_n]^{\mathrm{T}} \in \mathbb{R}^n$ and $u \in \mathbb{R}$ are the system states and the control input, respectively, $\varphi(x_1) \in \mathbb{R}^n$ is a known smooth nonlinear function, $d \in \mathbb{R}$ is the disturbance signal which satisfies $|d(t)| \leq \bar{d}$ with $\bar{d}$ a known constant, $A = \begin{bmatrix} 0 & & \\ \vdots & I_{n-1} & \\ 0 & \cdots & 0 \end{bmatrix} \in \mathbb{R}^{n\times n}$, and $b = [0, \ldots, 0, \bar{b}]^{\mathrm{T}} \in \mathbb{R}^n$ with $\bar{b} \in \mathbb{R}$ a known constant. The measurement $y \in \mathbb{R}^l$ from l sensors is given by

$$y = Cx + a(t), \tag{5.2}$$

where

$$C = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix} \in \mathbb{R}^{l\times n},\ a(t) = \begin{bmatrix} a_1(t) \\ a_2(t) \\ \vdots \\ a_l(t) \end{bmatrix} \in \mathbb{R}^l \tag{5.3}$$

with $a(t)$ denoting the sparse sensor attacks injected by the attackers. If the ith sensor ($i = 1, \ldots, l$) suffers from an attack, then $a_i(t)$ is nonzero; otherwise, $a_i(t) \equiv 0$. It is assumed that $a(t)$ and $u(t)$ do not tend to infinity in finite time.

The robotic manipulator can be equipped with sensing, actuation and communication capabilities to interact with the cyber domain. Since modern robotic systems often operate in open and unstructured environments, they are potentially subject to cyber attacks. The dynamics of the manipulator can be described as [110]

$$J\ddot{x}_1 + mg\phi\sin(x_1) + \gamma(t) = u, \tag{5.4}$$

where x_1, $\dot{x}_1$ and $\ddot{x}_1$ denote the link angle, link angular velocity and link angular acceleration, respectively, and u is the control torque. Constants J, m, g and ϕ represent the rotational inertia, mass of link, gravitational acceleration and distance from the joint axis to the link center of mass, respectively, and $\gamma(t)$ is the disturbance torque that is assumed to be bounded and piecewise continuous. By letting

$x_2 = \dot{x}_1, x = [x_1, x_2]^{\mathrm{T}}, \varphi(x_1) = [0, -\frac{mg\phi}{J}\sin(x_1)]^{\mathrm{T}}$, $\bar{b} = \frac{1}{J}$ and $d(t) = -\gamma(t)$, we can rewrite (5.4) in the form of (5.1) with $n = 2$. From the physical perspective, the disturbance $\gamma(t)$ could represent the reaction torque and constrained external force in the physical model.

The link angle measurement y is collected by encoders integrated to the manipulators. In order to enhance the security and reliability of manipulator measurements as well as detect potential faults, manipulators are commonly equipped with redundant encoders. Typical configurations for redundant encoders include multiple identical encoders, pairing of incremental and absolute encoders, and encoders of different measurement principles (such as optical/magnetic). The measurement from redundant encoders corresponds to the measurement model in (5.2). Sparse attack signals could be injected to the sensors by corrupting the cyber layer of the sensors.

The following assumption is made on the sparse attacks.

Assumption 5.2.1. The attack signal $a(t) \in \mathbb{R}^l$ in (5.2) has s nonzero elements, where s is known and no larger than $l - 1$, and $\mathrm{supp}(a(t))$ is constant over time t.

In this chapter, the objective is to design a secure state estimator for the system in (5.1) with the measurement (5.2), such that the estimation error converges to a residual set that can be made arbitrarily small in the presence of sparse attacks and disturbances.

Remark 5.2.1. In addition to robotic manipulators, the system model in (5.1) can also describe a wide range of practical systems, such as servomotors [111], spring-mass-damper systems [112] and ship dynamics [113]. The measurement model in (5.2) represents a set of l sensors with only partial measurement of the states. Many practical systems are equipped with redundant sensors, which can be used to improve the accuracy, and enhance the reliability of measurements. Practical examples of sensors that can be described by the measurement model in (5.2) include redundant encoders for robotic manipulators [114], and redundant inertial sensors for navigation systems. In the proposed method, the measurement redundancy is exploited to identify the sparse attack mode.

Remark 5.2.2. Assumption 5.2.1, also defined as s-sparse in literature [41, 43], places a restriction on the number of sensors that the attack can compromise, meaning that no more than s out of l sensors are under attack, and that the number of attacked sensors remains constant. This assumption is based on the reasoning that attack resources are limited, and similar assumptions can be found in [22, 50, 51, 52, 53], where only linear time-invariant systems are considered and s is required to be no more than $l/2$. By comparison, in this chapter, nonlinear systems are considered and s is only required to be no more than $l-1$. In many cases, the number of attacked sensors s is known to the users in advance. In the cases where s is unknown to users, the estimation scheme proposed in this chapter can still be implemented under the worst case assumption of $s = l - 1$.

5.3 Estimator Design

A schematic of the proposed method is presented in Figure 5.1, which includes modules depicting the system (5.1), sensors, sparse injection attacks, switching mechanism, and high-gain K-filters, respectively. In this section, the estimation scheme, including the high-gain K-filters, the monitoring function and the switching mechanism will be introduced.

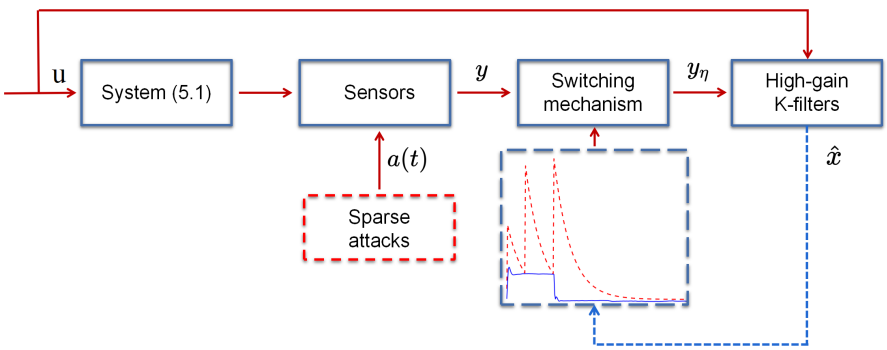

Figure 5.1: Schematic diagram of the proposed method

We refer to a possible set of attacked sensor locations as an attack mode. For l sensors under s sparse injection attacks, there will be a total of C_l^s possible attack modes. Denote by $\mathbb{S} = \{S \subset \{1, 2, \ldots, l\} : |S| = s\} = \{S_1, \ldots, S_{C_l^s}\}$ the set of all

attack modes. For the ηth attack mode S_η, we can define the corresponding switching function matrix $Q_\eta(t) = \mathrm{diag}\{\varrho_1(\eta(t)), \dots, \varrho_l(\eta(t))\}$, where $\varrho_i(\eta) = 0$ for $i \in S_\eta$, and $\varrho_i(\eta) = 1$ otherwise, $i = 1, \dots, l$. We design the switching index $\eta(t)$ as

$$\eta(t) = \mathrm{mod}(q-1, C_l^s) + 1, \ \forall t \in [t_{q-1}, t_q), \tag{5.5}$$

where $t_0 := 0$, and t_q $(q = 1, 2, 3, \dots)$ are switching time instants to be specified. It is clear that when $S_\eta = \mathrm{supp}(a(t))$, the attacked measurements are removed by the switching matrix and $Q_\eta(t)a(t) = 0$. A challenging aspect of resilient estimation is to identify the attack-free mode when no information on the channels of attacks are known to the defender. For this purpose, we define a switching measurement based on the switching matrix as

$$y_\eta = \frac{1}{(l-s)} \sum_{i=1}^{l} \tilde{y}_i, \tag{5.6}$$

where $\tilde{y}_i$ is the ith element of $\tilde{y} := Q_\eta y$. This definition ensures that $y_\eta = x_1$ when $Q_\eta(t)a(t) = 0$.

Choose a constant vector $K_0 = [k_1, \dots, k_n]^{\mathrm{T}} \in \mathbb{R}^n$ such that the matrix $A_0 = A - K_0 E^{\mathrm{T}}$ is Hurwitz (i.e., $s^n + k_1 s^{n-1} + \cdots + k_{n-1}s + k_n$ is a Hurwitz polynomial), where $E = [1, 0, \dots, 0]^{\mathrm{T}} \in \mathbb{R}^n$. For the nonlinear system in (5.1), We design a kind of high-gain K-filters based on the switching measurement y_η as follows:

$$\dot{\xi}_1 = A_\mu \xi_1 + K_\mu y_\eta, \tag{5.7}$$

$$\dot{\xi}_2 = A_\mu \xi_2 + \varphi(y_\eta), \tag{5.8}$$

$$\dot{\xi}_3 = A_\mu \xi_3 + bu, \tag{5.9}$$

where ξ_1, ξ_2, and ξ_3 are states of the filters, $A_\mu = A - K_\mu E^{\mathrm{T}}$ and $K_\mu = [\mu k_1, \dots, \mu^n k_n]^{\mathrm{T}}$ with $\mu \geq 1$ a design parameter. Based on the high-gain K-filters, the state estimation, denoted by $\hat{x}$, is given as

$$\hat{x} = \xi_1 + \xi_2 + \xi_3. \tag{5.10}$$

From (5.1) and (5.7)-(5.10), it can be checked that the state estimation error $\tilde{x} := x - \hat{x}$ satisfies

$$\begin{aligned} \dot{\tilde{x}} &= Ax + \varphi(x_1) + b(u+d) - A_\mu(\xi_1 + \xi_2 + \xi_3) - K_\mu y_\eta - \varphi(y_\eta) - bu \\ &= (A - K_\mu E^{\mathrm{T}})x + K_\mu(E^{\mathrm{T}}x - y_\eta) - A_\mu \hat{x} + \varphi(x_1) - \varphi(y_\eta) + bd \\ &= A_\mu \tilde{x} + K_\mu(x_1 - y_\eta) + \varphi(x_1) - \varphi(y_\eta) + bd. \end{aligned} \tag{5.11}$$

If $Q_\eta(t)a(t) = 0$ for all $t \geq t^*$ with t^* a finite time instant, then $y_\eta = x_1$ and thus

$$\dot{\tilde{x}}(t) = A_\mu \tilde{x}(t) + bd(t), \ \forall t \geq t^*. \tag{5.12}$$

Applying the transformation $\varepsilon = W\tilde{x}$ with $W = \mathrm{diag}\{1, \mu^{-1}, \ldots, \mu^{1-n}\}$, in view of (5.12), we have

$$\begin{aligned} \dot{\varepsilon}(t) &= WA_\mu W^{-1}\varepsilon(t) + Wbd(t) \\ &= \mu A_0 \varepsilon(t) + Wbd(t), \ \forall t \geq t^*. \end{aligned} \tag{5.13}$$

The following lemma gives the estimation performance of the high-gain K-filters when the attacked measurements are removed.

Lemma 5.3.1. Define $V_0 = \varepsilon^{\mathrm{T}} P_0 \varepsilon$, where $P_0 = P_0^{\mathrm{T}} > 0$ is the solution of the Lyapunov equation $A_0^{\mathrm{T}} P_0 + P_0 A_0 = -2I_n$. Consider the system in (5.1) with the measurement in (5.2) and the state estimation given by (5.7)-(5.10). Assuming that $Q_\eta(t)a(t) = 0$ for all $t \geq t^*$ with t^* a finite time instant, then for all $t \geq t^*$ we have

$$\|\tilde{x}(t)\|^2 \leq \frac{\mu^{2n-2} e^{-\frac{2\mu-1}{\lambda_{\max}(P_0)}(t-t^*)} V_0(t^*) + \frac{\lambda_{\max}(P_0) f}{2\mu-1}}{\lambda_{\min}(P_0)}, \tag{5.14}$$

where $\tilde{x} = x - \hat{x}$ is the estimation error, and $f = \|P_0\|^2 \bar{b}^2 \bar{d}^2$ is a constant independent of the design parameter μ. Moreover, $\tilde{x}$ converges to a residual set which can be made arbitrarily small by increasing μ.

Proof. In view of (5.13), the derivation of $V_0(t)$ yields

$$\begin{aligned} \dot{V}_0(t) &= -2\mu \varepsilon^{\mathrm{T}}(t)\varepsilon(t) + 2\varepsilon^{\mathrm{T}}(t) P_0 W bd(t) \\ &\leq -(2\mu - 1)\varepsilon^{\mathrm{T}}(t)\varepsilon(t) + \mu^{(2-2n)} \|P_0\|^2 \bar{b}^2 \bar{d}^2 \\ &\leq -\frac{2\mu - 1}{\lambda_{\max}(P_0)} V_0(t) + \mu^{(2-2n)} f, \ \forall t \geq t^*. \end{aligned} \tag{5.15}$$

It follows from (5.15) that

$$V_0(t) \leq e^{-\frac{2\mu-1}{\lambda_{\max}(P_0)}(t-t^*)} V_0(t^*) + \frac{\lambda_{\max}(P_0)\mu^{(2-2n)} f}{2\mu - 1}, \forall t \geq t^*. \tag{5.16}$$

As a result,

$$\|\varepsilon(t)\|^2 \leq \frac{e^{-\frac{2\mu-1}{\lambda_{\max}(P_0)}(t-t^*)} V_0(t^*) + \frac{\lambda_{\max}(P_0)\mu^{(2-2n)} f}{2\mu-1}}{\lambda_{\min}(P_0)}, \forall t \geq t^*. \tag{5.17}$$

On the other hand, it can be readily checked that

$$\|\tilde{x}\|^2 = \|W^{-1}\varepsilon\|^2 \leq \mu^{2n-2}\|\varepsilon\|^2. \tag{5.18}$$

Combining (5.17) and (5.18) gives (5.14). Further, by (5.14), we have

$$\lim_{t\to+\infty} \|\tilde{x}(t)\|^2 \leq \frac{\lambda_{\max}(P_0)f}{(2\mu-1)\lambda_{\min}(P_0)}. \tag{5.19}$$

It is clear from (5.19) that $\tilde{x}$ converges to a residual set which can be made arbitrarily small by increasing μ. This completes the proof. ■

Remark 5.3.1. Different from traditional K-filters [115], the high-gain K-filters designed in (5.7)-(5.9) offer an adjustable design parameter μ. As shown in Lemma 5.3.1, in the absence of sensor attacks, the high-gain K-filters can steer the state estimation error into an arbitrarily small residual set by increasing μ. This feature enables attenuation of the disturbance d to an arbitrary level, and will play an important role in the subsequent design and analysis.

Now, we shall propose a monitoring function and a switching scheme to specify the switching time instants. Let the ith elements of $\hat{x}$, $\tilde{x}$ and ε be denoted as $\hat{x}_i$, $\tilde{x}_i$ and ε_i, respectively, where $i = 1, \ldots, n$. The following assumptions are made.

Assumption 5.3.1. There exists a known constant β such that $\lim_{t\to+\infty} |\tilde{x}_1(t)| \leq \beta$ does not hold if $Q_\eta(t)a(t)$ does not remain 0 after a finite time instant, where β can be arbitrarily small.

Assumption 5.3.2. The system states $x_1, \ldots, x_n$ are bounded.

Remark 5.3.2. Assumption 5.3.1 avoids strictly undetectable attacks from the defenders' perspective. Works in [22] and [116] introduced the concept of completely stealthy attacks that can completely remove their influence on monitored residues and are strictly undetectable. But such attacks require complete knowledge of the system model and the detection mechanism, which is a very restrictive assumption. The secure estimation approach in this chapter is developed from the defenders' perspective, without prior knowledge on the attack signals. Therefore, it is necessary to introduce Assumption 5.3.1 to avoid strictly undetectable attacks. Thanks to the high-gain K-filters, the constant β is allowed to be arbitrarily small, which significantly reduces the

restrictiveness of Assumption 5.3.1. Assumption 5.3.2 is also reasonable since systems are often subject to physical constraints. For instance, the angle and angular velocity of a robotic manipulator are bounded due to mechanical restrictions [114, 117].

Reminding that (5.14) holds when the attack-free mode is identified, it is natural to construct a monitoring function based on (5.14). In view of (5.14) and noting $V_0(t^*) \leq \lambda_{\max}(P_0)\sum_{i=1}^n \varepsilon_i^2(t^*) = \lambda_{\max}(P_0)[\tilde{x}_1^2(t^*) + \sum_{i=2}^n \varepsilon_i^2(t^*)]$, it can be checked that

$$\begin{aligned}
& \lambda_{\min}(P_0)\tilde{x}_1^2(t) \\
\leq\ & \mu^{2n-2}e^{-\frac{2\mu-1}{\lambda_{\max}(P_0)}(t-t^*)}\lambda_{\max}(P_0)[\tilde{x}_1^2(t^*) + \sum_{i=2}^n \varepsilon_i^2(t^*)] + \frac{\lambda_{\max}(P_0)f}{2\mu-1} \\
\leq\ & \mu^{2n-2}e^{-\frac{2\mu-1}{\lambda_{\max}(P_0)}(t-t^*)}\lambda_{\max}(P_0)[\tilde{x}_1^2(t^*) + 2\sum_{i=2}^n \hat{x}_i^2(t^*)\mu^{2-2i} + 2\sum_{i=2}^n x_i^2(t^*)\mu^{2-2i}] \\
& + \frac{\lambda_{\max}(P_0)f}{2\mu-1}, \qquad \forall t \geq t^*. \qquad (5.20)
\end{aligned}$$

Introduce a monotonically increasing unbounded sequence $\alpha(j)$ $(j = 0, 1, 2\dots)$ which satisfies $\alpha(j) > 0$ and $\lim_{j\to+\infty}\alpha(j) = +\infty$. Taking (5.20) into consideration, a monitoring function $\psi(t)$ is designed as follows:

$$\begin{aligned}
\psi(t) \ =\ & \mu^{2n-2}e^{-\frac{2\mu-1}{\lambda_{\max}(P_0)}(t-t_{q-1})}\lambda_{\max}(P_0)[\tilde{x}_1^2(t_{q-1}) + 2\sum_{i=2}^n \hat{x}_i^2(t_{q-1})\mu^{2-2i} + \alpha(q-1)] \\
& + \frac{\lambda_{\max}(P_0)f}{2\mu-1}, \ \forall t \in [t_{q-1}, t_q). \qquad (5.21)
\end{aligned}$$

Define

$$\varpi(t) = \lambda_{\min}(P_0)\tilde{x}_1^2(t). \qquad (5.22)$$

Based on (5.21) and (5.22), we propose the following switching scheme to determine the switching time instant t_q:

$$t_q = \inf\{t > t_{q-1} \big| \varpi(t) = \lim_{\Delta t\to 0^-} \psi(t+\Delta t)\}. \qquad (5.23)$$

Meanwhile, we choose the design parameter μ such that

$$\frac{\lambda_{\max}(P_0)f}{(2\mu-1)\lambda_{\min}(P_0)} \leq \beta^2. \qquad (5.24)$$

Remark 5.3.3. The switching scheme in (5.23) together with the design in (5.5) drives the value of the switching index $\eta(t)$ to switch among $1, \dots, C_l^s$. The presence

of an increasing sequence $\alpha(q-1)$ ensures that the monitoring function $\psi(t)$ jumps at each switching instance, providing a margin for the next potential switching. In the following subsection, it will be proved theoretically that the switching index $\eta(t)$ will stop at the attack-free mode after a finite number of switchings.

5.4 Performance Analysis

Theorem 5.4.1.: Consider the nonlinear system in (5.1) with the measurement in (5.2). Suppose that Assumptions 5.2.1, 5.3.1 and 5.3.2 hold. Then, by means of the high-gain K-filters in (5.7)-(5.9) and the switching law in (5.23), the state estimation error $\tilde{x}$ converges to a residual set given by

$$\lim_{t\to+\infty} \|\tilde{x}(t)\| \leq \sqrt{\frac{\lambda_{\max}(P_0)f}{(2\mu-1)\lambda_{\min}(P_0)}}, \tag{5.25}$$

which can be made arbitrarily small by increasing the design parameter μ.

Proof. First, we prove that the switching will eventually stop after a finite number of switchings. Suppose by contradiction that the switching index $\eta(t)$ switches without stopping. Then, the increasing sequence $\alpha(q-1)$ increases unboundedly as $q \to +\infty$. In view of Assumption 5.3.2, there must exist a finite integer q^* such that

$$\alpha(q^*-1) > 2\sum_{i=2}^{n} x_i^2(t)\mu^{2-2i}, \ \forall t \geq t_{q^*-1}, \tag{5.26}$$

and

$$Q_\eta(t_{q^*-1})a(t) = 0. \tag{5.27}$$

Note that (5.27) implies that the attacked measurements are removed. Then, from (5.26) and (5.21), we have

$$\psi(t) \ > \ \mu^{2n-2}e^{-\frac{2\mu-1}{\lambda_{\max}(P_0)}(t-t_{q^*-1})}\lambda_{\max}(P_0)\sum_{i=1}^{n}\varepsilon_i^2(t_{q^*-1}) + \frac{\lambda_{\max}(P_0)f}{2\mu-1}, \tag{5.28}$$

where $t \geq t_{q^*-1}$. On the other hand, by (5.27) and Lemma 5.3.1, $\varpi(t) = \lambda_{\min}(P_0)\tilde{x}_1^2(t)$ satisfies

$$\varpi(t) \ \leq \ \mu^{2n-2}e^{-\frac{2\mu-1}{\lambda_{\max}(P_0)}(t-t_{q^*-1})}\lambda_{\max}(P_0)\sum_{i=1}^{n}\varepsilon_i^2(t_{q^*-1}) + \frac{\lambda_{\max}(P_0)f}{2\mu-1}, \tag{5.29}$$

where $t \geq t_{q^*-1}$. Combining (5.28) and (5.29) gives $\psi(t) > \varpi(t)$ when $t \geq t_{q^*-1}$, which together with (5.23) implies that no switching will occur after the time instant t_{q^*-1}. This leads to a contradiction. Therefore, we can conclude that the switching will stop after a finite number of switchings.

Let h denote the total number of switchings and t_h be the time instant of the last switching, both of which are finite. Then, from (5.21), we have

$$\begin{aligned}\psi(t) &= \mu^{2n-2} e^{-\frac{2\mu-1}{\lambda_{\max}(P_0)}(t-t_h)} \lambda_{\max}(P_0)[\tilde{x}_1^2(t_h) + 2\sum_{i=2}^{n} \hat{x}_i^2(t_h)\mu^{2-2i} + \alpha(h)] \\ &\quad + \frac{\lambda_{\max}(P_0) f}{2\mu - 1}, \qquad \forall t \geq t_h. \end{aligned} \tag{5.30}$$

Since $a(t)$ and $u(t)$ are bounded in finite time, it is clear from (5.2), (5.6)-(5.10) and Assumption 5.3.2 that $\hat{x}(t)$ and $\tilde{x}(t)$ are bounded for $t \in [0, t_h]$. As a result, $\tilde{x}_1^2(t_h)$ and $\sum_{i=2}^{n} \hat{x}_i^2(t_h)\mu^{2-2i}$ in (6.14) are bounded. With this fact in mind, using (5.22) and (5.24) and noting $\varpi(t) \leq \psi(t)$ for all $t \geq t_h$, it can be checked that

$$\begin{aligned}\lim_{t\to+\infty} \tilde{x}_1^2(t) &\leq \frac{1}{\lambda_{\min}(P_0)} \lim_{t\to+\infty} \psi(t) \\ &\leq \frac{\lambda_{\max}(P_0) f}{(2\mu-1)\lambda_{\min}(P_0)} \leq \beta^2. \end{aligned} \tag{5.31}$$

Subsequently, taking Assumption 5.3.1 into consideration, we know the attack-free model is identified and $Q_\eta(t)a(t)$ remains 0 for all $t \geq t_h$, which together with Lemma 5.3.1 indicates that (5.25) holds and $\hat{x}$ and $\tilde{x}$ are uniformly bounded for all $t \geq 0$. This completes the proof. ■

Remark 5.4.1. It should be pointed out that (5.24) can always be satisfied through the selection of μ. Owing to the high-gain K-filters, μ can be set to a large value. As a result, β is allowed to be small, which makes Assumption 5.3.1 mild. Besides, different from [52] and [53], the secure estimation scheme proposed in this chapter does not require solving any LMIs and, theoretically speaking, in our scheme it is much easier to choose the design parameters.

5.5 Simulation and Experimental Results

Most existing works focusing on sparse attacks are only devoted to linear systems, and only simulation results are presented. In this section, the proposed secure state estimation method is applied to a robotic manipulator, where both simulation and experimental studies are performed. The angle measurement is collected by encoders integrated to the manipulators. In this case, the manipulator is equipped with 4 independent encoders all subject to sparse attacks. This measurement configuration corresponds to the measurement model in (5.2) with $C = [1\ \ 0; 1\ \ 0; 1\ \ 0; 1\ \ 0]$. In our simulation and experiments, the physical parameters of the manipulator are $J = 8.5 \times 10^{-5}$ kg·m^2, $m = 0.08$ kg, $\phi = 0.055$ m and $g = 9.8$ m/s^2, and the sequence $\alpha(j)$ is chosen as $\alpha(j) = j + 1$.

In the simulation study, we consider the case where constant attack signals are injected to the 2nd and the 4th encoders. The attack vector is given as $a(t) = [0\ 5\ 0\ 5]^{\mathrm{T}}$ for all $t \geq 0$, and the control input is given as $u = 0.004 \sin t$ and the disturbance $\gamma(t)$ is set as a white noise upper bounded by 0.1. The initial conditions of the manipulator are $x_1(0) = 0.6$ rad and $x_2(0) = 0$ rad/s, and initial conditions of the high-gain K-filters are set to be zero. The design parameters are chosen as $\mu = 50, k_1 = 2$ and $k_2 = 1$, and the simulation results are shown in Figures 5.2 and 5.3. From Figure 5.2, one can see that the proposed K-filters estimate the angle and angular velocity of the manipulator. From Figure 5.3, it is shown that the estimation error activates the switching mechanism three times, eventually identifying the attack-free mode.

Following the simulation study, we further validate the proposed estimation method through a hardware experiment on the OpenMANIPULATOR-X manipulator. A schematic diagram of the experimental platform is given in Figure 5.4. The estimation and control algorithms are executed in MATLAB/Simulink RealTime environment. Sensor measurements are read by the U2D2 board, and sparse attacks are injected by the PC interface.

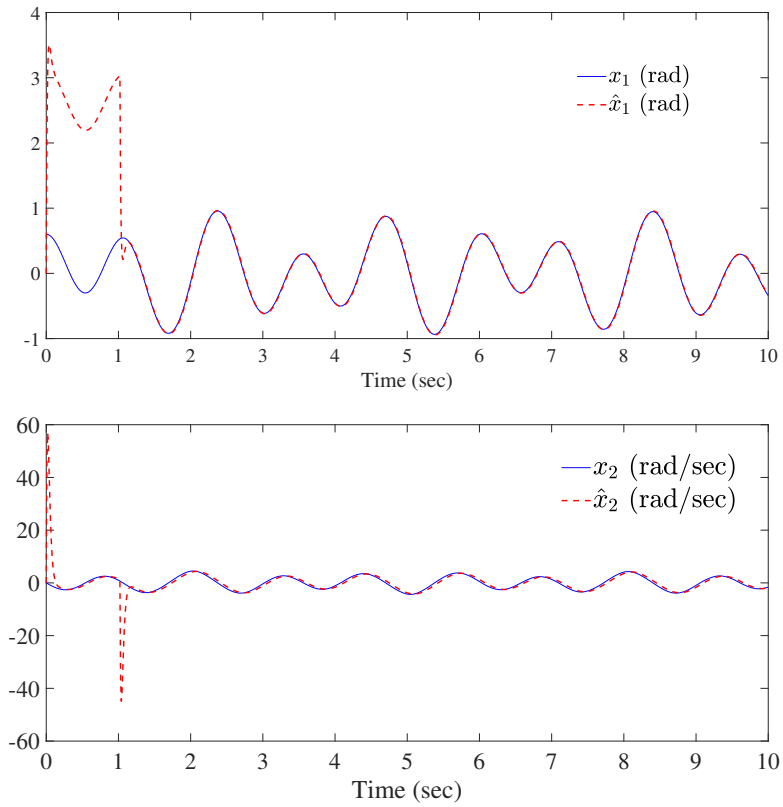

Figure 5.2: States and estimations from simulation.

5.5.1 Experiment 1-State Estimation

In the first experiment, the manipulator is programmed to follow a desired trajectory, and our proposed estimation scheme performs state estimation while the sensors are under sparse attacks. The attack vector is set as $a(t) = [0\ 5\ 0\ 5]^{\mathrm{T}}$ for all $t \geq 0$, and the design parameters of our estimation scheme are chosen as $\mu = 50, k_1 = 2$ and $k_2 = 1$. The initial conditions of the manipulator are $x_1(0) = 0.2$ rad and $x_2(0) = 0$ rad/s, and initial conditions of the high-gain K-filters are set to be zero. The manipulator trajectory and its estimation are given in Figure 5.5, which shows that our proposed scheme estimates the trajectory of the manipulator after a period of switching. From Figure 5.6, it is observed that the switching mechanism successfully switches to the attack-free mode.

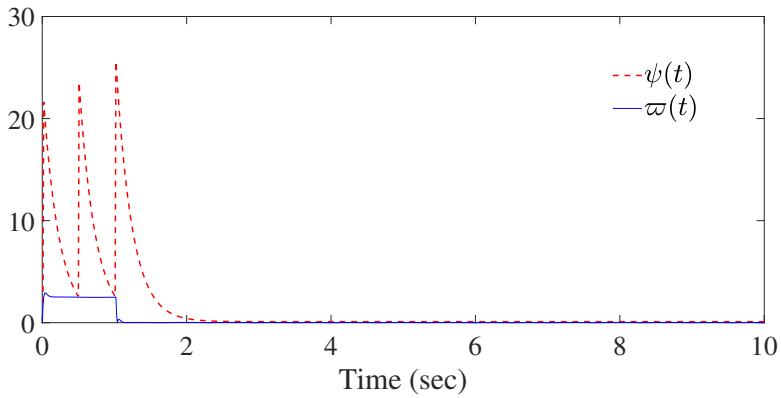

Figure 5.3: $\psi(t)$ and $\varpi(t)$ from simulation.

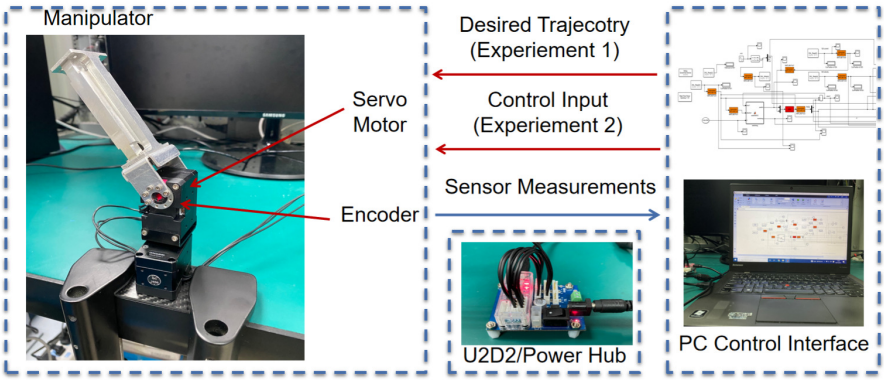

Figure 5.4: Schematic diagram of the experiment platform.

5.5.2 Experiment 2-Estimation-Based Control

Based on the first experiment, we now design a backstepping control scheme based on the estimated states with consideration to the estimation error and apply it to the manipulator.

Step 1. Define $z_1 = x_1 - x_{1d}$, where x_{1d} is the desired trajectory. Taking the derivative of z_1 yields

$$\dot{z}_1 = \dot{x}_1 - \dot{x}_{1d} = x_2 - \dot{x}_{1d} = \hat{x}_2 + \tilde{x}_2 - \dot{x}_{1d}. \tag{5.32}$$

Define $z_2 = \hat{x}_2 - \omega$, and choose $\omega = -c_1 z_1 + \dot{x}_{1d} - \frac{1}{4} z_1$, where $c_1 > 0$ is design parameter. Then, we have $\dot{z}_1 = -c_1 z_1 + z_2 + \tilde{x}_2 - \frac{1}{4} z_1$. Considering the first Lyapunov function candidate $V_1 = \frac{1}{2} z_1^2$, it can be checked that

$$\dot{V}_1 = -c_1 z_1^2 + z_1 z_2 + z_1 \tilde{x}_2 - \frac{1}{4} z_1^2 \leq -c_1 z_1^2 + z_1 z_2 + \tilde{x}_2^2. \tag{5.33}$$

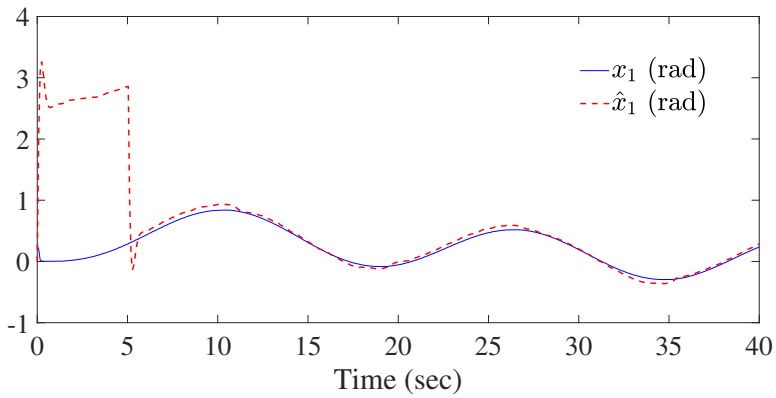

Figure 5.5: Trajectory and estimation from Experiment 1.

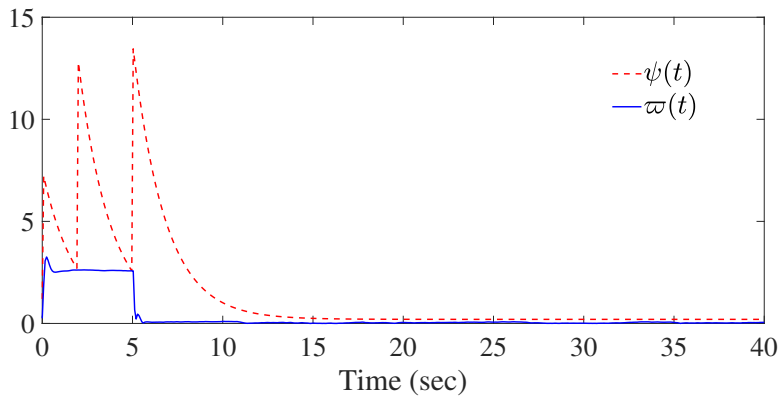

Figure 5.6: $\psi(t)$ and $\varpi(t)$ from Experiment 1.

Step 2. Noting $\dot{\omega} = -c_1\dot{z}_1 + \ddot{x}_{1d} - \frac{1}{4}\dot{z}_1 = -(c_1 + \frac{1}{4})(\hat{x}_2 - \dot{x}_{1d}) + \ddot{x}_{1d} - (c_1 + \frac{1}{4})\tilde{x}_2$, we have

$$\dot{z}_2 = \dot{\hat{x}}_2 - \dot{\omega} = \sigma + \bar{b}u + (c_1 + \frac{1}{4})\tilde{x}_2, \tag{5.34}$$

where $\sigma = -\mu^2 k_2 \xi_{1,1} + \mu^2 k_2 y_\eta - \mu^2 k_2 \xi_{2,1} + \frac{BG\Omega}{J}\sin(y_\eta) - \mu^2 k_2 \xi_{3,1} + (c_1 + \frac{1}{4})(\hat{x}_2 - \dot{x}_{1d}) - \ddot{x}_{1d}$. Let $V_2 = V_1 + \frac{1}{2}z_2^2$, whose derivative satisfies

$$\dot{V}_2 \leq -c_1 z_1^2 + z_1 z_2 + z_2 \bar{b}u + z_2\sigma + \frac{1}{4}(c_1 + \frac{1}{4})^2 z_2^2 + 2\tilde{x}_2^2. \tag{5.35}$$

Now, the control signal is chosen as $u = \bar{b}^{-1}[-c_2 z_2 - \sigma - \frac{1}{4}(c_1 + \frac{1}{4})^2 z_2 - z_1]$, which results in

$$\dot{V}_2 \leq -c_1 z_1^2 - c_2 z_2^2 + 2\tilde{x}_2^2 \leq -2\min\{c_1, c_2\}V_2 + 2\tilde{x}_2^2. \tag{5.36}$$

Since $\tilde{x}_2$ is bounded and converges to a residual set which can be made arbitrarily small by increasing the design parameter μ, it is clear from (5.36) that V_2, z_1 and z_2

are bounded and converge to some residual sets which can be made arbitrarily small by increasing μ, c_1 and c_2.

In Experiment 2, the control gains are chosen as $c_1 = c_2 = 2$. The experiment is carried out in an attack-free environment. From Figure 5.7, it can be seen that the estimation-based controller can force the link angle to track the desired trajectory x_{1d}.

From the simulation and experimental results, it has been demonstrated that the proposed method can estimate the state information of the robotic manipulator under sparse attacks and disturbances. It is noted that the results in [22, 43, 45, 46, 47, 48, 49, 50, 51, 52, 53] cannot deal with the state estimation of nonlinear systems, and thus is not applicable in this case study.

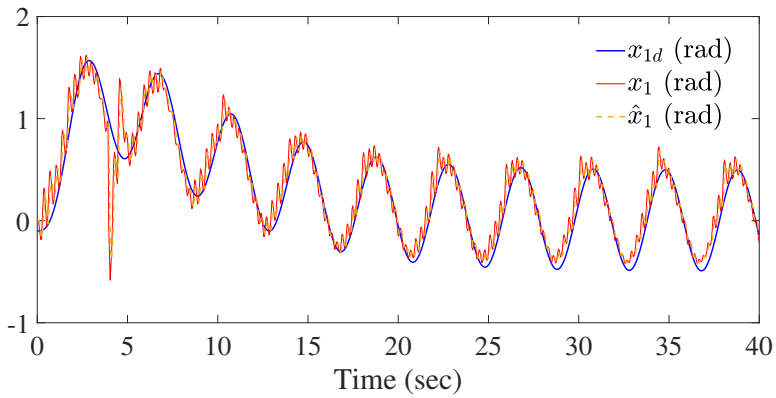

Figure 5.7: x_{1d}, x_1 and $\hat{x}_1$ from Experiment 2.

5.6 Conclusions

In this chapter, considering sparse sensor attacks and disturbances, a secure state estimation scheme has been proposed for a class of nonlinear systems with application to a robotic manipulator. Our design introduces a kind of high-gain K-filters, a monitoring function and a switching scheme. With these efforts and using a contradiction argument, it has been proved that all attacked sensors are precluded after a finite number of switchings and the estimation error can converge to an arbitrarily small residual set. The proposed method has been applied to a robotic manipulator with both simulation and experimental studies, where the effectiveness of the proposed scheme has

been validated. In the following chapter, we shall consider uncertainties on the actuator channel of distributed systems, and a resilient containment control scheme will be introduced for distributed heterogeneous MIMO nonlinear systems with unknown direction actuator faults.

Chapter 6

Containment Control for Heterogeneous MIMO Nonlinear Agents With Unknown Direction Actuator Faults

6.1 Introduction

Due to their scale and complexity, multi-agent systems are prone to faults on the actuator channel, which may lead to degradation of system performance or even instability. Aiming at additive faults and partial loss of effectiveness faults, many effective adaptive fault-tolerant control schemes have been proposed for SISO agents [62, 65, 67] and MIMO agents with known CGMs [68, 75, 76]. Though ignored by all the aforementioned control schemes, unknown direction actuator faults including reverse faults are frequently encountered by practical systems including spacecraft [86], power systems [87] and vehicles [88]. It should be pointed out that the joint influence of unknown CGMs and unknown direction actuator faults brings unique challenges to cooperative control of MIMO agents. Firstly, the faults result in an unknown time-varying matrix between the CGM and the control signal, which further complicates the disposal of

CGMs. Meanwhile, additions involving multiple Nussbaum functions are unavoidable in this case, and the actuation directions of actuators and the unknown parameters to be estimated experience jumps, where the effects of multiple Nussbaum functions may counteract each other and the jumps significantly increase the difficulty in state estimation, adaptive controller design and stability analysis. These problems make all the contradiction arguments used in existing Nussbaum function-based control schemes (see, e.g., [63, 64, 67, 88, 84] and [118]) no longer valid in face of unknown signs of leading principal minors of CGMs and unknown direction actuator faults.

In this chapter, a novel output-feedback adaptive containment control scheme is proposed for a class of nonlinear MIMO agents. The main contributions of this chapter are as follows:

1) The agents in the distributed system are completely heterogeneous in the sense that, except for the input-output dimension, all other characteristics are allowed to be different. With respect to the CGMs, we only require the signs of their leading principal minors to be nonzero, which considerably relaxes the assumptions on CGMs in existing cooperative control schemes [68, 75, 76, 119, 120, 121, 122, 123, 124].

2) Unknown direction actuator faults are considered simultaneously in the proposed control scheme. By introducing some Nussbaum functions, a novel contradiction argument and a matrix similarity transformation, the difficulties caused by the CGMs, actuator faults and jumps are successfully overcome and all closed-loop signals are proved to be globally uniformly bounded. To our best knowledge, this is the first adaptive cooperative control scheme capable of tolerating unknown direction actuator faults and unknown signs of leading principal minors of CGMs. Also, an event-triggering mechanism is introduced to avoid continuous communication among agents, which considerably reduces the communication burden.

6.2 Problem Formulation

Consider a group of $N+M$ agents, where agents $1,\ldots,N$ are followers and agents $N+1,\ldots,N+M$ are leaders. The followers under consideration are q-input q-output uncertain nonlinear systems in output-feedback form [115], and the dynamics of the ith follower is given by

$$\dot{x}_i = A_{oi}x_i + \sum_{p=1}^{\nu_i} G_{i,p}f_{i,p}(y_i) + B_iu_i, \quad y_i = C_ix_i, \tag{6.1}$$

$$A_{oi} = \begin{bmatrix} 0 & I_q & 0 & \cdots & 0 \\ 0 & 0 & I_q & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & I_q \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}, \; B_i = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ B_{i,m_i} \\ \vdots \\ B_{i,0} \end{bmatrix}, \tag{6.2}$$

where $x_i = [x_{i,1}^{\mathrm{T}},\ldots,x_{i,n_i}^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{R}^{qn_i}$ is the state with $x_{i,j} \in \mathbb{R}^q$, $i=1,\ldots,N$, $j=1,\ldots,n_i$; $u_i \in \mathbb{R}^q$ and $y_i \in \mathbb{R}^q$ are the input and output, respectively; $f_{i,p}(y_i) = [f_{i,p,1}^{\mathrm{T}}(y_i),\ldots,f_{i,p,n_i}^{\mathrm{T}}(y_i)]^{\mathrm{T}}$ with $f_{i,p,j}(y_i) \in \mathbb{R}^q$ are known smooth functions; $A_{oi} \in \mathbb{R}^{qn_i\times qn_i}$, $B_i \in \mathbb{R}^{qn_i\times q}$, $C_i = [I_p, 0, \cdots, 0] \in \mathbb{R}^{q\times qn_i}$ and $G_{i,p} = \mathrm{diag}\{A_{i,p},\cdots,A_{i,p}\} \in \mathbb{R}^{qn_i\times qn_i}$ with $A_{i,\nu_i},\ldots,A_{i,1} \in \mathbb{R}^{q\times q}$ and $B_{i,m_i},\ldots,B_{i,0} \in \mathbb{R}^{q\times q}$ being unknown constant matrices; and q,ν_i, n_i and m_i are known integers. The states $x_{i,2},\ldots,x_{i,n_i}$ are not measured. Define $\rho_i = n_i - m_i$ and $\rho = \max_{i=1,\ldots,N}\rho_i$.

The actuators of the followers may suffer from unknown faults, given by

$$u_{i,j}(t) = \begin{cases} \bar{u}_{i,j}(t), & 0 \le t < T_{i,j}, \\ \bar{\delta}_{i,j}\bar{u}_{i,j}(t), & t \ge T_{i,j}, \end{cases} \tag{6.3}$$

where $j=1,\ldots,q$, and $\bar{u}_i = \mathrm{diag}\{\bar{u}_{i,1},\ldots,\bar{u}_{i,q}\}$ is the control input to be designed, $\bar{\delta}_{i,j} \neq 0$ is a constant whose sign represents the fault direction, and $T_{i,j}$ is an unknown constant denoting the time instant at which the jth actuator of the ith follower suffers from faults. Both the magnitude and the sign of $\bar{\delta}_{i,j}$ are unknown. Letting

$$\delta_{i,j}(t) = \begin{cases} 1, & 0 \le t < T_{i,j}, \\ \bar{\delta}_{i,j}, & t \ge T_{i,j}, \end{cases} \tag{6.4}$$

we have

$$\dot{x}_i = A_{oi}x_i + \sum_{p=1}^{\nu_i} G_{i,p}f_{i,p}(y_i) + B_i\delta_i\bar{u}_i,\ y_i = C_ix_i, \tag{6.5}$$

where $\delta_i = \text{diag}\{\delta_{i,1}, \ldots, \delta_{i,q}\}$ and the signs of $\delta_{i,j}$ represent the actuation directions of actuators.

Remark 6.2.1. The agents in (6.1) are completely heterogeneous in the sense that, except for the input-output dimension, all other characteristics are allowed to be different. For example, for each follower, its relative degree ρ_i and order n_i can be different from those of other followers.

Remark 6.2.2. The actuator fault model in (6.3) covers partial loss of effectiveness ($0 < \bar{\delta}_{i,j} < 1$) and reverse faults ($-1 \leq \bar{\delta}_{i,j} < 0$). Reserve faults are not considered in most of existing fault-tolerant control schemes such as [62, 65, 67, 68, 75, 76], but they are prevalent in engineering systems including spacecraft [86], power systems [87] and vehicles [88]. Note that the fault directions in (6.3) are unknown and δ_i experiences jumps when actuator faults occur on the ith follower, which makes the control problem much more challenging.

A directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is used to characterize the communication network among the agents. The adjacency matrix $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{(N+M)\times(N+M)}$ of $\mathcal{G}$ is defined such that $a_{ii} = 0, a_{ij} = 1$ if $(j, i) \in \mathcal{E}$ and $a_{ij} = 0$ otherwise. The Laplacian matrix is denoted by $\mathcal{L} = [l_{ij}] \in \mathbb{R}^{(N+M)\times(N+M)}$, where $l_{ii} = \sum_{j=1,j\neq i}^{N+M} a_{ij}$ and $l_{ij} = -a_{ij}, \forall j \neq i$. The leaders have no in-neighbours, and $\mathcal{L}$ can be partitioned as

$$\mathcal{L} = \begin{bmatrix} \mathcal{L}_1 & \mathcal{L}_2 \\ 0_{M\times N} & 0_{M\times M} \end{bmatrix} \tag{6.6}$$

with $\mathcal{L}_1 \in \mathbb{R}^{N\times N}$ and $\mathcal{L}_2 \in \mathbb{R}^{N\times M}$. The following assumptions are made.

Assumption 6.2.1. The leading principal minors $\bar{\sigma}_{i,1}, \ldots, \bar{\sigma}_{i,q}$ of the CGM B_{i,m_i} are nonzero.

Assumption 6.2.2. For each of the N followers, there exists at least one leader that has a directed path to the follower.

Assumption 6.2.3. There exists a positive integer ρ known to all followers such that

$\rho \geq \rho_i, \forall i = 1, \ldots, N.$

Remark 6.2.3. In Assumption 6.2.1, both the magnitudes and the signs of $\bar{\sigma}_{i,1}, \ldots, \bar{\sigma}_{i,q}$ are allowed to be unknown. This assumption significantly relaxes the assumptions on the CGM made in existing distributed cooperative control schemes. In [68, 75, 76, 120, 121, 122, 123], the CGM is required to be exactly known or to be positive definite. As for [124], it requires the sign knowledge of $\bar{\sigma}_{i,1}, \ldots, \bar{\sigma}_{i,q}$ and continuous undirected communication among followers. Besides, the control scheme in [124] cannot handle actuator faults or guarantee global stability. Assumption 6.2.2 is a mild condition for containment control and can be widely found in the literature (see, e.g., [119] and [121]).

The trajectories of the leaders are denoted as $y_j(t) \in \mathbb{R}^q$ $(j = N+1, \ldots, N+M)$, where $y_j(t)$ and their derivatives up to the ρth order are bounded and piecewise continuous. The objective is to design a distributed control scheme such that all closed-loop signals are bounded, and the outputs of the followers move into the convex hull $Z(t)$ spanned by the leaders, where

$$Z(t) = \{ \sum_{j=N+1}^{N+M} \bar{g}_j y_j(t) \mid \bar{g}_j > 0, \sum_{j=N+1}^{N+M} \bar{g}_j = 1\}. \tag{6.7}$$

The following lemma will be used in our design and analysis.

Lemma 6.2.1. **[84]:** For all $i = 1, \ldots, N$ and $j = 1, \ldots, q$, given any nonzero constants $b_{i,j}$, the functions $\varsigma_j(\beta) = 2^{q-j} \sin(2^{j-1}\beta)$ satisfy

$$\text{sign}(b_{i,j})\varsigma_j(\beta) \leq 0, \text{ if } \beta \in [2h\pi + \bar{\varrho}_i, 2h\pi + \bar{\varrho}_i + 2^{-q}\pi], \tag{6.8}$$

and

$$\text{sign}(b_{i,j})\varsigma_j(\beta) \leq -1, \text{ if } \beta = 2h\pi + \bar{\varrho}_i + 2^{-q}\pi, \tag{6.9}$$

where $h = 1, 2, 3, \ldots$, and $\bar{\varrho}_i = \pi - 2^{-q}\pi + \sum_{j=1}^{q} 2^{-j} b_{i,j}\pi \geq 0$.

6.3 Controller Design

6.3.1 Auxiliary Filters and Event-Triggering Mechanism

Define $Y(t) = [y_{N+1}^{\mathrm{T}}(t), \ldots, y_{N+M}^{\mathrm{T}}(t)]^{\mathrm{T}}$ and

$$r(t) = [r_1^{\mathrm{T}}(t), \ldots, r_N^{\mathrm{T}}(t)]^{\mathrm{T}} = -(\mathcal{L}_1^{-1}\mathcal{L}_2 \otimes I_q)Y(t), \tag{6.10}$$

where $r_i(t) \in \mathbb{R}^q, i = 1, \ldots, N$, and $\otimes$ denotes the Kronecker product. As stated in [121], if Assumption 6.2.2 holds, then each row sum of $-\mathcal{L}_1^{-1}\mathcal{L}_2$ equals to one, and thus $r_i(t)$ belongs to $Z(t)$ in (6.7). We construct a network of N auxiliary filters, which utilizes local information and event-triggered communication to estimate r_i. The filter associated with the ith ($i = 1, \ldots, N$) follower is designed as

$$\dot{\eta}_{i,k} = \eta_{i,k+1}, \quad \dot{\eta}_{i,\rho} = \bar{v}_i, \quad k = 1, \ldots, \rho - 1, \tag{6.11}$$

where $\eta_{i,k} \in \mathbb{R}^q$ and $\eta_{i,\rho} \in \mathbb{R}^q$ are states of the filter, and $\bar{v}_i \in \mathbb{R}^q$ will be specified later. For the jth leader, let $\eta_{j,k} := y_j^{(k-1)}$, where $j = N+1, \ldots, N+M$ and $k = 1, \ldots, \rho$. Define $\varepsilon_i = \eta_{i,1} - r_i$ and $\bar{\varepsilon}_i = (\frac{d}{dt} + 1)^{\rho-1}\varepsilon_i = \sum_{k=0}^{\rho-1} \varrho_k \varepsilon_i^{(k)}$, where $\varrho_k = \frac{(\rho-1)!}{(\rho-1-k)!k!}$. Then, we have

$$\begin{aligned} \dot{\bar{\varepsilon}}_i &= \varepsilon_i^{(\rho)} + \sum_{k=0}^{\rho-2} \varrho_k \varepsilon_i^{(k+1)} \\ &= \bar{v}_i - \sum_{k=0}^{\rho-1} \varrho_k r_i^{(k+1)} + \sum_{k=0}^{\rho-2} \varrho_k \eta_{i,k+2}. \end{aligned} \tag{6.12}$$

Note that ε_i and $\bar{\varepsilon}_i$ will only be used for analysis. Further, for the jth agent ($j = 1, \ldots, N+M$), define $\psi_j = \sum_{k=0}^{\rho-1} \varrho_k \eta_{j,k+1}$. If the jth agent has out-neighbours, an event-triggering mechanism is introduced as follows:

$$t_{j,p+1} = \inf\left\{ t | t > t_{j,p}, ||\bar{\psi}_j(t)|| \geq \frac{\lambda_j}{\sigma} \right\}, \tag{6.13}$$

where $p = 0, 1, 2, \ldots, t_{j,0} := 0$, $\lambda_j > 0$ and $\sigma > 0$ are design parameters, and

$$\bar{\psi}_j(t) = \psi_j(t) - \psi_j(t_{j,p}), \quad \forall t \in [t_{j,p}, t_{j,p+1}). \tag{6.14}$$

For each $i = 1, \ldots, N$, $\bar{v}_i$ in (6.11) is designed as

$$\bar{v}_i = -\sigma \sum_{j=1}^{N+M} a_{ij}\Delta_{i,j} - \sum_{k=0}^{\rho-2} \varrho_k \eta_{i,k+2}, \tag{6.15}$$

where

$$\Delta_{i,j}(t) = \psi_i(t) - \psi_j(t_{j,p}), \quad \forall t \in [t_{j,p}, t_{j,p+1}). \tag{6.16}$$

Lemma 6.3.1. The auxiliary filters designed in (6.11) and (6.15) can ensure the boundedness of $\eta_{i,1}, \ldots, \eta_{i,\rho}$ and $\bar{v}_i$ and force $\eta_{i,1}$ to track r_i with the tracking error ε_i converging to a residual set which can be made arbitrarily small by increasing the design parameter σ. Moreover, Zeno behaviour is strictly precluded.

Proof. Define $\phi_i = \sum_{j=1}^{N+M} a_{ij}(\eta_{i,1} - \eta_{j,1})$, where $i = 1, \ldots, N$. Let $\phi = [\phi_1^{\mathrm{T}}, \ldots, \phi_N^{\mathrm{T}}]^{\mathrm{T}}$, $\varepsilon = [\varepsilon_1^{\mathrm{T}}, \ldots, \varepsilon_N^{\mathrm{T}}]^{\mathrm{T}}$, and $\eta_1 = [\eta_{1,1}^{\mathrm{T}}, \ldots, \eta_{N,1}^{\mathrm{T}}]^{\mathrm{T}}$. In view of (6.10), we have

$$\begin{aligned}\phi =& (\mathcal{L}_1 \otimes I_q)\eta_1 + (\mathcal{L}_2 \otimes I_q)Y \\ =& (\mathcal{L}_1 \otimes I_q)\left[\eta_1 + \left((\mathcal{L}_1^{-1}\mathcal{L}_2) \otimes I_q\right) Y\right] \\ =& (\mathcal{L}_1 \otimes I_q)\,\varepsilon.\end{aligned} \tag{6.17}$$

Define $\bar{\phi}_i = (\frac{d}{dt} + 1)^{\rho-1}\phi_i = \sum_{k=0}^{\rho-1} \varrho_k \phi_i^{(k)}$. Then, with $\bar{\phi} = [\bar{\phi}_1^{\mathrm{T}}, \ldots, \bar{\phi}_N^{\mathrm{T}}]^{\mathrm{T}}$ and $\bar{\varepsilon} = [\bar{\varepsilon}_1^{\mathrm{T}}, \ldots, \bar{\varepsilon}_N^{\mathrm{T}}]^{\mathrm{T}}$, we know $\bar{\phi}_i = \sum_{j=1}^{N+M} a_{ij}(\psi_i - \psi_j)$ and $\bar{\phi} = (\mathcal{L}_1 \otimes I_q)\bar{\varepsilon}$. Substituting (6.15) into (6.12) and noting (6.14), it can be checked that

$$\begin{aligned}\dot{\bar{\varepsilon}}_i =& -\sigma \sum_{j=1}^{N+M} a_{ij}\Delta_{i,j} - \sum_{k=0}^{\rho-1} \varrho_k r_i^{(k+1)} \\ =& -\sigma \sum_{j=1}^{N+M} a_{ij}(\psi_i - \psi_j) - \sigma \sum_{j=1}^{N+M} a_{ij}\bar{\psi}_j(t) - \sum_{k=0}^{\rho-1} \varrho_k r_i^{(k+1)} \\ =& -\sigma\bar{\phi}_i + \bar{R}_i,\end{aligned} \tag{6.18}$$

where $\bar{R}_i = -\sigma \sum_{j=1}^{N+M} a_{ij}\bar{\psi}_j(t) - \sum_{k=0}^{\rho-1} \varrho_k r_i^{(k+1)}$. It follows from (6.13) that $\| -\sigma \sum_{j=1}^{N+M} a_{ij}\bar{\psi}_j(t)\| \leq \sigma \sum_{j=1}^{N+M} a_{ij}\|\bar{\psi}_j(t)\| \leq \sum_{j=1}^{N+M} a_{ij}\lambda_j$. Subsequently, noting from (6.10) that $\sum_{k=0}^{\rho-1} \varrho_k r_i^{(k+1)}$ is bounded, we have

$$\|\bar{R}_i\| \leq \sum_{j=1}^{N+M} a_{ij}\lambda_j + \|\sum_{k=0}^{\rho-1} \varrho_k r_i^{(k+1)}\| \leq s_{i,1}, \tag{6.19}$$

where $s_{i,1} = \sum_{j=1}^{N+M} a_{ij}\lambda_j + \sup_{t\geq 0} \|\sum_{k=0}^{\rho-1} \varrho_k r_i^{(k+1)}(t)\|$ is a constant independent of the design parameter σ.

As stated in [121], under Assumption 6.2.2, there exists a positive diagonal matrix Q_1 such that $Q_2 = \mathcal{L}_1^{\mathrm{T}}Q_1 + Q_1\mathcal{L}_1$ is symmetric positive definite. Now, we consider the

following quadratic form:

$$V_0 = \frac{1}{2}\bar{\phi}^{\mathrm{T}}(Q_1 \otimes I_q)\bar{\phi}. \tag{6.20}$$

In view of (6.17) and (6.18), differentiating V_0 gives

$$\dot{V}_0 = -\frac{1}{2}\sigma\bar{\phi}^{\mathrm{T}}(Q_2 \otimes I_q)\bar{\phi} + \bar{\phi}^{\mathrm{T}}(Q_1 \otimes I_q)\mathcal{L}_1\bar{R}, \tag{6.21}$$

where $\bar{R} = [\bar{R}_1^{\mathrm{T}}, \ldots, \bar{R}_N^{\mathrm{T}}]^{\mathrm{T}}$. Using Young's inequality and (6.19), it can be checked that

$$\begin{aligned}\bar{\phi}^{\mathrm{T}}(Q_1 \otimes I_q)\mathcal{L}_1\bar{R} \leq & \frac{\sigma\lambda_{\min}(Q_2)}{4}\bar{\phi}^{\mathrm{T}}\bar{\phi} + \frac{\|(Q_1 \otimes I_q)\mathcal{L}_1\bar{R}\|^2}{\sigma\lambda_{\min}(Q_2)} \\ \leq & \frac{\sigma}{4}\bar{\phi}^{\mathrm{T}}(Q_2 \otimes I_q)\bar{\phi} + \frac{s_1}{\sigma},\end{aligned} \tag{6.22}$$

where $s_1 = \frac{\|(Q_1 \otimes I_q)\mathcal{L}_1\|^2}{\lambda_{\min}(Q_2)}\sum_{i=1}^{N} s_{i,1}^2$. Substituting (6.22) into (6.21) gives

$$\dot{V}_0 \leq -\frac{\sigma}{4}\bar{\phi}^{\mathrm{T}}(Q_2 \otimes I_q)\bar{\phi} + \frac{s_1}{\sigma} \leq -\frac{\sigma\lambda_{\min}(Q_2)}{2\lambda_{\max}(Q_1)}V_0 + \frac{s_1}{\sigma}. \tag{6.23}$$

Solving (6.23) yields

$$V_0(t) \leq \frac{2s_1\lambda_{\max}(Q_1)}{\sigma^2\lambda_{\min}(Q_2)} + \left[V_0(0) - \frac{2s_1\lambda_{\max}(Q_1)}{\sigma^2\lambda_{\min}(Q_2)}\right]e^{-\frac{\sigma\lambda_{\min}(Q_2)}{2\lambda_{\max}(Q_1)}t}, \tag{6.24}$$

which implies that V_0 and $\bar{\phi}$ are bounded. Then, noting the definition of $\bar{\phi}$, the boundedness of ε, $\eta_{i,1}, \ldots, \eta_{i,\rho}$ and $\bar{v}_i$ can be obtained. Moreover, it follows from (6.24) that $\lim_{t\to+\infty} V_0(t) \leq \frac{2s_1\lambda_{\max}(Q_1)}{\sigma^2\lambda_{\min}(Q_2)}$. Using (6.17) and (6.20), we can obtain $\lim_{t\to+\infty}\|\bar{\varepsilon}(t)\| \leq \sqrt{\frac{2\lim_{t\to+\infty}V_0(t)}{\lambda_{\min}(Q_3)}} \leq \frac{2\sqrt{s_1 s_2}}{\sigma}$, where $Q_3 = (\mathcal{L}_1^{\mathrm{T}} \otimes I_q)(Q_1 \otimes I_q)(\mathcal{L}_1 \otimes I_q)$ and $s_2 = \frac{\lambda_{\max}(Q_1)}{\lambda_{\min}(Q_2)\lambda_{\min}(Q_3)}$. Noting $\lim_{t\to+\infty}||\varepsilon_i(t)|| \leq \lim_{t\to+\infty}\|\bar{\varepsilon}(t)\| \leq \frac{2\sqrt{s_1 s_2}}{\sigma}$, it can be concluded that the errors ε_i $(i = 1, \ldots, N)$ converge to a residual set which can be made arbitrarily small by increasing the design parameter σ.

Next, we prove that Zeno behaviour can be strictly precluded. Define $F_j(t) = \bar{\psi}_j^{\mathrm{T}}(t)\bar{\psi}_j(t)$. From the boundedness of $\eta_{j,1}, \ldots, \eta_{j,\rho}$ and $\bar{v}_j$, it can be checked that $\bar{\psi}_j$ and $\dot{\psi}_j$ are bounded. As a result, there exists a constant ι_j such that

$$|\dot{F}_j(t)| = |2\bar{\psi}_j^{\mathrm{T}}(t)\dot{\psi}_j(t)| \leq \iota_j, \ \forall t \in (t_{j,p}, t_{j,p+1}). \tag{6.25}$$

On the other hand, according to (6.13), we have

$$F_j(t_{j,p}) = 0, \quad \lim_{t\to t_{j,q+1}^-} F_j(t) = \frac{\lambda_j^2}{\sigma^2}, \tag{6.26}$$

which together (6.25) with gives $t_{j,p+1} - t_{j,p} \geq (\lambda_j^2/\sigma^2\iota_j)$. Hence, Zeno behaviour is strictly precluded. This completes the proof. ■

Remark 6.3.1. The event-triggering mechanism in (6.13) avoids continuous communication among agents and reduces the communication burden. Meanwhile, the above design is fully distributed because each agent uses the states of its own filter to decide the triggering time instants. The estimation of r_i, *i.e.*, $\eta_{i,1}$, is always available to the ith follower, which allows us to solve the containment control problem by forcing y_i to track $\eta_{i,1}$.

6.3.2 Nussbaum Function and K-filters

To handle the unknown direction actuator faults and the unknown signs of the leading principal minors of the CGM, we introduce a group of Nussbaum functions as follows:

$$\begin{aligned} H_j(\beta) &= 2^{q-j}(2\beta^2+1)e^{\beta^2}\sin(2^{j-1}\beta) \\ &\quad +2^{q-1}\beta e^{\beta^2}\cos(2^{j-1}\beta),\ j=1,\ldots,q. \end{aligned} \tag{6.27}$$

It can be shown that

$$\int_0^\beta H_j(\kappa)d\kappa = \varsigma_j(\beta)\beta e^{\beta^2}, \tag{6.28}$$

where $\varsigma_j(\beta)$ is given in Lemma 6.2.1. These Nussbaum functions will be applied in the controller design.

The unmeasured states of each follower are estimated by K-filters. Let $K_{ci} := [\bar{k}_{i,1}I_q,\ldots,\bar{k}_{i,n_i}I_q]^{\mathrm{T}}$, where $\bar{k}_{i,j} > 0, j = 1,\ldots,n_i$, are chosen such that the matrix $A_{ci} = A_{oi} - K_{ci}C_i$ is Hurwitz. Define $E_{i,j} = \bar{e}_{i,j} \otimes I_q$, where $\bar{e}_{i,j}$ is the jth coordinate vector in $\mathbb{R}^{n_i}$. For the ith follower, we introduce the following K-filters:

$$\dot{\omega}_{i,0} = A_{ci}\omega_{i,0} + K_{ci}y_i, \tag{6.29}$$

$$\dot{\omega}_{i,p} = A_{ci}\omega_{i,p} + f_{i,p}(y_i), \quad p=1,\ldots,\nu_i, \tag{6.30}$$

$$\dot{\xi}_i = A_{ci}\xi_i + E_{i,n_i}\bar{u}_i. \tag{6.31}$$

Furthermore, define $\zeta_{i,j} = A_{ci}^j\xi_i$, $j = 0,\ldots,m_i$. Considering $A_{ci}^jE_{i,n_i} = E_{i,n_i-j}$, we can obtain

$$\dot{\zeta}_{i,j} = A_{ci}\zeta_{i,j} + E_{n_i-j}\bar{u}_i, \quad j=0,\ldots,m_i. \tag{6.32}$$

Based on the above signals, the estimation of the ith follower's state can be parametrised as

$$\hat{x}_i = \omega_{i,0} + \sum_{p=1}^{\nu_i} A_{i,p}\omega_{i,p} + \sum_{j=0}^{m_i} B_{i,j}\delta_i\zeta_{i,j}. \tag{6.33}$$

Let the time instants at which the ith follower suffers from new actuator faults be denoted as $\bar{T}_{i,1}, \bar{T}_{i,2}, \ldots, \bar{T}_{i,\bar{n}_i}$. Obviously, $\bar{n}_i \leq q$ and $\bar{T}_{i,\bar{n}_i}$ is finite. Define $\bar{T}_{i,0} = 0$ and $\bar{T}_{i,\bar{n}_i+1} = +\infty$. Note that, for each $j = 0, \ldots, \bar{n}_i$, δ_i is a constant during the time interval $(\bar{T}_{i,j}, \bar{T}_{i,j+1})$. With this fact in mind, it can be checked that the state estimation error $\epsilon_i = x_i - \hat{x}_i$ satisfies

$$\dot{\epsilon}_i = A_{ci}\epsilon_i, \qquad \forall t \in \bigcup_{j=0}^{\bar{n}_i}(\bar{T}_{i,j}, \bar{T}_{i,j+1}). \tag{6.34}$$

Let $\omega_{i,0}$, $\omega_{i,p}$, ξ_i, $\zeta_{i,j}$ and ϵ_i be partitioned as $\omega_{i,0} = [\omega_{i,0,1}^{\mathrm{T}}, \cdots, \omega_{i,0,n_i}^{\mathrm{T}}]^{\mathrm{T}}$, $\omega_{i,p} = [\omega_{i,p,1}^{\mathrm{T}}, \cdots, \omega_{i,p,n_i}^{\mathrm{T}}]^{\mathrm{T}}$, $\xi_i = [\xi_{i,1}^{\mathrm{T}}, \cdots, \xi_{i,n_i}^{\mathrm{T}}]^{\mathrm{T}}$, $\zeta_{i,j} = [\zeta_{i,j,1}^{\mathrm{T}}, \cdots, \zeta_{i,j,n_i}^{\mathrm{T}}]^{\mathrm{T}}$, and $\epsilon_i = [\epsilon_{i,1}^{\mathrm{T}}, \cdots, \epsilon_{i,n_i}^{\mathrm{T}}]^{\mathrm{T}}$, with $\omega_{i,0,k} \in \mathbb{R}^q$, $\omega_{i,p,k} \in \mathbb{R}^q$, $\xi_{i,k} \in \mathbb{R}^q$, $\zeta_{i,j,k} \in \mathbb{R}^q$ and $\epsilon_{i,k} \in \mathbb{R}^q$. Then, taking (6.5) and (6.33) into consideration, the derivative of y_i can be expressed as

$$\begin{aligned} \dot{y}_i &= x_{i,2} + \sum_{p=1}^{\nu_i} A_{i,p} f_{i,p,1}(y_i) \\ &= \omega_{i,0,2} + \sum_{p=1}^{\nu_i} A_{i,p}[f_{i,p,1}(y_i) + \omega_{i,p,2}] + \sum_{j=0}^{m_i} B_{i,j}\delta_i\zeta_{i,j,2} + \epsilon_{i,2}. \end{aligned} \tag{6.35}$$

6.3.3 Backstepping Design Procedure

In what follows, we aim at forcing y_i to track $\eta_{i,1}$ generated in Section 6.3.1. For each follower, we begin by defining

$$z_{i,1} = y_i - \eta_{i,1}, \;\; z_{i,j} = \zeta_{i,m_i,j} - \alpha_{i,j-1}, \quad j = 2, \ldots, \rho_i, \tag{6.36}$$

where $\alpha_{i,j-1}$ is a stabilizing function to be designed at the $(j-1)$th step. Let the kth element of $z_{i,j}$ be denoted as $z_{i,j,k}$, and

$$\alpha_{i,\rho_i} := \bar{u}_i + \zeta_{i,m_i,\rho_i+1}, \quad z_{i,\rho_i+1} := 0. \tag{6.37}$$

Introducing positive scalars $c_{i,j}$, $\gamma_{i,j}$ $(j = 1, \ldots, \rho_i)$, $\bar{\gamma}_{i,k}$ $(k = 1, \ldots, q)$, g_i and symmetric positive definite matrices $\Xi_{i,k} \in \mathbb{R}^{\bar{q}_i \times \bar{q}_i}$, $\Lambda_{i,k} \in \mathbb{R}^{\bar{q}_i \times \bar{q}_i}$, $\Gamma_{i,h} \in \mathbb{R}^{(q-h)\times(q-h)}$ $(h =$

$1, \ldots, q-1)$ with $\bar{q}_i := q(\nu_i + m_i + 1)$ as design parameters, the backstepping design procedure for the ith follower includes ρ_i steps.

Step 1: Based on (6.35) and (6.36), we have

$$\begin{aligned}\dot{z}_{i,1} &= -\gamma_{i,1} z_{i,1} + B_{i,m_i}\delta_i(z_{i,2} + \alpha_{i,1}) + \varpi_{i,1} + \epsilon_{i,2} + \sum_{j=0}^{m_i-1} B_{i,j}\delta_i\zeta_{i,j,2} \\ &\quad + \sum_{p=1}^{\nu_i} A_{i,p}\big(f_{i,p,1}(y_i) + \omega_{i,p,2}\big), \end{aligned} \tag{6.38}$$

where $\varpi_{i,1} = \gamma_{i,1} z_{i,1} + \omega_{i,0,2} - \eta_{i,2}$. From [125], if Assumption 6.2.1 holds, then B_{i,m_i} can be factored as $B_{i,m_i} = S_i D_i U_i$, where $S_i \in \mathbb{R}^{q\times q}$ is symmetric positive definite, $U_i \in \mathbb{R}^{q\times q}$ is unity upper triangular, and $D_i = \mathrm{diag}\{d_{i,1}, \ldots, d_{i,q}\} = \mathrm{diag}\{\mathrm{sign}(\bar{\sigma}_{i,1}), \mathrm{sign}(\bar{\sigma}_{i,2}\bar{\sigma}_{i,1}^{-1}), \ldots, \mathrm{sign}(\bar{\sigma}_{i,q}\bar{\sigma}_{i,q-1}^{-1})\}$. Applying this factorization and multiplying both sides of (6.38) by S_i^{-1}, it gives

$$S_i^{-1}\dot{z}_{i,1} = -\gamma_{i,1} S_i^{-1} z_{i,1} + D_i U_i \delta_i(z_{i,2} + \alpha_{i,1}) + \Theta_i \mu_{i,1} + S_i^{-1}\epsilon_{i,2}, \tag{6.39}$$

where $\Theta_i = [S_i^{-1}, S_i A_{i,\nu_i}, \ldots, S_i^{-1}A_{i,1}, S_i^{-1}B_{i,m_i-1}\delta_i, \ldots, S_i^{-1}B_{i,0}\delta_i] \in \mathbb{R}^{q\times\bar{q}_i}$, and $\mu_{i,1} = [\varpi_{i,1}^{\mathrm{T}}, f_{i,\nu_i,1}^{\mathrm{T}}(y_i) + \omega_{i,\nu_i,2}^{\mathrm{T}}, \ldots, f_{i,1,1}^{\mathrm{T}}(y_i) + \omega_{i,1,2}^{\mathrm{T}}, \zeta_{i,m_i-1,2}^{\mathrm{T}}, \ldots, \zeta_{i,0,2}^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{R}^{\bar{q}_i}$. Then, to handle the unknown actuator faults, we introduce the following similarity transformation:

$$W_i(t) = \delta_i^{-1}(t) U_i \delta_i(t). \tag{6.40}$$

It can be readily checked that W_i is also unity upper triangular, and $U_i\delta_i = \delta_i W_i$. It follows from (6.39) and (6.40) that

$$\begin{aligned} S_i^{-1}\dot{z}_{i,1} &= -\gamma_{i,1} S_i^{-1} z_{i,1} + D_i U_i \delta_i z_{i,2} + D_i\delta_i\alpha_{i,1} + D_i\delta_i[W_i(t) - I_q]\alpha_{i,1} \\ &\quad + \Theta_i\mu_{i,1} + S_i^{-1}\epsilon_{i,2}. \end{aligned} \tag{6.41}$$

Besides, we have

$$D_i\delta_i[W_i(t) - I_q]\alpha_{i,1} = [\theta_{i,1}^{\mathrm{T}} X_{i,1}, \ldots, \theta_{i,q-1}^{\mathrm{T}} X_{i,q-1}, 0]^{\mathrm{T}}, \tag{6.42}$$

where $\theta_{i,j} = d_{i,j}\delta_{i,j}[W_{i,j,j+1}, \ldots, W_{i,j,q}]^{\mathrm{T}} \in \mathbb{R}^{q-j}$ and $X_{i,j} = [\alpha_{i,1,j+1}, \ldots, \alpha_{i,1,q}]^{\mathrm{T}} \in \mathbb{R}^{q-j}$ $(j = 1, \ldots, q-1)$ with $W_{i,j,k}$ being the (j,k)th element of W_i and $\alpha_{i,1,k}$ being the kth element $\alpha_{i,1}$. Define $\varphi_i = \|D_i U_i \delta_i\|^2$, and let the jth column of Θ_i^{T} be

denoted as $\Theta_{i,j}$. Then, we consider the quadratic form

$$\begin{aligned} V_{i,1} &= \frac{1}{2}z_{i,1}^{\mathrm{T}}S_i^{-1}z_{i,1} + \frac{1}{2g_i}\tilde{\varphi}_i^2 + \frac{1}{2}\sum_{j=1}^{q}\tilde{\Theta}_{i,j}^{\mathrm{T}}\Xi_{i,j}^{-1}\tilde{\Theta}_{i,j} + \frac{1}{2}\sum_{j=1}^{q-1}\tilde{\theta}_{i,j}^{\mathrm{T}}\Gamma_{i,j}^{-1}\tilde{\theta}_{i,j} \\ &\quad + \frac{1}{4\gamma_{i,1}}\epsilon_i^{\mathrm{T}}P_{i,1}\epsilon_i, \end{aligned} \tag{6.43}$$

where $P_{i,1}$ is a positive definite matrix that satisfies $A_{ci}^{\mathrm{T}}P_{i,1}+P_{i,1}A_{ci} = -\operatorname{diag}\{S_i^{-1},\ldots,S_i^{-1}\}$, $\tilde{\varphi}_i := \hat{\varphi}_i - \varphi_i$, $\tilde{\Theta}_{i,j} := \hat{\Theta}_{i,j} - \Theta_{i,j}$, and $\tilde{\theta}_{i,j} := \hat{\theta}_{i,j} - \theta_{i,j}$ with $\hat{\varphi}_i, \hat{\Theta}_{i,j}$ and $\hat{\theta}_{i,j}$ the estimations of $\varphi_i, \Theta_{i,j}$ and $\theta_{i,j}$, respectively. Note that, for each $j = 0,\ldots,\bar{n}_i$, $V_{i,1}$ has no jump during the time interval $(\bar{T}_{i,j}, \bar{T}_{i,j+1})$. Differentiating (6.43) and noting (6.41) and (6.42), we have

$$\begin{aligned} \dot{V}_{i,1} &= -\gamma_{i,1}z_{i,1}^{\mathrm{T}}S_i^{-1}z_{i,1} + z_{i,1}^{\mathrm{T}}D_iU_i\delta_iz_{i,2} + z_{i,1}^{\mathrm{T}}D_i\delta_i\alpha_{i,1} + \sum_{j=1}^{q-1}z_{i,1,j}\theta_{i,j}^{\mathrm{T}}X_{i,j} \\ &\quad + \sum_{j=1}^{q}z_{i,1,j}\Theta_{i,j}^{\mathrm{T}}\mu_{i,1} + z_{i,1}^{\mathrm{T}}S_i^{-1}\epsilon_{i,2} + \frac{1}{g_i}\tilde{\varphi}_i\dot{\hat{\varphi}}_i + \sum_{j=1}^{q}\tilde{\Theta}_{i,j}^{\mathrm{T}}\Xi_{i,j}^{-1}\dot{\hat{\Theta}}_{i,j} + \sum_{j=1}^{q-1}\tilde{\theta}_{i,j}^{\mathrm{T}}\Gamma_{i,j}^{-1}\dot{\hat{\theta}}_{i,j} \\ &\quad - \sum_{j=1}^{n_i}\frac{1}{4\gamma_{i,1}}\epsilon_{i,j}^{\mathrm{T}}S_i^{-1}\epsilon_{i,j}, \quad \forall t \in \bigcup_{j=0}^{\bar{n}_i}(\bar{T}_{i,j}, \bar{T}_{i,j+1}). \end{aligned} \tag{6.44}$$

It can be checked that

$$z_{i,1}^{\mathrm{T}}D_iU_i\delta_iz_{i,2} \le \varphi_iz_{i,1}^{\mathrm{T}}z_{i,1} + \frac{1}{4}z_{i,2}^{\mathrm{T}}z_{i,2}, \tag{6.45}$$

$$z_{i,1}^{\mathrm{T}}S_i^{-1}\epsilon_{i,2} \le \gamma_{i,1}z_{i,1}^{\mathrm{T}}S_i^{-1}z_{i,1} + \frac{1}{4\gamma_{i,1}}\epsilon_{i,2}^{\mathrm{T}}S_i^{-1}\epsilon_{i,2}. \tag{6.46}$$

Let

$$\dot{\hat{\varphi}}_i = g_iz_{i,1}^{\mathrm{T}}z_{i,1},\ \dot{\hat{\Theta}}_{i,j} = \Xi_{i,j}\mu_{i,1}z_{i,1,j},\ j = 1,\ldots,q, \tag{6.47}$$

$$\dot{\hat{\theta}}_{i,j} = \Gamma_{i,j}X_{i,j}z_{i,1,j},\ j = 1,\ldots,q-1. \tag{6.48}$$

Substituting (6.45)-(6.48) into (6.44) gives

$$\begin{aligned} \dot{V}_{i,1} &\le -c_{i,1}z_{i,1}^{\mathrm{T}}z_{i,1} + \frac{1}{4}z_{i,2}^{\mathrm{T}}z_{i,2} + \sum_{j=1}^{q}z_{i,1,j}d_{i,j}\delta_{i,j}\alpha_{i,1,j} \\ &\quad - \sum_{j=1}^{q}z_{i,1,j}\bar{\alpha}_{i,1,j}, \qquad \forall t \in \bigcup_{j=0}^{\bar{n}_i}(\bar{T}_{i,j}, \bar{T}_{i,j+1}), \end{aligned} \tag{6.49}$$

where, for $j = 1,\ldots,q-1$,

$$\bar{\alpha}_{i,1,j} = -c_{i,1}z_{i,1,j} - \hat{\varphi}_iz_{i,1,j} - \hat{\Theta}_{i,j}^{\mathrm{T}}\mu_{i,1} - \hat{\theta}_{i,j}^{\mathrm{T}}X_{i,j}, \tag{6.50}$$

and

$$\bar{\alpha}_{i,1,q} = -c_{i,1}z_{i,1,q} - \hat{\varphi}_i z_{i,1,q} - \hat{\Theta}_{i,q}^{\mathrm{T}}\mu_{i,1}. \tag{6.51}$$

With the Nussbaum functions defined in (6.27), we design the jth element of the stabilizing function $\alpha_{i,1}$ as

$$\alpha_{i,1,j} = H_j(\beta_{i,j})\bar{\alpha}_{i,1,j}, \quad j = 1, \ldots, q, \tag{6.52}$$

where $\beta_{i,j}$ is generated by

$$\dot{\beta}_{i,j} = \bar{\gamma}_{i,j} z_{i,1,j}\bar{\alpha}_{i,1,j}. \tag{6.53}$$

Substituting (6.52) and (6.53) into (6.49) yields

$$\dot{V}_{i,1} \leq -c_{i,1}z_{i,1}^{\mathrm{T}}z_{i,1} + \frac{1}{4}z_{i,2}^{\mathrm{T}}z_{i,2} + \sum_{j=1}^{q}\frac{\dot{\beta}_{i,j}}{\bar{\gamma}_{i,j}}[d_{i,j}\delta_{i,j}H_j(\beta_{i,j}) - 1], \ \forall t \in \bigcup_{j=0}^{\bar{n}_i}(\bar{T}_{i,j}, \bar{T}_{i,j+1}). \tag{6.54}$$

Remark 6.3.2. In existing adaptive control schemes for single MIMO systems, when the factorization $B_{i,m_i} = S_i D_i U_i$ is applied to the CGM, the decomposition $U_i\alpha_{i,1} = \alpha_{i,1} + (U_i - I_q)\alpha_{i,1}$ is commonly used to avoid algebraic loops; see, e.g., [84] and [125]. However, this technique is no longer valid in this chapter, because, as can be seen from (6.39), the actuator faults bring in the unknown time-varying parameter matrix δ_i between U_i and $\alpha_{i,1}$. To overcome this difficulty, we introduce the similarity transformation in (6.40) and replace $U_i\delta_i$ by $\delta_i W_i$, where W_i is unity upper triangular. Then, we introduce the decomposition $W_i\alpha_{i,1} = \alpha_{i,1} + (W_i - I_q)\alpha_{i,1}$ to ensure that no algebraic loops exist in (6.50) and (6.51).

Step 2: It is noted that $\alpha_{i,1,q}$ is a smooth function of y_i and $\Psi_{i,1} = [\eta_{i,1}^{\mathrm{T}}, \eta_{i,2}^{\mathrm{T}}, \beta_{i,1}, \ldots, \beta_{i,q}, \hat{\theta}_{i,1}^{\mathrm{T}}, \ldots, \hat{\theta}_{i,q-1}^{\mathrm{T}}, \hat{\Theta}_{i,1}^{\mathrm{T}}, \ldots, \hat{\Theta}_{i,q}^{\mathrm{T}}, \hat{\varphi}_i, \omega_{i,0}^{\mathrm{T}}, \omega_{i,1}^{\mathrm{T}}, \ldots, \omega_{i,\nu_i}^{\mathrm{T}}, \xi_{i,1}^{\mathrm{T}}, \ldots, \xi_{i,m_i+1}^{\mathrm{T}}]^{\mathrm{T}}$, while $\alpha_{i,1,j}$, for $j = 1, \ldots, q-1$, is a smooth function of $\alpha_{i,1,j+1}, \ldots, \alpha_{i,1,q}, y_i$ and $\Psi_{i,1}$. Thus, $\alpha_{i,1}$ is in fact a smooth function of y_i and $\Psi_{i,1}$. With this fact in mind and using (6.32), (6.35) and (6.36), the derivative of $z_{i,2} = \zeta_{i,m_i,2} - \alpha_{i,1}$ can be expressed as

$$\dot{z}_{i,2} = z_{i,3} + \alpha_{i,2} - \varpi_{i,2} + \frac{\partial\alpha_{i,1}}{\partial y_i}\Omega_i\mu_{i,2} - \frac{\partial\alpha_{i,1}}{\partial y_i}\epsilon_{i,2}, \tag{6.55}$$

where $\varpi_{i,2} = \bar{k}_{i,2}\zeta_{i,m_i,1} + \frac{\partial\alpha_{i,1}}{\partial y_i}\omega_{i,0,2} + \frac{\partial\alpha_{i,1}}{\partial\Psi_{i,1}}\dot{\Psi}_{i,1}$, $\Omega_i = [-A_{i,\nu_i}, \ldots, -A_{i,1}, -B_{i,m_i}\delta_i, \ldots, -B_{i,0}\delta_i] \in \mathbb{R}^{q\times\bar{q}_i}$, and $\mu_{i,2} = [f_{i,\nu_i,1}^{\mathrm{T}}(y_i) + \omega_{i,\nu_i,2}^{\mathrm{T}}, \ldots, f_{i,1,1}^{\mathrm{T}}(y_i) + \omega_{i,1,2}^{\mathrm{T}}, \zeta_{i,m_i,2}^{\mathrm{T}}, \ldots, \zeta_{i,0,2}^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{R}^{\bar{q}_i}$. Let

$\hat{\Omega}_i$ be the estimation of Ω_i, where the jth columns of $\hat{\Omega}_i^{\mathrm{T}}$ and Ω_i^{T} are denoted as $\hat{\Omega}_{i,j}$ and $\Omega_{i,j}$, respectively. Define

$$V_{i,2} = V_{i,1} + \frac{1}{2} z_{i,2}^{\mathrm{T}} z_{i,2} + \frac{1}{2} \sum_{j=1}^{q} \tilde{\Omega}_{i,j}^{\mathrm{T}} \Lambda_{i,j}^{-1} \tilde{\Omega}_{i,j} + \frac{1}{4\gamma_{i,2}} \epsilon_i^{\mathrm{T}} P_{i,2} \epsilon_i, \tag{6.56}$$

where $P_{i,2}$ is a symmetric positive definite matrix that satisfies $A_{ci}^{\mathrm{T}} P_{i,2} + P_{i,2} A_{ci} = -I_{qn_i}$. It can be checked that

$$\begin{aligned} \dot{V}_{i,2} \leq & - c_{i,1} z_{i,1}^{\mathrm{T}} z_{i,1} + \sum_{j=1}^{q} \frac{\dot{\beta}_{i,j}}{\bar{\gamma}_{i,j}} [d_{i,j} \delta_{i,j} H_j(\beta_{i,j}) - 1] + z_{i,2}^{\mathrm{T}} \Big[\frac{1}{4} z_{i,2} + z_{i,3} + \alpha_{i,2} - \varpi_{i,2} \\ & + \frac{\partial \alpha_{i,1}}{\partial y_i} \hat{\Omega}_i \mu_{i,2} + \gamma_{i,2} \frac{\partial \alpha_{i,1}}{\partial y_i} (\frac{\partial \alpha_{i,1}}{\partial y_i})^{\mathrm{T}} z_{i,2} \Big] \\ & + \sum_{j=1}^{q} \tilde{\Omega}_{i,j}^{\mathrm{T}} \Lambda_{i,j}^{-1} (\dot{\hat{\Omega}}_{i,j} - \tau_{i,1,j}), \ \forall t \in \bigcup_{j=0}^{\bar{n}_i} (\bar{T}_{i,j}, \bar{T}_{i,j+1}) \end{aligned} \tag{6.57}$$

with $\tau_{i,1,j} = \sum_{k=1}^{q} \Lambda_{i,j} \mu_{i,2} \frac{\partial \alpha_{i,1,k}}{\partial y_{i,j}} z_{i,2,k}$. Note that $\frac{\partial \alpha_{i,1,k}}{\partial y_{i,j}}$ is the (k,j)th element of $\frac{\partial \alpha_{i,1}}{\partial y_i}$. Design the second stabilizing function as

$$\alpha_{i,2} = - c_{i,2} z_{i,2} - \frac{1}{4} z_{i,2} + \varpi_{i,2} - \frac{\partial \alpha_{i,1}}{\partial y_i} \hat{\Omega}_i \mu_{i,2} - \gamma_{i,2} \frac{\partial \alpha_{i,1}}{\partial y_i} (\frac{\partial \alpha_{i,1}}{\partial y_i})^{\mathrm{T}} z_{i,2}. \tag{6.58}$$

Then, (6.57) becomes

$$\begin{aligned} \dot{V}_{i,2} \leq & - \sum_{j=1}^{2} c_{i,j} z_{i,j}^{\mathrm{T}} z_{i,j} + \sum_{j=1}^{q} \frac{\dot{\beta}_{i,j}}{\bar{\gamma}_{i,j}} [d_{i,j} \delta_{i,j} H_j(\beta_{i,j}) - 1] + z_{i,2}^{\mathrm{T}} z_{i,3} \\ & + \sum_{j=1}^{q} \tilde{\Omega}_{i,j}^{\mathrm{T}} \Lambda_{i,j}^{-1} (\dot{\hat{\Omega}}_{i,j} - \tau_{i,1,j}), \ \forall t \in \bigcup_{j=0}^{\bar{n}_i} (\bar{T}_{i,j}, \bar{T}_{i,j+1}). \end{aligned} \tag{6.59}$$

Step h ($h = 3, \ldots, \rho_i$): Recall that $\alpha_{i,h-1}$ is a smooth function of y_i, $\hat{\Omega}_{i,1}, \ldots, \hat{\Omega}_{i,q}$ and $\Psi_{i,h-1} = [\eta_{i,1}^{\mathrm{T}}, \ldots, \eta_{i,h}^{\mathrm{T}}, \beta_{i,1}, \ldots, \beta_{i,q}, \hat{\theta}_{i,1}^{\mathrm{T}}, \ldots, \hat{\theta}_{i,q-1}^{\mathrm{T}}, \hat{\Theta}_{i,1}^{\mathrm{T}}, \ldots, \hat{\Theta}_{i,q}^{\mathrm{T}}, \hat{\varphi}_i, \ \omega_{i,0}^{\mathrm{T}}, \ldots, \omega_{i,\nu_i}^{\mathrm{T}}, \xi_{i,1}^{\mathrm{T}}, \ldots, \xi_{i,m_i+h-1}^{\mathrm{T}}]^{\mathrm{T}}$. The derivative of $z_{i,h} = \zeta_{i,m_i,h} - \alpha_{i,h-1}$ can be formulated as $\dot{z}_{i,h} = z_{i,h+1} + \alpha_{i,h} - \varpi_{i,h} + \frac{\partial \alpha_{i,h-1}}{\partial y_i} \Omega_i \mu_{i,2} - \frac{\partial \alpha_{i,h-1}}{\partial y_i} \epsilon_{i,2} - \sum_{j=1}^{q} \frac{\partial \alpha_{i,h-1}}{\partial \hat{\Omega}_{i,j}} \dot{\hat{\Omega}}_{i,j}$, where $\varpi_{i,h} = \bar{k}_{i,h} \zeta_{i,m_i,1} + \frac{\partial \alpha_{i,h-1}}{\partial y_i} \omega_{i,0,2} + \frac{\partial \alpha_{i,h-1}}{\partial \Psi_{i,h-1}} \dot{\Psi}_{i,h-1}$. Define

$$V_{i,h} = V_{i,h-1} + \frac{1}{2} z_{i,h}^{\mathrm{T}} z_{i,h} + \frac{1}{4\gamma_{i,h}} \epsilon_i^{\mathrm{T}} P_{i,2} \epsilon_i, \tag{6.60}$$

and $\bar{\zeta}_{i,h} = [\bar{\zeta}_{i,h,1}, \ldots, \bar{\zeta}_{i,h,q}]^{\mathrm{T}}$, where, for $k = 1, \ldots, q$,

$$\bar{\zeta}_{i,h,k} = \begin{cases} 0, & \text{if } h = 3, \\ \sum_{j=1}^{q} \sum_{p=3}^{h-1} z_{i,p}^{\mathrm{T}} \frac{\partial \alpha_{i,p-1}}{\partial \hat{\Omega}_{i,j}} \Lambda_{i,j} \mu_{i,2} \frac{\partial \alpha_{i,h-1,k}}{\partial y_{i,j}}, & \text{if } h > 3. \end{cases} \tag{6.61}$$

Choose $\tau_{i,h-1,j} = \tau_{i,h-2,j} + \sum_{k=1}^{q} \Lambda_{i,j}\mu_{i,2}\frac{\partial \alpha_{i,h-1,k}}{\partial y_{i,j}} z_{i,h,k}$ and

$$\begin{aligned}\alpha_{i,h} =& - c_{i,h}z_{i,h} - z_{i,h-1} + \varpi_{i,h} - \frac{\partial \alpha_{i,h-1}}{\partial y_i}\hat{\Omega}_i\mu_{i,2} - \gamma_{i,h}\frac{\partial \alpha_{i,h-1}}{\partial y_i}(\frac{\partial \alpha_{i,h-1}}{\partial y_i})^{\mathrm{T}} z_{i,h} \\ &+ \sum_{j=1}^{q} \frac{\partial \alpha_{i,h-1}}{\partial \hat{\Omega}_{i,j}}\tau_{i,h-1,j} + \bar{\zeta}_{i,h}. \end{aligned} \tag{6.62}$$

Then, for all $t \in \bigcup_{j=0}^{\bar{n}_i}(\bar{T}_{i,j}, \bar{T}_{i,j+1})$, it can be checked that

$$\begin{aligned}\dot{V}_{i,h} \leq& - \sum_{j=1}^{h} c_{i,j}z_{i,j}^{\mathrm{T}}z_{i,j} + \sum_{j=1}^{q} \frac{\dot{\beta}_{i,j}}{\bar{\gamma}_{i,j}}[d_{i,j}\delta_{i,j}H_j(\beta_{i,j}) - 1] + z_{i,h}^{\mathrm{T}}z_{i,h+1} \\ &+ \sum_{j=1}^{q} \tilde{\Omega}_{i,j}^{\mathrm{T}}\Lambda_{i,j}^{-1}(\dot{\hat{\Omega}}_{i,j} - \tau_{i,h-1,j}) + \sum_{j=1}^{q}\sum_{p=3}^{h} z_{i,p}^{\mathrm{T}}\frac{\partial \alpha_{i,p-1}}{\partial \hat{\Omega}_{i,j}}(\tau_{i,h-1,j} - \dot{\hat{\Omega}}_{i,j}). \end{aligned} \tag{6.63}$$

At Step ρ_i, design the adaptive law for $\hat{\Omega}_{i,j}$ as

$$\dot{\hat{\Omega}}_{i,j} = \tau_{i,\rho_i-1,j}, \quad j = 1, \ldots, q. \tag{6.64}$$

Recalling (6.37), the control signal $\bar{u}_i$ is given by

$$\bar{u}_i = \alpha_{i,\rho_i} - \zeta_{i,m_i,\rho_i+1}. \tag{6.65}$$

In (6.63), after setting $h = \rho_i$, for all $t \in \bigcup_{j=0}^{\bar{n}_i}(\bar{T}_{i,j}, \bar{T}_{i,j+1})$ we have

$$\dot{V}_{i,\rho_i} + \sum_{j=1}^{\rho_i} c_{i,j}z_{i,j}^{\mathrm{T}}z_{i,j} \leq \sum_{j=1}^{q} \frac{\dot{\beta}_{i,j}}{\bar{\gamma}_{i,j}}[d_{i,j}\delta_{i,j}H_j(\beta_{i,j}) - 1]. \tag{6.66}$$

Based on (6.66), we can establish the stability of the closed-loop system, as will be shown in the next section. The structure of our control scheme is summarised in Figure 6.1.

Remark 6.3.3. Different from existing control schemes handling unknown control directions (see, e.g., [63, 64, 67, 88, 84] and [118]), in the state estimation and each step of the backstepping design procedure, we have to face unknown jumps caused by the actuator faults. These jumps are inherent in $\delta_{i,j}, \epsilon_i, V_{i,1}, \ldots, V_{i,\rho_i}$ and prevent (6.66) being valid for all $t \geq 0$. Moreover, the sum $\sum_{j=1}^{q} \frac{\dot{\beta}_{i,j}}{\bar{\gamma}_{i,j}} d_{i,j}\delta_{i,j}H_j(\beta_{i,j})$ in (6.66) not only involves multiple Nussbaum functions in each agent, but also suffers from sign jumps of $\delta_{i,j}$ resulting from reverse faults. These problems significantly increase the difficulty in establishing system stability.

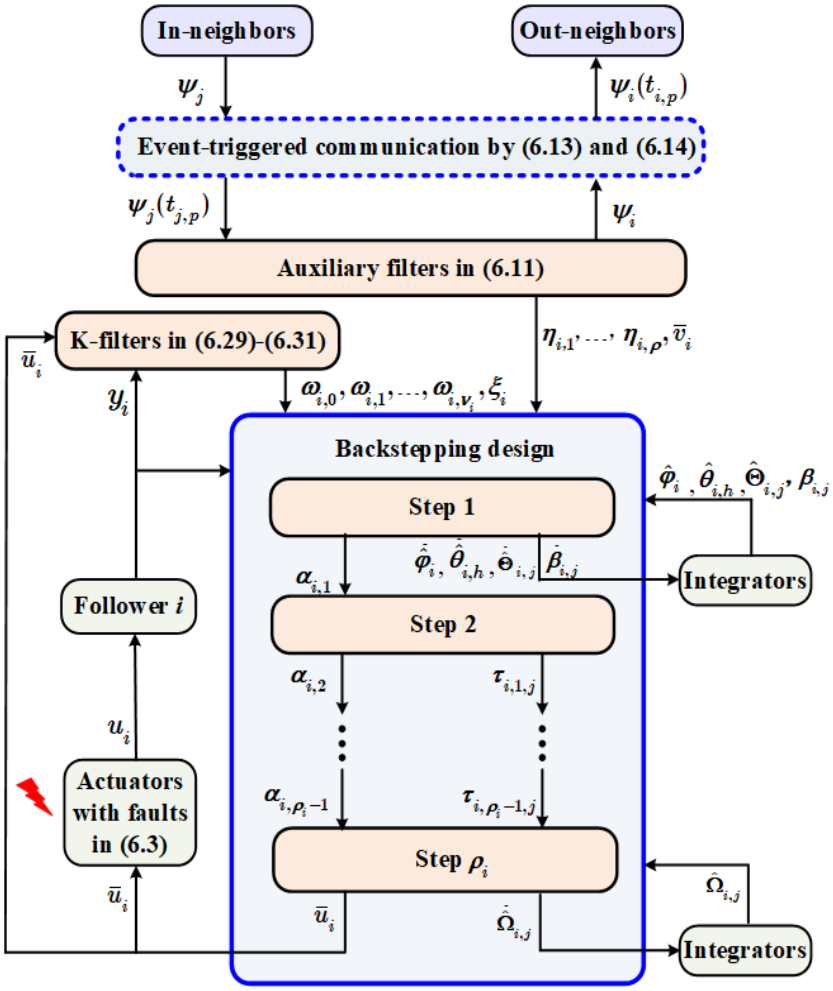

Figure 6.1: Structure of our control scheme from the ith follower's viewpoint.

6.4 Stability Analysis

Theorem 6.4.1. Consider the closed-loop system consisting of the M leaders, the N followers in (6.1), the auxiliary filters given by (6.11) and (6.15), the K-filters in (6.29)-(6.31), the adaptive laws in (6.47), (6.48) and (6.64), and the control laws in (6.65). Suppose that Assumptions 6.2.1-6.2.3 hold. Then, all signals of the closed-loop system are globally uniformly bounded, and the containment errors $y_i - r_i$ $(i = 1, \ldots, N)$ converge to a residual set which can be made arbitrarily small by adjusting the design parameters.

Proof. Integrating both sides of (6.66) and noting from (6.28) that $\int_0^{\beta} H_j(\kappa)d\kappa = \int_0^{|\beta|} H_j(\kappa)d\kappa$, for all $t \in [\bar{T}_{i,j}, \bar{T}_{i,j+1})$, we have

$$\begin{aligned}
&V_{i,\rho_i}(t) + \sum_{j=1}^{\rho_i} \int_{\bar{T}_{i,j}}^{t} c_{i,j} z_{i,j}^{\mathrm{T}}(\kappa) z_{i,j}(\kappa) d\kappa \\
&\quad \leq V_{i,\rho_i}(\bar{T}_{i,j}) + \sum_{j=1}^{q} \frac{1}{\bar{\gamma}_{i,j}} \beta_{i,j}(\bar{T}_{i,j}) - \sum_{j=1}^{q} \frac{1}{\bar{\gamma}_{i,j}} \beta_{i,j}(t) + \sum_{j=1}^{q} \int_{\beta_{i,j}(\bar{T}_{i,j})}^{\beta_{i,j}(t)} \frac{d_{i,j}\delta_{i,j}}{\bar{\gamma}_{i,j}} H_{i,j}(\kappa) d\kappa \\
&\quad \leq V_{i,\rho_i}(\bar{T}_{i,j}) + \Upsilon_i(\bar{T}_{i,j}) + \sum_{j=1}^{q} R_{i,j}(t) + \sum_{j=1}^{q} \frac{1}{\bar{\gamma}_{i,j}} \vartheta_{i,j}(t),
\end{aligned} \tag{6.67}$$

where $\Upsilon_i(\bar{T}_{i,j}) = -\sum_{j=1}^{q} \frac{d_{i,j}\delta_{i,j}}{\bar{\gamma}_{i,j}} \varsigma_{i,j}\big(\vartheta_{i,j}(\bar{T}_{i,j})\big) \vartheta_{i,j}(\bar{T}_{i,j}) e^{\vartheta_{i,j}^2(\bar{T}_{i,j})} + \sum_{j=1}^{q} \frac{1}{\bar{\gamma}_{i,j}} \beta_{i,j}(\bar{T}_{i,j})$ and

$$R_{i,j}(t) = \frac{d_{i,j}\delta_{i,j}}{\bar{\gamma}_{i,j}} \varsigma_{i,j}(\vartheta_{i,j}(t)) \vartheta_{i,j}(t) e^{\vartheta_{i,j}^2(t)}, \tag{6.68}$$

with $\vartheta_{i,j}(t) = |\beta_{i,j}(t)|$. Define

$$\bar{\beta}_i(t) = \max\{|\beta_{i,1}(t)|, \ldots, |\beta_{i,q}(t)|\}. \tag{6.69}$$

Next, we establish system stability based on a contradiction argument.

During the time interval $[\bar{T}_{i,j}, \bar{T}_{i,j+1})$, $d_{i,j}\delta_{i,j}$ is a nonzero constant. In this case, choose the constant $b_{i,j}$ in Lemma 6.2.1 as $b_{i,j} = d_{i,j}\delta_{i,j}$. Suppose that $\bar{\beta}_i(\bar{T}_{i,j})$ and $V_{i,\rho_i}(\bar{T}_{i,j})$ are bounded but $\bar{\beta}_i(t)$ is unbounded on $[\bar{T}_{i,j}, \bar{T}_{i,j+1})$. Then, there must exist a monotonously increasing sequence $\{t_{i,h}^*\} \in [\bar{T}_{i,j}, \bar{T}_{i,j+1}), h = h_0, h_0 + 1, h_0 + 2, \ldots,$ that satisfies $\bar{\beta}_i(t_{i,h}^*) = 2h\pi + \bar{\varrho}_i + 2^{-q}\pi$ and $2h_0\pi + \bar{\varrho}_i + 2^{-q}\pi \geq \bar{\beta}_i(\bar{T}_{i,j})$, where $\bar{\varrho}_i \geq 0$

is given in Lemma 6.2.1. For each h, define $\Pi = \{1, \ldots, q\}$ and

$$\Pi_{i,1,h} = \{j \mid j \in \Pi, \vartheta_{i,j}(t^*_{i,h}) = 2h\pi + \bar{\varrho}_i + 2^{-q}\pi\}, \tag{6.70}$$

$$\Pi_{i,2,h} = \{j \mid j \in \Pi, 2h\pi + \bar{\varrho}_i \leq \vartheta_{i,j}(t^*_{i,h}) < 2h\pi + \bar{\varrho}_i + 2^{-q}\pi\}, \tag{6.71}$$

$$\Pi_{i,3,h} = \{j \mid j \in \Pi, \vartheta_{i,j}(t^*_{i,h}) < 2h\pi + \bar{\varrho}_i\}. \tag{6.72}$$

It is clear that $\Pi_{i,1,h} \bigcup \Pi_{i,2,h} \bigcup \Pi_{i,3,h} = \Pi$ and the number of elements in $\Pi_{i,1,h}$ is no less than 1. From (6.68) and Lemma 6.2.1, for $j \in \Pi_{i,1,h}$, $\text{sign}(d_{i,j}\delta_{i,j})\varsigma_j(\vartheta_{i,j}(t^*_{i,h})) \leq -1$ stands. Therefore,

$$\begin{aligned}\sum_{j\in\Pi_{i,1,h}} R_{i,j}(t^*_{i,h}) &\leq -\sum_{j\in\Pi_{i,1,h}} s_{i,3}\vartheta_{i,j}(t^*_{i,h})e^{\vartheta^2_{i,j}(t^*_{i,h})} \\ &\leq -s_{i,3}(2h\pi + \bar{\varrho}_i + 2^{-q}\pi)e^{(2h\pi+\bar{\varrho}_i+2^{-q}\pi)^2},\end{aligned} \tag{6.73}$$

where $s_{i,3} = \min\{\frac{|\bar{b}_{i,1}|}{\bar{\gamma}_{i,1}}, \ldots, \frac{|\bar{b}_{i,q}|}{\bar{\gamma}_{i,q}}\}$ with $\bar{b}_{i,j} = \min\{|\bar{\delta}_{i,j}|, 1\}$. For $j \in \Pi_{i,2,h}$, it follows from Lemma 6.2.1 that $d_{i,j}\delta_{i,j}\varsigma_j(\vartheta_{i,j}(t^*_{i,h})) \leq 0$, which together with (6.68) results in

$$\sum_{j\in\Pi_{i,2,h}} R_{i,j}(t^*_{i,h}) \leq 0. \tag{6.74}$$

For $j \in \Pi_{i,3,h}$, noting that the number of elements in $\Pi_{i,3,h}$ is no more than $q-1$ and that $|d_{i,j}\varsigma_j(\vartheta_{i,j}(t^*_{i,h}))| \leq 2^{q-j}$, we have

$$\begin{aligned}&\sum_{j\in\Pi_{i,3,h}} R_{i,j}(t^*_{i,h}) + \sum_{j=1}^{q} \frac{1}{\bar{\gamma}_{i,j}}\vartheta_{i,j}(t^*_{i,h}) \\ &\leq \sum_{j\in\Pi_{i,3,h}} s_{i,4}\vartheta_{i,j}(t^*_{i,h})e^{\vartheta^2_{i,j}(t^*_{i,h})} + s_{i,5}\bar{\beta}_i(t^*_{i,h}) \\ &\leq (q-1)s_{i,4}(2h\pi + \bar{\varrho}_i)e^{(2h\pi+\bar{\varrho}_i)^2} + s_{i,5}(2h\pi + \bar{\varrho}_i + 2^{-q}\pi),\end{aligned} \tag{6.75}$$

where $s_{i,4} = \max\{\frac{2^{q-1}\bar{b}^*_{i,1}}{\bar{\gamma}_{i,1}}, \ldots, \frac{2^{q-q}\bar{b}^*_{i,q}}{\bar{\gamma}_{i,q}}\}$ with $\bar{b}^*_{i,j} = \max\{|\bar{\delta}_{i,j}|, 1\}$, and $s_{i,5} = q\max\{\frac{1}{\bar{\gamma}_{i,1}}, \ldots, \frac{1}{\bar{\gamma}_{i,q}}\}$. Combining (6.73)-(6.75) gives

$$\begin{aligned}&\sum_{j=1}^{q} R_{i,j}(t^*_{i,h}) + \sum_{j=1}^{q} \frac{1}{\bar{\gamma}_{i,j}}\vartheta_{i,j}(t^*_{i,h}) \\ &\leq -s_{i,3}(2h\pi + \bar{\varrho}_i + 2^{-q}\pi)e^{(2h\pi+\bar{\varrho}_i)^2}\Bigg[e^{2^{-q}\pi(4h\pi+2\bar{\varrho}_i+2^{-q}\pi)} \\ &\quad -(q-1)\frac{s_{i,4}}{s_{i,3}} - \frac{s_{i,5}}{s_{i,3}}e^{-(2h\pi+\bar{\varrho}_i)^2}\Bigg].\end{aligned} \tag{6.76}$$

According to (6.76), $\sum_{j=1}^{q} R_{i,j}(t^*_{i,h}) + \sum_{j=1}^{q} \frac{1}{\bar{\gamma}_{i,j}}\vartheta_{i,j}(t^*_{i,h}) \to -\infty$ as $h \to +\infty$, which contradicts (6.67). Therefore, if $\bar{\beta}_i(\bar{T}_{i,j})$ and $V_{i,\rho_i}(\bar{T}_{i,j})$ are bounded, then $\bar{\beta}_i(t)$ must be bounded on the time interval $[\bar{T}_{i,j}, \bar{T}_{i,j+1})$.

Then, noting that $\bar{\beta}_i(\bar{T}_{i,0})$ and $V_{i,\rho_i}(\bar{T}_{i,0})$ with $\bar{T}_{i,0} = 0$ are bounded, one can obtain the boundedness of $\bar{\beta}_i(t)$ over $[\bar{T}_{i,0}, \bar{T}_{i,1})$. From (6.69), (6.67) and Lemma 6.3.1, it can be established that $V_{i,\rho_i}(t)$ and all closed-loop signals are bounded over $[\bar{T}_{i,0}, \bar{T}_{i,1})$. At the time instant $\bar{T}_{i,1}$, as a result of the faults, bounded jumps could occur to φ_i, $\Theta_{i,j}$, $\theta_{i,j}$ and $\Omega_{i,j}$, while their estimations $\hat{\varphi}_i$, $\hat{\Theta}_{i,j}$, $\hat{\theta}_{i,j}$ and $\hat{\Omega}_{i,j}$ are continuous. The state estimation $\hat{x}_i$ in (6.33) also experiences bounded jumps at $\bar{T}_{i,1}$, while x_i is continuous. Denote the jump of V_{i,ρ_i} at $\bar{T}_{i,1}$ as $\nabla V_{i,\rho_i}(\bar{T}_{i,1})$. Since the jumps contributing to $\nabla V_{i,\rho_i}(\bar{T}_{i,1})$, namely the jumps in $\frac{1}{2g_i}\tilde{\varphi}_i^2$, $\frac{1}{2}\sum_{j=1}^{q}\tilde{\Theta}_{i,j}^{\mathrm{T}}\Xi_{i,j}^{-1}\tilde{\Theta}_{i,j}$, $\frac{1}{2}\sum_{j=1}^{q-1}\tilde{\theta}_{i,j}^{\mathrm{T}}\Gamma_{i,j}^{-1}\tilde{\theta}_{i,j}$, $\frac{1}{2}\sum_{j=1}^{q}\tilde{\Omega}_{i,j}^{\mathrm{T}}\Lambda_{i,j}^{-1}\tilde{\Omega}_{i,j}$, $\frac{1}{4\gamma_{i,1}}\epsilon_i^{\mathrm{T}}P_{i,1}\epsilon_i$ and $\sum_{j=2}^{\rho_i}\frac{1}{4\gamma_{i,j}}\epsilon_i^{\mathrm{T}}P_{i,2}\epsilon_i$ at $\bar{T}_{i,1}$, are bounded, we know $\nabla V_{i,\rho_i}(\bar{T}_{i,1})$ and thus $V_{i,\rho_i}(\bar{T}_{i,1})$ are bounded. Then, it can be concluded that all closed-loop signals are bounded over $[\bar{T}_{i,0}, \bar{T}_{i,1}]$, which in turn implies that $\bar{\beta}_i(t)$ is bounded over $[\bar{T}_{i,1}, \bar{T}_{i,2})$. Repeating the above procedure and noting $\bar{T}_{i,\bar{n}_i+1} = +\infty$ with $\bar{n}_i \leq q$, it can be concluded that all closed-loop signals are globally uniformly bounded on the time interval $[0, +\infty)$. Moreover, from (6.38) and (6.67), we know $\dot{z}_{i,1}(t)$ and $\int_0^{+\infty} z_{i,1}^{\mathrm{T}}(t)z_{i,1}(t)dt$ are bounded, which together with Barbalat's lemma implies that $\lim_{t\to+\infty} z_{i,1}(t) = 0$. Finally, taking Lemma 6.3.1 and the relationship $y_i - r_i = z_{i,1} + \varepsilon_i$ into consideration, it is clear that the containment errors converge to a residual set which can be made arbitrarily small by increasing the design parameter σ. The proof is completed. ■

Remark 6.4.1. Theorem 6.4.1 indicates the proposed scheme achieves the containment control objective and global stability of the closed-loop system with less prior information on the CGM, regardless of the unknown direction actuator faults. By comparison, existing containment control schemes impose much more restrictive assumptions on the CGM and cannot handle unknown direction actuator faults.

Remark 6.4.2. Due to the problems mentioned in Remark 6.4.1, all the contradiction arguments in [63, 64, 67, 88, 84] and [118] cannot be employed to prove Theorem 6.4.1. Instead, a novel contradiction argument is introduced. It first assumes that $\bar{\beta}_i(\bar{T}_{i,j})$ and $V_{i,\rho_i}(\bar{T}_{i,j})$ are bounded but $\bar{\beta}_i(t)$ is unbounded on $[\bar{T}_{i,j}, \bar{T}_{i,j+1})$. In this case, it shows that $\sum_{j\in\Pi_{i,1,h}} R_{i,j}(t_{i,h}^*)$ in (6.73) can force $\sum_{j=1}^{q} R_{i,j}(t_{i,h}^*) + \sum_{j=1}^{q}\frac{1}{\bar{\gamma}_{i,j}}\vartheta_{i,j}(t_{i,h}^*)$ in (6.76) to go to $-\infty$ as $h \to +\infty$, which contradicts (6.67) and gives the conclusion that $\bar{\beta}_i(t)$ must be bounded on $[\bar{T}_{i,j}, \bar{T}_{i,j+1})$ if $\bar{\beta}_i(\bar{T}_{i,j})$ and $V_{i,\rho_i}(\bar{T}_{i,j})$ are bounded. Then, starting from the boundedness of $\bar{\beta}_i(\bar{T}_{i,0})$ and $V_{i,\rho_i}(\bar{T}_{i,0})$ and using a recursive approach,

it gradually expands the time interval on which all closed-loop signals are bounded and finally establishes global stability of the closed-loop system.

Remark 6.4.3. As can be seen from the above design and analysis, the design parameters $c_{i,j}$, $\gamma_{i,j}$ $(j = 1, \ldots, \rho_i)$, $\bar{\gamma}_{i,k}$ $(k = 1, \ldots, q)$, g_i, $\Xi_{i,k}$, $\Lambda_{i,k}$, and $\Gamma_{i,h}$ affect the dynamics of $z_{i,j}, \beta_{i,k}, \hat{\varphi}_i, \hat{\Theta}_{i,k}, \hat{\Omega}_{i,k}$, and $\hat{\theta}_{i,h}$. Generally speaking, increasing $c_{i,j}$, $\gamma_{i,j}$, $\bar{\gamma}_{i,k}$, g_i, $\lambda_{\min}(\Xi_{i,k})$, $\lambda_{\min}(\Lambda_{i,k})$ and $\lambda_{\min}(\Gamma_{i,h})$ helps to reduce the containment errors but may increase the amplitude of control signals. The parameters $\bar{k}_{i,1}, \ldots, \bar{k}_{i,n_i}$ should be chosen such that the matrix $A_{ci} = A_{oi} - K_{ci}C_i$ is Hurwitz. Besides, increasing σ or decreasing λ_j helps to reduce the containment errors but may increase the communication burden among agents. In summary, the design parameters should be properly chosen to make a trade-off among the containment errors, the communication burden and the amplitude of control signals.

6.5 Simulation Results

To demonstrate the effectiveness of the proposed scheme, we consider a practical example of six agents, where agents 1-3 are followers, agents 4-6 are leaders. The followers are coupled inverted double pendulums described by [126]

$$\begin{aligned} \ddot{y}_{i,1} &= \tilde{M}_{i,1}\sin(y_{i,1}) - \tilde{M}_{i,2}u_{i,1} + \tilde{M}_{i,3}\tilde{\rho}_{i,1}(y_i), \\ \ddot{y}_{i,2} &= \tilde{M}_{i,1}\sin(y_{i,2}) - \tilde{M}_{i,2}u_{i,2} + \tilde{M}_{i,3}\tilde{\rho}_{i,2}(y_i), \end{aligned} \tag{6.77}$$

where $y_i = [y_{i,1}, y_{i,2}]^{\mathrm{T}}$ represents the pendulum angles in radians, and $u_i = [u_{i,1}, u_{i,2}]^{\mathrm{T}}$ is the control torque, $\tilde{M}_{i,1}$, $\tilde{M}_{i,2}$ and $\tilde{M}_{i,3}$ are nonzero constants assumed to be unknown, $\tilde{\rho}_{i,1}(y_i) = \sin(y_{i,2})\cos(y_{i,2}) - \sin(y_{i,1})\cos(y_{i,1})$ and $\tilde{\rho}_{i,2}(y_i) = \sin(y_{i,1})\cos(y_{i,1}) - \sin(y_{i,2})\cos(y_{i,2})$. Letting $x_i = [y_i^{\mathrm{T}}, \dot{y}_i^{\mathrm{T}}]^{\mathrm{T}}$, $A_{i,1} = \mathrm{diag}\{\tilde{M}_{i,1}, \tilde{M}_{i,1}\}$, $A_{i,2} = \mathrm{diag}\{\tilde{M}_{i,3}, \tilde{M}_{i,3}\}$, $f_{i,1}(y_i) = [0, 0, \sin(y_{i,1}), \sin(y_{i,2})]^{\mathrm{T}}$, $f_{i,2}(y_i) = [0, 0, \tilde{\rho}_{i,1}(y_i), \tilde{\rho}_{i,2}(y_i)]^{\mathrm{T}}$, and $B_{i,0} = -\,\mathrm{diag}\{\tilde{M}_{i,2}, \tilde{M}_{i,2}\}$, (6.77) can be expressed in the general form of (6.1). In the simulation, we set $\tilde{M}_{i,1} = 1$, $\tilde{M}_{i,2} = 1$ $(i = 1, 2, 3)$, $\tilde{M}_{1,3} = 0.25$, $\tilde{M}_{2,3} = 0.5$, and $\tilde{M}_{3,3} = 0.3$. The trajectory of the leaders are generated by $\ddot{y}_i + 2\dot{y}_i + y_i = \tilde{r}_i$, where $i = 4, 5, 6$, $\tilde{r}_4 = [\sin(0.3t), \cos(0.3t)]^{\mathrm{T}}$, $\tilde{r}_5 = [1.4\sin(0.3t + 0.15\pi), \cos(0.3t + 0.15\pi)]^{\mathrm{T}}$, and $\tilde{r}_6 = [1.6\sin(0.3t), 1.6\cos(0.3t)]^{\mathrm{T}}$. In the network topology, $a_{12} = a_{21} = a_{23} =$

$a_{32} = a_{14} = a_{34} = a_{25} = a_{36} = 1$, and all other adjacency elements are zero.

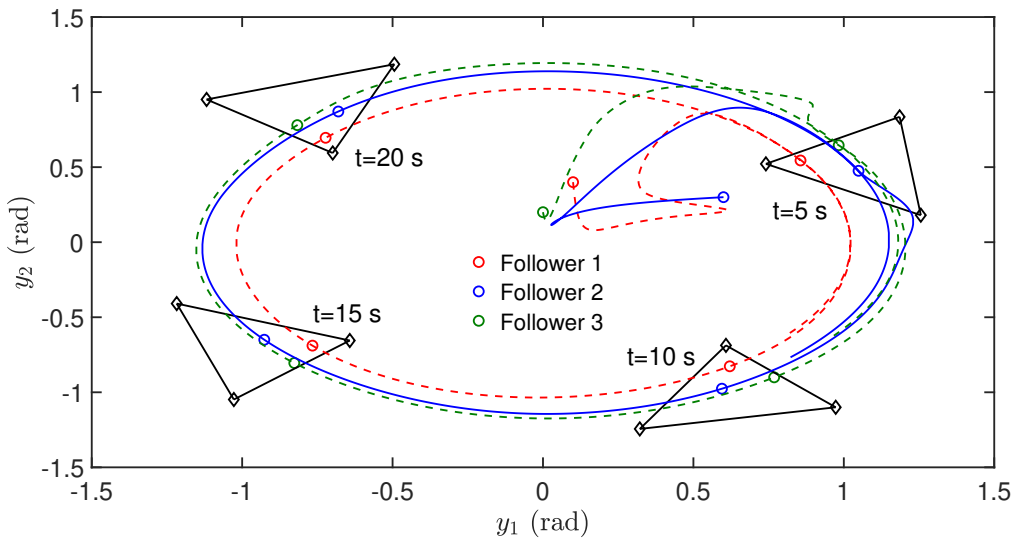

Figure 6.2: Output trajectories on 2-D space.

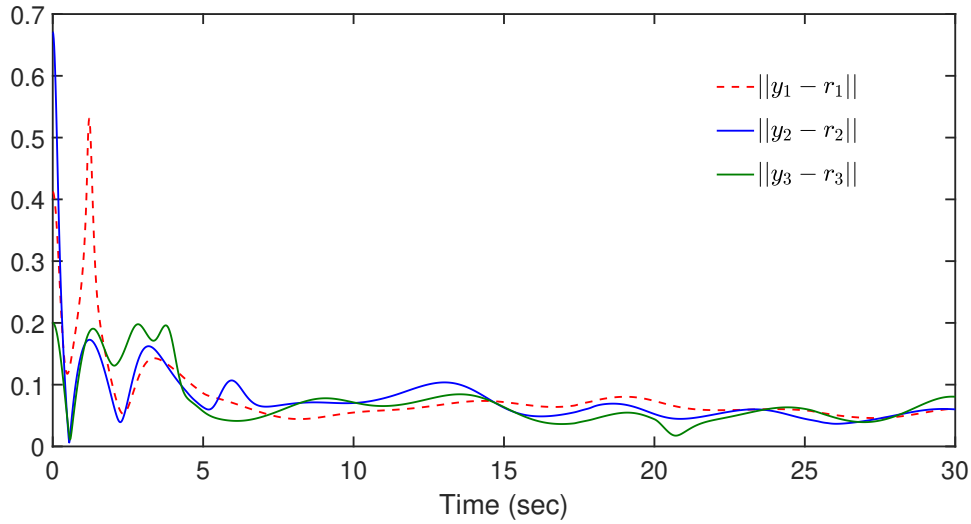

Figure 6.3: Containment errors.

In the simulation, we choose $\bar{k}_{i,1} = 2$ and $\bar{k}_{i,2} = 1$ $(i = 1, 2, 3)$ for the K-filters, and $\sigma = 1$ and $\lambda_j = 0.05$ $(j = 1, \ldots, 6)$ for the auxiliary filters. The other design parameters are chosen as $c_{i,1} = c_{i,2} = 5$, $\gamma_{i,1} = \gamma_{i,2} = 1$, $\bar{\gamma}_{i,1} = \bar{\gamma}_{i,2} = 1$, $g_i = 5$, $\Gamma_{i,1} = 2$, and $\Xi_{i,1} = \Xi_{i,2} = \Lambda_{i,1} = \Lambda_{i,2} = I_6$. The initial conditions of the followers are set as $x_1(0) = [0.1, 0.4, 0, 0]^{\mathrm{T}}$, $x_2(0) = [0.6, 0.3, 0, 0]^{\mathrm{T}}$ and $x_3(0) = [0, 0.2, 0, 0]^{\mathrm{T}}$. The unknown actuator faults are given by (6.3) with $\bar{\delta}_{1,1} = -1$, $\bar{\delta}_{1,2} = 0.7$, $\bar{\delta}_{2,1} = 0.3$, $\bar{\delta}_{3,1} = -1$, $\bar{\delta}_{3,2} = 0.5$, $T_{1,1} = 1s$, $T_{1,2} = 5s$, $T_{2,1} = 10s$, $T_{3,1} = 2s$ and $T_{3,2} = 20s$, where the second actuator of the second follower is free of faults in the simulation. The

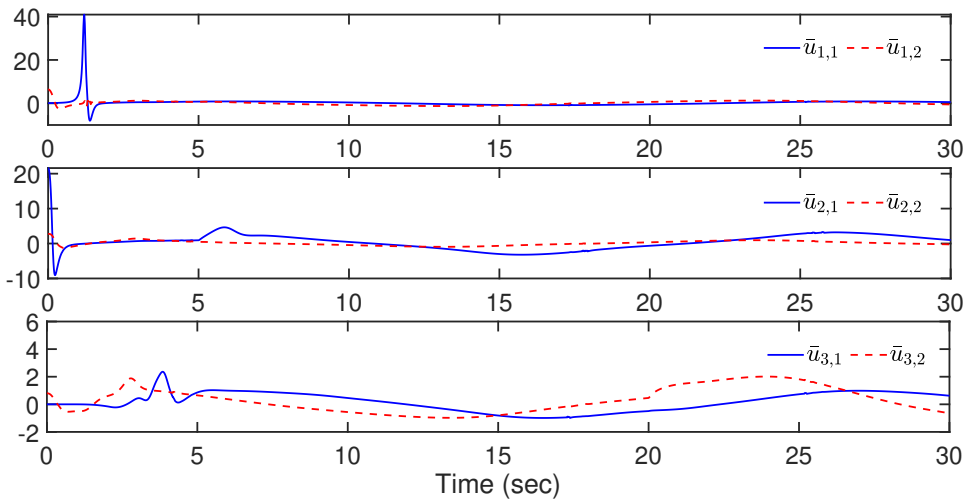

Figure 6.4: Control signals.

simulation results are shown in Figures 6.2-6.4. As shown in Figure 6.2, the followers are driven into the convex hull spanned by the leaders. From Figure 6.3, it can be seen that the containment errors $y_i - r_i$ converge to a small residual set in the presence of unknown direction actuator faults.

6.6 Conclusions

In this chapter, based on backstepping design, an output-feedback adaptive containment control scheme has been proposed for a class of heterogeneous nonlinear MIMO agents with unknown actuator faults. The unknown CGMs, unknown parameters, and unknown jumps introduced by the actuator faults are dealt with by a novel contradiction argument based on some Nussbaum functions and a matrix similarity transformation, which establishes the stability in a recursive fashion. Besides, continuous communication among agents is also avoided. We have shown that all closed-loop signals are globally uniformly bounded and the containment errors can converge to an arbitrarily small residual set.

Chapter 7

Conclusions and Future Work

In this chapter, the main contributions of this thesis are summarised and we discuss possible directions for future research.

7.1 Conclusions

In this thesis, we have introduced distributed resilient estimation and control against a range of adversaries on all channels of the distributed dynamic system, namely false data injection attacks and multiple disturbances on the sensor channel, denial-of-service attacks on the communication channel, sparse attacks on redundant sensors, and unknown direction faults on the actuator channel. In this thesis, a resilient estimation and control framework is introduced. The distributed control and estimation approaches covers the scope of typical adversaries faced by distributed systems, with particular focus placed on developing cohesive algorithms to deal with the joint effects of heterogeneous adversaries, and resilient control of nonlinear systems under a more general class of faults. Specifically, the following problems have been investigated in detail.

- For distributed systems subject to multiple disturbances and FDI attacks, an enhanced resilient distributed estimation scheme is introduced. In the initial stages

of estimation, a multi-layer anti-disturbance estimator is introduced to compensate and attenuate the effects of multiple disturbances. Then, an observer-based optimal attack detection scheme is introduced, where the residue signals are compared to an optimally obtained threshold to determine the presence of FDI attacks. Finally, an attack-resilient estimator that is activated by the detection of attacks is introduced to develop resilience towards FDI attacks. The proposed enhanced three-stage approach effectively deals with the coupling between FDI attacks and multiple disturbances. Compared with existing resilient estimation results, which only consider a single source of disturbance, the proposed approach is shown to be able to actively reject FDI attacks in the presence of multiple disturbances. Furthermore, the novel detection-triggered estimation structure reduces the computational load of the attack-resilient estimator.

- An event-based resilient distributed state estimation method has been proposed for distributed systems under system disturbances and multiple heterogeneous cyber-attacks. A novel event-based communication scheme is designed to reduce unnecessary data transmissions within the network, while guaranteeing desired estimation performance in the presence of aperiodic DoS attacks. A novel adaptive deception attack rejection scheme is introduced for the adaptive compensation of deception attacks. Moreover, a distributed disturbance observer is proposed to deal with disturbances in the system in a distributed manner. Sufficient conditions for convergence of the estimator are obtained via the Lyapunov function approach. A practical example on a 4-bus power grid is presented to demonstrate the effectiveness of the proposed estimation method, and the results show that the proposed method is capable of accurately estimating the state of the system in the presence of heterogeneous attacks.

- In view of sparse injection attacks and system disturbances, a secure state estimation scheme has been proposed for a class of nonlinear systems. Our design introduces a kind of high-gain K-filters, a monitoring function and a switching scheme. With the aforementioned efforts and a contradiction argument, it has been proved that all attacked sensors can be precluded after a finite number of switching and the estimation error can converge to an arbitrarily small residual

set. Furthermore, a backstepping controller is designed based on the estimation results, and the proposed method has been applied to a robotic manipulator with both simulation and experimental studies, where the effectiveness of the proposed scheme has been validated.

- An output-feedback adaptive containment control scheme based on backstepping design has been proposed for a class of heterogeneous nonlinear MIMO agents with unknown direction actuator faults. The unknown CGMs, unknown parameters, and unknown jumps introduced by the actuator faults are dealt with a novel Nussbaum function-based approach in conjunction with a contradiction statement and a matrix similarity transformation, which establishes the stability in a recursive fashion. Besides, an event-based communication scheme is introduced to preclude continuous communication among agents. It can be obtained that all closed-loop signals are globally uniformly bounded and the containment controller errors can converge to an residual set that can be made to be arbitrarily small.

7.2 Future Work

As mentioned in the conclusions section, the aim is to propose a cohesive resilient estimation and control framework that covers a wide range of heterogeneous adversaries. However, some notable gaps still exist in the research introduced in this thesis. Several potential extensions to our research are listed as follows.

- There has been research on stealthy FDI attacks able to bypass residue-based attack detection methods, as can be seen in References [127, 128] and [129]. Very recently, in Reference [127], a stealthy attack was developed from the attackers' perspective to guarantee that the attack keeps its effects on the attack detectors residue below a predefined level in the presence of norm-bounded disturbances. In addition, attacks that are theoretically strictly undetectable have been defined in References [22] and [41] by exploiting the zero-dynamics in the system. However, these types of attacks are designed from the attackers' perspective, and

require full knowledge of the model of the observed system as well as the detection mechanism, which is a very restrictive assumption. The attack detection and rejection approach in this thesis is developed from the defenders' perspective, with no prior knowledge or assumptions on the attack signals. In the future, we will endeavour to investigate the detection and rejection of stealthier attacks.

- In Chapters 3 and 4, the disturbances under consideration are formulated by an exogeneous system, which can describe a wide range of disturbances in practical scenarios, and an additional norm-bounded term is included to account for the uncertainties in the disturbance model. Future work will include utilization of identification techniques to deal with disturbances with unknown dynamic characteristics.

- In Chapters 5 and 6, the system under consideration is of output-feedback form, which can describe a wide range of practical engineering systems. Future work will include the extension of the proposed nonlinear estimation and control schemes to more general uncertain nonlinear systems to overcome the pertaining limitations of the system model considered in Chapters 5 and 6.

Bibliography

[1] V. Ugrinovskii, "Distributed h_∞ estimation resilient to biasing attacks," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 1, pp. 458–470, 2019.

[2] X.-M. Zhang, Q.-L. Han, X. Ge, D. Ding, L. Ding, D. Yue, and C. Peng, "Networked control systems: A survey of trends and techniques," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 1, pp. 1–17, 2019.

[3] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, 2007.

[4] R. A. Gupta and M.-Y. Chow, "Networked control system: Overview and research trends," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 7, pp. 2527–2535, 2009.

[5] X.-M. Zhang, Q.-L. Han, and X. Yu, "Survey on recent advances in networked control systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1740–1752, 2015.

[6] X. Ge, F. Yang, and Q.-L. Han, "Distributed networked control systems: A brief overview," *Information Sciences*, vol. 380, pp. 117–131, 2017.

[7] K.-D. Kim and P. R. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, 2012.

[8] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 20–23, 2015.

[9] Y. Chen, S. Kar, and J. M. Moura, "Resilient distributed estimation: Sensor attacks," *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3772–3779, 2018.

[10] P. Millán, L. Orihuela, C. Vivas, and F. R. Rubio, "Distributed consensus-based estimation considering network induced delays and dropouts," *Automatica*, vol. 48, no. 10, pp. 2726–2729, 2012.

[11] R. Olfati-Saber and P. Jalalkamali, "Coupled distributed estimation and control for mobile sensor networks," *IEEE Transactions on Automatic Control*, vol. 57, no. 10, pp. 2609–2614, 2012.

[12] V. Ugrinovskii, "Distributed robust estimation over randomly switching networks using h_∞ consensus," *Automatica*, vol. 49, no. 1, pp. 160–168, 2013.

[13] X. Ge, Q.-L. Han, and Z. Wang, "A threshold-parameter-dependent approach to designing distributed event-triggered h_∞ consensus filters over sensor networks," *IEEE Transactions on Cybernetics*, vol. 49, no. 4, pp. 1148–1159, 2018.

[14] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, 2011.

[15] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—attacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, 2016.

[16] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2016.

[17] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2618–2624, 2015.

[18] X. Wang, X. Luo, M. Zhang, and X. Guan, "Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers," *International Journal of Electrical Power & Energy Systems*, vol. 110, pp. 208–222, 2019.

[19] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, "Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach," *IEEE Transactions on Automatic Control*, vol. 62, no. 10, pp. 4917–4932, 2017.

[20] C. Wu, Z. Hu, J. Liu, and L. Wu, "Secure estimation for cyber-physical systems via sliding mode," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3420–3431, 2018.

[21] X. He, E. Hashemi, and K. H. Johansson, "Distributed control under compromised measurements: Resilient estimation, attack detection, and vehicle platooning," *Automatica*, vol. 134, p. 109953, 2021.

[22] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[23] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," *In Proceedings of the 49th IEEE Conference on Decision and Control*, pp. 5967–5972, 2010.

[24] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[25] W. Ao, Y. Song, and C. Wen, "Distributed secure state estimation and control for cpss under sensor attacks," *IEEE Transactions on Cybernetics*, vol. 50, no. 1, pp. 259–269, 2018.

[26] R. Olfati-Saber, "Distributed Kalman filtering for sensor networks," *46th IEEE Conference on Decision and Control*, pp. 5492–5498, 2007.

[27] B. Shen, Z. Wang, and Y. S. Hung, "Distributed h_∞-consensus filtering in sensor networks with multiple missing measurements: The finite-horizon case," *Automatica*, vol. 46, no. 10, pp. 1682–1688, 2010.

[28] X. Ge, Q.-L. Han, and Z. Wang, "A dynamic event-triggered transmission scheme for distributed set-membership estimation over wireless sensor networks," *IEEE Transactions on Cybernetics*, vol. 49, no. 1, pp. 171–183, 2017.

[29] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 48–59, 2017.

[30] W. Yang, Y. Zhang, G. Chen, C. Yang, and L. Shi, "Distributed filtering under false data injection attacks," *Automatica*, vol. 102, pp. 34–44, 2019.

[31] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Transactions on Automatic Control*, vol. 60, no. 10, pp. 2831–2836, 2015.

[32] B. Chen, D. W. Ho, W.-A. Zhang, and L. Yu, "Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 2, pp. 455–468, 2017.

[33] K. Ding, X. Ren, D. E. Quevedo, S. Dey, and L. Shi, "DoS attacks on remote state estimation with asymmetric information," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 2, pp. 653–666, 2018.

[34] X.-M. Zhang, Q.-L. Han, and X. Ge, "A novel approach to h_∞ performance analysis of discrete-time networked systems subject to network-induced delays and malicious packet dropouts," *Automatica*, vol. 136, p. 110010, 2022.

[35] Q. Liu, Z. Wang, X. He, and D. Zhou, "Event-triggered resilient filtering with measurement quantization and random sensor failures: Monotonicity and convergence," *Automatica*, vol. 94, pp. 458–464, 2018.

[36] X. Ge, Q.-L. Han, X.-M. Zhang, L. Ding, and F. Yang, "Distributed event-triggered estimation over sensor networks: A survey," *IEEE Transactions on Cybernetics*, vol. 50, no. 3, pp. 1306–1320, 2020.

[37] D. Ding, Z. Wang, and Q.-L. Han, "A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks," *IEEE Transactions on Automatic Control*, vol. 65, no. 4, pp. 1792–1799, 2019.

[38] Y. Liu and G.-H. Yang, "Event-triggered distributed state estimation for cyber-physical systems under DoS attacks," *IEEE Transactions on Cybernetics*, vol. 52, no. 5, pp. 3620–3631, 2022.

[39] ——, "Resilient event-triggered distributed state estimation for nonlinear systems against DoS attacks," *IEEE Transactions on Cybernetics*, vol. 52, no. 9, pp. 9076 – 9089, 2022.

[40] X. Li, G. Wei, and D. Ding, "Distributed resilient interval estimation for sensor networks under aperiodic denial-of-service attacks and adaptive event-triggered protocols," *Applied Mathematics and Computation*, vol. 409, p. 126371, 2021.

[41] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2079–2091, 2015.

[42] M. Showkatbakhsh, Y. Shoukry, S. N. Diggavi, and P. Tabuada, "Securing state reconstruction under sensor and actuator attacks: Theory and design," *Automatica*, vol. 116, p. 108920, 2020.

[43] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[44] L. An and G.-H. Yang, "Distributed secure state estimation for cyber–physical systems under sensor attacks," *Automatica*, vol. 107, pp. 526–538, 2019.

[45] Y. H. Chang, Q. Hu, and C. J. Tomlin, "Secure estimation based Kalman filter for cyber-physical systems against sensor attacks," *Automatica*, vol. 95, pp. 399–412, 2018.

[46] A. Y. Lu and G. H. Yang, "Secure luenberger-like observers for cyber-physical systems under sparse actuator and sensor attacks," *Automatica*, vol. 98, pp. 124–129, 2018.

[47] ——, "Secure switched observers for cyber-physical systems under sparse sensor attacks: A set cover approach," *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3949–3955, 2019.

[48] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, "Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach," *IEEE Transactions on Automatic Control*, vol. 62, no. 10, pp. 4917–4932, 2017.

[49] X. Luo, M. Pajic, and M. M. Zavlanos, "An optimal graph-search method for secure state estimation," *Automatica*, vol. 123, p. 109323, 2021.

[50] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observability of linear systems under adversarial attacks," *In Proceedings of the American Control Conference*, pp. 2439–2444, 2015.

[51] L. An and G. H. Yang, "Secure state estimation against sparse sensor attacks with adaptive switching mechanism," *IEEE Transactions on Automatic Control*, vol. 63, no. 8, pp. 2596–2603, 2017.

[52] R. Ma, P. Shi, and L. Wu, "Sparse false injection attacks reconstruction via descriptor sliding mode observers," *IEEE Transactions on Automatic Control*, vol. 66, no. 11, pp. 5369–5376, 2021.

[53] L. An and G.-H. Yang, "Supervisory nonlinear state observers for adversarial sparse attacks," *IEEE Transactions on Cybernetics*, vol. 52, no. 3, pp. 1575–1587, 2022.

[54] G.-B. Dai and Y.-C. Liu, "Distributed coordination and cooperation control for networked mobile manipulators," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5065–5074, 2016.

[55] D. Chen, Y. Zhang, and S. Li, "Tracking control of robot manipulators with unknown models: A Jacobian-matrix-adaption method," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3044–3053, 2017.

[56] L. Jin, S. Li, L. Xiao, R. Lu, and B. Liao, "Cooperative motion generation in a distributed network of redundant robot manipulators with noises," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 10, pp. 1715–1724, 2017.

[57] J. Alonso-Mora, E. Montijano, T. Nägeli, O. Hilliges, M. Schwager, and D. Rus, "Distributed multi-robot formation control in dynamic environments," *Autonomous Robots*, vol. 43, no. 5, pp. 1079–1100, 2019.

[58] S. Wilson, P. Glotfelter, L. Wang, S. Mayya, G. Notomista, M. Mote, and M. Egerstedt, "The robotarium: Globally impactful opportunities, challenges, and lessons learned in remote-access, distributed control of multirobot systems," *IEEE Control Systems Magazine*, vol. 40, no. 1, pp. 26–44, 2020.

[59] Y. Yan, D. Shi, D. Bian, B. Huang, Z. Yi, and Z. Wang, "Small-signal stability analysis and performance evaluation of microgrids under distributed control," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4848–4858, 2018.

[60] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3690–3701, 2020.

[61] C. Deng, C. Wen, W. Wang, X. Li, and D. Yue, "Distributed adaptive tracking control for high-order nonlinear multi-agent systems over event-triggered communication," *IEEE Transactions on Automatic Control*, 2022, DOI: 10.1109/TAC.2022.3148384.

[62] M. Khalili, X. Zhang, M. M. Polycarpou, M. Marios, T. Parisini, and Y. Cao, "Distributed adaptive fault-tolerant control of uncertain multi-agent systems," *Automatica*, vol. 87, pp. 142–151, 2018.

[63] Z. Ding, "Adaptive consensus output regulation of a class of nonlinear systems with unknown high-frequency gain," *Automatica*, vol. 51, pp. 348–355, 2015.

[64] B. Fan, Q. Yang, S. Jagannathan, and Y. Sun, "Output-constrained control of nonaffine multiagent systems with partially unknown control directions," *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3936–3942, 2019.

[65] P. Gong, W. Lan, and Q.-L. Han, "Robust adaptive fault-tolerant consensus control for uncertain nonlinear fractional-order multi-agent systems with directed topologies," *Automatica*, vol. 117, p. 109011, 2020.

[66] Z. Ding, "Distributed adaptive consensus output regulation of network-connected heterogeneous unknown linear systems on directed graphs," *IEEE Transactions on Automatic Control*, vol. 62, no. 9, pp. 4683–4690, 2017.

[67] C. Wang, C. Wen, and L. Guo, "Adaptive consensus control for nonlinear multi-agent systems with unknown control directions and time-varying actuator faults," *IEEE Transactions on Automatic Control*, vol. 66, no. 9, pp. 4222–4229, 2021.

[68] Y. Wang, Y. Song, M. Krstic, and C. Wen, "Fault-tolerant finite time consensus for multiple uncertain nonlinear mechanical systems under single-way directed communication interactions and actuation failures," *Automatica*, vol. 63, pp. 374–383, 2016.

[69] Y. Wang, Y. Song, and F. L. Lewis, "Robust adaptive fault-tolerant control of multiagent systems with uncertain nonidentical dynamics and undetectable actuation failures," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 6, pp. 3978–3988, 2015.

[70] W. Wang, C. Wen, J. Huang, and J. Zhou, "Adaptive consensus of uncertain nonlinear systems with event triggered communication and intermittent actuator faults," *Automatica*, vol. 111, p. 108667, 2020.

[71] C. Liu, B. Jiang, K. Zhang, and R. J. Patton, "Distributed fault-tolerant consensus tracking control of multi-agent systems under fixed and switching topologies," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 4, pp. 1646–1658, 2021.

[72] C. Deng, X.-Z. Jin, W.-W. Che, and H. Wang, "Learning-based distributed resilient fault-tolerant control method for heterogeneous mass under unknown leader dynamic," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 10, pp. 5504 – 5513, 2021.

[73] T. Li, W. Bai, Q. Liu, Y. Long, and C. P. Chen, "Distributed fault-tolerant containment control protocols for the discrete-time multi-agent systems via reinforcement learning method," *IEEE Transactions on Neural Networks and Learning Systems*, 2022, DOI: 10.1109/TNNLS.2021.3121403.

[74] C. Chen, F. L. Lewis, S. Xie, H. Modares, Z. Liu, S. Zuo, and A. Davoudi, "Resilient adaptive and h_∞ controls of multi-agent systems under sensor and actuator faults," *Automatica*, vol. 102, pp. 19–26, 2019.

[75] C. Chen, K. Xie, F. L. Lewis, S. Xie, and A. Davoudi, "Fully distributed resilience for adaptive exponential synchronization of heterogeneous multiagent systems against actuator faults," *IEEE Transactions on Automatic Control*, vol. 64, no. 8, pp. 3347–3354, 2019.

[76] M. Yadegar and N. Meskin, "Fault-tolerant control of nonlinear heterogeneous multi-agent systems," *Automatica*, vol. 127, p. 109514, 2021.

[77] C. Wang, C. Wen, and Q. Hu, "Event-triggered adaptive control for a class of nonlinear systems with unknown control direction and sensor faults," *IEEE Transactions on Automatic Control*, vol. 65, no. 2, pp. 763–770, 2020.

[78] Z. Ding, "Adaptive consensus output regulation of a class of nonlinear systems with unknown high-frequency gain," *Automatica*, vol. 51, pp. 348–355, 2015.

[79] W. Chen, X. Li, W. Ren, and C. Wen, "Adaptive consensus of multi-agent systems with unknown identical control directions based on a novel nussbaum-type function," *IEEE Transactions on Automatic Control*, vol. 59, no. 7, pp. 1887–1892, 2013.

[80] C. Chen, C. Wen, Z. Liu, K. Xie, Y. Zhang, and C. P. Chen, "Adaptive consensus of nonlinear multi-agent systems with non-identical partially unknown control

directions and bounded modelling errors," *IEEE Transactions on Automatic Control*, vol. 62, no. 9, pp. 4654–4659, 2016.

[81] Y.-W. Wang, Y. Lei, T. Bian, and Z.-H. Guan, "Distributed control of nonlinear multiagent systems with unknown and nonidentical control directions via event-triggered communication," *IEEE Transactions on Cybernetics*, vol. 50, no. 5, pp. 1820–1832, 2019.

[82] M. Guo, D. Xu, and L. Liu, "Cooperative output regulation of heterogeneous nonlinear multi-agent systems with unknown control directions," *IEEE Transactions on Automatic Control*, vol. 62, no. 6, pp. 3039–3045, 2016.

[83] T. Liu and J. Huang, "Cooperative output regulation for a class of nonlinear multi-agent systems with unknown control directions subject to switching networks," *IEEE Transactions on Automatic Control*, vol. 63, no. 3, pp. 783–790, 2017.

[84] C. Wang, C. Wen, and L. Guo, "Multivariable adaptive control with unknown signs of the high-frequency gain matrix using novel nussbaum functions," *Automatica*, vol. 111, p. 108618, 2020.

[85] C. Tan, G. Tao, R. Qi, and H. Yang, "A direct mrac based multivariable multiple-model switching control scheme," *Automatica*, vol. 84, pp. 190–198, 2017.

[86] Y. Ma, H. Ren, G. Tao, and B. Jiang, "Adaptive compensation for actuation sign faults of flexible spacecraft," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 2, pp. 1288–1300, 2020.

[87] A. Hooshyar, M. A. Azzouz, and E. F. El-Saadany, "Three-phase fault direction identification for distribution systems with DFIG-based wind DG," *IEEE Transactions on Sustainable Energy*, vol. 5, no. 3, pp. 747–756, 2014.

[88] X. Guo, W. Xu, J. Wang, and J. Park, "Distributed neuroadaptive fault-tolerant sliding-mode control for 2-d plane vehicular platoon systems with spacing constraints and unknown direction faults," *Automatica*, vol. 129, p. 109675, 2021.

[89] W. H. Young, "On classes of summable functions and their fourier series," *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, vol. 87, no. 594, pp. 225–229, 1912.

[90] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.

[91] Z. Meng, W. Ren, and Z. You, "Distributed finite-time attitude containment control for multiple rigid bodies," *Automatica*, vol. 46, no. 12, pp. 2092–2099, 2010.

[92] R. D. Nussbaum, "Some remarks on a conjecture in parameter adaptive control," *Systems & control letters*, vol. 3, no. 5, pp. 243–246, 1983.

[93] M. Deghat, V. Ugrinovskii, I. Shames, and C. Langbort, "Detection and mitigation of biasing attacks on distributed estimation networks," *Automatica*, vol. 99, pp. 369–381, 2019.

[94] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[95] L. Guo and S. Cao, "Anti-disturbance control theory for systems with multiple disturbances: A survey," *ISA Transactions*, vol. 53, no. 4, pp. 846–849, 2014.

[96] W.-H. Chen, J. Yang, L. Guo, and S. Li, "Disturbance-observer-based control and related methods—an overview," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 2, pp. 1083–1095, 2015.

[97] V. Ugrinovskii, "Distributed robust filtering with h_∞ consensus of estimates," *Automatica*, vol. 47, no. 1, pp. 1–13, 2011.

[98] X. Ge and Q.-L. Han, "Distributed event-triggered h_∞ filtering over sensor networks with communication delays," *Information Sciences*, vol. 291, pp. 128–142, 2015.

[99] A. Mitra and S. Sundaram, "Secure distributed observers for a class of linear time invariant systems in the presence of byzantine adversaries," *55th IEEE Conference on Decision and Control*, pp. 2709–2714, 2016.

[100] L. Guo and S. Cao, *Anti-Disturbance Control for Systems with Multiple Disturbances.* CRC Press, 2013.

[101] V. Ugrinovskii, "Conditions for detectability in distributed consensus-based observer networks," *IEEE Transactions on Automatic Control*, vol. 58, no. 10, pp. 2659–2664, 2013.

[102] S. Feng, A. Cetinkaya, H. Ishii, P. Tesi, and C. D. Persis, "Networked control under DoS attacks: Tradeoffs between resilience and data rate," *IEEE Transactions on Automatic Control*, vol. 66, no. 1, pp. 460–467, 2021.

[103] N. Hou, Z. Wang, D. W. Ho, and H. Dong, "Robust partial-nodes-based state estimation for complex networks under deception attacks," *IEEE Transactions on Cybernetics*, vol. 50, no. 6, pp. 2793–2802, 2019.

[104] L. Li, H. Yang, Y. Xia, and C. Zhu, "Attack detection and distributed filtering for state-saturated systems under deception attack," *IEEE Transactions on Control of Network Systems*, vol. 8, no. 4, pp. 1918–1929, 2021.

[105] H. Lin, J. Lam, and Z. Wang, "Secure state estimation for systems under mixed cyber-attacks: Security and performance analysis," *Information Sciences*, vol. 546, pp. 943–960, 2021.

[106] D. Du, X. Li, W. Li, R. Chen, M. Fei, and L. Wu, "ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1698–1711, 2019.

[107] W. Xu, D. W. Ho, J. Zhong, and B. Chen, "Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 10, pp. 3137–3149, 2019.

[108] H. Li, L. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1097–1107, 2012.

[109] M. Elkayam, S. Kolesnik, and A. Kuperman, "Guidelines to classical frequency-domain disturbance observer redesign for enhanced rejection of periodic uncertainties and disturbances," *IEEE Transactions on Power Electronics*, vol. 34, no. 4, pp. 3986–3995, 2019.

[110] C. Wang, C. Wen, and L. Guo, "Adaptive consensus control for nonlinear multi-agent systems with unknown control directions and time-varying actuator faults," *IEEE Transactions on Automatic Control*, vol. 66, no. 9, pp. 4222–4229, 2021.

[111] H. Hou, X. Yu, L. Xu, K. Rsetam, and Z. Cao, "Finite-time continuous terminal sliding mode control of servo motor systems," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 7, pp. 5647–5656, 2020.

[112] C. Wen, J. Zhou, Z. Liu, and H. Su, "Robust adaptive control of uncertain nonlinear systems in the presence of input saturation and external disturbance," *IEEE Transactions on Automatic Control*, vol. 56, no. 7, pp. 1672–1678, 2011.

[113] C. Wang, C. Wen, and Y. Lin, "Adaptive actuator failure compensation for a class of nonlinear systems with unknown control direction," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 385–392, 2017.

[114] H. Liang, L. Yan, and W. Xu, "A lightweight redundant manipulator with high stable wireless communication and compliance control," *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 6622–6627, 2018.

[115] M. Krstić, P. V. Kokotovic, and I. Kanellakopoulos, *Nonlinear and Adaptive Control Design*. New York, NY, USA: Wiley, 1995.

[116] T. Y. Zhang and D. Ye, "False data injection attacks with complete stealthiness in cyber-physical systems: A self-generated approach," *Automatica*, vol. 120, p. 109117, 2020.

[117] M. Bagheri, P. Naseradinmousavi, and M. Krstić, "Feedback linearization based predictor for time delay control of a high-dof robot manipulator," *Automatica*, vol. 108, p. 108485, 2019.

[118] H. E. Psillakis, "Further results on the use of nussbaum gains in adaptive neural network control," *IEEE Transactions on Automatic Control*, vol. 55, no. 12, pp. 2841–2846, 2010.

[119] S. Yoo, "Distributed adaptive containment control of uncertain nonlinear multi-agent systems in strict-feedback form," *Automatica*, vol. 49, no. 7, pp. 2145–2153, 2013.

[120] J. Mei, W. Ren, and Y. Song, "A unified framework for adaptive leaderless consensus of uncertain multi-agent systems under directed graphs," *IEEE Transactions on Automatic Control*, vol. 66, no. 12, pp. 6179–6186, 2021.

[121] J. Mei, W. Ren, and G. Ma, "Distributed containment control for lagrangian networks with parametric uncertainties under a directed graph," *Automatica*, vol. 48, no. 4, pp. 653–659, 2012.

[122] H. Wang, "Differential-cascade framework for consensus of networked lagrangian systems," *Automatica*, vol. 112, p. 10862, 2020.

[123] I. Katsoukis and G. A. Rovithakis, "A low complexity robust output synchronization protocol with prescribed performance for high-order heterogeneous uncertain mimo nonlinear multi-agent systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 6, pp. 3128–3133, 2022.

[124] C. Wang, C. Wen, Q. Hu, W. Wang, and X. Zhang, "Distributed adaptive containment control for a class of nonlinear multiagent systems with input quantization," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 6, pp. 2419–2428, 2018.

[125] A. K. Imai, R. R. Costa, H. Liu, G. Tao, and P. V. Kokotovic, "Multivariable adaptive control using high-frequency gain matrix factorization," *IEEE Transactions on Automatic Control*, vol. 49, no. 7, pp. 1152–1156, 2004.

[126] B. Song, "Decentralized dynamic surface control for a class of interconnected nonlinear systems," *In Proceedings of the American Control Conference*, pp. 130–135, 2006.

[127] X.-L. Wang, G.-H. Yang, and D. Zhang, "Optimal stealth attack strategy design for linear cyber-physical systems," *IEEE Transactions on Cybernetics*, vol. 52, no. 1, pp. 472–480, 2020.

[128] T.-Y. Zhang and D. Ye, "False data injection attacks with complete stealthiness in cyber–physical systems: A self-generated approach," *Automatica*, vol. 120, p. 109117, 2020.

[129] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 4–13, 2016.