Northumbria Research Link

Citation: Taoufik, Anass, Defoort, Michael, Busawon, Krishna, Dala, Laurent and Djemai, Mohamed (2020) A Distributed Observer-Based Cyber-Attack Identification Scheme in Cooperative Networked Systems under Switching Communication Topologies. Electronics, 9 (11). p. 1912. ISSN 2079-9292

Published by: MDPI

URL: https://doi.org/10.3390/electronics9111912 <https://doi.org/10.3390/electronics9111912>

This version was downloaded from Northumbria Research Link: http://nrl.northumbria.ac.uk/id/eprint/44758/

Northumbria University has developed Northumbria Research Link (NRL) to enable users to access the University's research output. Copyright © and moral rights for items on NRL are retained by the individual author(s) and/or other copyright owners. Single copies of full items can be reproduced, displayed or performed, and given to third parties in any format or medium for personal research or study, educational, or not-for-profit purposes without prior permission or charge, provided the authors, title and full bibliographic details are given, as well as a hyperlink and/or URL to the original metadata page. The content must not be changed in any way. Full items must not be sold commercially in any format or medium without formal permission of the copyright holder. The full policy is available online: http://nrl.northumbria.ac.uk/policies.html

This document may differ from the final, published version of the research and has been made available online in accordance with publisher policies. To read and/or cite from the published version of the research, please visit the publisher's website (a subscription may be required.)

Northumbria University NEWCASTLE

UniversityLibrary

electronics

MDPI

Article

A Distributed Observer-Based Cyber-Attack Identification Scheme in Cooperative Networked Systems under Switching Communication Topologies

Anass Taoufik [1,2,*], Michael Defoort [2], Krishna Busawon [1], Laurent Dala [1] and Mohamed Djemai [2]

[1] Department of Mechanical and Construction Engineering, Northumbria University,
Newcastle upon Tyne NE1 8ST, UK; krishna.busawon@northumbria.ac.uk (K.B.);
laurent.dala@northumbria.ac.uk (L.D.)

[2] LAMIH UMR CNRS 8201, Université Polytechnique Hauts-de-France, 59313 Valenciennes, France;
michael.defoort@uphf.fr (M.D.); mohamed.djemai@uphf.fr (M.D.)

* Correspondence: anass.taoufik@northumbria.ac.uk; Tel.: +447721071289

Received: 16 October 2020; Accepted: 11 November 2020; Published: 13 November 2020

Abstract: This paper studies an approach for detecting cyber attacks against networked cooperative systems (NCS) that are assumed to be working in a cyber-physical environment. NCS are prone to anomalies both due to cyber and physical attacks and faults. Cyber-attacks being more hazardous given the cooperative nature of the NCS may lead to disastrous consequences and thus need to be detected as soon as they occur by all systems in the network. Our approach deals with two types of malicious attacks aimed at compromising the stability of the NCS: intrusion attacks/local malfunctions on individual systems and deception/cyber-attacks on the communication between the systems. In order to detect and identify such attacks under switching communication topologies, this paper proposes a new distributed methodology that solves global state estimation of the NCS where the aim is identifying anomalies in the networked system using residuals generated by monitoring agents such that coverage of the entire network is assured. A cascade of predefined-time sliding mode switched observers is introduced for each agent to achieve a fast estimate of the global state whereby the settling time is an a priori defined parameter independently of the initial conditions. Then, using the conventional consensus algorithm, a set of residuals are generated by the agents that is capable of detecting and isolating local intrusion attacks and communication cyber-attacks in the network using only locally exchanged information. In order to prove the effectiveness of the proposed method, the framework is tested for a velocity synchronization seeking network of mobile robots.

Keywords: cyber security; networked control systems; predefined-time observers; multi-agent systems; cyber-physical systems; fault detection and isolation; switching topologies

1. Introduction

Networked Control Systems are control systems where the control loops are closed through a communication network whereby necessary signals for the control mission are exchanged among the system components through a network, namely wireless. Indeed, one of the main advantages of such systems is the capability of connecting their cyberspace to their physical space thus enabling the execution of several tasks from long distance. Figure 1 represents an example of a NCS, its environment and basic components. These systems, sometimes referred to as cyber-physical systems (CFS) [1,2] or multi-agent systems (MAS) in the literature [3], have attracted a lot of research interest in recent years due to their numerous potential use in various applications and industries ranging from flocking of mobile vehicles, terrestrial exploration, manufacturing plant monitoring, formation control in spacecraft flights to unmanned aerial vehicles and autonomous underwater vehicles, just to mention a few (see [4–9]).

However, the nature of NCS makes them extremely vulnerable to external malicious attacks while sharing information through a wireless network, which may compromise the efficiency of cooperative control algorithms and can lead to heavily degraded performances of the overall system and possibly to catastrophic effects. Consequently, the issue of cyber security in such systems has been attracting considerable attention in the literature [10,11].

Some of the research works have focused on local physical component faults, namely actuator and sensor faults (e.g., [12–16]). A relatively recent survey of different approaches to fault diagnosis in swarm systems was presented in [17], where the advantages of distributed designs in contrast with centralized and decentralized ones have been highlighted.

System security plays an increasingly enhanced role in the reliability of NCS as it allows for maintaining unbiased user defined coordination between the agents by detecting violating and malicious information. A few potential ways to violate security measures are deception or cyber-attacks. Indeed, these types of attacks are usually more difficult to identify as they can be coordinated. They typically include false data injection attacks (FDIA) [18], denial of service (DoS) [19], replay attacks [20], amongst others. Indeed, such types of attacks are aimed at destabilising the network by injecting control structures with deceptive information. A number of instances have been outlined in the past [21]. Detecting them has thus become a central focus for system security and control.

2. Related Work and Contribution

When it comes to cyber security in NCS, some of the works in literature has tackled problems such as false data injection in state estimation [18], secure computations in networked systems [22], to name a few. One way to increase resilience of MAS with respect to these faults is to design a robust control algorithm that is resilient to the effects of certain faults and attacks [23]. Another way, as pointed out in [24], is to develop monitoring schemes to detect failures in the MAS caused by attacks and faults.

On the other hand, [25] has provided an exhaustive literature review on model-based techniques in fault detection and isolation where observer-based techniques have proven to be powerful software-based tools in fault diagnosis due to their efficiency and online implementation capability. Such techniques have been used for instance in [26–35] for cyber-attack detection in NCS.

However, most of the works on observer-based attack detection of control systems consider centralized architectures, second order systems or do not consider the case of a possibly dynamic communication topologies. Unfortunately, the study of global fault detection for NCS with switching topologies subject to cyber-attacks is still in its infancy.

Motivated by all of the above and the recent works in [36] where a novel approach called predefined-time stability has been proposed, this paper introduces a new approach to identify faults and deception attacks in a cooperating networked system with a switching topology. The objective in this work is to deal with these non-cooperative and malicious activities. The proposed protocol makes an agent act as a central node monitoring the whole system activities in a distributed fashion. Compared to the existing works in the literature, our main contributions are:

(1) The design of a bank of distributed predefined-time sliding mode observers (SMO) for global state estimation for a multi-agent system with integrator dynamics whereby the convergence time is an a priori user defined parameter, in order to overcome the problem of attack detection under switching topologies.

(2) A residual based approach is proposed where the equivalent control concept is used to detect different faults and attacks that might occur anywhere in the system (i.e., an intrusion attack reflective of a local malfunction in agent or a cyber-attack affecting a communication link between

two agents) in a distributed way based on the topological properties of the network. This allows detection and identification of multiple simultaneous attacks and intrusions.

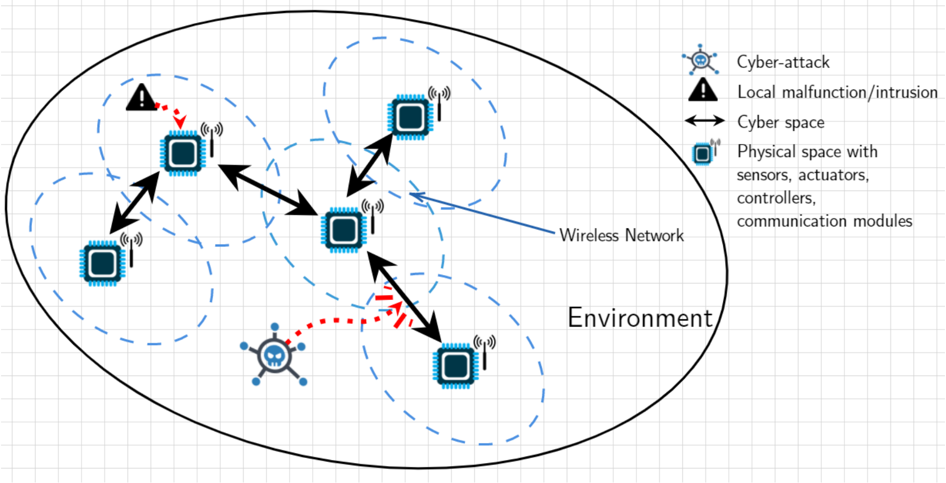

Cyber-attack
Local malfunction/intrusion
Cyber space
Physical space with sensors, actuators, controllers, communication modules
Wireless Network
Environment

Figure 1. An illustration of a networked control system, basic components, cyber-physical layers and possible attack types.

The rest of the manuscript is organized as follows: Section 2 provides a brief background on graph theory. Section 3 introduces some important definitions, lemmas and the problem formulation of the global fault detection and identification issue. Section 4 presents the main results, namely the design of banks of distributed predefined-time sliding mode observers for state estimation and residual generation based on local information. Section 5 presents numerical simulation results, where our approach is applied in the context of a practical application to consensus seeking fleet of mobile robots, in order to show the efficacy of our approach. Finally, Section 6 draws the main conclusions of this work and present future scopes for research on the considered topic.

Notations: The superscript T stands for the matrix transpose and we denote by I the identity matrix and by $\mathbf{1}$ the vector with all elements one, both with appropriate dimensions. The set of real-valued $m \times n$ matrices is given by $\mathbb{R}^{m\times n}$. $\lambda_{\min}(\cdot)$ represents the smallest non-zero eigenvalue of a square matrix $[\cdot]$. $\|\cdot\|_1$ and $\|\cdot\|_2$ denote the 1- and 2- norms, respectively. $(\cdot)_{eq}$ refers to the equivalent control value of $(\cdot)$ and $\mathcal{D}^+(\cdot)$ refers to the upper right-hand Dini derivative of $(\cdot)$. For the sake of simplicity, the time argument is omitted when it is not required for clarity. Table 1 presents a list of the employed acronyms:

Table 1. List of acronyms.

NCS	Networked Control Systems
CPS	Cyber-Physical Systems
MAS	Multi-Agent Systems
FDI	Fault Detection and Isolation
SMO	Sliding Mode Observers
FDIA	False Data Injection Attacks
DoS	Denial of Service

3. Graph Theory

In this paper, we are going to refer to networked systems as multi-agent systems and given that networked multi-agent systems need to exchange information amongst them, it is natural to model them using graph theory. In general, a communication topology composed of N systems is represented by $\mathcal{Q} = (\mathcal{N}, \mathcal{F})$ whereby $\mathcal{N} = \{1, ..., N\}$ is the node set consisting of N nodes/vertices each representing an agent, and $\mathcal{F} \subseteq \mathcal{N} \times \mathcal{N}$ is the edge set representing the communication links between two agents. Here, we shall assume that $\mathcal{Q}$ is connected, undirected and $\mathcal{N}_i \subset \{1, ..., N\} \backslash \{i\}$ is a non-empty subset of agents that agent i can interact with. In this work, we shall further assume that the communication topology is time-varying. As a result, we denote by $\tilde{T} = \{\tau_1, \tau_2, ..., \tau_M\}$ set of all possible known topologies and by $\mathcal{M} := \{1, ..., M\}$ the set of indices corresponding to these topologies. More precisely, the communication topology is characterised by a switching graph $\mathcal{Q}^{\sigma(t)} = \mathcal{Q}(t)$ where $\sigma(t) : [0, \infty) \longrightarrow \mathcal{M}$ is piecewise constant switching signal and determines the communication topology with $0 = t_0 < t_1 < t_2 ...$ being the switching instants of $\sigma(t)$. Furthermore, it is assumed that $\sigma(t)$ satisfies the minimum dwell time condition [37], and $t_{w+1} - t_w = \tau_w < T_w$ with T_w a known constant. Therefore, when $\sigma(t) = \mathrm{s} \in \mathcal{M}$, the topology $\mathcal{Q}(t) = \mathcal{Q}^{\sigma(t)} = \mathcal{Q}^{\mathrm{s}}$ is activated. For the rest of this paper, we refer to the active mode using the superscript s. The adjacency matrix $A^{\mathrm{s}} = [a^{\mathrm{s}}_{ij}] \in \mathbb{R}^{N \times N}$ is defined by $a^{\mathrm{s}}_{ij} > 0$ when the i^{th} agent can receive information from the j^{th} agent and $a^{\mathrm{s}}_{ij} = 0$ otherwise. The diagonal of matrix A^{s} is null since self-connections are not allowed. Let $\mathcal{D}^{\mathrm{s}}$ be the in-degree diagonal matrix with entries $d^{\mathrm{s}}_i = \sum_{j=1}^{N} a^{\mathrm{s}}_{ij}$. Then, the Laplacian matrix $\mathcal{L}^{\mathrm{s}}$ is defined as:

$$\mathcal{L}^{\mathrm{s}} = \mathcal{D}^{\mathrm{s}} - A^{\mathrm{s}} \in \mathbb{R}^{N \times N}$$

Let us denote by $\mathcal{L}^{\mathrm{s}}_i \in \mathbb{R}^{(N-1)\times(N-1)}$ the Laplacian matrix $\mathcal{L}^{\mathrm{s}}$ defined without agent i, and by:

$$\mathcal{L}^{i,\mathrm{s}} = diag(\ell^{i,\mathrm{s}}_1, \ldots, \ell^{i,\mathrm{s}}_{i-1}, \ell^{i,\mathrm{s}}_{i+1}, \ldots, \ell^{i,\mathrm{s}}_N) \in \mathbb{R}^{(N-1)\times(N-1)}$$

the associated diagonal matrix defining the interconnections between agent i and the remaining agents under the active topology s, $\ell^{i,\mathrm{s}}_k > 0$ if information of agent i is accessible by the k^{th} agent; otherwise $\ell^{i,\mathrm{s}}_k = 0$.

4. Preliminaries and Problem Statement

Before stating the main results, a brief overview of the techniques employed in our work are presented hereafter.

4.1. Definitions and Useful Lemmas

Consider the following nonlinear system:

$$\begin{cases} \dot{\xi}(t) & = \Phi(t, \xi(t); \phi) \\ \xi(0) & = \xi_0 \end{cases} \tag{1}$$

where $\xi(t) \in \mathbb{R}^n$ is the state and $\phi \in \mathbb{R}^g$ where $g \in \mathbb{N}$ is the system parameters considered to be constant ($\dot{\phi} = 0$). $\Phi : \mathbb{R}_+ \times \mathbb{R}^n$ is assumed to be a nonlinear function with its origin as an equilibrium point, i.e., $\Phi(t, 0; \phi) = 0$.

Definition 1 ([38]). *The origin of* (1) *is said to be globally finite-time stable if it is globally asymptotically stable and any solution* $\xi(t, \xi_0)$ *of* (1) *reaches the equilibrium point at some finite time moment, i.e.,* $\forall t \geqslant \Gamma(\xi_0)$, $\xi(t, \xi_0) = 0,$ *where* $\Gamma : \mathbb{R}^n \longrightarrow \mathbb{R}_+ \cup \{0\}$ *is called the settling-time function.*

Definition 2 ([39]). *The origin of* (1) *is a globally fixed-time equilibrium if it is globally finite-time stable and there exists a strictly positive number* T_{max} *such that for all* $\xi_0 \in \mathbb{R}^n$ *the settling-time function* $\Gamma : \mathbb{R}^n \to \mathbb{R}_+$ *is bounded, i.e.,* $\Gamma(\xi_0) \leqslant T_{max}$ *for all* $\xi_0 \in \mathbb{R}^n$*, the solution* $\xi(t, \xi_0)$ *of system* (3) *is defined and* $\xi(t, \xi_0) \in \mathbb{R}^n$ *for* $t \in [0, T_{max}) : \lim_{t \to T_{max}} \xi(t, \xi_0) = 0.$

Definition 3 ([36]). *For the parameter vector* ϕ *of system* (1) *and a constant* $T_p := T_p(\phi) > 0$*, the origin of* (1) *is said to be predefined-time stable if it is fixed-time stable and the settling-time function* $\Gamma : \mathbb{R}^n \to \mathbb{R}$ *is such that for all* $\xi_0 \in \mathbb{R}^n$, $\Gamma(\xi_0) \leqslant T_p$ *and* $T_p = \sup_{\xi_0 \in \mathbb{R}^n} \Gamma(\xi_0)$.

Let us recall some lemmas concerning predefined-time stability.

Lemma 1 ([40]). *Consider the system*

$$\dot{\xi}(t) = -\left(\alpha|\xi(t)|^p + \eta|\xi(t)|^q\right)^r sign(\xi(t)), \quad \xi(0) = \xi_0$$

with $\xi \in \mathbb{R}$. The parameters of the system are real numbers $\alpha, \eta, p, q, r \ > 0$ satisfying the constraints $rp < 1$, $rq > 1$. Let $\phi = [\alpha, \eta, p, q, r]^T \in \mathbb{R}^5$ be the parameter vector, then its origin $\xi = 0$ is fixed-time stable and the settling time function satisfies $T(\xi_0) \leq T_f = \gamma(\phi)$, where:

$$\gamma(\phi) = \frac{\Gamma(\frac{1-rp}{q-p})\Gamma(\frac{rq-1}{q-p})}{\Gamma(r)(q-p)\alpha^r}\left(\frac{\alpha}{\eta}\right)^{\frac{1-rp}{q-p}} \tag{2}$$

and $\Gamma(\cdot)$ is the well known Gamma function defined as $\Gamma(z) = \int_0^{+\infty} e^{-t}t^{z-1}dt$.

Remark 1. *The concept of predefined-time stability is introduced where a settling time bound T_p is set in advance as a function of system parameters ϕ, i.e., $T_p = T_p(\phi)$, and a strong notion of this class of stability is given when $T_p = T_f$, i.e., T_p is the least upper bound of the settling time.*

Lemma 2 ([40]). *Let us consider the nonlinear system (1) with $\xi(0)$ as the initial condition, where $\xi(t) \in \mathbb{R}^n$ is the state and $\phi \in \mathbb{R}^u$ with $u \in \mathbb{N}$, is the system parameters considered to be constant. $\Phi : \mathbb{R}_+ \times \mathbb{R}^n$ is assumed to be a nonlinear function with its origin as an equilibrium point. Suppose there exists a continuous radially unbounded candidate Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}$ such that*

$$\begin{aligned} &V(0) = 0 \\ &V(\xi) > 0, \quad \forall \xi \in \mathbb{R}^n \backslash \{0\}, \end{aligned}$$

and its derivative along the trajectories of (1) satisfies

$$\mathcal{D}^+ V(\xi) \leqslant -\tfrac{\gamma(\phi)}{T_p}\left(\alpha V^p + \eta V^q\right)^r, \quad \forall \xi \in \mathbb{R}^n \backslash \{0\},$$

with $\alpha, \eta,\ p,\ q,\ r > 0$, $rp < 1$, $rq > 1$, $\gamma(\phi)$ is given in (2) and $\mathcal{D}^+ V$ is the upper right-hand Dini derivative of $V(\xi)$. Then, the origin is predefined-time stable with predefined time T_p.

Now, let us recall some complementary key lemmas that will be used throughout this paper.

Lemma 3. *Let $n \in N$. If $a = (a_1, \ldots, a_n)$ is a sequence of positive numbers, then the following inequality is satisfied:*

$$\frac{1}{n}\sum_{i=1}^{N} a_i\left(\alpha a_i^p + \eta a_i^q\right)^k \geqslant \left(\frac{1}{n}\sum_{i=1}^{N} a_i\right)\left(\alpha\left(\frac{1}{n}\sum_{i=1}^{N} a_i\right)^p + \eta\left(\frac{1}{n}\sum_{i=1}^{N} a_i\right)^q\right)^k$$

for $\alpha, \eta, p, q, k \ > 0$ with $pk < 1$ and $qk > 1$.

Lemma 4. *Let f be the function defined as*

$$f(z) = z(\alpha z^p + \eta z^q)^k$$

for $\alpha, \eta, p, q, k \ > 0$ with $pk < 1$ and $qk > 1$. Then, $f(z)$ is monotonically increasing for all $z > 0$.

Lemma 5 ([41]). *Let* $z = [z_1, \dots, z_N]^T \in \mathbb{R}^N$ *and*

$$||z||_p = \sqrt[p]{\sum_{i=1}^{N} |z_i|^p}$$

Then, $\forall l \geqslant r$: $||z||_l \leqslant ||z||_r$.

4.2. Problem Statement

Consider a homogeneous multi-agent system composed of N agents labelled by $i \in \{1, ..., N\}$, and described by the following nth-order dynamics

$$\begin{cases} \dot{\xi}_{i,1}(t) & = \xi_{i,2}(t) \\ \dot{\xi}_{i,2}(t) & = \xi_{i,3}(t) \\ \vdots & \\ \dot{\xi}_{i,n-1}(t) & = \xi_{i,n}(t) \\ \dot{\xi}_{i,n}(t) & = u_i(t) + f_i^a(t) \\ z_i(t) & = \xi_{i,1}(t) \end{cases} \tag{3}$$

where $\xi_{i,l}(t) \in \mathbb{R}$ is agent i's l^{th} state variable with $\xi_i(t) = [\xi_{i,1}(t), \xi_{i,2}(t), ..., \xi_{i,n}(t)]^T \in \mathbb{R}^n$, $f_i^a(t) \in \mathbb{R}$ is a process fault affecting the dynamics of the agent which could be exogenous and might correspond to an internal malfunction, local intrusion attack, etc, $u_i(t) \in \mathbb{R}$ is the control input and $z_i(t) \in \mathbb{R}$ is agent i's internal measurement. Note that there is a multitude of practical applications of such systems, namely robotic systems, power systems, etc. Research on cyber-attack identification for such systems is of both practical and theoretical significance.

Furthermore, it is considered that agents have access to their control inputs, but they do not receive their neighbours' inputs. If needed, they have to reconstruct them using state estimates from exchanged information which are possibly corrupted. The exchanged information is expressed as

$$\begin{cases} z_{ki}(t) = \ell_k^{i,\mathsf{s}}(z_i(t) + \check{f}_{ki}^e(t)), \\ \hat{z}_i^{kj}(t) = a_{kj}^{\mathsf{s}}(\hat{z}_i^j(t) + f_{kj}^e(t)) \end{cases} \tag{4}$$

where $z_{ki}(t) \in \mathbb{R}$ is agent i's output signal sent to agent k with $z_{kk}(t) = z_k(t)$, and $\hat{z}_i^{kj}(t) \in \mathbb{R}$ is agent j's estimate of agent i's output which is sent to agent k, the term $\hat{z}_i^j(t)$ will be defined in the next Section. Both pieces of information are subject to an edge fault denoted $\check{f}_{ki}^e(t) \in \mathbb{R}$ and $f_{kj}^e(t) \in \mathbb{R}$, respectively. Note that, these types of faults may affect all broadcasted information of an agent to another. This might include DoS, FDIA, deception attacks, cyber-attacks, etc. In this paper, a solution to the following questions is investigated:

- How can we detect a cyber-attack anywhere in the MAS while keeping a distributed approach of the detection scheme?
- How can we distinguish said attacks from local malfunctions/intrusions?

The conceptual idea in this work is that information locally produced by the sensors is considered to be secure, while the one sent over the communication network/cyber layer of the system is vulnerable to external attacks. The next section lays out our main results.

5. Proposed Methodology

The proposed distributed bank of predefined-time observers for output and state estimation and global cyber-attack detection scheme is laid out in this section.

5.1. Global Output and State Estimation

Let us define the 'monitored' agent i as the agent to be diagnosed by a 'monitoring' agent k. First, let us consider the case of a fixed communication topology, where no cyber-attack exists in the system (i.e., $\check{f}^e_{ki} = f^e_{kj} = 0$). Denote by $\hat{\xi}^k_{i,l}$, agent k's estimate of the l^{th} state variable of agent i and by $\hat{z}^k_i$, agent k's estimate of agent i's output. The proposed distributed switched observer takes the following structure:

$$\begin{cases} \dot{\hat{\xi}}^k_{i,1} & = \hat{\xi}^k_{i,2} + \mathcal{V}(\mathcal{I}^k_{i,1}) = \hat{z}^k_i \\ \vdots & \\ \dot{\hat{\xi}}^k_{i,n-1} & = \hat{\xi}^k_{i,n} + E^{\mathsf{s}}_{n-2}\mathcal{V}(\mathcal{I}^k_{i,n-1}) \\ \dot{\hat{\xi}}^k_{i,n} & = E^{\mathsf{s}}_{n-1}\mathcal{V}(\mathcal{I}^k_{i,n}) \end{cases} \tag{5}$$

with $\mathcal{V}(\mathcal{I}^k_{i,l}) = \kappa^{k,\mathsf{s}}_l\big((\alpha|\mathcal{I}^k_{i,l}|^p + \eta|\mathcal{I}^k_{i,l}|^q)^r + \delta^{\mathsf{s}}_l\big)\mathrm{sign}(\mathcal{I}^k_{i,l})$,

$$\begin{cases} \mathcal{I}^k_{i,1} = \sum_{j=1}^N a^{\mathsf{s}}_{kj}(\hat{z}^{kj}_i - \hat{z}^k_i) + \ell^{i,\mathsf{s}}_k(z_{ki} - \hat{z}^k_i) \\ \mathcal{I}^k_{i,m} = \tilde{\xi}^k_{i,m} - \hat{\xi}^k_{i,m}, \quad m \in \{2, ..., n\} \end{cases} \tag{6}$$

The auxiliary state variables $\tilde{\xi}^k_{i,m}$, $\forall m \in \{2, ..., n\}$ are defined as

$$\begin{cases} \tilde{\xi}^k_{i,2} & = \hat{\xi}^k_{i,2} + E^{\mathsf{s}}_1\kappa^{k,\mathsf{s}}_1\delta^{\mathsf{s}}_1\mathrm{sign}(\mathcal{I}^k_{i,1})_{eq} \\ \vdots & \\ \tilde{\xi}^k_{i,n-1} & = \hat{\xi}^k_{i,n-1} + E^{\mathsf{s}}_{n-2}\kappa^{k,\mathsf{s}}_{n-2}\delta^{\mathsf{s}}_{n-2}\mathrm{sign}(\mathcal{I}^k_{i,n-2})_{eq} \\ \tilde{\xi}^k_{i,n} & = \hat{\xi}^k_{i,n} + E^{\mathsf{s}}_{n-1}\kappa^{k,\mathsf{s}}_{n-1}\delta^{\mathsf{s}}_{n-1}\mathrm{sign}(\mathcal{I}^k_{i,n-1})_{eq} \end{cases} \tag{7}$$

where the subscript eq denotes the equivalent value of sign function. In the following, it is assumed that the effect of the filter dynamics is negligible w.r.t. those of the observer. Let us define the errors as

$$\begin{cases} \varepsilon^k_{i,1} & = z_{ki} - \hat{z}^k_i \\ \varepsilon^k_{i,m} & = \xi_{i,m} - \hat{\xi}^k_{i,m}, \quad \forall m \in \{2, ..., n\} \end{cases}$$

Differentiating them yields the following error dynamics:

$$\begin{cases} \dot{\varepsilon}^k_{i,1} & = \varepsilon^k_{i,2} - \kappa^{k,\mathsf{s}}_1\big((\alpha|\mathcal{I}^k_{i,1}|^p + \eta|\mathcal{I}^k_{i,1}|^q)^r + \delta^{\mathsf{s}}_1\big)\mathrm{sign}(\mathcal{I}^k_{i,1}) \\ \vdots & \\ \dot{\varepsilon}^k_{i,n-1} & = \varepsilon^k_{i,n} - E^{\mathsf{s}}_{n-2}\kappa^{k,\mathsf{s}}_{n-1}\big((\alpha|\mathcal{I}^k_{i,n-1}|^p + \eta|\mathcal{I}^k_{i,n-1}|^q)^r \\ & \quad +\delta^{\mathsf{s}}_{n-1}\big)\mathrm{sign}(\mathcal{I}^k_{i,n-1}) \\ \dot{\varepsilon}^k_{i,n} & = u_i + f^a_i - E^{\mathsf{s}}_{n-1}\kappa^{k,\mathsf{s}}_n\big((\alpha|\mathcal{I}^k_{i,n}|^p + \eta|\mathcal{I}^k_{i,n}|^q)^r + \delta^{\mathsf{s}}_n\big)\mathrm{sign}(\mathcal{I}^k_{i,n}) \end{cases} \tag{8}$$

where $\mathcal{I}^k_{i,1}$ can be expressed in terms of the output estimation errors as $\mathcal{I}^k_{i,1} = \sum_{j=1}^N a^{\mathsf{s}}_{kj}(\varepsilon^j_{i,1} - \varepsilon^k_{i,1}) + \ell^{i,\mathsf{s}}_k\varepsilon^k_{i,1}$. Putting (8) in compact form, the following is obtained:

$$\begin{cases} \dot{\mathcal{E}}_{i,1} & = \mathcal{E}_{i,2} - \mathcal{H}(\mathcal{E}_{i,1}) \\ \vdots & \\ \dot{\mathcal{E}}_{i,n-1} & = \mathcal{E}_{i,n} - E^{\mathsf{s}}_{n-2}\mathcal{H}(\mathcal{E}_{i,n-1}) \\ \dot{\mathcal{E}}_{i,n} & = \mathbf{1}(u_i + f^a_i) - E^{\mathsf{s}}_{n-1}\mathcal{H}(\mathcal{E}_{i,n}) \end{cases} \tag{9}$$

where for each agent $\forall i \in \{1, ..., N\}$ and $\forall l \in \{1, ..., n\}$, the estimation errors, the state estimates and the auxiliary variables are concatenated in the vectors: $\mathcal{E}_{i,l} = [\varepsilon^1_{i,l}, ..., \varepsilon^N_{i,l}]^T$, $\hat{X}_{i,l} = [\hat{\xi}^1_{i,l}, ..., \hat{\xi}^N_{i,l}]^T$, $\tilde{X}_{i,l} = [\tilde{\xi}^1_{i,l}, ..., \tilde{\xi}^N_{i,l}]^T$. Let us denote $L^{\mathsf{s}}_i = \mathcal{L}^{i,\mathsf{s}} + \mathcal{L}^{\mathsf{s}}_i$. The terms $\mathcal{H}(\mathcal{E}_{i,l}), \forall l \in \{1, ..., n\}$ are expressed as

$$\begin{cases} \mathcal{H}(\mathcal{E}_{i,1}) & = \kappa_1^{i,\mathsf{s}}\big((\alpha|L_i^{\mathsf{s}}\mathcal{E}_{i,1}|^p + \eta|L_i^{\mathsf{s}}\mathcal{E}_{i,1}|^q)^k + \delta_1^{\mathsf{s}}\big)\mathrm{sign}(L_i^{\mathsf{s}}\mathcal{E}_{i,1}) \\ \mathcal{H}(\mathcal{E}_{i,m}) & = \kappa_m^{i,\mathsf{s}}\big((\alpha|\mathcal{E}_{i,m}|^p + \eta|\mathcal{E}_{i,m}|^q)^k + \delta_m^{\mathsf{s}}\big)\mathrm{sign}(\mathcal{E}_{i,m}), \quad \forall m \in \{2, ..., n\} \end{cases}$$

Assumption 1. *For every agent, the state variables, the control and fault signals are bounded, and their maximum values are known, i.e., for $\bar{\xi}_{i,l}, \bar{u}, \bar{f}^a \in \mathbb{R}_+$, $i \in \{1, ..., N\}$ and $l \in \{1, ..., n\}$: $|\xi_{i,l}(t)| \leqslant \bar{\xi}_{i,l}$, $|u_i(t)| \leqslant \bar{u}$, $|f_i^a(t)| \leqslant \bar{f}^a$.*

Theorem 1. *Given Assumption 1, for a fixed communication topology and in the absence of cyber-attack, for each agent, the observation errors (9) converge towards zero in a predefined time $T^{\mathsf{s}} = \sum_{j=1}^{n-1} T_p^{j,\mathsf{s}}$ independently of initial conditions, with the observer gains:*

$$\begin{cases} \delta_q^{\mathsf{s}} & = \dfrac{\bar{\xi}_{i,q+1}}{\kappa_q^{\mathsf{s}}}, \quad \forall q \in \{1, ..., n-1\} \\ \delta_n^{\mathsf{s}} & = \dfrac{\bar{u} + \bar{f}^a}{\kappa_n} \end{cases} \tag{10}$$

with

$$\begin{cases} \kappa_1^{i,\mathsf{s}} & = \dfrac{N\gamma(\phi)}{\lambda_i^{\mathsf{s}} T_p^{1,\mathsf{s}}} \\ \kappa_m^{i,\mathsf{s}} & = \dfrac{N\gamma(\phi)}{T_p^{m,\mathsf{s}}}, \quad \forall m \in \{2, ..., n\} \end{cases}$$

and

$$E_q^{\mathsf{s}} = \begin{cases} 1 & \textit{when} \quad t \geqslant \sum_{j=1}^{q} T_p^{j,\mathsf{s}} \\ 0 & \textit{otherwise} \end{cases}, \quad \forall q \in \{1, ..., n-1\}$$

where $\kappa_m^{\mathsf{s}} = min\{\kappa_m^{1,\mathsf{s}}, \ldots, \kappa_m^{N,\mathsf{s}}\}$ and $\lambda_{min}(L_i^{\mathsf{s}}) = \lambda_i^{\mathsf{s}}$. $\gamma(\phi)$ is defined in Equation (2), E_m^{s} represents the observer switches and $T_p^{m,\mathsf{s}}$ is the settling-time for each dynamic which is an user-defined parameter, considered to be the same for all of the m^{th} dynamics of the agents for notational convenience.

Proof of Theorem 1. The proof is done step by step by taking advantage of the switching conditions. Indeed, due to this, at each step, only a one-dimensional, corresponding sub-dynamical system is studied.

Step 1: Initially, $E_1^{\mathsf{s}} = E_2^{\mathsf{s}} = ... = 0$, the error dynamics are expressed as

$$\begin{cases} \dot{\mathcal{E}}_{i,1} & = \mathcal{E}_{i,2} - \mathcal{H}(\mathcal{E}_{i,1}) \\ \vdots & \\ \dot{\mathcal{E}}_{i,n-1} & = \mathcal{E}_{i,n} \\ \dot{\mathcal{E}}_{i,n} & = \mathbf{1}(f_i^a + u_i) \end{cases} \tag{11}$$

Consider the following Lyapunov function associated with the concatenated first error dynamics of the agents

$$V_1^i = \frac{1}{N}\sqrt{\lambda_i^{\mathsf{s}} \mathcal{E}_{i,1}^T L_i^{\mathsf{s}} \mathcal{E}_{i,1}}$$

Differentiating it results in

$$\mathcal{D}^+ V_1^i = \frac{1}{N}\sqrt{\frac{\lambda_i^{\mathsf{s}}}{\mathcal{E}_{i,1}^T L_i^{\mathsf{s}} \mathcal{E}_{\,i,1}}}\, \mathcal{E}_{i,1}^T L_i^{\mathsf{s}}(\mathcal{E}_{i,2} - \mathcal{H}(\mathcal{E}_{i,1})) \tag{12}$$

By setting $\mathcal{S}_1 = [s_1^1, \ldots, s_1^N]^T = L_i^{\mathsf{s}}\mathcal{E}_{i,1}$, one obtains

$$\begin{aligned} \mathcal{D}^{+}V_1^i &= \frac{\sqrt{\lambda_i^{\mathsf{s}}}}{N}\Bigg(-\frac{1}{\sqrt{\mathcal{E}_{i,1}^T L_i^{\mathsf{s}} \mathcal{E}_{i,1}}} \textstyle\sum_{i=1}^N \kappa_1^{i,\mathsf{s}} |s_1^i| (\alpha |s_1^i|^p + \eta |s_1^i|^q)^r \\ &\quad -\frac{\delta_1^{\mathsf{s}}}{\sqrt{\mathcal{E}_{i,1}^T L_i^{\mathsf{s}} \mathcal{E}_{i,1}}} \textstyle\sum_{i=1}^N \kappa_1^{i,\mathsf{s}} |s_1^i| + \frac{\mathcal{E}_{i,1}^T L_i^{\mathsf{s}} \mathcal{E}_{i,2}}{\sqrt{\mathcal{S}_1^T \mathcal{E}_{i,1}}} \Bigg) \end{aligned} \tag{13}$$

Then, it follows that

$$\mathcal{D}^{+}V_1^i = \frac{\sqrt{\lambda_i^{\mathsf{s}}}}{N}(-\Delta_1(\mathcal{S}_1) + \Delta_2(\mathcal{S}_1))$$

with

$$\begin{cases} \Delta_1(\mathcal{S}_1) &= (\mathcal{E}_{i,1}^T L_i^{\mathsf{s}} \mathcal{E}_{i,1})^{-\frac{1}{2}} \sum_{i=1}^N \kappa_1^{i,\mathsf{s}} |s_1^i| (\alpha |s_1^i|^p + \eta |s_1^i|^q)^r \\ \Delta_2(\mathcal{S}_1) &= -\delta_1^{\mathsf{s}} (\mathcal{E}_{i,1}^T L_i^{\mathsf{s}} \mathcal{E}_{i,1})^{-\frac{1}{2}} \sum_{i=1}^N \kappa_1^{i,\mathsf{s}} |s_1^i| + \mathcal{E}_{i,1}^T L_i^{\mathsf{s}} \mathcal{E}_{i,2} (\mathcal{S}_1^T \mathcal{E}_{i,1})^{-\frac{1}{2}} \end{cases}$$

Considering Lemma 3, and taking into account the fact that $\sum_{i=1}^N \kappa_1^{i,\mathsf{s}} \geqslant \kappa_1^{\mathsf{s}}$ and $||\mathcal{S}_1||_1 = \sum_{i=1}^N |s_1^i|$, the term $\Delta_1(\mathcal{S}_1)$ can be expressed as

$$\Delta_1(\mathcal{S}_1) \geqslant \frac{\kappa_1^{\mathsf{s}} ||\mathcal{S}_1||_1}{\sqrt{\mathcal{E}_{i,1}^T L_i^{\mathsf{s}} \mathcal{E}_{i,1}}} (\alpha (\tfrac{1}{N} \textstyle\sum_{i=1}^N ||\mathcal{S}_1||_1)^p + \eta (\tfrac{1}{N} \textstyle\sum_{i=1}^N ||\mathcal{S}_1||_1)^q)^r \tag{14}$$

Using Lemma 5, it can be shown that

$$||\mathcal{S}_1||_1 \geqslant ||\mathcal{S}_1||_2 = (\mathcal{S}_1)^T(\mathcal{S}_1) = \sqrt{(\mathcal{E}_{i,1})^T (L_i^{\mathsf{s}})^2 (\mathcal{E}_{i,1})} \tag{15}$$

By expressing $\mathcal{E}_{i,1}$ as a linear combination of the eigenvectors of L_i^{s}, the term $\mathcal{E}_{i,1}^T (L_i^{\mathsf{s}})^2 \mathcal{E}_{i,1}$ can be bounded as

$$\mathcal{E}_{i,1}^T (L_i^{\mathsf{s}})^2 \mathcal{E}_{i,1} \geqslant \lambda_i^{\mathsf{s}} \mathcal{E}_{i,1}^T L_i^{\mathsf{s}} \mathcal{E}_{i,1}$$

Thus, using Lemma 4, one has

$$-\Delta_1(\mathcal{S}_1) \leqslant -\kappa_1^{\mathsf{s}} \sqrt{\lambda_i^{\mathsf{s}}} \big(\alpha (V_1^i)^p + \eta (V_1^i)^q\big)^r \tag{16}$$

On the other hand, from the second term $\Delta_2(\mathcal{S}_1)$, the following can be deduced

$$\begin{aligned} \Delta_2(\mathcal{S}_1) &\leqslant \lambda_i^{\mathsf{s}} \Bigg(-\frac{\delta_1^{\mathsf{s}}}{||\mathcal{S}_1||} \textstyle\sum_{i=1}^N \kappa_1^{i,\mathsf{s}} |s_1^i| + \frac{(\mathcal{S}_1)^T}{||\mathcal{S}_1||} (\mathcal{E}_{i,2}) \Bigg) \\ &\leqslant \lambda_i^{\mathsf{s}} (-\kappa_1^{\mathsf{s}} \delta_1^{\mathsf{s}} + \bar{\xi}_{i,2}) \\ &\leqslant 0 \end{aligned} \tag{17}$$

By combining (16) and (17), the following is obtained from (13)

$$\begin{aligned} \mathcal{D}^{+}V_1^i &\leqslant -\frac{\kappa_1^{\mathsf{s}}}{N} \lambda_i^{\mathsf{s}} \big(\alpha (V_1^i)^p + \eta (V_1^i)^q\big)^r \\ &\leqslant -\frac{\gamma(\phi)}{T_p^{1,\mathsf{s}}} \big(\alpha (V_1^i)^p + \eta (V_1^i)^q\big)^r \end{aligned} \tag{18}$$

Therefore, in accordance with Lemma 2, $\mathcal{E}_{i,1}$ converges towards the origin with the settling time $T_p^{1,\mathsf{s}}$ (i.e., $\mathcal{E}_{i,1} = \dot{\mathcal{E}}_{i,1} = 0$). As a result, at $t = T_p^{1,\mathsf{s}}$ ($E_1^{\mathsf{s}} = 1$), we have

$$\begin{aligned} \mathcal{E}_{i,2} - \mathcal{H}(\mathcal{E}_{i,1})_{eq} &= X_{i,2} - \hat{X}_{i,2} - \mathcal{H}(\mathcal{E}_{i,1})_{eq} \\ &= 0 \end{aligned} \tag{19}$$

Hence, one gets $\tilde{X}_{i,2} = X_{i,2}$. At this point, one can go to the next step.

Step 2: At $t = T_p^{1,\mathsf{s}}$, the error dynamics become

$$\begin{cases} \dot{\mathcal{E}}_{i,2} & = \mathcal{E}_{i,3} - \mathcal{H}(\mathcal{E}_{i,2}) \\ \vdots & \\ \dot{\mathcal{E}}_{i,n-1} & = \mathcal{E}_{i,n} \\ \dot{\mathcal{E}}_{i,n} & = \mathbf{1}(f_i^a + u_i) \end{cases} \tag{20}$$

Selecting the Lyapunov function $V_2^i = \frac{1}{N}\sqrt{\mathcal{E}_{i,2}^T \mathcal{E}_{i,2}}$ and by following the same reasoning as before, one gets

$$\begin{array}{ll} -\Delta_1(\mathcal{S}_2) & \leqslant -\kappa_2^{\mathsf{s}}\big(\alpha(V_2^i)^p + \eta(V_2^i)^q\big)^r \\ \Delta_2(\mathcal{S}_2) & \leqslant -\dfrac{\delta_2^{\mathsf{s}}}{||\mathcal{S}_2||}\sum_{i=1}^N \kappa_2^{i,\mathsf{s}}|s_2^i| + \dfrac{(\mathcal{S}_2)^T(\mathcal{E}_{i,3})}{||\mathcal{S}_2||} \\ & \leqslant -\kappa_2^{\mathsf{s}}\delta_2^{\mathsf{s}} + \bar{\bar{\xi}}_{i,3} \\ & \leqslant 0 \end{array} \tag{21}$$

with $\mathcal{S}_2 = [s_2^1, \ldots, s_2^N]^T = \mathcal{E}_{i,2}$. Then, it is straightforward to show that $\mathcal{D}^+ V_2^i \leqslant -\frac{\gamma(\phi)}{T_p^{2,\mathsf{s}}}\big(\alpha(V_2^i)^p + \eta(V_2^i)^q\big)^r$. Consequently, $\mathcal{E}_{i,2}$ converges towards the origin with the settling time $T_p^{1,\mathsf{s}} + T_p^{2,\mathsf{s}}$ (i.e., $\mathcal{E}_{i,2} = \dot{\mathcal{E}}_{i,2} = 0$). Therefore, at $t = T_p^{1,\mathsf{s}} + T_p^{2,\mathsf{s}}$ and $E_2^{\mathsf{s}} = 1$.

Step n: Now, fast forward to the *nth* step, at $t = \sum_{j=1}^{n-1} T_p^{j,\mathsf{s}}$, the error dynamics become

$$\dot{\mathcal{E}}_{i,n} \quad = \mathbf{1}(f_i^a + u_i) - \mathcal{H}(\mathcal{E}_{i,n}) \tag{22}$$

Taking as the Lyapunov function $V_n^i = \frac{1}{N}\sqrt{(\mathcal{E}_{i,n})^T(\mathcal{E}_{i,n})}$ and by setting $\mathcal{S}_n = [s_n^1, \ldots, s_n^N]^T = \mathcal{E}_{i,n}$, and following the same procedure as before, the following inequalities are obtained for the terms $\Delta_1(\mathcal{S}_n)$ and $\Delta_2(\mathcal{S}_n)$

$$\begin{array}{ll} -\Delta_1(\mathcal{S}_n) & \leqslant -\kappa_n^{\mathsf{s}}\big(\alpha(V_n^i)^p + \eta(V_n^i)^q\big)^r \\ \Delta_2(\mathcal{S}_2) & \leqslant -\dfrac{\delta_n^{\mathsf{s}}}{||\mathcal{S}_n||}\sum_{i=1}^N \kappa_n^{i,\mathsf{s}}|s_n^i| + \dfrac{(\mathcal{S}_n)^T\mathbf{1}(\bar{u} + \bar{f}^a)}{||\mathcal{S}_n||} \\ & \leqslant -\kappa_n^{\mathsf{s}}\delta_n^{\mathsf{s}} + \bar{u} + \bar{f}^a \\ & \leqslant 0 \end{array} \tag{23}$$

The proof is thus concluded at the *nth* step. □

Now, let us consider the presence of a possible cyber-attack in the network. Due to the presence of these attacks, the output estimation errors is expressed as

$$\varepsilon_{i,1}^k \quad = z_i - \hat{z}_i^k + \ell_k^{i,\mathsf{s}}\check{f}_{ki}^e + \sum_{j=1}^N a_{kj}^{\mathsf{s}} f_{kj}^e \tag{24}$$

In this case, the following theorem can be stated.

Theorem 2. *Given Assumption 1 and in the presence of one or multiple cyber attacks incident to agent k, in the case of fixed communication topology, the observation errors converge towards zero in a predefined time* $T^{\mathsf{s}} = \sum_{j=1}^{n-1} T_p^{j,\mathsf{s}}$ *independently of initial conditions, and the gains are given as*

$$\begin{cases} \delta_q^{\mathsf{s}} & = \dfrac{\bar{\bar{\xi}}_{i,q+1} + \bar{F}_k^{\mathsf{s}^{(q)}}}{\kappa_q^{\mathsf{s}}}, \quad \forall q \in \{1, \ldots, n-1\} \\ \delta_n^{\mathsf{s}} & = \dfrac{\bar{u} + \bar{f}^a + \bar{F}_k^{\mathsf{s}^{(n)}}}{\kappa_n^{\mathsf{s}}} \end{cases} \tag{25}$$

with

$$F_k^{\mathsf{s}^{(l)}} = \frac{d^l}{dt^l}(\ell_k^{i,\mathsf{s}} \check{f}_{ki}^e + \sum_{j=1}^{N} a_{kj}^{\mathsf{s}} f_{kj}^e), \quad \forall l \in \{1, ..., n\}$$

where $F_k^{\mathsf{s}^{(l)}}$ *corresponds to the* l^{th} *time derivative of* $F_k^{\mathsf{s}} = \ell_k^{i,\mathsf{s}} \check{f}_{ki}^e + \sum_{j=1}^N a_{kj}^{\mathsf{s}} f_{kj}^e$ *and* $\bar{F}_k^{\mathsf{s}^{(l)}}$ *is the corresponding upper bound. The gains* $\kappa_l^{i,\mathsf{s}}$ *and the observer switches* E_m^{s} *remain the same as in Theorem 1.*

Proof of Theorem 2. When cyber-attacks are considered, (6) becomes

$$\begin{cases} \mathcal{I}_{i,1}^k = \sum_{j=1}^N a_{kj}^{\mathsf{s}}(\hat{z}_i^j - \hat{z}_i^k) + \ell_k^{i,\mathsf{s}}(z_i - \hat{z}_i^k) \\ + \sum_{j=1}^N a_{kj}^{\mathsf{s}} f_{kj}^e + \ell_k^{i,\mathsf{s}} \check{f}_{ki}^e, \\ \mathcal{I}_{i,m}^k = \tilde{\xi}_{i,m}^k - \hat{\xi}_{i,m}^k, \quad m \in \{2, ..., n\} \end{cases} \tag{26}$$

Furthermore, the auxiliary variables (7) become

$$\begin{cases} \tilde{\xi}_{i,2}^k & = \hat{\xi}_{i,2}^k + E_1^{\mathsf{s}} \mathcal{V}(\mathcal{I}_{i,1}^k)_{eq} = \hat{\xi}_{i,2}^k + \varepsilon_{i,2}^k - \ell_k^{i,\mathsf{s}} \dot{\check{f}}_{ki}^e \\ & - \sum_{j=1}^N a_{kj}^{\mathsf{s}} \dot{f}_{kj}^e \\ \vdots & \\ \tilde{\xi}_{i,n}^k & = \hat{\xi}_{i,n}^k + E_{n-1}^{\mathsf{s}} \mathcal{V}(\mathcal{I}_{i,n-1}^k)_{eq} = \hat{\xi}_{i,n}^k + \varepsilon_{i,n}^k \\ & - \ell_k^{i,\mathsf{s}} \check{f}_{ki}^{e(n-1)} - \sum_{j=1}^N a_{kj}^{\mathsf{s}} f_{kj}^{e(n-1)} \end{cases} \tag{27}$$

and the concatenated errors are expressed as

$$\begin{cases} \dot{\mathcal{E}}_{i,1} & = \mathcal{E}_{i,2} + \mathbf{1} F_k^{\mathsf{s}^{(1)}} - \mathcal{H}(\mathcal{E}_{i,1}) \\ \vdots & \\ \dot{\mathcal{E}}_{i,n-1} & = \mathcal{E}_{i,n} + \mathbf{1} F_k^{\mathsf{s}^{(n-1)}} - E_{n-2}^{\mathsf{s}} \mathcal{H}(\mathcal{E}_{i,n-1}) \\ \dot{\mathcal{E}}_{i,n} & = \mathbf{1}(u_i + f_i^a + F_k^{\mathsf{s}^{(n)}}) - E_{n-1}^{\mathsf{s}} \mathcal{H}(\mathcal{E}_{i,n}) \end{cases} \tag{28}$$

The rest of the proof straightforwardly follows the same reasoning as Theorem 1 and is thus omitted for brevity. □

Note that the use of the predefined-time concept is very useful when dealing with switching topologies. Indeed, using our proposed scheme, one can immediately derive the following proposition:

Proposition 1. *Consider the switching topologies described in Section 2. Selecting* T^{s} *such that* $T^{\mathsf{s}} < T_w$, $\forall \mathsf{s} \in \mathcal{M}$ *and observer parameters (25), the distributed switched observers guarantee the predefined-time stability of the estimation errors regardless of initial conditions at each switching instant.*

Remark 2. *The global fault estimation protocol proposed in this paper, is a distributed one. Each neighbouring agent can only exchange local information during the fault estimation process. Furthermore, provided that all of the possible topologies are known to all agents, constants* λ_i^{s} *and therefore* $\kappa_1^{\mathsf{s}} = min\{\kappa_1^{1,\mathsf{s}}, \ldots, \kappa_1^{N,\mathsf{s}}\}$ *can be computed a priori. If all* $T_p^{m,\mathsf{s}}$ *are the same (i.e.,* $T_p^{1,\mathsf{s}} = \ldots = T_p^{n,\mathsf{s}} = T_p$*),* $\kappa_1^{\mathsf{s}} = \frac{N\gamma(\phi)}{gT_p}$ *with* $g = \max\{\lambda_1^{\mathsf{s}}, \ldots, \lambda_N^{\mathsf{s}}\}$*.*

5.2. Residual Definition and Cyber-Attack Identification

The idea is to compute the difference between the actual input of an agent and the estimated input effort. The difference should indeed be null in the case of no attacks or faults. The next step is to identify the source and type of faults, specifically deception attacks and thus trigger the appropriate alarms and further corrective measures. Note that, for Theorems 1 and 2, the upper bounds of the control inputs are used in Assumption 1 to design the predefined-time distributed observers. In this section, we will show through a residual based approach how one can detect process or communication faults/cyber-attacks with a global approach using input estimates if the control structure is known. In the following, let us consider the following typical linear higher-order consensus control algorithm [42,43], used with the available information

$$u_i = -\sum_{j \in \mathcal{N}_i} a^{\mathsf{s}}_{ij} \left[\gamma^{\mathsf{s}}_1 (z_i - z_{ij}) + \sum_{m=2}^{n} \gamma^{\mathsf{s}}_m (\tilde{\xi}^{i}_{i,m} - \tilde{\xi}^{i}_{j,m}) \right] + \mu^{\mathsf{s}}_i \tilde{\xi}^{i}_{i,n} \tag{29}$$

where $\forall l \in \{1, ..., n\}$, $\forall i \in \{1, ..., N\}$, γ^{s}_l and μ^{s}_i are the consensus gains. It can be noticed that communication faults spread in the MAS through u_i, and thus need to be detected as they occur. In the absence of edge faults, consensus is achieved provided a suitable selection of μ^{s}_i, γ^{s}_1 and γ^{s}_m due to the fixed-time stability property of the proposed distributed observers [44].

Proposition 2. *Define agent k as the monitoring agent, agent i as the monitored agent, agents $p \in \mathcal{N}_k$ as agent k's neighbours and agents $j \in \mathcal{N}_i$ as agent i's neighbours, where agent i may or may not be a direct neighbour of k and $j \neq i$. Using protocol (29), an agent k can detect a deception attack on a communication link incident to agent k or i and local malfunctions/intrusions f^a_i anywhere in the fleet, given one type fault happens at a time, using the following residual signal:*

$$r^k_i(t) = \mathcal{V}(\mathcal{I}^k_{i,n})_{eq} - \hat{u}^k_i \tag{30}$$

where

$$\hat{u}^k_i = -\sum_{j \in \mathcal{N}_i} a^{\mathsf{s}}_{ij} [\gamma^{\mathsf{s}}_1 (\hat{z}^k_i - \hat{z}^k_j) + \sum_{m=2}^{n} \gamma^{\mathsf{s}}_m (\tilde{\xi}^k_{i,m} - \tilde{\xi}^k_{j,m})] + \mu^{\mathsf{s}}_i \tilde{\xi}^k_{i,n}$$

is agent i's reconstructed input by agent k with $\hat{u}^k_k = u_k$.

Proof of Proposition 2. After the convergence of errors, the actual applied control input for each agent becomes

$$\begin{aligned} u_i = \quad & -\textstyle\sum_{j \in \mathcal{N}_i} a^{\mathsf{s}}_{ij} \left[\gamma^{\mathsf{s}}_1 (z_i - z_j) + \sum_{m=2}^{n} \gamma^{\mathsf{s}}_m (\xi_{i,m} - \xi_{j,m}) \right] \\ & + \mu^{\mathsf{s}}_i \xi_{i,n} - \textstyle\sum_{j \in \mathcal{N}_i} a^{\mathsf{s}}_{ij} (\gamma^{\mathsf{s}}_1 \check{f}^e_{ij} + \sum_{m=2}^{n} \gamma^{\mathsf{s}}_m \check{f}^{e^{(m-1)}}_{ij}) \end{aligned}$$

Furthermore, the reconstructed input generated by the monitoring agent k is expressed as

$$\begin{aligned} \hat{u}^k_i = \quad & -\textstyle\sum_{j \in \mathcal{N}_i} a^{\mathsf{s}}_{ij} \left[\gamma^{\mathsf{s}}_1 (z_i - z_j) + \sum_{m=2}^{n} \gamma^{\mathsf{s}}_m (\xi_{i,m} - \xi_{j,m}) \right] \\ & + \mu^{\mathsf{s}}_i \xi_{i,n} - \textstyle\sum_{j \in \mathcal{N}_i} \gamma^{\mathsf{s}}_1 a^{\mathsf{s}}_{ij} \left[\ell^{i,\mathsf{s}}_k \check{f}^e_{ki} - \ell^{j,\mathsf{s}}_k \check{f}^e_{kj} + \sum_{p \in \mathcal{N}_k} a^{\mathsf{s}}_{kp} f^e_{kp} \right. \\ & \left. - \textstyle\sum_{p \in \mathcal{N}_k} a^{\mathsf{s}}_{kp} f^e_{kp} \right] + \textstyle\sum_{j \in \mathcal{N}_i} \sum_{m=2}^{n} a^{\mathsf{s}}_{ij} \gamma^{\mathsf{s}}_m \left[\ell^{i,\mathsf{s}}_k \check{f}^{e^{(m-1)}}_{ki} \right. \\ & \left. + \ell^{j,\mathsf{s}}_k \check{f}^{e^{(m-1)}}_{kj} \right] + \mu^{\mathsf{s}}_i \left[\ell^{i,\mathsf{s}}_k \check{f}^{e^{(n-1)}}_{ki} + \textstyle\sum_{p \in \mathcal{N}_k} a^{\mathsf{s}}_{kp} f^{e^{(n-1)}}_{kp} \right] \end{aligned}$$

Therefore, the residual signals (30) become

$$\begin{aligned} r^k_i(t) \quad & = (u_i - \hat{u}^k_i) + f^a_i - \ell^{i,\mathsf{s}}_k \check{f}^{e^{(n)}}_{ki} - \textstyle\sum_{p \in \mathcal{N}_k} a^{\mathsf{s}}_{kp} f^{e^{(n)}}_{kp} \\ & = \Theta^k_{f^e} + f^a_i \end{aligned} \tag{31}$$

where $\Theta^k_{f^e}$ is

$$\begin{aligned}\Theta^k_{fe} &= \textstyle\sum_{j\in\mathcal{N}_i}\gamma^{\mathsf{s}}_1 a^{\mathsf{s}}_{ij}\left[\ell^{i,\mathsf{s}}_k \check{f}^e_{ki} - \ell^{j,\mathsf{s}}_k \check{f}^e_{kj} + \sum_{p\in\mathcal{N}_k} a^{\mathsf{s}}_{kp} f^e_{kp} - \sum_{p\in\mathcal{N}_k} a^{\mathsf{s}}_{kp} f^e_{kp}\right] \\ &\quad - \textstyle\sum_{j\in\mathcal{N}_i}\sum_{m=2}^{n} a^{\mathsf{s}}_{ij}\gamma^{\mathsf{s}}_m\left[\ell^{i,\mathsf{s}}_k \check{f}^{e(m-1)}_{ki} + \ell^{j,\mathsf{s}}_k \check{f}^{e(m-1)}_{kj}\right] - \mu^{\mathsf{s}}_i\left[\ell^{i,\mathsf{s}}_k \check{f}^{e(n-1)}_{ki}\right. \\ &\quad \left. + \textstyle\sum_{p\in\mathcal{N}_k} a^{\mathsf{s}}_{kp} f^{e(n-1)}_{kp}\right] - \sum_{j\in\mathcal{N}_i} a^{\mathsf{s}}_{ij}\left(\gamma^{\mathsf{s}}_1 \check{f}^e_{ij} + \sum_{m=2}^{n}\gamma^{\mathsf{s}}_m \check{f}^{e(m-1)}_{ij}\right) \\ &\quad - \ell^{i,\mathsf{s}}_k \check{f}^{e(n)}_{ki} - \textstyle\sum_{p\in\mathcal{N}_k} a^{\mathsf{s}}_{kp} f^{e(n)}_{kp}\end{aligned} \tag{32}$$

Note that, when the control efforts u_i are known to other agents in the network, the term $(u_i - \hat{u}^k_i)$ in Equation (31) disappears. In this case, the residual signals become

$$\begin{aligned} r^k_i(t) &= f^a_i - \ell^{i,\mathsf{s}}_k \check{f}^{e(n)}_{ki} - \textstyle\sum_{p\in\mathcal{N}_k} a^{\mathsf{s}}_{kp} f^{e(n)}_{kp} \\ &= \Theta^k_{fe} + f^a_i \end{aligned} \tag{33}$$

where $\Theta^k_{fe} = -\ell^{i,\mathsf{s}}_k \check{f}^{e(n)}_{ki} - \sum_{p\in\mathcal{N}_k} a^{\mathsf{s}}_{kp} f^{e(n)}_{kp}$. As a result, the defined residual signals (30) generated by the monitoring agent k are able to detect the presence of a cyber-attack or a local malfunction. □

Residual evaluation: Once the residual signals are generated, it is important to be able to interpret them in order to find the root of the fault and thus make corrective measures accordingly. Indeed, from Equation (30), it can be noticed that, when a cyber-attack incident to agent k or i occurs while there is no local malfunction, agent k's generated residual signal for itself is $r^k_k = 0$ and $r^k_i \neq 0$ for all $k \neq i$ regardless of whether or not agent i is a neighbour of k. On the other hand, when there is no cyber-attack, the residuals provide explicit estimations of the local malfunctions/intrusions, with $r^k_k = f^a_k$ and $r^k_i = f^a_i$. r^k_k is thus used to identify a cyber-attack in the system as it is only sensitive to local malfunctions/intrusions. The proposed cyber-attack identification scheme is thus summarized in the following Algorithm 1:

Algorithm 1: Observer Design and Decision Logic

```
Result: Distributed Cyber-attack Identification
while communication topology s is active do
    Choose observer convergence time $T^{\mathsf{s}}$ in accordance with Proposition 1;
    Define Laplacian sub-matrices $\mathcal{L}^{\mathsf{s}}_i$ and $\mathcal{L}^{i,\mathsf{s}}$;
    Compute observer gains from Theorems 1–2;
    Define a monitoring agent $k$;
    for $q \in \{1, 2, ..., N\}$ do
        Generate residual signals $r^k_q$ from Equation (30);
    end
    if $r^k_k = 0$ and $r^k_i = 0$ then
        No cyber-attack or local malfunctions/intrusions exist in the network;
        else if $r^k_k = 0$ and $r^k_i \neq 0$, $\forall i \neq k$ then
            A cyber-attack has occurred in the network;
        else if $r^k_k \neq 0$ and $r^k_i = 0$ then
            A local malfunction has occurred in agent $k$;
        else if $r^k_k = 0$ and $\exists! i \neq k$ such that $r^k_i \neq 0$ then
            A local malfunction has occurred in agent $i$;
    end
end
```

Remark 3. *Note that our approach does not present limitation with respect to the number of detectable attacks in the system, contrary to some existing works, for instance in [26]. Indeed, Proposition 2 can be used to detect simultaneous local malfunctions/intrusions and cyber-attacks, and discern them from each other thus achieving* *the cyber-attack identification objective. Moreover, the predefined-time stability principle is useful to design fast converging switched observers to solve the problem of switching communication topologies as pointed out in Proposition 1. This allows for avoiding false alarms and achieving fast convergence of the estimation errors before the next topology switching instant. Furthermore, it is worth mentioning that our proposed approach can also be used when sudden communication breaks occur or when communication attacks on the communication weights and sudden abnormal quality drops of the exchanged information (i.e., attacks on communication parameters a_{ij}^{s} defined in Section 2) are considered. Indeed, these types of attacks manifest themselves in the generated residuals as exponentially decaying signals.*

6. Practical Example

Cyber-Attack Identification in Cooperative Multi-Robot Systems

In this section, an illustrative numerical example is given for a practical application in order to show the effectiveness of the proposed global cyber-attack identification protocol. For this, let us consider a team of $N = 5$ omnidirectional wheeled mobile robots (WMR) that are labelled with numbers 1 through 5 and are moving in a two-dimensional plane (see Figure 2). In this example, the robots have to cooperate in order to render the steady state axial jerk null and thus achieve constant linear acceleration synchronization of the network of WMR.

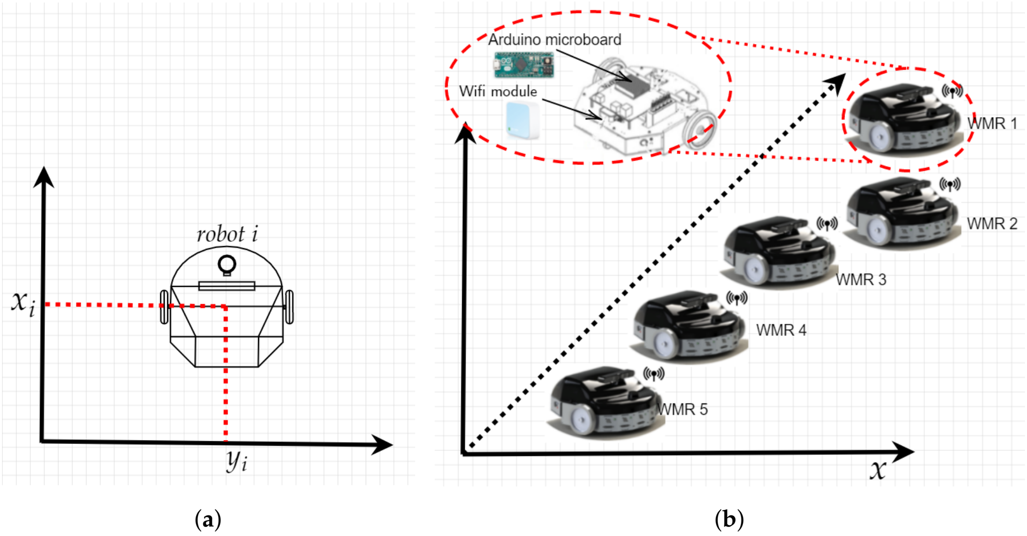


Figure 2. The setup of the studied problem where: (**a**) represents the upper perspective view of a WMR on the x-y 2D plane and (**b**) represents an illustration of the setup of the five mobile robots.

Here, we assume non-slipping and pure rolling conditions and since our aim is to achieve linear acceleration synchronization, only the dynamics along the x-direction are considered. In this case, each robot can be modelled with the following simplified triple integrator dynamics which is a special case of system (3):

$$\begin{cases} \dot{x}_i(t) &= \dot{\xi}_{i,1}(t) &= \xi_{i,2}(t) \\ \dot{v}_i(t) &= \dot{\xi}_{i,2}(t) &= \xi_{i,3}(t) \\ \dot{a}_i(t) &= \dot{\xi}_{i,3}(t) &= u_i(t) + f_i^a(t) \\ z_i(t) &= \xi_{i,1}(t) \end{cases}$$

where $\xi_{i,1}(t)$, $\xi_{i,2}(t)$, $\xi_{i,3}(t)$ and $f_i^a(t)$ are the x-position, the linear velocity on the x-axis, the linear acceleration on the x-axis and an internal fault affecting the local jerk of a robot. The proposed residual observer-based cyber-attack identification algorithm can be implemented on the on-board micro-controllers as depicted in Figure 2. Furthermore, the robots are assumed to be equipped with WiFi modules and broadcast their information through a wireless network described by the graph topologies illustrated in Figures 3 and 4 respectively, which are characterised by the Laplacian matrices:

$$\mathcal{L}^1 = \begin{bmatrix} 3 & -1 & -1 & 0 & -1 \\ -1 & 2 & 0 & -1 & 0 \\ -1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad \text{and} \quad \mathcal{L}^2 = \begin{bmatrix} 3 & -1 & 0 & -1 & -1 \\ -1 & 2 & -1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

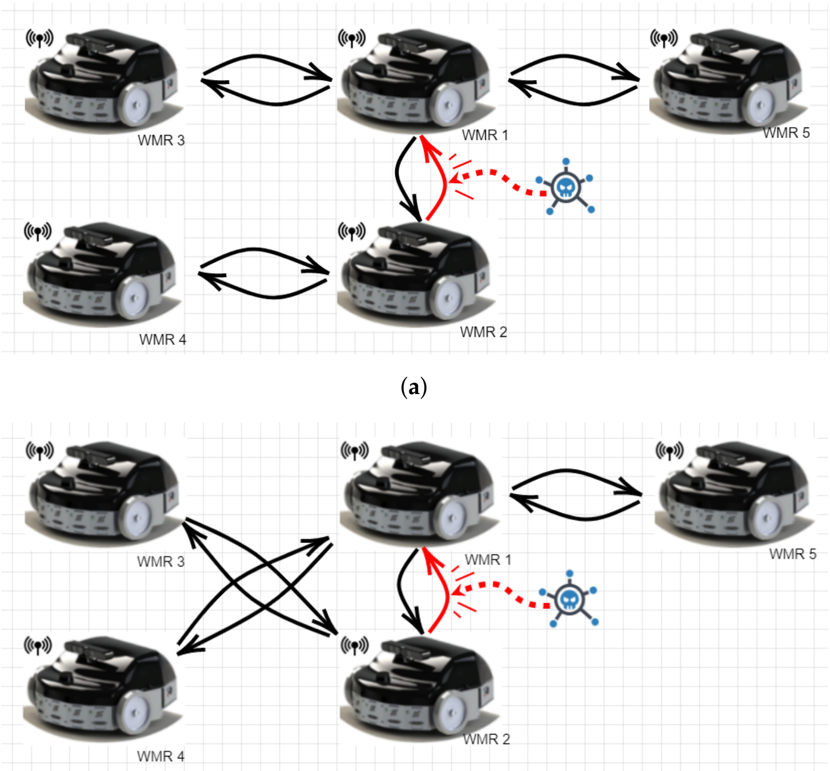
The communication topology is assumed to switch from $\mathcal{L}^1$ to $\mathcal{L}^2$ at $t_1 = 12$ s. In this example, in order to achieve acceleration consensus, the following cooperative control is used for each robot

$$u_i = a_i^r(t) + \mu_i^{\mathsf{s}} \tilde{\xi}^{i}_{i,3} - \textstyle\sum_{j=1}^{5} a_{ij}^{\mathsf{s}} \left[\gamma_1^{\mathsf{s}}(z_1 - z_{ij}) - \gamma_2^{\mathsf{s}}(\tilde{\xi}^{i}_{i,2} - \tilde{\xi}^{i}_{j,2}) - \gamma_3^{\mathsf{s}}(\tilde{\xi}^{i}_{i,3} - \tilde{\xi}^{i}_{j,3}) \right]$$

where $\forall i \in \{1, ..., N\}$, μ_i^{s}, γ_1^{s}, γ_2^{s} and γ_3^{s} are the consensus gains set to 5, 4, 3, and, 2.5, respectively, for both possible communication topology modes $\mathsf{s} \in \{1, 2\}$, and $a_i^r(t) = -\mu_i^{\mathsf{s}}\, 1\,\mathrm{m\,s^{-2}}$ is the reference acceleration. Hence, $\forall \mathsf{s} \in \{1, 2\}$, the exchanged signals between agents are given as

$$z_{ki}(t) = \ell_k^{i,\mathsf{s}}(z_i(t) + \check{f}_{ki}^{e}(t) + \Delta z_{ki}(t)), \quad \text{and} \quad \hat{z}_i^{kj}(t) = a_{kj}^{\mathsf{s}}(\hat{z}_i^{j}(t) + f_{kj}^{e}(t) + \Delta \hat{z}_i^{kj}(t))$$

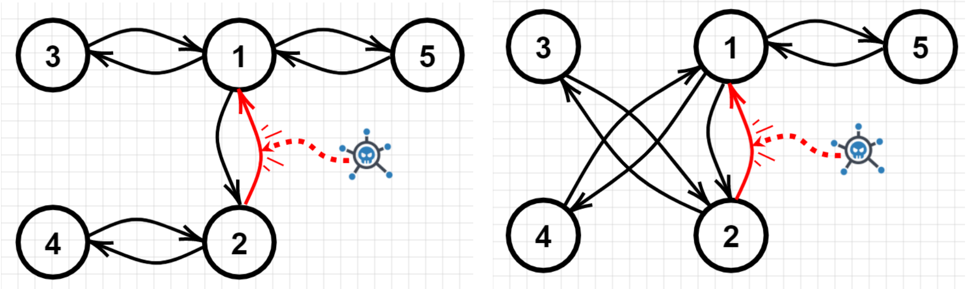
where $\Delta z_{ki}(t) = 0.1 \sin(z_{ki}(t))$, and $\Delta \hat{z}_i^{kj}(t) = 0.01 \sin(\hat{z}_i^{kj}(t))$ are noise due to some communication uncertainties.



(**a**)

(**b**)

Figure 3. An illustration of the interaction between the robots: (**a**) in the first 12 s and (**b**) after 12 s, where an arrow indicates the direction of information flow amongst two designated robots.



(**a**) (**b**)

Figure 4. The corresponding graph topology models, where: (**a**) corresponds to $\mathcal{L}^1$ and (**b**) to $\mathcal{L}^2$.

The initial positions of the five agents on the x-axis are given as $\xi_{1,1}(0) = 0$ m, $\xi_{2,1}(0) = 1.5$ m, $\xi_{3,1}(0) = 3$ m, $\xi_{4,1}(0) = 4.5$ m and $\xi_{5,1}(0) = 0.5$ m respectively, while the initial velocities and acceleration are set to 0. For each of the mobile robots, the distributed observers are designed to estimate the global state in the desired predefined time $T^1 = T^2 = 3$ s with $T_p^{1,1} = T_p^{2,1} = T_p^{3,1} = T_p^{1,2} = T_p^{2,2} = T_p^{3,2} = 1$ s which satisfies the conditions of Proposition 1. The observer parameters are chosen as

$$\phi = [\alpha, \eta, p, q, r]^T = [1, 2, 1.5, 3, 0.5]^T$$

used for each corresponding topology. On the other hand, to obtain the equivalent values, first-order low pass filters are used with cut-off frequency of 100 s^{-1} for the first dynamics and 10 s^{-1} for the second and third dynamics. In order to verify the performance of the proposed scheme, the following two simulation scenarios are carried out on MATLAB.

First Scenario: In the 1st scenario, an intrusion occurs in robot 3 causing an out of control situation that affects its local jerk simulated by the following function $f_3^a(t)$:

$$f_3^a(t) = \begin{cases} 0 & t < 4s \\ 0.5\sin(5t) + 15 & 5s \leqslant t \leqslant 8.5s \\ 0 & t > 8.5s \end{cases}$$

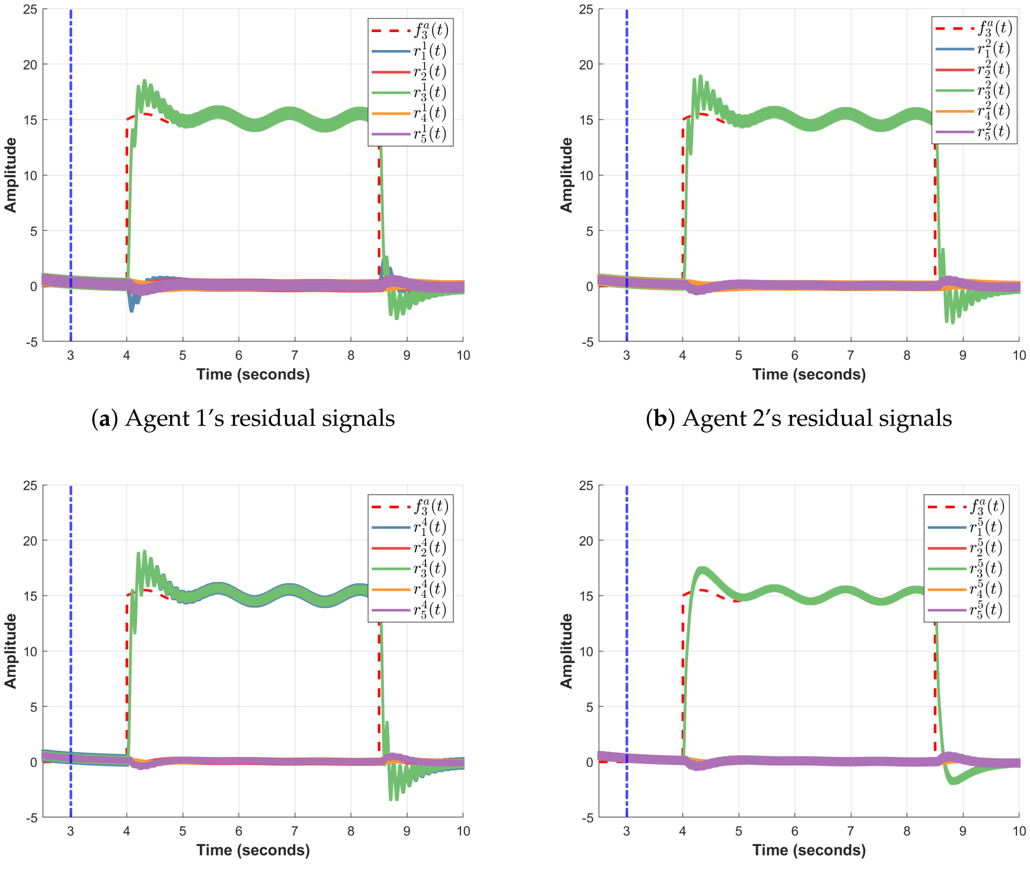
This fault only represents a local malfunction in the robot 3 and thus needs to be distinguished from a cyber-attack. It can be clearly seen from Figure 5 corresponding to the 1st scenario that the residuals generated by the monitoring agents for the monitored agent 3, i.e., r_3^1, r_3^2, r_3^4 and r_3^4 respectively, provide an explicit estimation of f_3^a.

Second Scenario: In the 2nd scenario, a communication fault occurs in exchanges flowing from robots 1 to 2 at $t = T^e = 10$ s, for the first topology such that

$$\check{f}_{12}^e(t) = f_{12}^e(t) = \begin{cases} 0 & t < 10\text{ s} \\ 100(1 - e^{1-0.1t}) & t \geqslant 10\text{ s} \end{cases}$$

Note that the topology switches at $t_1 = 13$ s and $\check{f}_{12}^e(t) = f_{12}^e(t)$ remains throughout the topology change (see Figure 4). Therefore, the gains are computed from Theorem 2 and Remark 2 as

$$\left\{ \begin{array}{ll} \kappa_1^1 & = 56.98 \\ \kappa_2^1 & = 24.98 \\ \kappa_3^1 & = 24.98 \\ \delta_1^1 & = 0.35 \\ \delta_2^1 & = 1.2 \\ \delta_3^1 & = 1.5 \end{array} \right. \quad \text{and} \quad \begin{array}{ll} \kappa_1^2 & = 58.92 \\ \kappa_2^2 & = 24.98 \\ \kappa_3^2 & = 19.98 \\ \delta_1^2 & = 0.33 \\ \delta_2^2 & = 1.2 \\ \delta_3^2 & = 1.5 \end{array}$$



(**a**) Agent 1's residual signals

(**b**) Agent 2's residual signals

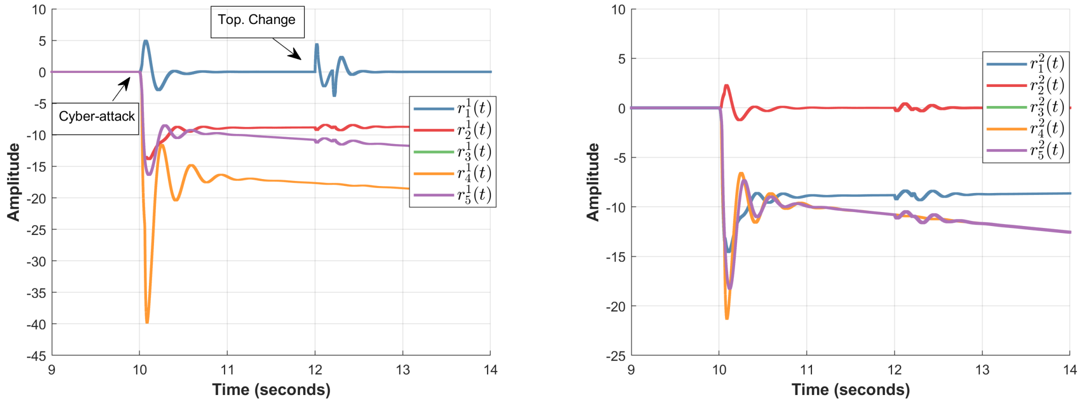
(**c**) Agent 4's residual signals

(**d**) Agent 5's residual signals

Figure 5. Residuals in scenario 1 by agents 1, 2, 4, and 5, shown in sub-figures (**a**–**d**) respectively. The vertical dashed blue line represents the convergence time.

It should be recalled that these gains are valid for both scenarios. Figure 6 corresponding to the 2nd scenario shows that a cyber-attack in the form of the simulated functions $\check{f}^e_{12}(t)$ and $f^e_{12}(t)$, incident to agent 1 in both topologies, can be distinguished even in the presence of some reasonable communication noise. Indeed, the residual signals r_1^1, r_2^2, r_3^3, r_4^4 and r_5^5 stay around 0 after the cyber-attack appears in the system and throughout the topology change.

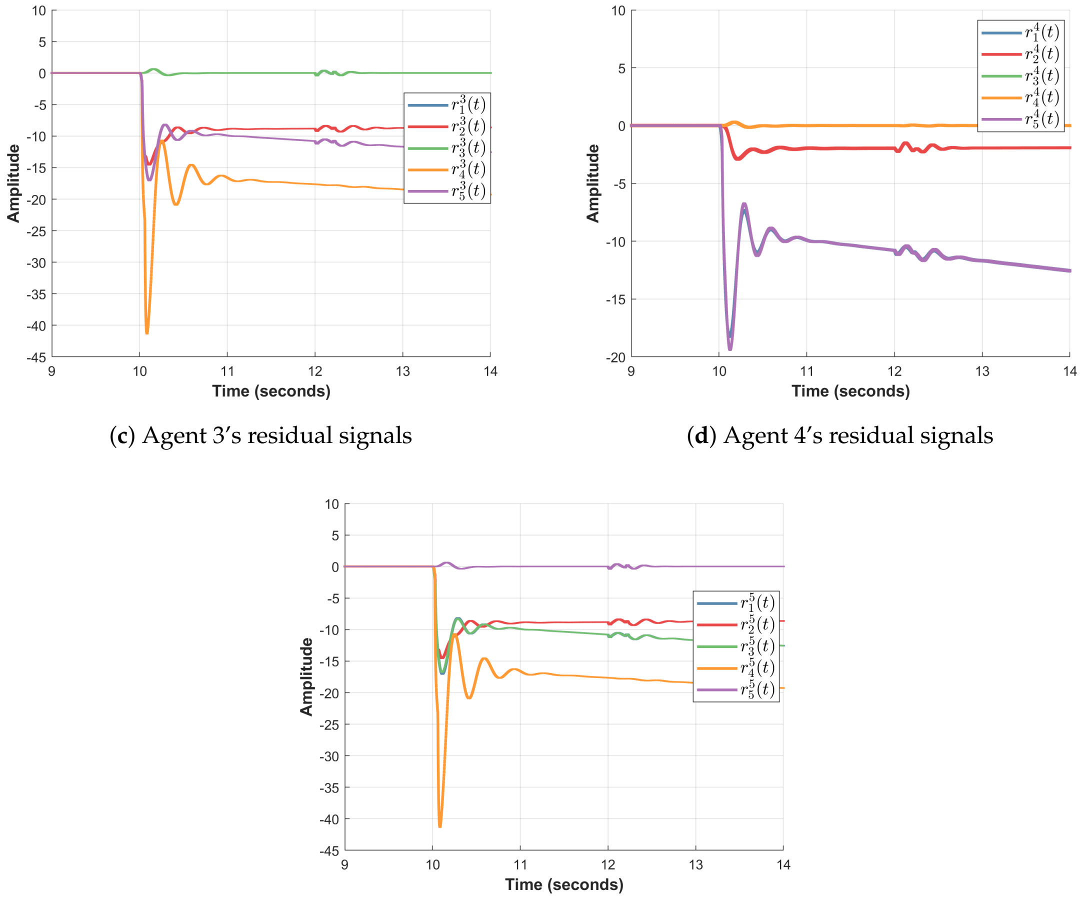
Consequently, according to Proposition 2, one can distinguish and identify a cyber-attack in the networked system.



(**a**) Agent 1's residual signals

(**b**) Agent 2's residual signals

Figure 6. *Cont.*



(**c**) Agent 3's residual signals

(**d**) Agent 4's residual signals

(**e**) Agent 5's residual signals

Figure 6. Residuals generated by all agents in scenario 2.

7. Conclusions and Future Work

In this paper, a novel distributed cyber-attack identification scheme was proposed for NCS with switching topologies subject to cyber-attacks, where any agent/node can act as a monitor to the whole system behavior and can thus detect and identify intrusion and cyber attacks. This is done by employing a bank of distributed predefined-time observers to estimate the global system state through auxiliary states whereby the settling time is an a priori user defined parameter, independently of the initial conditions. Numerical simulation results have been carried out by implementing the proposed scheme on a synchronization seeking network of mobile robots. Future works will include the design of a control reconfiguration algorithm based on the estimated faults from our FDI scheme.

Author Contributions: Conceptualization, A.T.; methodology, A.T.; validation, M.D. (Michael Defoort), K.B., M.D. (Mohamed Djemai); formal analysis, M.D. (Michael Defoort), K.B.; investigation, M.D. (Michael Defoort), K.B.; resources, M.D. (Michael Defoort), K.B., M.D. (Mohamed Djemai), A.T.; writing—original draft preparation, A.T.; writing—review and editing, A.T., M.D. (Michael Defoort), K.B., M.D. (Mohamed Djemai); supervision, M.D. (Michael Defoort), K.B., M.D. (Mohamed Djemai); Funding Acquisition, L.D.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Baheti, R.; Gill, H. Cyber-physical systems. *Impact Control Technol.* **2011**, *12*, 161–166.
2. Wu, C.; Hu, Z.; Liu, J.; Wu, L. Secure estimation for cyber-physical systems via sliding mode. *IEEE Trans. Cybern.* **2018**, *48*, 3420–3431. [CrossRef]
3. Shamma, J. *Cooperative Control of Distributed Multi-Agent Systems*; John Wiley & Sons: Hoboken, NJ, USA, 2008.
4. Cao, Y.; Yu, W.; Ren, W.; Chen, G. An overview of recent progress in the study of distributed multi-agent coordination. *IEEE Trans. Ind. Inform.* **2012**, *9*, 427–438. [CrossRef]
5. Yang, Z.; Zhang, Q.; Chen, Z. Flocking of multi-agents with nonlinear inner-coupling functions. *Nonlinear Dyn.* **2010**, *60*, 255–264. [CrossRef]
6. Olfati-Saber, R. Flocking for multi-agent dynamic systems: Algorithms and theory. *IEEE Trans. Autom. Control* **2006**, *51*, 401–420. [CrossRef]
7. Oh, K.K.; Park, M.C.; Ahn, H.S. A survey of multi-agent formation control. *Automatica* **2015**, *53*, 424–440. [CrossRef]
8. Su, H.; Chen, M.Z.; Wang, X. Global coordinated tracking of multi-agent systems with disturbance uncertainties via bounded control inputs. *Nonlinear Dyn.* **2015**, *82*, 2059–2068. [CrossRef]
9. Ren, W.; Beard, R.W. *Distributed Consensus in Multi-Vehicle Cooperative Control*; Springer: Berlin/Heidelberg, Germany, 2008; Volume 27.
10. Cárdenas, A.A.; Amin, S.; Sastry, S. Research Challenges for the Security of Control Systems. In Proceedings of the 3rd Conference on Hot Topics in Security, HOTSEC'08, Berkeley, CA, USA, 29 July 2008.
11. Guo, M.; Dimarogonas, D.V.; Johansson, K.H. Distributed real-time fault detection and isolation for cooperative multi-agent systems. In Proceedings of the IEEE 2012 American Control Conference (ACC), Montreal, QC, Canada, 27–29 June 2012; pp. 5270–5275.
12. Shames, I.; Teixeira, A.M.; Sandberg, H.; Johansson, K.H. Distributed fault detection for interconnected second-order systems. *Automatica* **2011**, *47*, 2757–2764. [CrossRef]
13. Taoufik, A.; Busawon, K.; Defoort, M.; Djemai, M. An output observer approach to actuator fault detection in multi-agent systems with linear dynamics. In Proceedings of the 2020 28th Mediterranean Conference on Control and Automation (MED), Saint-Raphaël, France, 15–18 September 2020; pp. 562–567.
14. Chadli, M.; Davoodi, M.; Meskin, N. Distributed state estimation, fault detection and isolation filter design for heterogeneous multi-agent linear parameter-varying systems. *IET Control Theory Appl.* **2016**, *11*, 254–262. [CrossRef]
15. Meskin, N.; Khorasani, K. Actuator fault detection and isolation for a network of unmanned vehicles. *IEEE Trans. Autom. Control* **2009**, *54*, 835–840. [CrossRef]
16. Taoufik, A.; Michael, D.; Djemai, M.; Busawon, K.; Sánchez-Torres, J.D. Distributed global actuator fault-detection scheme for a class of linear multi-agent systems with disturbances. In Proceedings of the IFAC World Congress, Berlin, Germany, 12–17 July 2020.
17. Qin, L.; He, X.; Zhou, D. A survey of fault diagnosis for swarm systems. *Syst. Sci. Control Eng. Open Access J.* **2014**, *2*, 13–23. [CrossRef]
18. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2011**, *14*, 1–33. [CrossRef]
19. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1630–1638. [CrossRef]
20. Pasqualetti, F.; Dörfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
21. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE Commun. Surv. Tutorials* **2012**, *14*, 998–1010. [CrossRef]
22. Pasqualetti, F.; Bicchi, A.; Bullo, F. Distributed intrusion detection for secure consensus computations. In Proceedings of the 2007 46th IEEE Conference on Decision and Control, New Orleans, LA, USA, 12–14 December 2007; pp. 5594–5599.
23. Pasqualetti, F.; Bicchi, A.; Bullo, F. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Trans. Autom. Control* **2011**, *57*, 90–104. [CrossRef]
24. Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K.H. Distributed fault detection and isolation resilient to network model uncertainties. *IEEE Trans. Cybern.* **2014**, *44*, 2024–2037. [CrossRef]

25. Ding, S.X. *Model-Based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2008.
26. Teixeira, A.; Sandberg, H.; Johansson, K.H. Networked control systems under cyber attacks with applications to power networks. In Proceedings of the 2010 American Control Conference, Baltimore, MD, USA, 30 June–2 July 2010; pp. 3690–3696.
27. Pasqualetti, F. Secure Control Systems: A Control-Theoretic Approach to Cyber-Physical Security. 2012. Available online: http://www.fabiopas.it/PhD_Dissertation.pdf (accessed on 21 September 2020).
28. Smith, R.S. Covert misappropriation of networked control systems: Presenting a feedback structure. *IEEE Control Syst. Mag.* **2015**, *35*, 82–92.
29. Boem, F.; Gallo, A.J.; Ferrari-Trecate, G.; Parisini, T. A distributed attack detection method for multi-agent systems governed by consensus-based control. In Proceedings of the 2017 IEEE 56th Annual Conference on Decision and Control (CDC), Melbourne, Australia, 12–15 December 2017; pp. 5961–5966.
30. Khan, A.S.; Khan, A.Q.; Iqbal, N.; Sarwar, M.; Mahmood, A.; Shoaib, M.A. Distributed fault detection and isolation in second order networked systems in a cyber-physical environment. *ISA Trans.* **2020**, *103*, 131–142. [CrossRef]
31. Luo, X.; Yao, Q.; Wang, X.; Guan, X. Observer-based cyber attack detection and isolation in smart grids. *Int. J. Electr. Power Energy Syst.* **2018**, *101*, 127–138. [CrossRef]
32. Jahanshahi, N.; Ferrari, R.M. Attack detection and estimation in cooperative vehicles platoons: A sliding mode observer approach. *IFAC-PapersOnLine* **2018**, *51*, 212–217. [CrossRef]
33. Lemma, L.N.; Kim, S.H.; Choi, H.L. An unknown-input-observer based approach for cyber attack detection in formation flying UAVs. In Proceedings of the AIAA Infotech@ Aerospace, San Diego, CA, USA, 4–8 January 2016; p. 0916.
34. Lv, M.; Yu, W.; Lv, Y.; Cao, J.; Huang, W. An integral sliding mode observer for CPS cyber security attack detection. *Chaos Interdiscip. J. Nonlinear Sci.* **2019**, *29*, 043120. [CrossRef]
35. Sahoo, S.; Mishra, S.; Peng, J.C.H.; Dragičević, T. A Stealth Cyber-Attack Detection Strategy for DC Microgrids. *IEEE Trans. Power Electron.* **2018**, *34*, 8162–8174. [CrossRef]
36. Sánchez-Torres, J.D.; Gómez-Gutiérrez, D.; López, E.; Loukianov, A.G. A class of predefined-time stable dynamical systems. *IMA J. Math. Control Inf.* **2018**, *35*, i1–i29. [CrossRef]
37. Jadbabaie, A.; Lin, J.; Morse, A.S. Coordination of groups of mobile autonomous agents using nearest neighbor rules. *IEEE Trans. Autom. Control* **2003**, *48*, 988–1001. [CrossRef]
38. Bhat, S.P.; Bernstein, D.S. Finite-time stability of continuous autonomous systems. *SIAM J. Control Optim.* **2000**, *38*, 751–766. [CrossRef]
39. Polyakov, A. Nonlinear feedback design for fixed-time stabilization of linear control systems. *IEEE Trans. Autom. Control* **2011**, *57*, 2106–2110. [CrossRef]
40. Aldana-López, R.; Gómez-Gutiérrez, D.; Jiménez-Rodríguez, E.; Sánchez-Torres, J.D.; Defoort, M. Enhancing the settling time estimation of a class of fixed-time stable systems. *Int. J. Robust Nonlinear Control* **2019**, *29*, 4135–4148. [CrossRef]
41. Basile, G.; Marro, G. *Controlled and Conditioned Invariants in Linear System Theory*; Prentice Hall: Englewood Cliffs, NJ, USA, 1992.
42. Ren, W.; Moore, K.L.; Chen, Y. High-order and model reference consensus algorithms in cooperative control of multivehicle systems. *J. Dyn. Syst. Meas. Control* **2007**, *129*, 678–688. [CrossRef]
43. Ren, W.; Atkins, E. Distributed multi-vehicle coordinated control via local information exchange. *Int. J. Robust Nonlinear Control* **2007**, *17*, 1002–1033. [CrossRef]
44. Jiang, F.; Wang, L. Consensus seeking of high-order dynamic multi-agent systems with fixed and switching topologies. *Int. J. Control* **2010**, *83*, 404–420. [CrossRef]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).