

Article

Not peer-reviewed version

Time-Delay Resilient Cooperative Filters for Cyber-Physical Systems

[Shahram Shahkar](#) *

Posted Date: 10 July 2025

doi: 10.20944/preprints202507.0897.v1

Keywords: cyber physical systems; cybersecurity; time-delay cyberattacks; multi-agent systems; load frequency control; cooperative filters



Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

Time-Delay Resilient Cooperative Filters for Cyber-Physical Systems

Shahram Shahkar 

Electrical and Computer Engineering Department, Concordia University, Montreal, Canada; shahram.shahkar@icloud.com

Abstract

Reliable real-time and uninterrupted data tele-communication between subsystems in a Cyber Physical System (CPS) is at the core of secure operation of the CPS. Time-delay and Denial-of-Service (DoS) cyberattacks are among CPS cyber threats that could impair normal functioning in the CPS, through intentional latency in the data tele-communication systems by infliction of data congestion, routing issues, parasitic electro-magnetic interference, etc. Load Frequency Control (LFC) in smart grids are among critical CPS controllers where certain time-delays in the transmission of remote system parameters could cause instability and pervasive havoc within seconds, if not detected and contained promptly. This paper considers a general interconnected CPS of heterogeneous subsystems where information is randomly delayed from one subsystem to another. The paper circumvents time-delays caused at the tele-communication layer by augmenting a Multi-Agent System (MAS) of cooperative filters that restore random information delays with negligible and controllable time-delays. Consequently, real-time information would be accessible by the subsystem controllers at all times, regardless of the delays inflicted in the tele-communication layer. The LFC problem has been considered as an example of a challenging CPS that is highly vulnerable to time-delay cyberattacks, and the proposed cooperative filters were used to validate the theoretical results through numerical simulations.

Keywords: cyber physical systems; cybersecurity; time-delay cyberattacks; multi-agent systems; load frequency control; cooperative filters

1. Introduction

Cyber-Physical Systems (CPS) are usually networked systems composed of a number of heterogeneous systems characterized by independent system dynamics, coupled through a set of signals that are transmitted to other systems, where information is exchanged between the systems to enable computation of control commands, in order to regulate or track desired outputs in the systems with reference to an overall control objective in the CPS. In cases where large number of interconnecting nodes are involved it is often advantageous to administer exchange of information merely among adjacent neighbours (i.e., distributed control), rather than deploying a central control architecture that communicates with all the individual nodes. This is particularly important in order to ensure security and reliability, since in this case communication signals can be kept covert and contained in a local fashion. The dispersed nature of CPS often requires public tele-communication infrastructures to be employed for information exchange, rather than dedicated (i.e., leased) communication lines (due to cost and operating expenses). This especially poses threat to the CPS in the form of cyberattacks, and may encounter highly unwanted consequences [1,2]. Therefore, the security of the CPS has to be considered and addressed properly in the CPS design phase. A CPS with a distributed control philosophy in which the systems take part in a cooperative control network to achieve a common goal is referred to a Multi-Agent System (MAS), and the systems are referred to as the agents. Specifically, power generating stations in the LFC problem are subsystems (or agents) of the power system (i.e., the CPS) where system states are collected from remote locations and tele-metered to the controllers

through a communication system, in order to regulate the frequency of the grid, and exact the desirable amount of electric power to be traded between the power areas.

Cyberattacks are broadly categorized in the literature into deception, and time-delay or DoS attacks [4]. In deception attacks an adversary attempts to maliciously alter the information packets that are transmitted among the agents in order to cause an intended consequence in the CPS, while time-delays and DoS attacks are obstructive means conducted by adversaries to delay or interrupt in the normal flow of information. The authors in [3,4] have considered the cooperative output regulation problem for heterogeneous linear multi-agent systems in the presence of communication constraints. Cooperative output regulation is a generalization of the leader-follower consensus problem in MAS. Load sharing in power systems as explained in [5] can be formulated from a MAS point of view, in which the area power systems are considered as agents, and limited information are exchanged among the agents to achieve a secondary coordinated control in a decentralized fashion. In [6] the authors have presented a distributed secondary control scheme for power allocation and voltage restoration in islanded DC micro-grids employing MAS consensus control techniques. As far as the LFC problem is concerned, the authors in [24] have performed a thorough literature review with respect to the inadequacies in the literature with regard to LFC with time-delays and packet dropouts. According to their studies "existing works have incorporated either DoS cyberattacks, or time-delays in the control loops", where time-delay resiliency methods in the literature either aim at major modifications in the existing communication systems and controllers (such as in [26]), or suggest gain re-adjustments in PLC controllers [24], or complicated LMI equations that require precise knowledge of system models [25,27,28].

2. Contributions

The contribution of this paper is in the transformation of a "time-delayed CPS" (i.e., a system of systems in which certain information are transmitted from one subsystem to another subsystem through tele-communication channels with random and unknown time-delays) into a "delay-resilient" CPS (that is a CPS with negligible and controllable time-delays in all tele-communication channels), and (importantly) without any modification to any of the existing physical systems, nor with any required knowledge of the constituting subsystems. This is particularly important in industrial CPS where state owned and privately owned systems are involved and intertwined, and where the dynamic models of physical systems are unknown to others (either due to security reasons, or due to the nature of the CPS). Certain examples include the LFC problem in a smart grid, where there are privately owned power generating units with certain security constraints, or in Advanced Air Mobility where anonymous aerial vehicles randomly join and disconnect from the air traffic system. In these cases, various system dynamics with unknown characteristics are involved and it is impractical to modify subsystem's internal controllers (due to certification, privacy, security issues, etc.). Hence, it is fundamental to involve delay-resilient methodologies at the tele-communication system layer, in a way that is independent of the internal dynamics of the physical subsystems. The authors of this paper strongly believe that such solutions are unprecedented state-of-the-art, and not available in the literature as of this date.

3. Related Works

The conditions for "consensusability" in linear homogenous MASs has been presented in [7, 8], where output feedback consensus protocols were given and the closed-loop MAS was shown to be achieving asymptotic consensus if the topology had a spanning tree. Output consensus for heterogeneous MAS with Markovian switching network topologies has been discussed in [9] and can be used as the basis for studying MAS under DoS cyberattacks assuming that DoS attacks can be represented as switching topologies. Unfortunately, [9] does not address communication time-delays and instability issues that can be caused due to information reception delays. The authors in [11] have also attempted to solve the output consensus problem in a leader-follower heterogeneous MAS under DoS attack. Unfortunately, the solution proposed in [11] can neither be applicable in real-world, since

leader's dynamic is unknown to the follower agents in most scenarios (especially, in a MAS where the leader is randomly switched from time to time, such as in a MAS of UAVs where the leader may have to be switched randomly from one agent to another for the system to be robust against the leader's internal faults and outages).

The subject of distributed consensus of heterogenous MAS subject to switching topologies and communication time-delays has been a recent research problem in the literature (as in [10]) with a focus on power systems. This article provides a comprehensive solution for stability and control of heterogenous MAS systems considering a switching controller that alters the controller gain based on the knowledge that a time-delay attack has taken place. The authors in [3] have investigated cooperative resilient output regulation problem with time-delay constraints for a specific class of heterogenous MAS with uniform exogenous inputs (following a LTI dynamics with pure imaginary eigenvalues). Unfortunately, the authors have assumed an exogenous signal that has a predetermined dynamics, which violates a fully arbitrary output trajectory condition for the leaders (as we discussed earlier), due to the fact that the followers are assuming a consensus law that is based on some predefined system parameters. The authors in [4] have recently addressed the same subject for a class of CPS systems with non-uniform but bounded communication delays under denial-of-service (DoS) attacks, where a switching resilient control approach is proposed. However, the proposed controller is only functional for DoS attacks (where agents are assumed to understand "missing" information from neighbour agents) but does not address time-delay attacks.

The authors in [12] have studied consensus in a homogenous MAS, where the agents are expected to follow a given reference command under intrinsic and communication time-delays and disturbances. The authors in [13] have considered consensus problem for discrete-time homogenous multi-agent systems over an undirected, fixed network communication graph, focusing on the robustness of consensus with respect to communication delay. The authors in [15,16] have discussed the problem of output synchronization in a multi-agent system subject to time-delays, with linear right-invertible agents that is subject to arbitrary time-delays. The authors in [17] have addressed adaptive consensus tracking for a class of nonlinear multi-agent systems under time varying actuator faults. Several other recent publications have also paid attention to time-delayed nonlinear MAS output regulation using data-driven consensus [18]. The authors in [19] have discussed consensus problem in a discrete-time nonlinear MAS using sliding mode control laws. The authors in [20] have investigated the consensus problem of MAS with time-varying delays subject to switching topologies with less conservative consensus conditions. The authors in [21] have very recently investigated the group consensus problem for heterogeneous MAS with time-delays via pinning control in the frequency domain. For the LFC problem subject to time-delays which nowadays continues as an ongoing and challenging problem in the literature, the authors in [23] have addressed cybersecurity using linear feedback control employing a set of LMIs. The authors in [24] have used a filtered PID controller that is tuned in the LFC using the particle swarm optimization (PSO) algorithm to solve the problem. More recent research works on the same topic include [26]-[28] to name a few.

4. Definitions and Assumptions

Let us consider an interconnected CPS $\mathcal{S}$, and its N constituent subsystems $\mathcal{S}_i \subset \mathcal{S}$, $i \in \{1, 2, \dots, N\}$, hereinafter referred to as "subsystems". Generally, subsystems in a CPS may (or may) not involve states that are shared with other subsystems.

Definition 1. We define an "exogenous state" as a shared state between dynamically coupled subsystems whose value is transmitted from one subsystem to another subsystem through a tele-communication channel. On the other hand "endogenous states" are defined as subsystem states when the coupling between the subsystems are removed. Therefore, one may assume that exogenous states are prone to cyberattacks, and endogenous states are immune against cyberattacks.

Exogenous states are distinct from exogenous signals in a sense that time-delays in exogenous states can cause instability in the systems. The dynamic couplings between the subsystems can be physical (such as in interconnected power systems) or non-physical (such as in automated air traffic systems in advanced air mobility).

Definition 2. Let $x_{j(\ell)} \in \mathbb{R}$ denote the ℓ^{th} state of $\mathcal{S}_j$, and $x_{j(\ell),i} \in \mathbb{R}$ denote the value of $x_{j(\ell)}$ after transmission to $\mathcal{S}_i$, and $x_{j,i}$ denote the exogenous state vector of $\mathcal{S}_i$ that is transmitted from $\mathcal{S}_j$ to $\mathcal{S}_i$. In a delayed communication system $x_{j(\ell),i}(t) = x_{j(\ell)}(t - \tau_{j,i})$ and $x_{j,i}(t) = x_j(t - \tau_{j,i})$, where $\tau_{j,i} \in \mathbb{R}^+$ is a random time-delay of the communication link from $\mathcal{S}_j \rightarrow \mathcal{S}_i$. Therefore, $x_i + \sum_{\mathcal{S}_j} x_{j,i}$ represents the full state vector of $\mathcal{S}_i$ which is the sum of the endogenous (i.e., x_i) and exogenous states $\sum_{\mathcal{S}_j} x_{j,i}$.

When the subsystems in a CPS are dynamically coupled, in order to model subsystem dynamics the state of other subsystems involve. One can imagine a very heavy load that is chained and transported by multiple helicopters, or a power system that involves interconnected power areas, which are examples of physically and dynamically coupled subsystems. Autonomous air traffic control in urban air mobility is another example where the coupling between subsystems are non-physical.

Remark 1. It is generally problematic to model a dynamically coupled CPS in which randomly time-delayed exogenous states are involved, and where the dynamic model of the subsystems are unavailable to other subsystems.

In this article we consider a multi-agent system framework in order to facilitate time-delay recovery in the CPS. Therefore, we consider an undirected graph $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathcal{A})$ where $\mathcal{N}$ is the set of nodes representing N number of subsystems (or agents), $\mathcal{E} \in \mathcal{N} \times \mathcal{N}$ as the set of edges (or communication links between the subsystems), and $\mathcal{A} = [a_{ij}]_{N \times N}$, $a_{ij} \in \{0, 1\}$, representing the adjacency matrix. The elements of $\mathcal{A}$ are defined such that $a_{ij} = 1$, if $(i, j) \in \mathcal{E}$, and $a_{ij} = 0$, if $(i, j) \notin \mathcal{E}$. Let $\mathcal{N}_i$ denote the neighbour set of agent i (where, $a_{ij} = 1$). The Laplacian matrix $L := \mathcal{D} - \mathcal{A} = [\ell_{ij}] \in \mathbb{R}^{n \times n}$, associated to $\mathcal{G}$ is defined such that,

$$\ell_{ii} = \sum_{j=1}^n a_{ij}, \quad \ell_{ij} = -a_{ij}, \quad \text{for } i \neq j, \quad (1)$$

where $\mathcal{D} = [\ell_{ii}]$ is the diagonal in-degree matrix. Generally, a heterogeneous linear subsystem $\mathcal{S}_i \subset \mathcal{S}$ with a time-delay tele-communication system can be defined by the equations,

$$\begin{aligned} \dot{x}_i(t) &= A_i x_i(t) + B_i u_i(t) + D_i w_i(t) + \sum_{j \in \mathcal{N}_i} E_{j,i} x_{j,i}(t), \\ y_i(t) &= C_i x_i(t) + \sum_{j \in \mathcal{N}_i} C_{j,i} x_{j,i}(t), \end{aligned} \quad (2)$$

where $x_{j,i}(t) \in \mathbb{R}^{N_{x_i}}$ denotes the exogenous states of $\mathcal{S}_i$ according to Definition 2. Furthermore, $x_i \in \mathbb{R}^{N_{x_i}}$ denotes the endogenous state vector of $\mathcal{S}_i$, $u_i \in \mathbb{R}^{N_{u_i}}$ denotes the local control command vector, and $w_i \in \mathbb{R}^{N_{w_i}}$ denotes a vector of bounded unknown disturbances, and finally $y_i \in \mathbb{R}^{N_{y_i}}$ denotes the output vector of $\mathcal{S}_i$, where matrices $A_i, B_i, D_i, E_{j,i}$ and $C_{j,i}$ have appropriate dimensions. System matrices are such that when there is no time-delay present in the tele-communication system Equation (2) could be represented as,

$$\dot{x}_i(t) = (A_i + \sum_{j \in \mathcal{N}_i} E_{j,i})(x_i(t) + x_{j,i}(t)) + B_i u_i(t) + D_i w_i(t),$$

as later exemplified in Remark 5 (in Section 8).

Definition 3. Time-delay resiliency in a CPS is defined as a condition where $|x_{j(\ell),i}(t) - x_{j(\ell)}(t)| < \epsilon$, $\forall i, j \in \mathcal{N}$, $\forall \ell \in \{1, 2, \dots, N_{x_i}\}$, and for all $t > \tau_{j,i} > 0$, where $\epsilon \in \mathbb{R}^+$ is an arbitrarily small number, where from Definition 2 we had $x_{j(\ell),i}(t) = x_{j(\ell)}(t - \tau_{j,i})$.

Assumption 1. We assume that the network $\mathcal{G}$ is a connected network with N agents, where all subsystems are stable when there is no time-delay in the tele-communication channels. In other words, the endogenous states $x_{i(\ell)}$ are continuous Lipchitz functions of time, and there exists a small $\epsilon \in \mathbb{R}^+$, such that $|x_{i(\ell)}(t) - x_{i(\ell)}(t - T_s)| < \epsilon$, for an arbitrarily small $T_s \in \mathbb{R}^+$.

Assumption 2. Let us assume that $(A_i + \sum_{j \in \mathcal{N}_i} E_{j,i}, B_i)$ constitute a controllable pair, and $(A_i + \sum_{j \in \mathcal{N}_i} E_{j,i}, C_i + \sum_{j \in \mathcal{N}_i} C_{j,i})$ constitute an observable pair, for all $\mathcal{S}_i \subset \mathcal{S}$.

Assumption 3. We assume that a Denial of Service (DoS) attack on agent i from j is equivalent to the condition $a_{ij} = 0, j \in \mathcal{N}_i$ in a finite duration in time. This is due to the fact that $a_{ij} = 0$ is equivalent to the edge (i, j) being removed from $\mathcal{E}$, implying no communication service from j to i , hence DoS on i from j .

5. The Load Frequency Control (LFC) Example

The LFC example clarifies the definitions raised in the previous section, and explains the complexities behind modelling of a CPS. The literature [5] models the states of a generating station $\mathcal{S}_i$ as $x_i = [\Delta f_i, \Delta P_{m_i}, \Delta P_{v_i}, \Lambda_i, \Delta P_{ij}]^T \in \mathbb{R}^5$ denoting the fluctuations and variations in the area frequency, the mechanical power of the prime mover, the governor valve position, the integrated Area Control Error (ACE) of the equivalent generating units, where $\text{ACE} = K_i B_i \Delta f_i + K_i \Delta P_{ij}$, and the interconnecting tie-line power, respectively, as in Figure 1, where,

$$\Lambda_i(t) = \int_{s=0}^t K_i B_i \Delta f_i(s) + K_i \Delta P_{ij}(s) ds, \quad (3)$$

$$\Delta P_{ij}(t) = 2\pi T_{ij} \int_{s=0}^t [\Delta f_i(s) - \Delta f_j(s)] ds, \quad (4)$$

where $K_i, B_i, T_{ij} \in \mathbb{R}^+$ are positive constants, and where Λ_i is a control variable calculated by the Central Control Station (CCS) and transmitted to $\mathcal{S}_i$ as shown in Figure 1. ΔP_{d_i} in the figure denotes variations in the power of the area transmission lines and intermittent renewable energies, and is considered as a random variable. The objective of the LFC as the name implies is to control the area frequency with respect to changes in ΔP_{d_i} , while maintaining the preset amount of energy exchange between the areas (i.e., P_{ij}). In other words, the objective of the LFC is that,

$$\lim_{t \rightarrow \infty} |\Delta f_i(t)|^2 + |\Delta P_{ij}(t)|^2 \approx 0, \quad \forall \Delta P_{d_i}(t). \quad (5)$$

This is due to the fact that $P_{ij}(t)$ is often a time-varying contracted variable between two areas and is set by the main input $u_i(t)$ in Figure 1, where one area commits to supply a regulated amount of energy to the other area, irrespective of the variations in area load. Λ_i and ΔP_{ij} are exogenous states for $\mathcal{S}_i$, and the first three entries of x_i are endogenous states for $\mathcal{S}_i$.

A time-delay cyberattack on the tele-communication channels of $\mathcal{S}_i$ causes the actual $\Lambda_i(t)$ to be observed by the controller in $\mathcal{S}_i$ as $\Lambda_i(t - \tau_{\Lambda_i})$, where $\tau_{\Lambda_i} \in \mathbb{R}^+$ is an unknown random time-delay. Similarly, let P_{ij} denote the desirable power to be traded between $\mathcal{S}_i$ and its adjacent power area $\mathcal{S}_j$. The sensor collecting the instantaneous power $P_{ij} + \Delta P_{ij}(t)$ is often remote from the controller in $\mathcal{S}_i$. Therefore, the practice is to install Remote Terminal Units (RTUs) inside the power substations (controlling circuit breakers, disconnector switches, and other electric apparatus associated with transmission lines) to continuously read $P_{ij} + \Delta P_{ij}(t)$ and transmit the value to the CCS through a tele-communication line for the computation of $\Lambda_i(t)$. However, the tele-communication time-delays result in $P_{ij} + \Delta P_{ij}(t - \tau_{P_{ij}})$, and $f_i + \Delta f_i(t - \tau_{f_i})$ being observed in the CCS. Therefore, time-delays $\tau_{P_{ij}}, \tau_{f_i} \in \mathbb{R}^+$ affect the computed value $\Lambda_i(t)$, and $\Lambda_i(t)$ is further delayed by τ_{Λ_i} to finally affect $x_i(t)$. In the LFC example of Figure 2, Λ 's are the only exogenous states that are actually required by the generating areas for the operation. However, the CCS requires the tie-line power values (i.e., ΔP_{ij} 's) and the area frequencies Δf 's to compute the Λ 's. Figure 2 depicts the interconnection of the area

generating stations in an LFC through power transmission lines and the flow of information, as an example of a CPS.

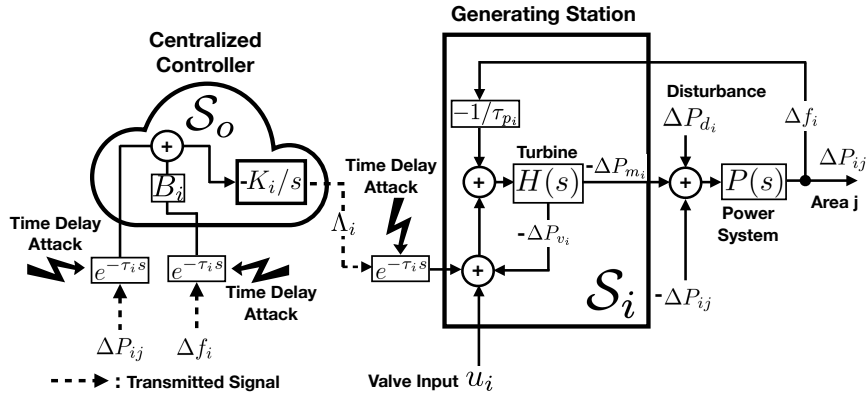


Figure 1. Block diagram of a frequency control mechanism for a generating station S_i contributing the LFC in a multi-area power system. The solid lines are hard-wired measurements/commands that are presumably immune from cyberattacks (as they are confined in S_i), where the dashed lines represent tele-metered data that are subject to TDS/DoS cyberattacks. Borrowed from [5].

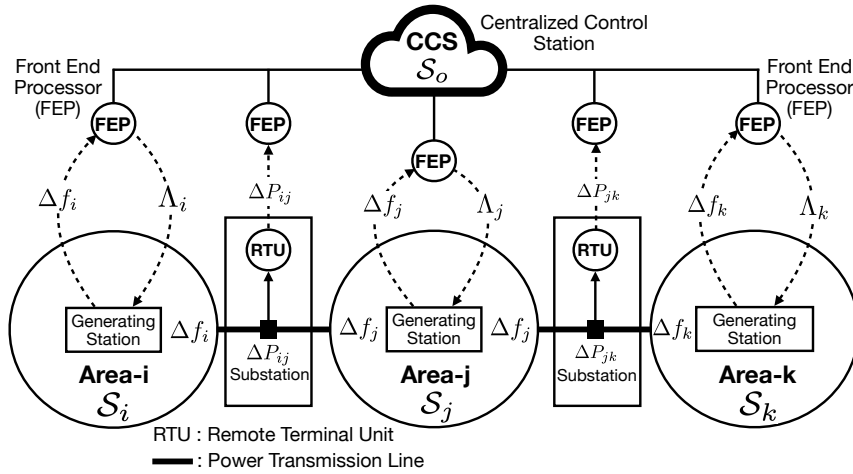


Figure 2. Schematics of a LFC power system with three area generating stations S_i, S_j, S_k and the Centralized Control Station S_o . The CPS $\mathcal{S}$ in this figure can be represented as $\mathcal{S} = \{S_i \cup S_j \cup S_k \cup S_o \cup S_{SS_{ij}} \cup S_{SS_{jk}}\}$ where $S_{SS_{ij}}, S_{SS_{jk}}$ denote the two substations, each also considered as a subsystem of the CPS. The tele-communication system can be further regarded as a subsystem in a more comprehensive model. However, this is not considered in this paper. The CCS S_o and the tele-communication system comprise the cyber part of the system that is responsible for the data collection and processing, and the power system comprises the physical part of the CPS. The Front-End Processors (FEPs) are electronic apparatus inside the CCS that transmit/receive tele-communication signals and demodulate the state variables. The Remote Terminal Unit (RTU) is a micro-scale FEP with a similar function located in every substation. ΔP_{ij} is a system state whose sensor (i.e., current and voltage power transformers) is located in a substation, and whose instantaneous value is transmitted to the CCS through an RTU. The CCS receives all $\Delta P, \Delta f$, and computes Λ for individual generating stations.

6. Problem Statement

Before we formally state the problem let us note from the definitions and the assumptions that $x_{j(\ell)}(t) - \epsilon \leq x_{j(\ell),i}(t) \leq x_{j(\ell)}(t) + \epsilon, \forall j, \ell$, resulting $x_j(t) - \epsilon \mathbf{1}_{N_{x_i}} \leq x_{j,i}(t) \leq x_j(t) + \epsilon \mathbf{1}_{N_{x_i}}, \forall j$, where $\mathbf{1}_{N_{x_i}} \in \mathbb{R}^{N_{x_i}}$ is a vector of ones. Through substitution in Equation (2) it follows that,

$$\dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) + \sum_{j \in \mathcal{N}_i} E_{j,i} x_j(t) \pm \sum_{j \in \mathcal{N}_i} E_{j,i} \mu \mathbf{1}_{N_{x_i}} + D_i w_i(t),$$

where $\mu \in \mathbb{R}^+$, $\mu \leq \epsilon$, and due to the controllability condition in Assumption 2 one would be able to design a feedback control law such as $u_i(t) = K_i x_i(t) + \sum_{j \in \mathcal{N}_i} K_{j,i} x_{j,i}(t)$ using H_∞ methods, so that $\lim_{t \rightarrow \infty} \|y_i(t)\|^2 < \epsilon_{y_i}^2$, $\forall i$, and for an arbitrarily small $\epsilon_{y_i}^2 > 0$, ensuring stability of the CPS in a Lyapunov sense. This would be always possible since $\sum_{j \in \mathcal{N}_i} E_{j,i} \mu \vec{1}_{N_{x_i}}$ could be considered as a small disturbance similar to $D_i w_i(t)$ and rejected through an appropriate state feedback. Therefore,

Remark 2. A time-delay resilient CPS as in Definition 3 guarantees stability of the CPS under all random time-delays $t > \tau_{j,i} > 0$, including the objective in Equation (5).

Let $\mathcal{G}$ denote a connected graph of a CPS $\mathcal{S} = \mathcal{S}_o \cup \mathcal{S}_i \cup \mathcal{S}_j \cup \dots$ with random communication delays between the constituent subsystems $o, i, j, \dots$. Let $x_{o(\ell)}(t) \in \mathcal{S}_o \subset \mathcal{S}$ be an endogenous state of $\mathcal{S}_o$ to be transmitted to all other subsystems $\mathcal{S}_i, \mathcal{S}_j, \dots$, and let $x_{o(\ell),i}(t), x_{o(\ell),j}(t), \dots$ denote the delayed value of $x_{o(\ell)}(t)$ at $\mathcal{S}_i, \mathcal{S}_j, \dots$, respectively, where $x_{o(\ell),i}(t) = x_{o(\ell)}(t - \tau_{o,i})$, $x_{o(\ell),j}(t) = x_{o(\ell)}(t - \tau_{o,j}), \dots$

The problem is to recover the real-time value of $x_{o(\ell)}(t) \approx x_{o(\ell)}(t - T_s)$ at all recipient subsystems $\mathcal{S}_i, \mathcal{S}_j, \dots$, with an arbitrarily negligible time-delay T_s , by cooperative-filtering of the delayed signals. In particular, the objective is to find an LTI filter with impulse response $h(t)$ so that,

$$x_{o(\ell)}(t - T_s) = (\alpha_i x_{o(\ell),i}(t) + \sum_{j \in \mathcal{N}_i} \alpha_j x_{o(\ell),j}(t - \tau_{j,i})) * h(t), \quad (6)$$

for all $\mathcal{S}_i \subset \mathcal{S}$, where α 's are real constant coefficients, $T_s > 0$ is an arbitrarily small transient time for the filter $h(t)$, and where $x_{o(\ell),i}(t) = x_{o(\ell)}(t - \tau_{o,i})$ is the input of the filter, and $x_{o(\ell),j}(t) = x_{o(\ell)}(t - \tau_{o,j})$, $\forall j \in \mathcal{N}_i$ are auxiliary inputs from the neighbouring subsystems of $\mathcal{S}_i$.

Definition 4. A CPS that incorporates the exchange of information among constituent subsystems in order to achieve a common goal (i.e., time-delay resiliency) in a distributed system framework is referred to as a Multi Agent System (MAS), and the processing component (e.g., the filter) in each subsystem that involves the exchange of information is referred to as an "agent". Therefore, the cooperative filter proposed in Equation (6) is a MAS.

7. Main Results

The multi-agent filtering structure in Figure 3 guarantees time-delay resiliency in the CPS despite of the random time-delay cyberattacks on the communication channels, and the objective is to attain the real-time value of a state $x_{o(\ell)}(t) \in \mathcal{S}_o$ in agent $\mathcal{S}_i$.

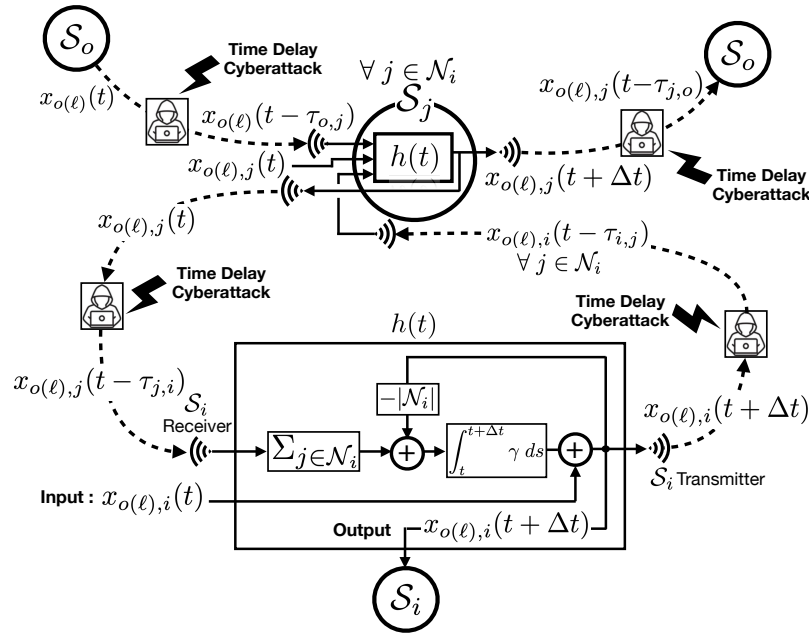


Figure 3. Schematics of a MAS time-delay resilient CPS, and the schematics of the cooperative filter $h(t)$. The agents in the MAS exchange information in order to recover a time-delayed state $x_{o(\ell)}(t) \in \mathcal{S}_o$. $x_{o(\ell),i}(t) = x_{o(\ell)}(t - \tau_{o,i})$ is the input of the filter in $\mathcal{S}_i$ (if $o \in \mathcal{N}_i$, or can be any other conjecture available to $\mathcal{S}_i$ which needs not be a correct estimate), and the output of the filter is $x_{o(\ell),i}(t + \Delta t)$, where $\Delta t > 0$ is a small response time. It will be shown that $\lim_{\Delta t \rightarrow T_s} x_{o(\ell),i}(t + \Delta t) = x_{o(\ell)}(t)$, where T_s is a negligible arbitrary settling time for the filter that will be controlled by the filter gain $\gamma \in \mathbb{R}^+$.

The filters $h(t)$ are identical in all agents and are located immediately after the data receivers. The internal block diagram of the filter $h(t)$ is as shown in the box for $\mathcal{S}_i$ where the input $x_{o(\ell),i}(t)$ can be $x_{o(\ell)}(t - \tau_{o,i})$ if there is a direct communication link between $\mathcal{S}_o \rightarrow \mathcal{S}_i$, or any arbitrary conjecture available to $\mathcal{S}_i$. The output of the filter is $x_{o(\ell),i}(t + \Delta t)$ where Δt is a controllable transient time for the filter that can be arbitrarily adjusted through the filter gain γ , and is fed to the internal controller in $\mathcal{S}_i$ and simultaneously shared with the neighbouring agents. The interesting and important characteristic of the multi-agent filtering scheme is that the outputs of all filters will become identical after lapse of the filter transients and within a negligible settling time $T_s > 0$. In particular, for any arbitrary set of inputs $x_{o(\ell),1}(t), x_{o(\ell),2}(t), \dots, x_{o(\ell),N}(t)$ one will have,

$$\lim_{\Delta t \rightarrow T_s} x_{o(\ell),i}(t + \Delta t) = x_{o(\ell),j}(t + \Delta t), \forall i, j \in \{1, \dots, N\},$$

regardless of the time delays in the tele-communication channels. Consequently, if any single agent such as $\mathcal{S}_o$ temporarily maintains its output at $x_{o(\ell)}(t + \Delta t) = x_{o(\ell)}(t)$, $T_s \geq \Delta t \geq 0$, then it follows that,

$$\lim_{\Delta t \rightarrow T_s} x_{o(\ell),i}(t + \Delta t) = x_{o(\ell)}(t), \forall i \in \mathcal{N}, \quad (7)$$

which satisfies the objective in Equation (6). This implies that any single agent in the MAS such as $\mathcal{S}_o$ where its output follows its input for a time period $T_s \geq \Delta t \geq 0$ will act as the leader in the MAS and all other agents in $\mathcal{S}$ will follow and track the output $x_{o(\ell)}(t)$. More specifically,

Remark 3. The connected MAS shown in Figure 3 will achieve consensus as in Equation (7) regardless of the time-delays in the tele-communication links, and the consensus value will be equal to the output of the leader only if there is a single leader such as $\mathcal{S}_o$ available in the MAS, and where the leader is characterized by the equation $\dot{x}_{o(\ell)}(t + \Delta t) = 0$, $\forall T_s \geq \Delta t \geq 0$.

Remark 4. Clearly, realization of time-delay resiliency through the cooperative filters $h(t)$ does not involve dynamic models of the subsystems (as it is evident from Figure 3). Furthermore, T_s can be arbitrarily reduced to improve the error ϵ in Definition 3 by increasing the filter gain γ (refer to [30] Theorem-2). Finally, cooperative filters are components that can be added to existing communication systems without necessary modifications to the existing subsystems. These characteristics are unique advantages that would make the presented technique an ideal solution for CPS time-delay security.

However, in case there are multiple leaders in the MAS the consensus output will be the centroid of the leaders outputs. In what follows the statement in Remark 3 will be justified mathematically, which constitutes firstly, proof of the stability of the MAS filter scheme in the presence of time-delays, and secondly, the output consensus of the MAS under all random time-delays. The following equations can be derived from the schematics of $h(t)$ in Figure 3.

$$x_{o(\ell),i}(t + \Delta t) = x_{o(\ell),i}(t) + \gamma \int_t^{t+\Delta t} \sum_{j \in \mathcal{N}_i} (x_{o(\ell),j}(s - \tau_{j,i}) - x_{o(\ell),i}(s)) ds,$$

or,

$$\begin{aligned} \dot{x}_{o(\ell),i}(t + \Delta t) - \dot{x}_{o(\ell),i}(t) &= \gamma \sum_{j \in \mathcal{N}_i} (x_{o(\ell),j}(t + \Delta t - \tau_{j,i}) - x_{o(\ell),i}(t + \Delta t)) \\ &\quad - \gamma \sum_{j \in \mathcal{N}_i} (x_{o(\ell),j}(t - \tau_{j,i}) - x_{o(\ell),i}(t)) \end{aligned}$$

which follows that,

$$\dot{x}_{o(\ell),i}(t) = \gamma \sum_{j \in \mathcal{N}_i} (x_{o(\ell),j}(t - \tau_{j,i}) - x_{o(\ell),i}(t)), \forall t > 0, i \in \mathcal{N}, \quad (8)$$

In order to simplify the notations let $\eta_i \triangleq x_{o(\ell),i}, \forall i \neq o \in \mathcal{N}$ and $\eta_o \triangleq x_{o(\ell)}$. With this simplification, the input/output equation of the MAS in Figure 3 reduces in a compact form to,

$$\dot{\eta}(t) = -\gamma \mathcal{D} \eta(t) + \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \mathcal{A}_{ji} \eta(t - \tau_{j,i}), \quad (9)$$

where $\mathcal{D}$ is the diagonal in-degree matrix as defined earlier, $\eta = [\eta_1, \dots, \eta_N]^T$, and $\mathcal{A}_{ji}$ is the adjacency matrix of the nodes with time delay $\tau_{j,i}$, where $\mathcal{A} = \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \mathcal{A}_{ji}$. Note that in case of no time delay, the input-output relation of Figure 3 could be simply represented as $\dot{\eta}(t) = -\gamma L \eta(t)$, where the laplacian matrix would be $L = \mathcal{D} - \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \mathcal{A}_{ji}$.

Lemma 1. For a connected MAS $\mathcal{S}$ with no time-delays, the cooperative filter in Figure 3 with a sufficiently large gain $\gamma > 0$ ensures that $|\eta_i - \eta_o| < \epsilon$, as $\Delta t \rightarrow T_s, \forall \mathcal{S}_i \subset \mathcal{S}$, if $x_{o(\ell)} \in \mathcal{S}_o \subset \mathcal{S}$ is not filtered, while all other agents $\mathcal{S}_i, \mathcal{S}_j, \dots \subset \mathcal{S}$ use $h(t)$ to filter their inputs as depicted in the figure.

The proof is straightforward and can be found in standard MAS textbooks. The implication of Lemma 1 is that the schematics in Figure 3 guarantees that the agents filter outputs simultaneously converges to $x_{o(\ell)}(t)$ if all the agents except $\mathcal{S}_o$ use $h(t)$ to filter their inputs, and if the output of $\mathcal{S}_o$ is simply connected to the input of $\mathcal{S}_o$, when there is no time-delay in the system. Theorem 1 and Theorem 3 below will prove that this would be the case even if there is a time-delay in the communication channels, and this would prove time-delay resiliency of the MAS in Figure 3. The condition $\lim_{\Delta t \rightarrow T_s} \|\eta(t + \Delta t) - \eta(t)\| < N\epsilon$ would be equivalent to $\lim_{t \rightarrow \infty} \|\eta(t) - \eta(0)\| < N\epsilon$ for an arbitrarily small T_s and a sufficiently large γ .

Theorem 1. Given the connected MAS $\mathcal{S}$ in Figure 3, the time-delayed system in Equation (9) is marginally stable (i.e., $\|\eta_i(t)\|^2$ remains bounded, for all $i \in \mathcal{N}$, as $t \rightarrow \infty$) for all finite time-delays, and all $\gamma > 0$.

Proof. Assume the Lyapunov candidate function,

$$V(\eta) = \|\eta(t)\|^2 + \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \int_{t-\tau_{ji}}^t \|\eta(\xi)\|^2 d\xi. \quad (10)$$

In order to prove the theorem it would be sufficient to show that $\dot{V}(\eta) \leq 0$, since in this case $V(t) \leq V(0)$, $\forall t > 0$, or $\|\eta(t)\|^2 \leq \|\eta(0)\|^2$, $\forall t > 0$, or $\sum_{i=1}^N \eta_i^2(t) \leq \|\eta(0)\|^2$, $\forall t > 0$, implying boundedness of $\eta_i(t)$, $\forall i \in \mathcal{N}$. However, from Equation (10) it follows that,

$$\begin{aligned} \dot{V}(\eta) = & -2\gamma \eta^T(t) \mathcal{D} \eta(t) + \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \eta^T(t) \mathcal{A}_{ji} \eta(t - \tau_{ji}) + \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \eta^T(t - \tau_{ji}) \mathcal{A}_{ji}^T \eta(t) \\ & + \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \|\eta(t)\|^2 - \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \|\eta(t - \tau_{ji})\|^2, \end{aligned}$$

which can be written in a compact form as,

$$\begin{aligned} \dot{V}(\eta) = & -\gamma [\eta^T(t) \ \eta^T(t - \tau_1) \ \cdots \ \eta^T(t - \tau_N)] \\ & \begin{bmatrix} 2\mathcal{D} - \sum_{i=1}^N \Gamma_i & -\mathcal{A}_1 & \cdots & -\mathcal{A}_N \\ -\mathcal{A}_1^T & +\Gamma_1 & \cdots & 0_{N \times N} \\ \vdots & \vdots & \ddots & \vdots \\ -\mathcal{A}_N^T & 0_{N \times N} & \cdots & +\Gamma_N \end{bmatrix} \begin{bmatrix} \eta(t) \\ \eta(t - \tau_1) \\ \vdots \\ \eta(t - \tau_N) \end{bmatrix} \end{aligned}$$

where, $\eta(t - \tau_i) = [\eta^T(t - \tau_{1,i}), \dots, \eta^T(t - \tau_{N,i})]^T$, excluding $\eta^T(t - \tau_{i,i})$, and $\mathcal{A}_i = [\mathcal{A}_{1i}, \dots, \mathcal{A}_{Ni}]$, excluding $\mathcal{A}_{ii}$, and $\Gamma_i = \mathbf{Diag}(\Gamma_{1i}, \dots, \Gamma_{Ni})$, excluding Γ_{ii} , where $\Gamma_{ji} = \mathbf{Diag}(0, \dots, a_{ij}, \dots, 0)$ is a diagonal matrix with all entries being zeros except $[\Gamma_{ji}]_{jj} = a_{ij}$. Therefore, one can write,

$$\begin{aligned} \dot{V}(\eta) = & -\gamma [\eta^T(t) \ \eta^T(t - \tau_1) \ \cdots \ \eta^T(t - \tau_N)] \\ & \check{L}_\tau [\eta^T(t) \ \eta^T(t - \tau_1) \ \cdots \ \eta^T(t - \tau_N)]^T \end{aligned} \quad (11)$$

where it is denoted that,

$$\check{L}_\tau \triangleq \begin{bmatrix} 2\mathcal{D} - \sum_{i=1}^N \Gamma_i & -\mathcal{A}_1 & \cdots & -\mathcal{A}_N \\ -\mathcal{A}_1^T & +\Gamma_1 & \cdots & 0_{N \times N} \\ \vdots & \vdots & \ddots & \vdots \\ -\mathcal{A}_N^T & 0_{N \times N} & \cdots & +\Gamma_N \end{bmatrix}$$

and the sufficient condition for marginal stability is to have $\check{L}_\tau \geq 0$. We use the Gershgorin disk theorem to evaluate the eigenvalues of $\check{L}_\tau$, which states that "if $M = [m_{ij}]$ is an $m \times m$ real matrix, then all the eigenvalues of M are located in the union of the following sets",

$$\cup_i \{z \in \mathbb{C} \mid |z - m_{ii}| \leq \sum_{j=1, \dots, m}^{j \neq i} |m_{ij}|\}.$$

Figure 4 is an illustration of the spectrum of $\check{L}_\tau$ according to the Gershgorin disk theorem, where each disk corresponds to one row in $\check{L}_\tau$, and encloses an eigenvalue of $\check{L}_\tau$. Therefore, the eigenvalues of $\check{L}_\tau$ are encapsulated by the union of the disks illustrated in Figure 4.

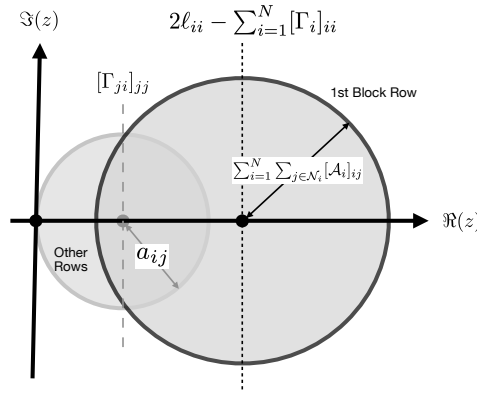


Figure 4. Spectrum of $\check{L}_\tau$ with reference to the Gershgorin disk theorem, is the union of several disks where each disk corresponds to a row in $\check{L}_\tau$. The bigger circle represents the first N rows, referred to as the first block row, where the center of the disk is on the real axis and at $2\ell_{ii} - \sum_{i=1}^N [\Gamma_i]_{ii}$ to the right, with a radius ℓ_{ii} . The smaller disk represents the set of other block rows where each row is represented by a disk with its center on the real axis at $[\Gamma_{ji}]_{jj}$ and a radius a_{ij} , and a set of null disks located at the origin.

Consequently, the condition $\check{L}_\tau \geq 0$ is equivalent to satisfying the following conditions simultaneously,

$$\begin{cases} 1) & 2|\ell_{ii}| - \sum_{i=1}^N [\Gamma_i]_{ii} \geq |\ell_{ii}|, \quad \forall i \in \mathcal{N}, \\ 2) & |[\Gamma_{ji}]_{jj}| \geq a_{ij}, \quad \forall i \neq j \in \mathcal{N}, \end{cases}$$

or,

$$\check{L}_\tau \geq 0 \equiv \begin{cases} 1) & |\ell_{ii}| \geq \sum_{i=1}^N [\Gamma_i]_{ii}, \quad \forall i \in \mathcal{N}, \\ 2) & |[\Gamma_{ji}]_{jj}| \geq a_{ij}, \quad \forall i \neq j \in \mathcal{N}, \end{cases}$$

where the second condition always hold since $|[\Gamma_{ji}]_{jj}| = a_{ij}$. On the other hand $\sum_{i=1}^N [\Gamma_i]_{ii} = \sum_{i=1}^N [\mathbf{Diag}(\Gamma_{1i}, \Gamma_{2i}, \dots, \Gamma_{Ni})]_{ii} = \sum_{j \in \mathcal{N}_i} a_{ij}$, where $\sum_{j \in \mathcal{N}_i} a_{ij} = \ell_{ii}$, validating the first condition for all i . In conclusion, for all finite $t > \tau_{ji} > 0$ one may assume $\check{L}_\tau \geq 0$, which completes the proof of the theorem. $\square$

Theorem 2 below will examine consensus in a delayed cyber-system that is governed by the control protocol in Theorem 1.

Theorem 2. *The connected MAS with finite time-delays in Theorem 1 achieves consensus. In other words, there exists some $\kappa \in \mathbb{R}$, such that $\eta(t - \tau) \rightarrow \kappa \vec{\mathbf{1}}$, $\forall t > \tau > 0$, as $t \rightarrow \infty$, where $\vec{\mathbf{1}}$ is a column vector with all unit entries.*

Proof. One can prove consensus if $\eta = [\eta^T(t) \ \eta^T(t - \tau_1) \ \dots \ \eta^T(t - \tau_N)]^T = \kappa \vec{\mathbf{1}}$ at $\dot{V} = 0$ (i.e., the equilibrium), and if equilibrium point is at $\eta = \kappa \vec{\mathbf{1}}$. Therefore, consensusability would be equivalent to the condition, where firstly, the sum of all the entries in every row of $\check{L}_\tau$ is zero, and secondly, if $\eta \neq \kappa \vec{\mathbf{1}} \Rightarrow \dot{V} \neq 0$.

In Theorem 1, it was specified that $\mathcal{A}_i = [\mathcal{A}_{1i}, \mathcal{A}_{2i}, \dots, \mathcal{A}_{Ni}]$, and $\Gamma_i = \mathbf{Diag}(\Gamma_{1i}, \Gamma_{2i}, \dots, \Gamma_{Ni})$, $[\Gamma_{ji}]_{jj} = a_{ij}$ (with every other entry being zero), and $[\mathcal{A}_{ji}]_{ji} = a_{ij}$ (with every other entry being zero). This implies that $\vec{\mathbf{1}}^T(\Gamma_{ji} - \mathcal{A}_{ji}) = 0$ and $(\Gamma_{ji} - \mathcal{A}_{ji})\vec{\mathbf{1}} = 0$, or $\vec{\mathbf{1}}^T(\Gamma_i - \mathcal{A}_i) = 0$, and $(\Gamma_i - \mathcal{A}_i)\vec{\mathbf{1}} = 0$, $\forall i \in \mathcal{N}$. On the other hand, since $(\mathcal{D} - \sum_{i=1}^N \mathcal{A}_i)\vec{\mathbf{1}} = \vec{\mathbf{0}}$, and $\mathcal{D} = \sum_{i=1}^N \Gamma_i$, it follows that, $(2\mathcal{D} - \sum_{i=1}^N \Gamma_i - \sum_{i=1}^N \mathcal{A}_i)\vec{\mathbf{1}} = \vec{\mathbf{0}}$, and finally, $\vec{\mathbf{1}}^T \check{L}_\tau = 0$ and $\check{L}_\tau \vec{\mathbf{1}} = 0$, which proves that $\kappa \vec{\mathbf{1}}$ is an equilibrium for V . On the other hand, since $\eta = \vec{\mathbf{1}}$ is the only solution for $(2\mathcal{D} - \sum_{i=1}^N \Gamma_i - \sum_{i=1}^N \mathcal{A}_i)\eta = \vec{\mathbf{0}}$, it follows that $\kappa \vec{\mathbf{1}}$ is the only equilibrium, which completes the proof of the theorem. $\square$

Theorem 3. *A time-delayed connected MAS with the cooperative filter scheme in Figure 3 is time-delay resilient with respect to $x_{o(\ell)}(t) \in \mathcal{S}_o \subset \mathcal{S}$ against all bounded time-delay attacks, if $x_{o(\ell)}(t)$ is the output of $\mathcal{S}_o$. In other words $\lim_{\Delta t \rightarrow T_s} x_{o(\ell),i}(t + \Delta t) = x_{o(\ell)}(t)$, $\forall i \in \mathcal{N}$.*

We omit the proof of this lemma due to space constraints. However, one can have a non-rigorous proof to this theorem from the implication of Theorem 2, which states that the output of all the agents in Figure 3 at $t + T_s$ is necessarily equal regardless of their inputs at time t , and since the output of $\mathcal{S}_o$ is $x_{o(\ell)}(t)$ for all t including $t + T_s$, it follows that the output of all the filters at $t + T_s$ is $x_{o(\ell)}(t)$, which proves the theorem.

As discussed in the Assumptions, a DoS cyberattack from agent i to j can be represented by the assumption $a_{ij} = 0$. Therefore, a DoS cyberattack on a random set of edges $\tilde{\mathcal{E}}_k \subset \mathcal{E}$ (where $\tilde{\mathcal{E}}_k$ represents the k^{th} attack on some edges) in the time duration $\tilde{T}_k$ would result a random subgraph $\tilde{\mathcal{G}}_k \subset \mathcal{G}$ and a new Laplacian matrix $\tilde{L}_k$ where, $\mathbf{eig}(\tilde{L}_k) \geq 0$.

Theorem 4. *The cooperative filter scheme in Figure 3 achieves asymptotic consensus under arbitrarily random DoS cyberattacks, if there is no infinite DoS attack that disconnects the graph.*

Proof. Let us denote that $\delta_i = \eta_i - \eta_o$, and $\delta = [\delta_1, \dots, \delta_N]^T$. Let us also denote the Laplacian matrix of the MAS comprising the leader $\mathcal{S}_o$ and the followers $\mathcal{S}_i$, $i \in \mathcal{N}$ as $\tilde{L}$. We have seen from Theorem 1 that for a non switching topology η_i and therefore δ_i are asymptotically stable for all $i \in \mathcal{N}$. However, in case of random DoS attacks (refer to [14]) we assume that there are N_σ possible topologies that an adversary may inflict in the network as a result of DoS attack on one or more communication channels, including disconnections in the grid among the followers as well as the leader. Let us consider N_σ Laplacian matrices corresponding to each scenario, denoted by $\tilde{L}_1, \tilde{L}_2, \dots, \tilde{L}_{N_\sigma}$ where $\tilde{L}_i \geq 0$ (where $\mathbf{Rank}(\tilde{L}_i) = 0$ implies disconnections in the network). Corresponding to each scenario $\tilde{L}_i$ let us consider a symmetric positive definite matrix P_i with the same dimension (i.e., $N \times N$), and let us additionally consider a Lyapunov function $V(\delta(t)) = \delta^T(t) P_i \delta(t)$.

We will further assume that a random switching scenario σ_k takes place for $t \in [t_k, t_{k+1})$ where $T_k = t_{k+1} - t_k$ is finite for all σ_k . In order to prove Theorem 4 it would be sufficient to prove that for an arbitrary σ_k and an arbitrary topology (denoted by $\tilde{L}_i$ and P_i), one could find a P_j up to the next switching scenario σ_{k+1} (with topology $\tilde{L}_j$) such that $V(\delta(t_{k+2})) < V(\delta(t_{k+1}))$. For this, one could simply derive $V(\delta(t_{k+1}))$ and $V(\delta(t_{k+2}))$ as,

$$V(\delta(t_{k+1})) = \delta^T(t_k) e^{-\tilde{L}_i^T T_k} P_i e^{-\tilde{L}_i T_k} \delta(t_k) \quad (12)$$

and,

$$V(\delta(t_{k+2})) = \delta^T(t_{k+1}) e^{-\tilde{L}_j^T T_{k+1}} P_j e^{-\tilde{L}_j T_{k+1}} \delta(t_{k+1}). \quad (13)$$

Substituting $\delta(t_{k+1}) = e^{-\tilde{L}_i T_k} \delta(t_k)$ in Equation (13), one could obtain,

$$V(\delta(t_{k+2})) = \delta^T(t_k) e^{-\tilde{L}_i^T T_k} e^{-\tilde{L}_j^T T_{k+1}} P_j e^{-\tilde{L}_j T_{k+1}} e^{-\tilde{L}_i T_k} \delta(t_k). \quad (14)$$

However, if

$$e^{-\tilde{L}_j^T T_{k+1}} P_j e^{-\tilde{L}_j T_{k+1}} < P_i$$

or equivalently,

$$P_j < e^{\tilde{L}_j^T T_{k+1}} P_i e^{\tilde{L}_j T_{k+1}} \quad (15)$$

then $V(\delta(t_{k+2})) < V(\delta(t_{k+1}))$, or simply $V(t_{k+2}) < V(t_{k+1})$, for all $t_{k+2} > t_{k+1}$, implying that $\dot{V}(t) < 0$, $\forall t > 0$, which further implies that $\delta(t) \rightarrow 0$, as $t \rightarrow \infty$, or $\eta_i(t) \rightarrow \eta_o$, $\forall i \in \mathcal{N}$, as $t \rightarrow \infty$.

This could always be possible even if $\tilde{L}_i = 0$ or $\tilde{L}_j = 0$, which proves that there always exists positive symmetric matrices $P_1, P_2, \dots$ for all $T_1, T_2, \dots$ such that the Lyapunov function uniformly decays for all scenarios σ_k , under the condition that a disconnection does not last infinitely, which completes the proof of the theorem. $\square$

8. Simulations and Case Studies

The results derived in Section 7 can be validated by examining the LFC problem discussed in Figure 2, when the CPS is under time-delay attacks and multiple tele-metered variables such as $\Delta P_{ij}, \Lambda_i, \Delta f_j$ are simultaneously attacked by different random time-delays, and when ΔP_{d_i} is a random non-predictable bounded disturbance in the area load. To the best of the knowledge of this authors the above problem is yet a state-of-the-art open problem constituting an open challenge in the literature. The objective is to guarantee that $|\Delta P_{ij}|^2 + |\Delta f_i|^2 \rightarrow 0$ for all bounded load variations ΔP_{d_i} , regardless of the time-delay cyberattacks. The time-delayed LFC equation for area $\mathcal{S}_i$ can be represented by,

$$\dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) + E_{CCS,i} x_{CCS,i}(t - \tau_{CCS,i}) + D_i w_i(t) \quad (16)$$

where $x_i = [\Delta f_i, \Delta P_{m_i}, \Delta P_{v_i}, 0, \Delta P_{ij}]^T$ is the state vector of the endogenous states in $\mathcal{S}_i$, $x_{CCS,i} = [0, 0, 0, \Lambda_i, 0]^T$ is the vector of the exogenous states in $\mathcal{S}_i$ from $\mathcal{S}_{CCS}$ (i.e., the central control station CCS) as in Figure 1, and where,

$$A_i = \begin{bmatrix} -1/\tau_{p_i} & k_{p_i}/\tau_{p_i} & 0 & 0 & -k_{p_i}/\tau_{p_i} \\ 0 & -1/\tau_{ch_i} & 1/\tau_{ch_i} & 0 & 0 \\ -1/R_i \tau_{g_i} & 0 & -1/\tau_{g_i} & 0 & 0 \\ K_i B_i & 0 & 0 & 0 & K_i \\ 2\pi T_1 & 0 & 0 & 0 & -2\pi T_1 \end{bmatrix}, \quad (17)$$

$$E_{CCS,i} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{\tau_{g_i}} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, B_i = \begin{bmatrix} 0 \\ 0 \\ 1/\tau_{g_i} \\ 0 \\ 0 \end{bmatrix}, D_i = \begin{bmatrix} -k_{p_i}/\tau_{p_i} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

and where $w_i = \Delta P_{d_i}$ is a disturbance in the LFC representing the variations in the area load, and the renewable energies that contribute to the area power generation.

Remark 5. Clearly, in a real-time LFC without time-delays $x_i + x_{CCS,i}$ is the state vector for $\mathcal{S}_i$ as explained in outset of Section 5, and $A_i + E_{CCS,i}$ is the state matrix of the LTI system.

Refer to the explanations provided prior to Definition 3 for details.

In the simulation results below, a relatively significant and sudden load change in ΔP_{d_i} ($\pm 10\%$ of the nominal area load at time 0.1sec. and 0.8sec., as per the dashed line Figure 6) that triggers swings in the power system which has to be contained automatically. Time-delay attacks (if present) are capable of inducing severe instability in the power system if not appropriately circumvented as shown by the thinner line in Figure 5, which depicts the variations in the area frequency Δf_i when resilient filters are not present.

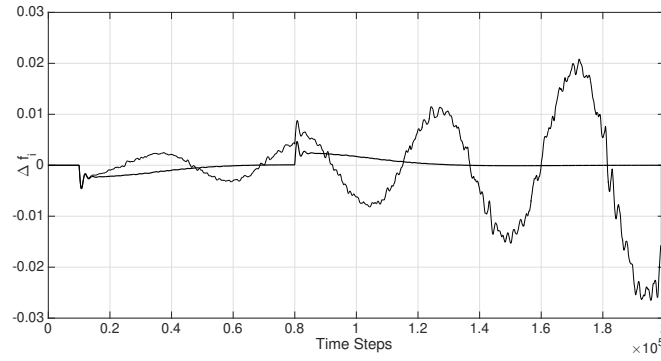


Figure 5. Performance of the time-delay resilient filter. The thin line represents Δf_i in response to a +10% load variation in ΔP_{d_i} , at 0.1sec. and back to 0 at 0.8sec., for the case where a conventional LFC is in operation. Perilous swings in the system frequency are clear when the telemetered data are attacked by sufficiently long time-delays, resulting in pervasive instability in the power system (thinner line). The same scenario is repeated when resilient cooperative filters are deployed (solid thicker line) which demonstrates stability and a satisfactory LFC control.

The solid curve in Figure 5 illustrates the simulation results in the presence of cooperative filters (outlined in Figure 3), where all tele-metered signals were conditioned by $h(t)$ before they were applied to the agents $\mathcal{S}_o, \mathcal{S}_i$. Corresponding to each exogenous state variable (i.e., $\Delta f_i, \Delta f_j, \Delta P_{ij}$, and Λ_i) a cooperative filter is deployed to recover time-delays in the signals. As a result, the instability in the power system can be maintained and the swings in the frequency in result to load variations are rapidly contained.

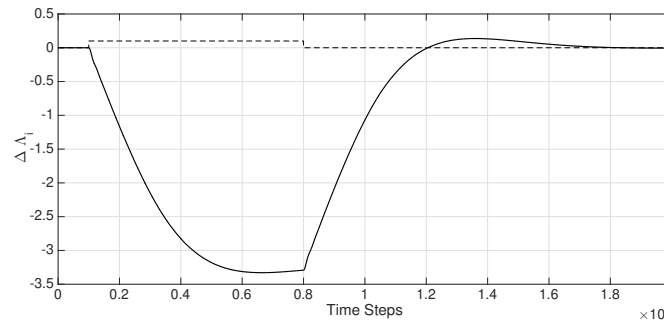


Figure 6. Variations in Λ_i as a result of $\Delta P_{d_i}(t)$.

The thick line in Figure 6 depicts the ACE Λ_i in response to a 10% load variations $\Delta P_{d_i}(t)$ (the dashed line). The ACE is the control parameter telemetered by the CCS $\mathcal{S}_o$ to all individual power generating units participating in the LFC. In the absence of a resilient filter mechanism, time-delay attacks on tele-communication links cause delayed inputs to CCS and delayed commands transmitted to the generating units.

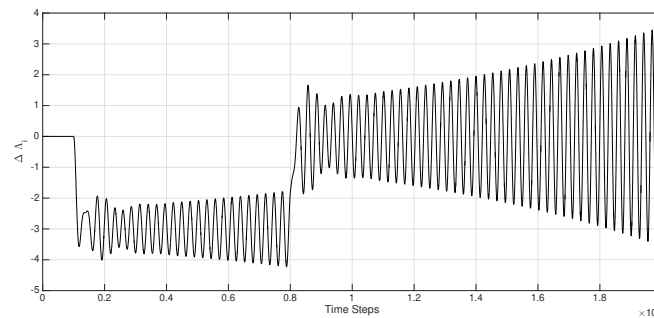


Figure 7. Time-Delayed ACE signal Λ_i transmitted from $\mathcal{S}_{CCO}$ without the employment of a delay-resilient cooperative filter system, and as a result of a 10% load disturbance ΔP_{d_i} .

This inflicts uncontrollable swings in the area power system that disseminates to the entire power system $\mathcal{S}$ as exemplified in 5. For the purpose of comparison, the time-delayed ACE signal $\Lambda_i(t - \tau_{\Lambda_i})$ without deploying delay-resilient cooperative filters would be as in Figure 7. It is important to note that the CCS requires ΔP_{ij} to be transmitted from $\mathcal{S}_{RTU} \rightarrow \mathcal{S}_{CCS}$ (as explained in Figure 2), as well as Δf_i to be transmitted from $\mathcal{S}_i \rightarrow \mathcal{S}_{CCS}$, in order to compute Λ_i according to Equation (3). Without employment of a time-delay resilient methodology, the delayed information $\Delta P_{ij}(t - \tau_{RTU,CCS})$ and $\Delta f_i(t - \tau_{f_i,CCS})$ would cause instability in the CCS controlled which will be disseminated to $\mathcal{S}_i$, which indeed is the phenomenon taking place in our case studies. Clearly, being at $\mathcal{S}_i$ it appears to be heuristically impossible to recover the real-time signal $\Lambda_i(t)$ from $\Lambda_i(t - \tau_{\Lambda_i})$, since the instability observed in $\mathcal{S}_i$ stems from a delayed signal transmitted from $\mathcal{S}_{RTU} \rightarrow \mathcal{S}_{CCS}$. Consequently, recovery of $\Lambda_i(t - \tau_{\Lambda_i})$ (while being at $\mathcal{S}_i$) requires information that is clearly beyond the reach of $\mathcal{S}_i$. The significance of the proposed methodology in this paper would now become clear, as it has been possible to restore normality in the entire CPS without requirement of subsystem's information, and only through the filtering of available signals at the subsystems.

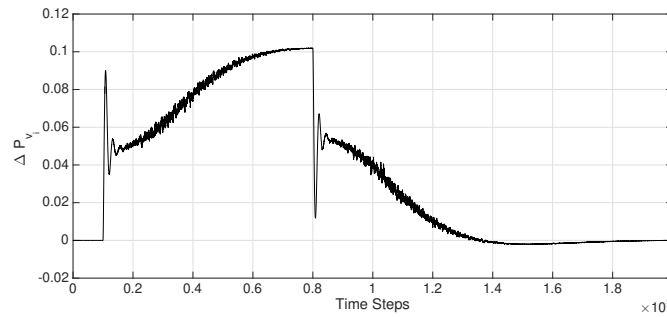


Figure 8. Adjustment of the servo-valve electric signal in response to the area load variations depicted in Figures 5.

Figure 8 depicts the electric signal to the governor servo-valve of the generator in $\mathcal{S}_i$ in response to the disturbance ΔP_{d_i} in the area load. It is evident that the $\pm 10\%$ load change triggers a $\pm 10\%$ command to the servo-valve in order to compensate for the load, ensuring complete balance in the supply-demand, which expectedly guarantees that $\Delta f_i \rightarrow 0$ and $\Delta P_{ij} \rightarrow 0$.

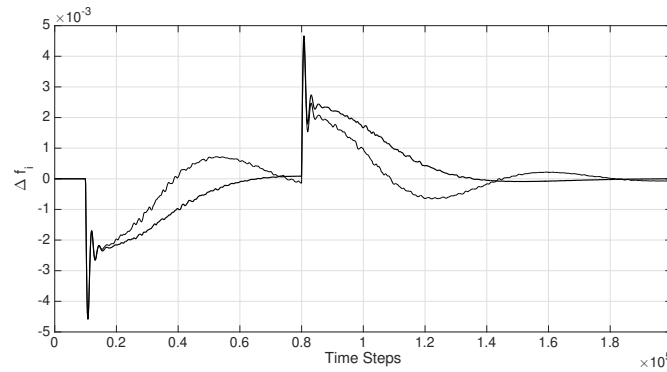


Figure 9. Affect of the tele-communication bandwidth. Inadequate bandwidth in tele-communication channels result in marginal instability as depicted by the thin line.

However, satisfactory functioning of the time-delay resilient LFC control scheme proposed in this paper strictly depends on the bandwidth of the tele-communication system and the speed of data transported between the system controllers, in comparison to the natural frequency of the system states. Figure 9 illustrates the importance of the tele-communication system bandwidth by comparing two scenarios. In the first scenario (thick line) a high bandwidth system is deployed, and in another attempt low bandwidth communication channels were being used. It is evident that inadequate bandwidth gives rise to instability in the power system (as depicted by the thin line in Figure 9).

Finally, Figure 10 is a general schematic of a part of an interconnected CPS with a random topology. It is assumed that the subsystems are transmitting equivalent reference signals to others, where each signal is subject to a random time-delay.

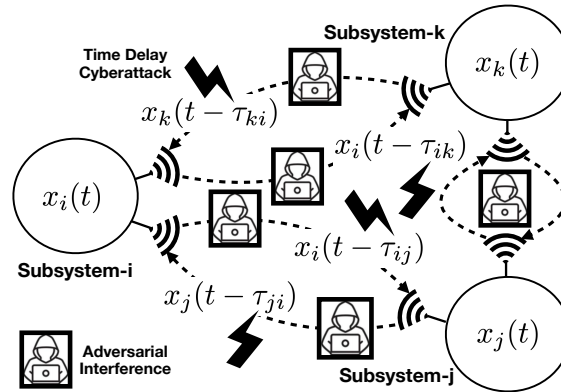


Figure 10. General architecture of a CPS, subject to adversarial time-delay cyberattacks. The exogenous states of the systems (x_i, x_j, x_k) are transmitted to adjacent subsystems with unknown time-delay and the output of $h(t)$ filters in each subsystem transmits the conditioned signal back to the source, hence, cooperative filters. The architecture shown in this figure results in time-delay resiliency in the CPS as demonstrated in Figure 11.

Figure 11 is the simulation result of the cooperative filters for five interconnected subsystems in a discrete-time framework. It is evident that the filters can track the real-time reference signal despite of the unknown time-delays within a time-duration T_s .

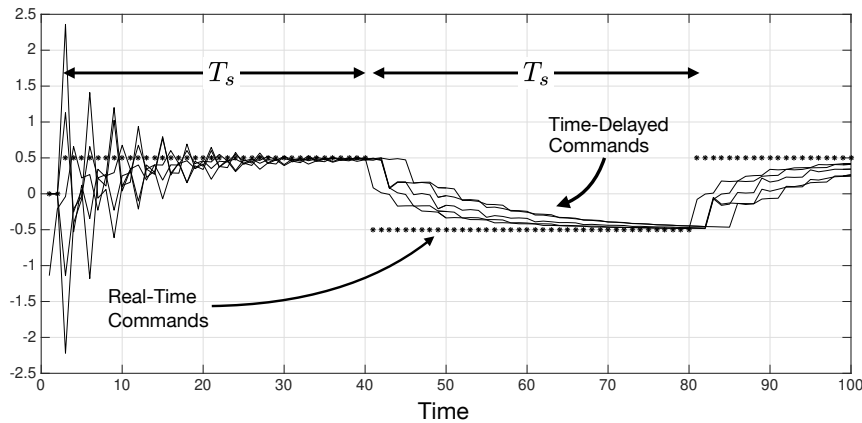


Figure 11. A discrete-time network of five interconnected agents transmitting equivalent reference signals (shown by the asterisks) to adjacent subsystems. The tele-communication channels are randomly delayed and the output of the cooperative filters are shown by thinner lines for each subsystem. It is evident that the delayed signals follow the real-time reference signal in a time-duration T_s that is dependent of the filter gain and the topology of the network.

9. Conclusion

Resiliency against time-delay and DoS cyberattacks on CPS, and in particular, the LFC problem in smart grids have been investigated in this paper. It has been shown that augmentation of the tele-communication receivers with certain cooperative filters that exchange their outputs with neighbouring filters (in a multi-agent system framework) can circumvent time-delay sabotage, without any modification to the systems internal controllers. In essence, the cooperative filters receive the time-delayed outputs of their neighbouring filters and augment this information with a locally derived conjecture of the real-time value of some exogenous state that is under time-delay cyberattack, to derive the true real-time value of the attacked state under question. The paper has also shown that finite-time denial of service (DoS) cyberattacks cannot distract the convergence of the cooperative filters and

invalidate the results. Theoretical results of the proposed methodology has been examined through a case study in a simulation platform that involves a load frequency control problem in a multi-area power system. Complicated control problems such as random time-delays in the transportation of data packets in the LFC that normally elevate instability issues and severe frequency swings had been successfully contained through the proposed cooperative filtering scheme as a result of the simulation.

References

1. Z. Feng, G. Wen, and G. Hu, Distributed Secure Coordinated Control for Multiagent Systems under Strategic Attacks, *IEEE Trans. Cybern.*, Vol. 47, No. 5, Pages 1273-1284, May 2017.
2. D. R. Ding, Z. D. Wang, D. W. C. Ho, and G. L. Wei, Observer Based Event-Triggering Consensus Control for Multiagent Systems with Lossy Sensors and Cyber-Attacks, *IEEE Trans. Cybern.*, Vol. 47, No. 8, Pages 1936-1947, Aug. 2017.
3. A. Abdessameud, A. Tayebi, Cooperative Output Regulation of Linear Multi-Agent Systems with Communication Constraints, *IEEE 55th Conference on Decision and Control (CDC)*, Las Vegas, USA, December 12-14, 2016.
4. C. Deng, C. Wen, MAS Based Distributed Resilient Control for a Class of Cyber-Physical Systems With Communication Delays Under DoS Attacks, *IEEE Transactions on Cybernetics*, Early Access DOI: 10.1109/TCYB.2020.2972686, March 2020.
5. S. Shahkar, K. Khorasani, A Resilient Control Against Time-Delay Switch and Denial of Service Cyber Attacks on Load Frequency Control of Distributed Power Systems, *4th IEEE Conference on Control Technology and Applications (CCTA 2020)*, Montréal, Canada, August 24-26, 2020.
6. F. Guo, Q. Xu, C. Wen, L. Wang, P. Wang, Distributed Secondary Control for Power Allocation and Voltage Restoration in Islanded DC Micro-grids, *IEEE Trans. Sustain. Energy*, Vol. 9, No. 4, Pages 1857-1869, doi: 10.1109/TSTE.2018.2816944, Oct. 2018.
7. S. E. Tuna, LQR-Based Coupling Gain for Synchronization of Linear Systems [Online]. Available: <http://arxiv.org/abs/0801.3390>.
8. C. Ma, J. Zhang, Necessary and Sufficient Conditions for Consensusability of Linear Multi-Agent Systems, *IEEE Transactions on Automatic Control*, Vol. 55, No. 5, May 2010.
9. M. Meng, L. Liu, G. Feng, Output Consensus for Heterogeneous Multiagent Systems with Markovian Switching Network Topologies, *International Journal of Robust and Nonlinear Control*, DOI: 10.1002/rnc.3918, Feb. 2018.
10. M. Meng, G. Xiao, C. Zhai, G. Li, Z. Wang, Distributed Consensus of Heterogeneous Multi-Agent Systems Subject to Switching Topologies and Delays, *Journal of the Franklin Institute* 357, 6899-6917, 2020.
11. D. Zhang, G. Feng, A New Switched System Approach to Leader-Follower Consensus of Heterogeneous Linear Multiagent Systems With DoS Attack, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, DOI:10.1109/TSMC.2019.2895097, February 2019.
12. Z. Ahmed, M.M. Khan, M.A. Saeed, W. Zhang, Consensus Control of Multi-Agent Systems with Input and Communication Delay: A Frequency Domain Perspective, *ISA Transactions* 101, Pages 69-77, 2020.
13. T. Qi, L. Qiu, J. Chen, Fellow, MAS Consensus and Delay Limits Under Delayed Output Feedback, *IEEE Transactions on Automatic Control*, Vol. 62, No. 9, Sep. 2017.
14. J. C. Geromel, P. Colaneri, Stability and Stabilization of Continuous-Time Switched Linear Systems, *SIAM J. Control Optimization*, Vol. 45, No. 5, Pages 1915-1930, 2006.
15. M. Zhanga, A. Saberria, A. A. Stoorvogel, Synchronization in the Presence of Unknown, Nonuniform and Arbitrarily Large Communication Delay, *European Journal of Control* 38, Pages 63-72, 2017.
16. Z. Liu, D. Nojavanzadeh, A. Saberi, A. A. Stoorvogel, Scale-Free Collaborative Protocol Design for Output Synchronization of Heterogeneous Multi-Agent Systems With Nonuniform Communication Delays, *IEEE Transactions on Network Science and Engineering*, Vol. 9, No. 4, August 2022.
17. C. Wang, C. Wen, L. Guo, Adaptive Consensus Control for Nonlinear Multiagent Systems With Unknown Control Directions and Time-Varying Actuator Faults, *IEEE Transactions on Automatic Control*, Vol. 66, No. 9, September 2021.
18. S. Xiong, Z. Hou, L. Fan, Consensus Control of Unknown Nonlinear Discrete-Time Multi-Agent Systems with Nonuniform Time-Delays, *IEEE 12th Data Driven Control and Learning Systems Conference*, Xiangtan, China, May 12-14, 2023.

19. L. Yuan, J. Li, Consensus of Discrete-Time Nonlinear Multiagent Systems Using Sliding Mode Control Based on Optimal Control, *IEEE Access*, Vol.10, 2022.
20. X. J. Peng, Y. He, Consensus of Multi-Agent Systems With Time-Varying Delays and Switching Topologies Based on Delay-Product-Type Functionals, *IEEE Transactions on Cybernetics*, Digital Object Identifier 10.1109/TCYB.2022.3200686, 2022.
21. F. Sun, X. Wu, J. Kurths, W. Zhu, Group Consensus for Heterogeneous Multi-Agent Systems With Time Delays Based on Frequency Domain Approach, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 53, No. 5, May 2023.
22. L. Solyman, A. Elbadawy, A. Meroth, Single Model Scheme Based Smith Predictor for the Mitigation of the Effects of Network Imperfections in Consensus Control of Multi Agent Systems, 10th International Conference on Control, Decision and Information Technologies (CoDIT), 2024.
23. Z. Cheng, D. Yue, S. Hu, X. Xie, C. Huang, Detection-Based Weighted H-Infinity LFC for Multi-Area Power Systems under DoS Attacks, *IET Control Theory Applications*, Vol. 13, Issue 12, Pages 1909-1919, 2019.
24. D.K. Panda, S. Das, S. Townley, Towards a More Renewable Energy Based LFC under Random Packet Transmissions and Delays with Stochastic Generation and Demand, *IEEE Transactions on Automation Science and Engineering*, <http://hdl.handle.net/10871/124292>, 2021.
25. X. Zhao, Z. Ma, S. Li and S. Zou, Robust LFC of Power Systems With Wind Power Under Packet Losses and Communication Delays, in *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, Vol. 12, No. 1, Pages 135-148, doi: 10.1109/JETCAS.2022.3141108, March 2022.
26. X. C. Shangguan, C.K. Zhang, Y. Zhao, Resilient Load Frequency Control of Power Systems to Compensate Random Time Delays and Time-Delay Attacks, *IEEE Transactions on Industrial Electronics*, Vol. 70, No. 5, Pages 5115-5128, doi: 10.1109/TIE.2022.3186335, May 2023.
27. J. Yang, Q. Zhong, K. Shi, S. Zhong, Distributed Coordination LFC Approach for Interconnected Power Systems Under Detection and Compensation Mechanism Targeting DoS Attacks, *IEEE Transactions on Industrial Informatics*, Vol. 19, No. 11, Pages 11008-11018, doi: 10.1109/TII.2023.3242587, Nov. 2023.
28. Y. Wang, Z. Wang, J. Gan, H. Zhang and R. Wang, Switched Observer-Based Adaptive Event-Triggered Load Frequency Control for Networked Power Systems Under Aperiodic DoS Attacks, *IEEE Transactions on Smart Grid*, Vol. 14, No. 6, Pages 4816-4826, doi: 10.1109/TSG.2023.3260269, Nov. 2023.
29. K. Karoui, F.B. Ftima, H.B. Ghezala, A Multi-Agent Framework for Anomalies Detection on Distributed Firewalls Using Data Mining Techniques, In: Cao, L. (eds) *Data Mining and Multi-agent Integration*, Springer, Boston, MA. <https://doi.org/10.1007/978-1-4419-0522-2-18>, 2009.
30. S. Shahkar, Cooperative Localization of Multi-Agent Autonomous Aerial Vehicle (AAV) Networks in Intelligent Transportation Systems, *IEEE Open Journal of Intelligent Transportation Systems (OJITS)*, Digital Object Identifier 10.1109/OJITS.2025.3531363, 2025.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.