Preprints of the 23rd IFAC World Congress
Busan, Republic of Korea, August 23-28, 2026

Opacity Verification for Multi-Agent Cyber-Physical Systems

Jing Wu * **Tarek Raïssi** ** **Zhiwu Li** ***,*

* *School of Mechano-Electronic Engineering, Xidian University , Xi'an 710071, China (e-mail: jingwu@stu.xidian.edu.cn).*
** *CEDRIC-Lab, Conservatoire National des Arts et Metiers, Paris 75141, France (e-mail:tarek.raissi@cnam.fr).*
*** *Institute of Systems Engineering, Macau University of Science and Technology, Macau 999078, China (e-mail: zwli@must.edu.mo).*

Abstract: This paper addresses the opacity verification problem for multi-agent cyber-physical systems governed by P-type iterative learning control. The system's confidentiality and opacity are formally defined by linking the anti-interference capability to the output error. A verification framework is developed based on the attacker's observation capability, and sufficient conditions are established to ensure opacity preservation. Unlike discrete abstraction methods, the proposed approach directly analyzes continuous-time dynamics, simplifying verification while retaining intrinsic system characteristics. Theoretical analysis and simulations demonstrate that the P-type iterative learning control scheme enables multi-agent systems to achieve accurate tracking performance while maintaining opacity against potential intrusions.

Keywords: Cyber-physical systems, iterative learning control, multi-agent systems, opacity.

1. INTRODUCTION

Multi-agent cyber-physical systems (MAS-CPSs) are widely applied in areas such as marine surface vehicles, autonomous vehicles, and cooperative robotics He et al. (2022a,b); Chen et al. (2015). These systems consist of interacting agents that improve performance through feedback control and information exchange. However, such architectures also introduce security vulnerabilities, as attacks on individual agents or communication links can propagate across the network and compromise overall system robustness Cui et al. (2025); Jia et al. (2024). Existing studies on opacity in distributed architectures mainly address multi-attacker scenarios. As a privacy notion, opacity characterizes whether confidential system information can be inferred by external observers. Decentralized opacity and its verification have been extensively studied Paoli and Lin (2012); Wu et al. (2018); Ramasubramanian et al. (2020). However, limited attention has been paid to single external attackers inferring sensitive information from system outputs, which may degrade performance or disrupt cooperation. Therefore, ensuring both system resilience and information confidentiality remains a critical challenge in MAS-CPSs.

Iterative learning control (ILC) Arimoto et al. (1984) is widely used to improve performance in repetitive tasks. By leveraging past errors, it enables iterative input updates for accurate tracking and disturbance rejection Huang et al. (2021); Wu et al. (2023); Chi et al. (2020). However, its potential for concealing critical system attributes from external observers remains largely unexplored.

System opacity quantifies a system's ability to conceal confidential information. Originating in DES, it is broadly classified into language-based Habbachi et al. (2026, 2022); Tong et al. (2016) and state-based forms Dong et al. (2022, 2025); Duan et al. (2023); Li et al. (2025). With the rise of CPSs, opacity has been extended to continuous-state systems to capture information concealment in dynamic and networked environments An and Yang (2020); Yin et al. (2021); Liu and Zamani (2021); John and Katewa (2025); Liu et al. (2025). In particular, An and Yang (2020) treats interference attenuation capability as a confidential dynamic property of a system and investigates the enhancement of opacity from a security perspective, where continuous dynamics may become targets for adversarial inference. Inspired by An and Yang (2020), this paper regards the anti-interference capability (AIC) as a secret dynamic property and develops a framework over a bounded time horizon. Different from An and Yang (2020), the notion of opacity is formulated based on error evolution, and the analysis is extended to more complex multi-agent systems.

However, in multi-agent environments governed by ILC, the challenge is inherently twofold: the system must not only ensure robust performance under disturbances but also prevent external attackers from inferring the existence of such capabilities through observation. Due to the iterative nature of the control process and the intricate network interactions among agents, existing opacity verification methods cannot be directly applied to this setting. Motivated by this research gap, this study investigates opacity

⋆ This work was supported in part by the Science and Technology Development Fund, Macao Special Admiristrative Region (MSAR), under Grant 0029/2022/AGJ and Grant 0029/2023/RIA1, and in part by the Program of Guangdong under Grant 2023A0505020003. J. Wu was also supported by the Program of China Scholarship Council under Grant 202506960006

©2026 the authors. Accepted by IFAC for publication under a Creative Commons Licence CC-BY-NC-ND

verification for MAS-CPS governed by P-type iterative learning control (P-ILC).

The notion studied in this paper differs from classical opacity. Here, the secret is not a system state but a dynamic property, namely the AIC under the P-ILC framework. Moreover, the proposed framework is defined over a bounded time horizon, unlike many existing models. The main contributions of this paper are summarized as follows:

1) For MAS-CPSs under P-ILC, the concepts of system confidentiality and opacity are formally defined by establishing a connection between the AIC and the output error.

2) A verification framework for system opacity is proposed based on the attacker's observation capability, along with sufficient conditions to ensure opacity preservation.

3) Theoretical analysis and simulation results demonstrate that, under P-ILC control, multi-agent systems can achieve tracking performance while preserving opacity.

2. PRELIMINARIES

2.1 Notations

For clarity and consistency, the main mathematical notations used throughout this paper are summarized in this subsection. The symbol $\otimes$ denotes the Kronecker product. The superscript $(\cdot)^{\mathrm{T}}$ denotes matrix transposition. I_n represents the $n \times n$ identity matrix. The set of positive integers is denoted by $\mathbb{Z}^+$. $\mathbb{N}$ denotes the number of agents. $\mathbb{R}^n$ denotes the n-dimensional Euclidean space, and $\mathbb{R}^{m\times n}$ represents the set of all real matrices with m rows and n columns. For any vector $x(t) \in \mathbb{R}^n$, $\|x(t)\| = \sqrt{x(t)^{\mathrm{T}}x(t)}$ denotes its Euclidean norm, and the λ-norm is defined as $\|x\|_\lambda = \sup_{t\in[0,T]}\{e^{-\lambda t}\|x(t)\|\}$, where $\lambda > 0$. For a matrix $A \in \mathbb{R}^{m\times n}$, $\|A\|$ denotes its induced 2-norm. The notation $diag\{a_1, a_2, \cdots, a_n\}$ stands for a diagonal matrix with diagonal entries $a_1, a_2, \cdots, a_n$.

2.2 MASs Communication Topology

Agents in a MAS exchange information via a directed communication topology $\mathbb{G} = (\mathcal{V}, \mathcal{E}, \mathcal{G})$, where $\mathcal{V} = \{1, 2, \cdots, \mathbb{N}\}$ denotes the set of agents, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ represents the set of directed edges capturing the communication links among agents, and $\mathcal{G} = [g_{i,j}]$ is the weighted adjacency matrix that characterizes the presence of these links. In particular, each entry $g_{i,j}$ of $\mathcal{G}$ is defined as

$$g_{i,j} = \begin{cases} 1, \text{if there exists a directed link from agent } j \text{ to } i, \\ 0, \text{otherwise.} \end{cases}$$

And let $\mathcal{D} = diag\{d_1, d_2, \cdots, d_{\mathbb{N}}\}$ denote the in-degree matrix of the graph, where d_i represents the in-degree of vertex i, which is defined as the sum of the weights of all incoming edges to agent i, that is,

$$d_i = \sum_{j=1}^{\mathbb{N}} g_{i,j}.$$

$\mathbb{N}_i$ means a collection of neighbor agents of agent i. The Laplacian matrix of the directed graph $\mathbb{G}$ is then defined as $\mathcal{L} = \mathcal{D} - \mathcal{G}$. Let $S = diag\{s_1, s_2, \cdots, s_{\mathbb{N}}\}$ denote the diagonal matrix representing the direct communication links between the virtual leader and the agents. Each element s_i is defined as $s_i = 1$ if agent i can directly receive information from the leader agent, and $s_i = 0$ otherwise. The matrix $\mathcal{L} + S$ is then used to describe the augmented communication topology that incorporates the leader's influence on the multi-agent network.

3. BACKGROUND

3.1 System Model

The research object of this study is a repetitively operated linear MAS-CPS, which is modeled by the following equations:

$$\begin{cases} \dot{x}_i(k,t) = Ax_i(k,t) + Bu_i(k,t), \\ z_i(k,t) = Cx_i(k,t) + Du_i(k,t), \end{cases} \tag{1}$$

where $t \in [0, T]$ denotes the continuous time within a finite time interval, $k \in \mathbb{Z}^+$ represents the iteration index associated with repeated executions of the same task, and $i \in \{1, 2, \cdots, \mathbb{N}\}$ is the agent index in the multi-agent system. The vector $x_i(k,t) \in \mathbb{R}^n$ denotes the system state, $u_i(k,t) \in \mathbb{R}^m$ is the control input, and $z_i(k,t) \in \mathbb{R}^p$ represents the controlled output. The matrices $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $C \in \mathbb{R}^{p\times n}$, and $D \in \mathbb{R}^{p\times m}$ are constant matrices with appropriate dimensions that describe the system's dynamics, input, and output relationships.

It is worth noting that the plant dynamics are iteration-invariant, with A, B, C, and D fixed. The iteration dependence in (1) stems from repeated task execution and input updates, causing the state and output trajectories $x_i(k,t)$ and $z_i(k,t)$ to evolve along the iteration axis.

To focus on the influence of attacker-induced disturbances on the AIC, we introduce the following assumption.

Assumption 1. The MAS-CPS is assumed to operate without any external process or measurement noise.

The assumption of a noise-free system is adopted to simplify the presentation of the methodology; the inclusion of process and measurement noise will be addressed in future work.

3.2 Attacker Model

Due to limited resources, continuous full-spectrum attacks are impractical. Thus, attacks on MAS-CPSs typically proceed in three stages: probing the system with injected signals, inferring its dynamics from observed responses, and launching targeted attacks to degrade consensus tracking. This paper focuses on the first two stages. On this basis, the attacker is assumed to infer the system's secret, namely its AIC, under the following capabilities and constraints. A formal definition will be given later.

1) The attacker can inject an attack signal into the state channel and output channel of MAS-CPS over a finite time interval $[0, T]$. The injected signal is modeled in the general form

$$a_i(k,t) = \rho_i(t)\omega_i(k,t), \tag{2}$$

where $\omega_i(k,t)$ denotes the attack waveform and $\rho_i(t)$ is a time-window function indicating when the attack is active. Moreover, the attack waveform is assumed to have a uniformly bounded increment across iterations: there exists a constant $L_\omega > 0$ such that, for all agents i, all iterations $k > 0$ and all $t \in [0,T]$,

$$\|\omega_i(k+1,t) - \omega_i(k,t)\| \leqslant L_\omega. \tag{3}$$

2) The attacker has access only to partial output measurements of the MAS-CPS; the observable output is denoted by the general form

$$y_i(k,t) = Ez_i(k,t) + Ga_i(k,t). \tag{4}$$

where E is the observation mapping and G is the observation error matrix with appropriate dimensions.

3) The attacker has the knowledge of the desired trajectories that the MAS-CPS is intended to follow.

4) Since they are internal parameters of the system, their specific values are generally unavailable to external parties. The attacker does not have access to the system matrices A, B, C and D.

Then the dynamics of the i-th agent under attack during iteration k and time $t \in [0,T]$ are modeled as

$$\begin{cases} \dot{x}_i^a(k,t) = Ax_i^a(k,t) + Bu_i(k,t) + Fa_i(k,t), \\ z_i(k,t) = Cx_i^a(k,t) + Du_i(k,t), \\ y_i(k,t) = Ez_i(k,t) + Ga_i(k,t). \end{cases} \tag{5}$$

For each iteration k and all agents i, the variables $x_i^a(k,t), u_i(k,t), z_i(k,t), y_i(k,t)$, and $a_i(k,t)$ are represented in the following compact vector format:

$$\begin{aligned} \mathcal{X}_a(k,t) &:= (x_1^{a\mathrm{T}}(k,t), x_2^{a\mathrm{T}}(k,t), \cdots, x_{\mathbb{N}}^{a\mathrm{T}}(k,t))^{\mathrm{T}}, \\ \mathcal{U}(k,t) &:= (u_1^{\mathrm{T}}(k,t), u_2^{\mathrm{T}}(k,t), \cdots, u_{\mathbb{N}}^{\mathrm{T}}(k,t))^{\mathrm{T}}, \\ \mathcal{Z}(k,t) &:= (z_1^{\mathrm{T}}(k,t), z_2^{\mathrm{T}}(k,t), \cdots, z_{\mathbb{N}}^{\mathrm{T}}(k,t))^{\mathrm{T}}, \\ \mathcal{Y}(k,t) &:= (y_1^{\mathrm{T}}(k,t), y_2^{\mathrm{T}}(k,t), \cdots, y_{\mathbb{N}}^{\mathrm{T}}(k,t))^{\mathrm{T}}, \\ \mathcal{A}(k,t) &:= (a_1^{\mathrm{T}}(k,t), a_2^{\mathrm{T}}(k,t), \cdots, a_{\mathbb{N}}^{\mathrm{T}}(k,t))^{\mathrm{T}}. \end{aligned}$$

3.3 ILC Algorithm

Since the MAS-CPS repeatedly performs the same task over $[0,T]$, ILC is adopted to improve tracking and consensus performance across iterations. The plant model remains unchanged, while the control input is updated using the previous iteration's error. P-ILC is a widely used ILC scheme that updates control inputs based on past errors, enabling simple and efficient learning-based correction.

The control objective of this study is to ensure that the consensus error between any two agents asymptotically converges to zero along the iterative domain. To achieve this, let $y_d(t)$ represent a virtual leader in the communication topology, denoted as vertex 0, and define the extended graph as $\mathbb{G}* = \{\mathcal{V} \cup \{0\}, \mathcal{E}*, \mathcal{G}*\}$. The consensus controlled error between the i-th follower and the virtual leader during the k-th iteration is then expressed as

$$e_i^z(k,t) = y_d(t) - z_i(k,t). \tag{6}$$

For the subsequent analysis, the attacker observes only the corrupted measurement $y_i(k,t)$ rather than $z_i(k,t)$. Accordingly, the measurement error from the attacker's perspective is defined as

$$e_i^y(k,t) = y_d(t) - y_i(k,t), \tag{7}$$

and they are written in the following compact form

$$\begin{aligned} e_z(k,t) &= (e_1^{z\mathrm{T}}(k,t), e_2^{z\mathrm{T}}(k,t), \cdots, e_{\mathbb{N}}^{z\mathrm{T}}(k,t))^{\mathrm{T}}, \\ e_y(k,t) &= (e_1^{y\mathrm{T}}(k,t), e_2^{y\mathrm{T}}(k,t), \cdots, e_{\mathbb{N}}^{y\mathrm{T}}(k,t))^{\mathrm{T}}. \end{aligned}$$

Consider all the information received by the i-th follower within each iteration k over the time interval $[0,T]$, which is defined as

$$\phi_i^z(k,t) = \sum_{j \in \mathbb{N}_i} g_{i,j}(z_j(k,t) - z_i(k,t)) + s_i(y_d(t) - z_i(k,t)). \tag{8}$$

It includes the information transmitted from other follower agents $j \in \mathcal{N}_i$ and from the virtual leader agent d. Its compact form is expressed as

$$\Phi_z(k,t) = (\phi_1^{z\mathrm{T}}(k,t), \phi_2^{z\mathrm{T}}(k,t), \cdots, \phi_{\mathbb{N}}^{z\mathrm{T}}(k,t))^{\mathrm{T}}.$$

Combining Eqs. (6) and (8) yields the following expression

$$\Phi_z(k,t) = ((\mathcal{L} + S) \otimes I_z) e_z(k,t). \tag{9}$$

The P-ILC is designed as

$$\mathcal{U}(k+1,t) = \mathcal{U}(k,t) + ((\mathcal{L} + S) \otimes \Gamma) e_z(k,t), \tag{10}$$

where Γ is referred to as the learning operator.

4. PROBLEM FORMULATION

4.1 Confidentiality

The system's secret is defined as the AIC, which characterizes resilience by quantifying performance under disturbances. From a control perspective, the AIC is fundamentally determined by the system's controlled output error, which characterizes its behavioral response under attack. Accordingly, the following definition is introduced to formally describe the system's confidentiality.

Definition 1. Consider a MAS-CPS described by (5). The system is said to possess AIC if the following condition is satisfied

$$\lim_{k \to \infty} \|e_z(k+1,t)\| = 0. \tag{11}$$

In the considered attack scenario, the attacker launches the attack after the MAS-CPS has sufficiently converged under the P-ILC law. Hence, the controlled error $\|e_z(k,t)\|$ is already close to zero at the attack instant, thereby indicating AIC.

4.2 Problem Statement

Building on the above definition of system secrecy, the concept of opacity is introduced to characterize the information-hiding property of a system with respect to its AIC.

Definition 2. Given a constant $\beta > 0$, the MAS-CPS (5) is said to be bounded-horizon error-based opaque with respect to its AIC if, whenever the system possesses AIC, an external attacker is unable to correctly infer this fact from the available observations, that is,

$$\lim_{k\to\infty} \|e_y(k+1,t)\| \geqslant \beta > 0. \tag{12}$$

The asymptotic formulation is primarily for theoretical analysis. In practice, the attack is launched when the MAS-CPS operates near the AIC regime, such that the separation between $\|e_z(k,t)\|$ and $\|e_y(k,t)\|$ can already be observed at small iteration indices.

5. MAIN RESULTS

The initial value conditions of all agents for the repetitively operated linear multi-agent cyber-physical system (5) are assumed as follows.

Assumption 2. The initial state is assumed to remain identical across all iterations, i.e.,

$$x_i(k,0) = c, \tag{13}$$

where c is a constant.

Remark 1. For clarity of presentation, the initial state of the system is assumed to be fixed. It should be noted that the proposed method also applies to scenarios with initial state deviations, and this extension will be addressed in future work.

Assumption 3. $D \in \mathbb{R}^{p\times m}$ is row full rank.

Remark 2. The P-ILC algorithm ensures convergence only when the matrix D is of full rank; otherwise, the system may exhibit oscillatory behavior and fail to converge. When $D = 0$, a PD-ILC scheme can be employed as an alternative to guarantee stability and convergence of the iterative process.

The following theorem is provided to demonstrate the system's AIC.

Theorem 1. Consider the MAS-CPS (5), with the initial value conditions (13). The system is said to possess AIC if the following condition is satisfied:

$$\|I - ((\mathcal{L}+S)\otimes D\Gamma)\| < 1. \tag{14}$$

Proof. To establish the system's AIC, it is necessary to compute the controlled output error using (6) and (10),

$$e_i^z(k+1,t) = e_i^z(k,t) - C\Delta x_i(k+1,t) - D\Gamma\phi_i^z(k,t), \tag{15}$$

where $\Delta x_i(k+1,t) \triangleq x_i(k+1,t) - x_i(k,t)$. Its compact form is

$$\begin{aligned} e_z(k+1,t) = {} & (I - ((\mathcal{L}+S)\otimes D\Gamma))e_z(k,t) \\ & - C\Delta\mathcal{X}_a(k+1,t), \end{aligned} \tag{16}$$

where $\Delta\mathcal{X}_a(k+1,t) \triangleq \mathcal{X}_a(k+1,t) - \mathcal{X}_a(k,t)$ denotes the inter-iteration difference. Evaluating (5) at iterations $k+1$ and k, and integrating their difference over $[0,t]$ under identical initial conditions, yields the following difference dynamics:

$$\begin{aligned} & \Delta\mathcal{X}_a(k+1,t) \\ = {} & A\int_0^t \Delta\mathcal{X}_a(k+1,\tau)\mathrm{d}\tau + ((\mathcal{L}+S)\otimes B\Gamma)\int_0^t e_z(k,\tau)\mathrm{d}\tau \\ & + F\int_0^t \Delta\mathcal{A}(k+1,\tau)\mathrm{d}\tau, \end{aligned} \tag{17}$$

where $\Delta\mathcal{A}(k+1,t) \triangleq \mathcal{A}(k+1,t) - \mathcal{A}(k,t)$. Next, substituting the result of equation (17) into equation (16) and using the definition of norm, yields

$$\begin{aligned} & \|e_z(k+1,t)\| \\ \leqslant {} & \|I - ((\mathcal{L}+S)\otimes D\Gamma)\|\|e_z(k,t)\| + \|CF\|L_\omega T \\ & + \|CA\|\int_0^t \|\Delta\mathcal{X}_a(k+1,\tau)\|\mathrm{d}\tau \\ & + \|(\mathcal{L}+S)\otimes CB\Gamma\|\int_0^t \|e_z(k,\tau)\|\mathrm{d}\tau. \end{aligned} \tag{18}$$

The result of taking the λ-norm of the above equation is given as follows

$$\begin{aligned} & \|e_z(k+1)\|_\lambda \\ \leqslant {} & \|I - ((\mathcal{L}+S)\otimes D\Gamma)\|\|e_z(k)\|_\lambda + \|CF\|L_\omega T e^{-\lambda t} \\ & + \|CA\|\|\Delta\mathcal{X}_a(k+1)\|_\lambda \frac{1-e^{-\lambda t}}{\lambda} \\ & + \|(\mathcal{L}+S)\otimes CB\Gamma\|\|e_z(k)\|_\lambda \frac{1-e^{-\lambda t}}{\lambda}. \end{aligned} \tag{19}$$

Under the condition (14), let $\lambda > 0$ and be sufficiently large; then, the following holds

$$\lim_{k\to\infty} \|e_z(k+1)\|_\lambda = 0. \tag{20}$$

It means

$$\lim_{k\to\infty} \sup_{t\in[0,T]} \{\|e_z(k+1,t)\|e^{-\lambda t}\} = 0. \tag{21}$$

Then we derive that

$$\lim_{k\to\infty} \|e_z(k+1,t)\| = 0. \tag{22}$$

By applying the definition of AIC, it follows that the MAS-CPS (5) possesses AIC. This completes the proof of Theorem 1.

Next, Theorem 2 is presented to verify the opacity of the MAS-CPS.

Theorem 2. Let the MAS-CPS (5) satisfy the condition of Theorem 1, and let the attacker possess the capabilities and constraints described in Subsection 3.2. Then the system is bounded-horizon error-based opaque.

Proof. Firstly, based on (7) and (10), the norm of the measurable output error compact form is written as

$$\begin{aligned} \|e_y(k+1,t)\| \leqslant {} & \|e_y(k,t)\| + \|EC\|\|\Delta\mathcal{X}_a(k+1,t)\| \\ & + \|G\|\|\Delta\mathcal{A}(k+1,t)\| \\ & + \|(\mathcal{L}+S)\otimes ED\Gamma\|\|e_z(k,t)\|. \end{aligned} \tag{23}$$

By using an argument similar to that in the proof of Theorem 1, together with the persistence of the attack term, it follows that the measurable output error cannot

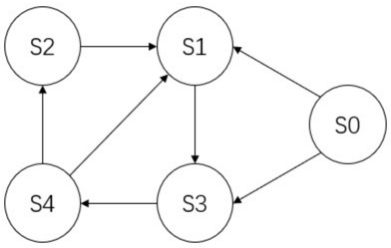


Fig. 1. Communication topology

asymptotically converge to zero along the iteration axis. Hence, there exists a constant $c > 0$ such that $\|e_y(k+1,t)\| \geqslant \|e_y(k,t)\| + c$, where $c > 0$. Evidently, for any fixed time instant t, $\|e_y(k+1,t)\|$ forms a monotonically non-increasing sequence bounded below, that is,

$$\|e_y(k+1,t)\| \geqslant \delta, \tag{24}$$

with $\delta > 0$. Combining it with equation (22), it follows that the MAS-CPS (5) possesses AIC, while the attacker perceives that it does not. Hence, when the AIC is regarded as the secret, the system is opaque. The proof of Theorem 2 is concluded.

6. SIMULATION

This section considers a linear MAS-CPS denoted as

$$A = \begin{bmatrix} -2 & 0.1 \\ 0.08 & -3 \end{bmatrix}, B = \begin{bmatrix} -1 & 0.3 \\ 0 & -0.6 \end{bmatrix}, C = \begin{bmatrix} 0.1 & 0 \\ 0.2 & 0 \end{bmatrix}, D = \begin{bmatrix} 3 & 3 \\ 0 & 2 \end{bmatrix}$$

$$E = \begin{bmatrix} 0.9 & 0.1 \\ 0.5 & 0.75 \end{bmatrix}, F = \begin{bmatrix} -1 & 0.3 \\ 0.5 & -0.6 \end{bmatrix}, G = \begin{bmatrix} 1 & 1 \\ 0.5 & -0.6 \end{bmatrix},$$

in $t \in [0, 20]$, which is composed of one virtual leader and four follower agents to verify the feasibility of the proposed theorems.

The communication topology of the MAS-CPS is illustrated in Fig. 1. According to the considered communication topology, $S = diag\{1, 0, 1, 0\}$. It consists of a virtual leader 0 and four follower agents 1–4, where each edge represents the information exchange between connected agents. The interaction among the agents is further characterized by the following Laplacian matrix

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

The attack signal is defined as $\rho_i(t) = 1_{t \geqslant t_i^a}$, where $1_{t \geqslant t_i^a}$ denotes the indicator function, i.e., $1_{t \geqslant t_i^a} = 1$ for $t \geqslant t_i^a$ and $1_{t \geqslant t_i^a} = 1$ otherwise. $t^a = (8, 12, 10, 15)$, and t_i^a is its i-th element. $\omega_1 = [0.01t; -0.005t], \omega_2 = [-0.08t; -0.07t]$, $\omega_3 = [0.06t^2; -0.04t^2]$ and $\omega_4 = [-0.05 + t; 0.09 + t]$. Let the output of leader agent 0 as $z_d(t) = [0.1t; 0.06t + 1.5]$.

The ILC algorithm is given as

$$\mathcal{U}(k+1,t) = \mathcal{U}(k,t) + \left((\mathcal{L} + S) \otimes \begin{bmatrix} 0.07 & -0.05 \\ 0.03 & 0.07 \end{bmatrix} \right) e_z(k,t);$$

then from the above matrices value, it follows that $\|I - ((\mathcal{L}+S) \otimes D\Gamma)\| \approx 0.94 < 1$, which satisfies condition (14).

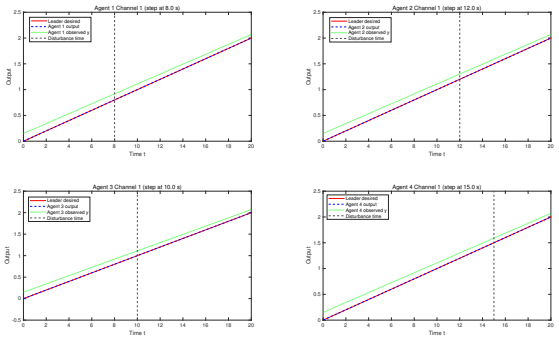


Fig. 2. Output of the leader agent 0, follower agents1–4 and observed by attacker (Channel 1).

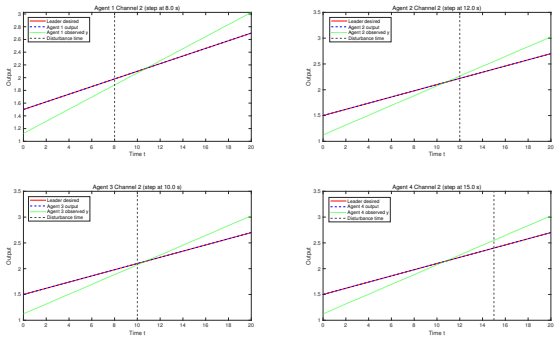


Fig. 3. Output of the leader agent 0, follower agents1–4 and observed by attacker (Channel 2).

After 60 repetitive iterations, the controlled and measured output trajectories of the system are shown in Figs. 2 and 3. Under the P-ILC in (10), all followers can resist the attack signal, indicating AIC. However, the attacker-observed outputs (green curves in Figs. 2–3) fail to track the desired trajectory, implying opacity when AIC is confidential. The outputs converge after 60 iterations, showing stable disturbance rejection.

To illustrate the system's opacity more clearly from the perspective of error analysis, Fig. 4 presents a comparison between the controlled output error and the measured output error trajectories. As shown in Fig. 4, the controlled error e_i^z converges to zero along the iterative axis, while the measurement error e_i^y remains bounded. This implies AIC but leads an external attacker to infer degraded tracking, indicating opacity.

7. CONCLUSION

This paper presented an opacity verification framework for MAS-CPSs under P-ILC. By relating AIC to output errors, system confidentiality and opacity were defined, and sufficient conditions based on the attacker's observation capability were derived. Results show that the proposed scheme achieves accurate tracking while preserving opacity. Future work will consider delays, disturbances, and adaptive learning.

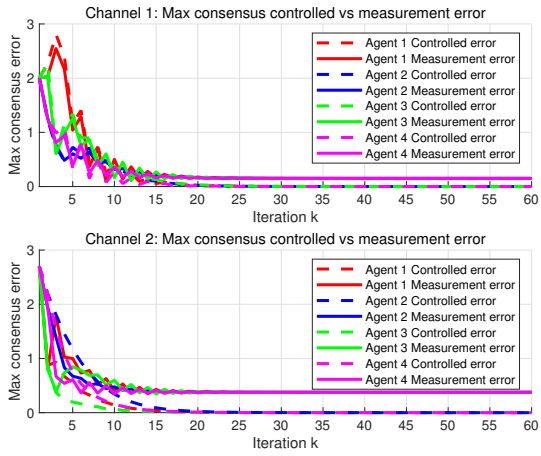


Fig. 4. Comparison between the controlled and the measured output error.

REFERENCES

An, L. and Yang, G.H. (2020). Opacity enforcement for confidential robust control in linear cyber-physical systems. *IEEE Transactions on Automatic Control*, 65(3), 1234–1241.

Arimoto, S., Kawamura, S., and Miyazaki, F. (1984). Bettering operation of robots by learning. *Journal of Robotic Systems*, 1(2), 123–140.

Chen, J., Gauci, M., Li, W., Kolling, A., and Groß, R. (2015). Occlusion-based cooperative transport with a swarm of miniature mobile robots. *IEEE Transactions on Robotics*, 31(2), 307–321.

Chi, R., Hui, Y., Huang, B., and Hou, Z. (2020). Adjacent-agent dynamic linearization-based iterative learning formation control. *IEEE Transactions on Cybernetics*, 50(10), 4358–4369.

Cui, Y., Jenabzadeh, A., Ahmed, Z., Zhang, W., and Huang, T. (2025). Resilient distributed control and target tracking in multiagent systems against composite attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 55(2), 1252–1263.

Dong, Y., Lefebvre, D., and Li, Z. (2025). k-step opacity verification and enforcement of time labeled Petri net systems. *IEEE Transactions on Automatic Control*, 70(9), 5848–5863.

Dong, Y., Li, Z., and Wu, N. (2022). Symbolic verification of current-state opacity of discrete event systems using Petri nets. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(12).

Duan, W., Liu, R., Fanti, M.P., Hadjicostis, C.N., and Li, Z. (2023). Edit mechanism synthesis for opacity enforcement under uncertain observations. *IEEE Control Systems Letters*, 7, 2041–2046.

Habbachi, S., Ben Hafaiedh, I., and Li, Z. (2026). Language-based opacity in modular discrete event systems: Compositional secret-based verification using labeled Petri nets. *Information Sciences*, 724, 122701.

Habbachi, S., Li, Z., Wu, N., and Khalgui, M. (2022). Language-based opacity verification and enforcement in the framework of labeled Petri nets. *Science progress*, 105(1), 368504221075466.

He, S., Dai, S.L., Zhao, Z., and Zou, T. (2022a). Uncertainty and disturbance estimator-based distributed synchronization control for multiple marine surface vehicles with prescribed performance. *Ocean Engineering*, 261, 111867.

He, S., Xu, R., Zhao, Z., and Zou, T. (2022b). Vision-based neural formation tracking control of multiple autonomous vehicles with visibility and performance constraints. *Neurocomputing*, 492, 651–663.

Huang, D., Chen, Y., Meng, D., and Sun, P. (2021). Adaptive iterative learning control for high-speed train: A multi-agent approach. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 51(7), 4067–4077.

Jia, X., Li, H., Chi, X., and Lv, T. (2024). Edge-based dynamic event-triggered leader-following output consensus of uncertain heterogeneous multi-agent systems with multi-channel hybrid cyber-attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 54(9), 5543–5555.

John, V.M. and Katewa, V. (2025). Opacity versus security in linear dynamical systems. *IEEE Transactions on Automatic Control*, 70(1), 323–338.

Li, J., Lefebvre, D., Hadjicostis, C.N., and Li, Z. (2025). Verification of state-based timed opacity for constant-time labeled automata. *IEEE Transactions on Automatic Control*, 70(1), 503–509.

Liu, S., Yin, X., Dimarogonas, D.V., and Zamani, M. (2025). On approximate opacity of stochastic control systems. *IEEE Transactions on Automatic Control*, 70(6), 3846–3861.

Liu, S. and Zamani, M. (2021). Verification of approximate opacity via barrier certificates. *IEEE Control Systems Letters*, 5(4), 1369–1374.

Paoli, A. and Lin, F. (2012). Decentralized opacity of discrete event systems. In *2012 American Control Conference (ACC)*, 6083–6088.

Ramasubramanian, B., Cleaveland, R., and Marcus, S.I. (2020). Notions of centralized and decentralized opacity in linear systems. *IEEE Transactions on Automatic Control*, 65(4), 1442–1455.

Tong, Y., Ma, Z., Li, Z., Seactzu, C., and Giua, A. (2016). Verification of language-based opacity in Petri nets using verifier. In *2016 American Control Conference (ACC)*, 757–763.

Wu, B., Dai, J., and Lin, H. (2018). Synthesis of insertion functions to enforce decentralized and joint opacity properties of discrete-event systems. In *2018 Annual American Control Conference (ACC)*, 3026–3031.

Wu, J., Dai, X., Tian, S., and Huang, Q. (2023). Iterative learning consensus control of nonlinear impulsive distributed parameter multi-agent systems. *European Journal of Control*, 71, 100785.

Yin, X., Zamani, M., and Liu, S. (2021). On approximate opacity of cyber-physical systems. *IEEE Transactions on Automatic Control*, 66(4), 1630–1645.