Secure Control Against Multiplicative and Additive False Data Injection Attacks

Hongming Zhu, Lezhong Xu, Zeyu Bao, Yifan Liu, Liyuan Yin, Weiran Yao, *Member, IEEE*, Chengwei Wu, *Member, IEEE*, and Ligang Wu, *Fellow, IEEE*

***Abstract*—In this article, the secure control problem of the cyber-physical systems (CPS) is investigated when the communication network connecting a controller and an actuator is interfered by malicious adversaries. Both multiplicative and additive false data attacks are considered, and a general attack model is given to describe such attacks. Sufficient conditions are proposed to validate that whether a given controller is capable of maintaining the desired performance of CPS or not under a given attack scenario. Furthermore, conditions are given to design a secure controller for CPS with both multiplicative and additive false data attacks. Eventually, numerical simulation results are given to illustrate the effectiveness of the proposed secure control scheme in this article.**

***Index Terms*—Cyber-physical systems, multiplicative and additive false data injection attack, secure control.**

I. Introduction

NOWADAYS, with the rapid development of communication and computing technology, the influence and economic potential of cyber-physical systems (CPS) in society cannot be underestimated. CPS play a leading role in the future military field and civilian critical infrastructure facilities including power systems, industrial systems, transportation networks, intelligent manufacturing, multi-agent system and other fields [1], [2], [3], [4], [5], [6]. However, as mentioned in [7], the open network layer interconnected with the physical layer in CPS is vulnerable to attacks. For instance, in 2019, a cyberattack on Venezuela's Guri hydropower plant disrupted power supplies and caused massive traffic congestion [8]. Similarly, in 2020, the MailTo ransomware attacked Australian shipping and logistics company Topline Group for three months, forcing it to provide many customer services offline [9]. These incidents demonstrate that cyber attacks, such as denial-of-service attacks [10], false data injection (FDI) attacks [11], and replay attacks [12], pose serious potential security risks to systems. Therefore, it is extraordinarily important to ensure the security of CPS in the control system.

As subtle attacks, FDI attacks are designed elaborately to bypass attack detection schemes without triggering an alarm, allowing attackers to take over the physical system or deteriorate its performance. Researchers have made considerable progress in solving the security problems of CPS under FDI attacks, as evidenced by the literature [13], [14], [15], [16], [17]. However, most existing results rely on the assumption that only additive FDI attacks occur in the sensor-controller or controller-actuator communication network. Multiplicative FDI attacks are more effective since such attacks can change the eigenvalue of the closed-loop system. To fully analyze the negative effects of FDI attacks, a general actuator FDI attack model including both multiplicative and additive attacks is considered, and the security analysis and secure control problems are investigated for CPS under such an attack model in this article.

A. Related Literature Review

Attackers have the ability to arbitrarily access transmitted data and modify it in accordance with the malicious adversary's objective, which poses a significant threat to the normal operation of the system. Through the research of malicious attacks, it is necessary to systematically study the various forms of attacks so as to design new defense mechanisms. As an important form of attack, report and research on FDI attacks are increasing day by day. By way of example, as mentioned in [18], many FDI attack intrusion monitoring systems were rule-based, and there were still some limitations in detecting new attack intrusions. New defense mechanisms required to be designed by learning the malicious attacks. The patterns of FDI attacks were analyzed in [19], [20], [21]. These studies adopted different methods to conceal FDI attacks, including designing the demanded imperfect attack sequence, analyzing the potential attack mechanism for the distributed control system, as well as coding the output signal of the sensor. Thus, these methods were used to destroy a part of the communication link and decrease the performance of the estimator. [22] improved the previous

Manuscript received 20 April 2023; revised 13 June 2023; accepted 3 July 2023. Date of publication 10 July 2023; date of current version 25 July 2023. This work was supported in part by the National Science Foundation of China under Grants 62203136, 62033005, 62022030, 62106062, and 62173107, and in part by the the Key R&D Program of Heilongjiang Province under Grant 2022ZX01A18. *(Corresponding author: Chengwei Wu.)*

Hongming Zhu, Yifan Liu, Liyuan Yin, Weiran Yao, Chengwei Wu, and Ligang Wu are with the Department of Control Science and Engineering, Harbin Institute of Technology, Harbin 150001, China (e-mail: 22b904052@stu.hit.edu.cn; soadisse@163.com; liyuanyin@hit.edu.cn; yaoweiran@hit.edu.cn; chengweiwu@hit.edu.cn; ligangwu@hit.edu.cn).

Lezhong Xu is with the College of Mechanical and Electrical Engineering, Northeast Forestry University, Harbin 150040, China (e-mail: xyzdblydx1017@163.com).

Zeyu Bao is with the China Academy of Space Technology, Beijing 100081, China (e-mail: baozy_2012@163.com).

Digital Object Identifier 10.1109/TICPS.2023.3293789

FDI attack mechanism and method so that the attacker could greatly influence the state estimation even under the premise of using a security state estimator.

Furthermore, various techniques have been proposed to address FDI attacks, including sliding mode control [23], robust control [24], adaptive control [25], [26], optimal control [17], fuzzy control [27], [28], and observers including full-order observer, reduced-order observer, unknown input observer, robust observer, [6], [29], [30], etc. For example, based on quadratic performance index, Ding et al. [31] addressed the secure control problem of stochastic nonlinear systems with FDI attack. The authors of [32] investigated sliding mode control problems for a class of random system under both denial-of-service and FDI attacks. Liu et al. [33] applied extended Kalman filtering to a stochastic nonlinear system and employed optimal control to combat FDI attacks. Wu et al. [17] the secure control problem for CPS under actuator FDI attacks, providing a zero-sum game based optimal schemes. Considering CPS with multiple inputs and multiple outputs in the measurement channel, a model-free adaptive control scheme was proposed to mitigate FDI attack in [34]. However, only additive FDI attacks were considered in aforementioned results. To address multiplicative attacks in combination with additive attacks, Chen et al. [35] designed a generalized measurement model containing multiplicative and additive FDI attacks and a new nonlinear Kalman filter to deal with the state estimation problem when both multiplicative and additive FDI attacks occur. A Bayesian approximate filtering algorithm was proposed to enhance the system's robustness under cyber attacks in [36]. Nonetheless, there are few literature on the secure control of CPS with FDI attacks including both multiplicative and additive attacks, which motivates the present article.

B. Contributions of This article

This article investigates the secure control problem of CPS when the communication network connecting the controller and the actuator is interfered by both multiplicative and additive FDI attacks. A generalized attack model including multiplicative and additive attacks is given to describe such FDI attacks. Sufficient conditions are proposed to guarantee that the CPS under both multiplicative and additive FDI attacks are stochastically asymptotic stable, based on which a theorem is given to design a secure control scheme. The main contributions of this article can be summarized as follows.

1) This article presents a generalized FDI attack model including both multiplicative and additive attacks. In contrast to existing results, see for example [17], [29], [33], which only considered additive attacks. The generalized FDI attack model can describe various FDI attack scenarios involving additive, multiplicative, or both types of FDI attacks.
2) Sufficient conditions are proposed to analyze the performance of CPS in the presence of actuator multiplicative and additive FDI attacks. A secure control scheme, which is capable of dealing with both types of FDI attacks, is proposed in this article.

The remainder of this article is organized as follows. Section II provides a preliminary description of the generalized FDI attack model and formulate the problem to be addressed. Section III presents the stability analysis of the system and the design idea of the control gain. The simulation results acquired based on the proposed method are provided in Section IV, and Section V concludes this article.

Notation: The notations used throughout the article are defined as follows. $\mathbb{R}^n$ denotes the n dimensional Euclidean space. The superscript T denotes the matrix transpose, for instance, matrix A^T is matrix A transpose. $\mathbb{E}\{x\}$ means the expectation of the stochastic variable x. $\|x\| = \sqrt{x^T x}$ denotes 2-norm of the vector. $\langle , \rangle$ is the inner product in $\mathbb{R}^n$, i.e., $\langle x, y\rangle = x^T y$. Moreover, The asterisk $*$ is used for the blocks induced by symmetry. I denotes an appropriate dimension identity matrix.

II. Preliminaries and Problem Formulation

Consider a discrete-time system governed by the following model:

$$x_{k+1} = Ax_k + B\bar{u}_k, \tag{1}$$

where $x_k \in \mathbb{R}^n$ is the state vector, $\bar{u}_k \in \mathbb{R}^m$ is an input vector of m-dimension at discrete time k under FDI attacks, and $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times m}$ are constant matrices of appropriate dimensions.

In this model, it is assumed that attackers use FDI attacks that may be dependent or independent of the true data. The following two models of FDI attacks are established for false data, namely multiplicative attack and additive attack, as described in [33], [36]. Therefore,the input vector $\bar{u}_k$ in (1) can be expressed in the following two forms

$$\bar{u}_k = Mu_k, \tag{2}$$

$$\bar{u}_k = u_k + \Gamma f(D_L x_k), \tag{3}$$

where $u_k \in \mathbb{R}^m$ is the attack-free control input, $M \in \mathbb{R}^{m\times m}$ is the multiplicative attack matrix, Γ is a diagonal matrix with appropriate dimensions, and its diagonal elements are either 0 or 1. $D_L \in \mathbb{R}^{m\times n}$ is a known constant matrix. The vector function $f(D_L x_k) : \mathbb{R}^m \to \mathbb{R}^m$ satisfies the following one-sided Lipschitz non-linearity and quadratic inner-boundary definitions:

Definition 1: [37] The nonlinear function $f(D_L x_k)$ verifies the one-sided Lipschitz condition if there exists $\xi \in \mathbb{R}, \forall x_1, x_2 \in R^n$ such that

$$\langle f(D_L x_1) - f(D_L x_2), D_L(x_1 - x_2)\rangle \leq \xi \|D_L(x_1 - x_2)\|^2. \tag{4}$$

Definition 2: [38] The nonlinear function $f(D_L x_k)$ verifies the quadratic inner-boundary condition if there exists $\psi, \gamma \in \mathbb{R}, \forall x_1, x_2 \in R^n$ such that

$$(f(D_L x_1) - f(D_L x_2))^T (f(D_L x_1) - f(D_L x_2)) \leq \psi \|D_L(x_1 - x_2)\|^2$$

$$+\gamma\left\langle D_L(x_1-x_2), f(D_Lx_1)-f(D_Lx_2)\right\rangle. \tag{5}$$

Note that $f(D_Lx_k)$ represents the nonlinear additive attack of the system. The constants ξ, ψ and γ in (1) and (2) are one-sided Lipschitz constants, which means they can be positive, negative or even zero, unlike the well-known Lipschitz constants [38]. As shown in [37] and [38], the well-known Lipschitz constant is generally much larger than that of one-sided Lipschitz.

The case where attackers can inject incorrect addition or multiplication attack is considered. Therefore, $\bar{u}_k$ is redefined as a generalized attack model that can handle both additive and multiplicative FDI attacks, as described in [35],

$$\bar{u}_k = \alpha_k M u_k + (1-\alpha_k)(u_k + \Gamma f(D_Lx_k)), \tag{6}$$

where α_k is a Bernoulli random variable, which satisfies

$$\begin{aligned}
\mathbb{E}[\alpha_k] &= \mathbb{E}[(\alpha_k)^i] = \mathbb{E}[\bar{\alpha}_k + \widetilde{\alpha}_k] = \mathbb{E}[\bar{\alpha}_k] + \mathbb{E}[\widetilde{\alpha}_k]\\
&= \mathbb{E}[\bar{\alpha}_k] = P(\alpha_k = 1) * 1 = p_m,\\
\mathbb{E}[1-\alpha_k] &= \mathbb{E}[(1-\alpha_k)^i] = \mathbb{E}[1-\bar{\alpha}_k]\\
&= P(\alpha_k = 0) * 1 = 1 - p_m,\\
\mathbb{E}[\widetilde{\alpha}_k] &= E[\alpha_k - p_m] = P(\alpha_k = 0) * 0 = 0,\\
\mathbb{E}[\widetilde{\alpha}_k^2] &= \mathbb{E}[(\alpha_k - p_m)^2]\\
&= \mathbb{E}[(\alpha_k)^2] - \mathbb{E}[\alpha_k]^2 = p_m(1-p_m),
\end{aligned} \tag{7}$$

where $\mathbb{E}[\cdot]$ represents the expectation, $i \geq 2$ is constant as well as $\bar{\alpha}_k$ and $\widetilde{\alpha}_k$ represent the Bernoulii random variable at $a_k = 1$ and $a_k = 0$, respectively.

Remark 1: When $\alpha_k = 1$, it indicates the occurrence of multiplicative false data, causing $\bar{u}_k$ to change as described in (2). Likewise, $\bar{u}_k$ turns to (3) when $\alpha_k = 0$, indicating the occurrence of additive false data, which follows the properties shown in (7) with $P(\alpha_k = 1) = p_m$. A special case occurs when M is the identity matrix and $\alpha_k = 1$, meaning that $\bar{u}_k = u_k$ and there is no attack. Therefore, this generalized attack model can deal with multiplicative, additive, or both types of attacks, and no attacks occurring simultaneously.

Substituting (6) into the system (1) yields

$$x_{k+1} = Ax_k + B[\alpha_k M u_k + (1-\alpha_k)(u_k + \Gamma f(D_Lx_k))]. \tag{8}$$

In this article, assuming that all states are measurable. Thus, the following state-feedback controller is designed

$$u_k = -Kx_k, \tag{9}$$

where $K \in \mathbb{R}^{m\times n}$ is the controller gain.

Then, combined (8) with (9), the system (1) can be modeled as

$$\begin{aligned}
x_{k+1} = {} & [A - (1-\alpha_k)BK - \alpha_k BMK]x_k\\
& + (1-\alpha_k)B\Gamma f(D_Lx_k).
\end{aligned} \tag{10}$$

Substituting $\alpha_k = \bar{\alpha}_k + \widetilde{\alpha}_k$ into above equation, it results in the final form of the attacks

$$x_{k+1} = Tx_k + Uf(D_Lx_k), \tag{11}$$

where $T = A - (1-\bar{\alpha}_k)BK + \widetilde{\alpha}_k BK - \bar{\alpha}_k BMK - \widetilde{\alpha}_k BMK$ and $U = (1-\bar{\alpha}_k)B\Gamma - \widetilde{\alpha}_k B\Gamma$.

The aim of the present study is to explore the stability of system (1) by calculating the Lyapunov function on the premise of constructing the generalized FDI attack model (11), and solving for the appropriate control gain K under the condition of multiplicative and additive attacks occurrence probabilities, in order to achieve secure control.

Remark 2: The matrix M, acting as a multiplicative attack matrix, carries out the amplitude of the original input data u_k. Additionally, M requires to satisfy the condition that the eigenvalues of $A - BMK$ are outside the unit circle under multiplicative attacks, causing the system to be unstable and achieving the purpose of FDI attacks [39]. Since the system is unstable with only multiplicative attacks,the generalized attack model proposed in this article cannot address the situation of solely multiplicative attacks (i.e., when $p_m = 1$), but it can explore the scenario of only additive attacks (i.e., when $p_m = 0$). Besides, the study of only multiplicative attacks will be conducted in future research. For example, the multiplicative and additive attacks are analyzed with different attack probabilities or the individual multiplicative attacks are estimated with an appropriate observer. In addition, the role of Γ in (3) can be regarded as an attack control matrix used to determine which input signals in the original input data u_k are attacked by the nonlinear additive attack function $f(D_Lx_k)$.

Remark 3: In practice situations, attackers may intend to destabilize the stability of the system or manipulate the plant to achieve their desired outcomes by injecting false data. In this article, the attack model considered is when injecting multiplicative and additive attacks at each discrete time step k to manipulate the original data, leading to a reduction or destruction of system performance. However, a significant amount of energy is consumed by an arbitrarily unbounded attacks which are rare in real attack cases [40]. Besides, large amplitude attacks might be detected easily by some detectors such as χ^2 failure detectors. On the contrary, to achieve more effective attacks, attackers are generally more inclined to send bounded false data to cover up their attack behavior. Although the energy consumption and detection of attacks are important considerations in practical scenarios, this article primarily focuses on the effectiveness of the newly constructed attack model in solving for the control gain K. Future studies may consider more realistic attack models, such as those discussed in [41], where the number of sensors that can be attacked limited, and energy expenditure is taken into account.

III. Main Results

In this section, the stability of system (11) under multiplicative and additive actuator FDI attacks is analyzed, and sufficient conditions are proposed to guarantee that the asymptotical stability of (11) can be preserved. Following such conditions, a theorem is given to design a secure controller to mitigate FDI attacks.

Before presenting the main results, the following lemma is given.

Lemma 1: [42] If $\eta_1(z) = z^T R_1 z \geq 0$ is regular, the following two conditions are equivalent:

1) $\eta_0(z) = z^T R_0 z > 0, \forall z \neq 0$ such that $\eta_1(z) \geq 0$.
2) there exists $\phi \geq 0$ such that $R_0 - \phi R_1 > 0$.

A. Stability Analysis Under Hybrid Attacks

The following theorem is presented to show the stability condition.

Theorem 1: Assuming that $f(D_L x_k)$ satisfies Definitions–1–2, and with the given constants $\phi_i > 0 (i = 1, 2)$ and (7), if there exists a control gain $K \in \mathbb{R}^{m \times n}$ and a positive definite matrix $P \in \mathbb{R}^{n \times n}$ such that

$$\bar{A}^T \bar{P} \bar{A} + \Delta < 0, \tag{12}$$

where $\bar{P} = diag(P, P)$ and

$$\bar{A} = \begin{bmatrix} \bar{A}_{11} & \bar{A}_{12} \\ \bar{A}_{21} & 0 \end{bmatrix}, \Delta = \begin{bmatrix} -P + \Delta_{11} & \Delta_{12} \\ * & \Delta_{22} \end{bmatrix},$$

$$\begin{aligned} \bar{A}_{11} &= \sqrt{1 - p_m}(A - BK),\ \bar{A}_{12} = \sqrt{1 - p_m} B\Gamma, \\ \bar{A}_{21} &= \sqrt{p_m}(A - BMK), \\ \Delta_{11} &= \phi_1 \xi D_L^T D_L + \phi_2 \psi D_L^T D_L, \\ \Delta_{12} &= -\frac{1}{2}\phi_1 D_L^T + \frac{1}{2}\phi_2 \gamma D_L^T,\ \Delta_{22} = -\phi_2 I, \end{aligned}$$

then the system (8) is stochastically asymptotic stable.

Proof: Consider the following Lyapunov function

$$V_k = x_k^T P x_k. \tag{13}$$

To prove the following inequality,

$$\Delta_k = V_{k+1} - V_k = x_{k+1}^T P x_{k+1} - x_k^T P x_k < 0, \tag{14}$$

firstly, substitute (11) into V_{k+1}

$$\begin{aligned} V_{k+1} &= x_{k+1}^T P x_{k+1} \\ &= (Tx_k + Uf(D_L x_k))^T P (Tx_k + Uf(D_L x_k)) \\ &= x_k^T T^T P T x_k + f^T(D_L x_k) U^T P U f(D_L x_k) \\ &\quad + x_k^T T^T P U f(D_L x_k) + f^T(D_L x_k) U^T P T x_k. \end{aligned} \tag{15}$$

Denoting that $\varsigma_k = [x_k^T \quad f^T(D_L x_k)]^T$, (15) becomes

$$V_{k+1} = {\varsigma_k}^T \widehat{P} \varsigma_k, \tag{16}$$

where

$$\widehat{P} = \begin{bmatrix} P_{xx} & P_{xf} \\ * & P_{ff} \end{bmatrix}, \tag{17}$$

$$\begin{aligned} P_{xx} &= T^T P T \\ &= A^T P A - (1 - \bar{\alpha}_k) A^T P B K + \tilde{\alpha}_k A^T P B K \\ &\quad - \bar{\alpha}_k A^T P B M K - \tilde{\alpha}_k A^T P B M K \\ &\quad - (1 - \bar{\alpha}_k) K^T B^T P A + (1 - \bar{\alpha}_k)^2 K^T B^T P B K \\ &\quad - (1 - \bar{\alpha}_k) \tilde{\alpha}_k K^T B^T P B K \\ &\quad + (1 - \bar{\alpha}_k) \bar{\alpha}_k K^T B^T P B M K \\ &\quad + (1 - \bar{\alpha}_k) \tilde{\alpha}_k K^T B^T P B M K \\ &\quad + \tilde{\alpha}_k K^T B^T P A - \tilde{\alpha}_k (1 - \bar{\alpha}_k) K^T B^T P B K \\ &\quad + \tilde{\alpha}_k^2 K^T B^T P B K - \tilde{\alpha}_k \bar{\alpha}_k K^T B^T P B M K \\ &\quad - \tilde{\alpha}_k^2 K^T B^T P B M K - \bar{\alpha}_k K^T M^T B^T P A \\ &\quad + \bar{\alpha}_k (1 - \bar{\alpha}_k) K^T M^T B^T P B K \\ &\quad - \bar{\alpha}_k \tilde{\alpha}_k K^T M^T B^T P B K \\ &\quad + \bar{\alpha}_k^2 K^T M^T B^T P B M K \\ &\quad + \bar{\alpha}_k \tilde{\alpha}_k K^T M^T B^T P B M K - \tilde{\alpha}_k K^T M^T B^T P A \\ &\quad + \tilde{\alpha}_k (1 - \bar{\alpha}_k) K^T M^T B^T P B K \\ &\quad - \tilde{\alpha}_k^2 K^T M^T B^T P B K \\ &\quad + \tilde{\alpha}_k \bar{\alpha}_k K^T M^T B^T P B M K \\ &\quad + \tilde{\alpha}_k^2 K^T M^T B^T P B M K, \\ P_{xf} &= T^T P U \\ &= (1 - \bar{\alpha}_k) A^T P B \Gamma - \tilde{\alpha}_k A^T P B \Gamma \\ &\quad - (1 - \bar{\alpha}_k)^2 K^T B^T P B \Gamma \\ &\quad + \tilde{\alpha}_k (1 - \bar{\alpha}_k) K^T B^T P B \Gamma \\ &\quad + \tilde{\alpha}_k (1 - \bar{\alpha}_k) K^T B^T P B \Gamma \\ &\quad - \tilde{\alpha}_k^2 K^T B^T P B \Gamma - \bar{\alpha}_k (1 - \bar{\alpha}_k) K^T M^T B^T P B \Gamma \\ &\quad + \bar{\alpha}_k \tilde{\alpha}_k K^T M^T B^T P B \Gamma \\ &\quad - \tilde{\alpha}_k (1 - \bar{\alpha}_k) K^T M^T B^T P B \Gamma \\ &\quad + \tilde{\alpha}_k^2 K^T M^T B^T P B \Gamma, \\ P_{ff} &= U^T P U \\ &= (1 - \bar{\alpha}_k)^2 \Gamma B^T P B \Gamma - \tilde{\alpha}_k (1 - \bar{\alpha}_k) \Gamma B^T P B \Gamma \\ &\quad - \tilde{\alpha}_k (1 - \bar{\alpha}_k) \Gamma B^T P B \Gamma + \tilde{\alpha}_k^2 \Gamma B^T P B \Gamma. \end{aligned} \tag{18}$$

If the system is stable, condition (14) is satisfied, then (7) and (16) are introduced to obtain the expectation of condition (14), then this condition becomes

$$\mathbb{E}[V_{k+1}] - V_k = \mathbb{E}[{\varsigma_k}^T \widehat{P} \varsigma_k] - {x_k}^T P x_k < 0. \tag{19}$$

For $\widehat{P}$ in (19), the expected values of its internal counterpart are as follows:

$$\begin{aligned} \mathbb{E}[P_{xx}] &= A^T P A - (1 - p_m) A^T P B K \\ &\quad - (1 - p_m) K^T B^T P A + (1 - p_m) K^T B^T P B K \\ &\quad - p_m A^T P B M K - p_m K^T M^T B^T P A \\ &\quad + p_m K^T M^T B^T P B M K \end{aligned}$$

$$
\begin{aligned}
&= (1-p_m)(A^T - K^T B^T)P(A-BK)\\
&\quad + p_m(A^T - K^T M^T B^T)P(A-BMK),\\
\mathbb{E}[P_{xf}] &= (1-p_m)A^T PB\Gamma - (1-p_m)K^T B^T PB\Gamma\\
&= (1-p_m)(A^T - K^T B^T)PB\Gamma,\\
\mathbb{E}[P_{ff}] &= (1-p_m)\Gamma B^T PB\Gamma. \qquad (20)
\end{aligned}
$$

In this case, $\mathbb{E}[\widehat{P}]$ can be decomposed into the following two parts

$$
\mathbb{E}[\widehat{P}] = \mathbb{E}[\widehat{P}_1] + \mathbb{E}[\widehat{P}_2], \qquad (21)
$$

where

$$
\begin{aligned}
\mathbb{E}[\widehat{P}_1] &= (1-p_m)\\
&\begin{bmatrix} (A-BK)^T P(A-BK) & (A-BK)^T PB\Gamma \\ * & \Gamma B^T PB\Gamma \end{bmatrix},\\
\mathbb{E}[\widehat{P}_2] &= p_m \begin{bmatrix} (A-BMK)^T P(A-BMK) & 0 \\ * & 0 \end{bmatrix}.
\end{aligned}
$$

Then, (21) can be rewritten as the following form

$$
\mathbb{E}[\widehat{P}] = A_1^T PA_1 + A_2^T PA_2, \qquad (22)
$$

where $A_1 = [\bar{A}_{11} \quad \bar{A}_{12}]$ and $A_2 = [\bar{A}_{21} \quad 0]$. Therefore, $\bar{A}^T \bar{P} \bar{A}$ in (12) can be obtained by augmenting the matrices in (22).

Additionally, by introducing the condition (4) in Definition 1, one can obtain for any constant $\phi_1 > 0$ [37]

$$
{\varsigma_k}^T \begin{bmatrix} \phi_1 \xi D_L^T D_L & -\frac{1}{2}\phi_1 D_L^T \\ * & 0 \end{bmatrix} \varsigma_k \geq 0. \qquad (23)
$$

Similarly, any constant $\phi_2 > 0$ is available to be obtained by considering the quadratic inner-boundary condition (5) in Definition 2 [38]

$$
{\varsigma_k}^T \begin{bmatrix} \phi_2 \psi D_L^T D_L & \frac{1}{2}\phi_2 \gamma D_L^T \\ * & -\phi_2 I \end{bmatrix} \varsigma_k \geq 0. \qquad (24)
$$

In view of Lemma 1, (22), (23) and (24), then (14) becomes

$$
\mathbb{E}[V_{k+1}] - V_k \leq {\varsigma_k}^T (\bar{A}^T \bar{P} \bar{A} + \Delta)\varsigma_k < 0. \qquad (25)
$$

Thus, it can be seen that if the condition of (25) is satisfied, then the inequality (14) stands, and the system is asymptotically stable. The proof is complete. □

In fact, due to the coupling terms, the control gain K cannot be directly solved with the sufficient condition (12). In the next subsection, linear matrix inequities will be utilized to obtain an equivalent form and solve for K.

B. Secure Control Strategy

The following theorem is presented to show the strategy of designing a secure controller.

Theorem 2: Assuming that $f(D_L x_k)$ satisfies Definitions 1–2, and with the given constants $\phi_i > 0 (i = 1, 2)$ and (7), if there exist a positive definite matrix $Q \in \mathbb{R}^{n \times n}$ and a matrix $Y \in \mathbb{R}^{m \times n}$ such that

$$
\begin{bmatrix}
-I & 0 & 0 & \vartheta Q & 0 \\
* & -Q & 0 & \bar{A}_{11}Q & \bar{A}_{12} \\
* & * & -Q & \bar{A}_{21}Q & 0 \\
* & * & * & -Q & Q\Delta_{12} \\
* & * & * & * & \Delta_{22}
\end{bmatrix} < 0, \qquad (26)
$$

where $\vartheta = \sqrt{\phi_1 \xi + \phi_2 \psi} D_L$. $\bar{A}_{11}$, $\bar{A}_{12}$, $\bar{A}_{21}$, Δ_{12} and Δ_{22} are already given in (12). Then, the system (8) is stochastically asymptotic stable. The control gain K and the positive definite matrix P can be obtained by calculating $K = YQ^{-1}$ and $P = Q^{-1}$, respectively.

Proof: According to the Schur Complement Lemma [43], the inequality (12) can be equivalent to the following form

$$
\begin{bmatrix}
-P^{-1} & 0 & \bar{A}_{11} & \bar{A}_{12} \\
* & -P^{-1} & \bar{A}_{21} & 0 \\
* & * & -P + \Delta_{11} & \Delta_{12} \\
* & * & * & \Delta_{22}
\end{bmatrix} < 0. \qquad (27)
$$

Splitting Δ_{11} into the matrix product form, (27) can be transformed into

$$
\begin{bmatrix}
-P^{-1} & 0 & \bar{A}_{11} & \bar{A}_{12} \\
* & -P^{-1} & \bar{A}_{21} & 0 \\
* & * & -P & \Delta_{12} \\
* & * & * & \Delta_{22}
\end{bmatrix} + \bar{\vartheta}^T \bar{\vartheta} < 0, \qquad (28)
$$

where $\bar{\vartheta} = [0 \quad 0 \quad \vartheta \quad 0]$.

Applying the Schur Complement Lemma again and involving $Q = P^{-1}$, (28) becomes

$$
\begin{bmatrix}
-I & 0 & 0 & \vartheta & 0 \\
* & -Q & 0 & \bar{A}_{11} & \bar{A}_{12} \\
* & * & -Q & \bar{A}_{21} & 0 \\
* & * & * & -Q^{-1} & \Delta_{12} \\
* & * & * & * & \Delta_{22}
\end{bmatrix} < 0. \qquad (29)
$$

Pre- and post-multiplying $diag(I, I, I, Q, I)$ in accordance with the congruent transformation results in transforming the constraint (29) into (26). In this case, as the solutions of (26), Q and Y can be calculated. Setting $K = YQ^{-1}$ and $P = Q^{-1}$, the secure control strategy scheme is feasible. This completes the proof of Theorem 2. □

IV. Simulation Results

In this section, a two-wheeled mobile robot is adopted to validate the proposed control scheme. The control objective is to drive such a robot to track a predefined trajectory. Two attack scenarios are considered, that is, the control signal is interfered by only additive FDI attacks and both multiplicative and additive FDI attacks are executed to modify control signals. Considering that the linear quadratic regulator (LQR) is often applied to automatic driving, comparisons of the proposed controller and LQR are conducted.

Both the kinematic model and the tracking error model of the mobile robot are presented in [44], [45], based on which the matrices of the linear discrete-time tracking error model of the mobile robot are given as

$$A = \begin{bmatrix} 1 & wT_s & 0 \\ -wT_s & 1 & vT_s \\ 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} T_s & 0 \\ 0 & 0 \\ 0 & T_s \end{bmatrix},$$

where v, w and T_s represents the linear velocity, angular velocity and sampling time of the mobile robot, respectively. The specific values for these parameters are $v = 1.0$ m/s, $w = 0.1$ rad/s, $T_s = 0.1$ s. According to system (1), the state $x_k = [x_e(k) \quad y_e(k) \quad \theta_e(k)]^T$, and the input of the system is $u_k = [v_e(k) \quad \omega_e(k)]^T$, where $x_e(k)$, $y_e(k)$, $\theta_e(k)$, $v_e(k)$ and $\omega_e(k)$ represent respectively the errors between the system position (x, y), the heading angle, linear velocity and angular velocity and the corresponding values of the reference model.

For the matrices involved in the FDI attack model, they are given as below

$$M = \text{diag}(0.2, -0.3),\ \Gamma = \text{diag}(1, 1),\ D_L = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix},$$

where $\Gamma = \text{diag}(1, 1)$ means that both the linear velocity and angular velocity are interfered by additive FDI attacks.

For the additive FDI attack, it is given as

$$f(D_L x_k) = \begin{bmatrix} sin^2(x_e(k)) + 3x_e(k) \\ sin^2(y_e(k)) + 3y_e(k) \end{bmatrix}.$$

By defining the constants $\xi = -0.1$, $\psi = 0.3$, $\gamma = 0.1$, $\phi_1 = 0.1$, and $\phi_2 = 0.1$, it can be verified that $f(D_L x_k)$ satisfies the conditions (23) and (24). In the simulation, the control objective is to drive the mobile to track a predefined circle trajectory. The initial state of the robot is set as $x_0 = [-5.0 \quad 0.2 \quad -0.1]^T$. The comparisons between the LQR method and the proposed method are presented in the following two cases, where only additive FDI attacks and multiplicative additive mixed FDI attacks are considered.

Case 1 : Only additive FDI attacks

In this subsection, the parameter $p_m = 0.3$ is chosen to calculate K. Solving (26) yields

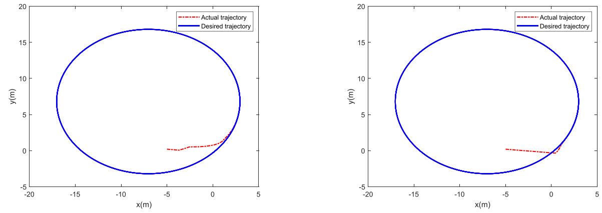
$$K = \begin{bmatrix} 10.8611 & 4.1573 & -0.1180 \\ -0.2462 & 5.6014 & 9.0638 \end{bmatrix}.$$

When there is only an additive attack, i.e., $P(\alpha_k = 1) = 0$ and $P(\alpha_k = 0) = 1$, Fig. 1(a) and (b) present the actual trajectories under the case of using the LQR method and the proposed controller, respectively. To clearly demonstrate the negative effect of additive FDI attacks and the effectiveness of the proposed control scheme, the tracking errors under these two control methods in this case are depicted in Fig. 2. As seen from these simulations, although additive FDI attacks bring some negative effects on the tracking performance, the proposed control scheme can outperform the LQR control, which illustrate the effectiveness of the proposed control scheme.

Case 2 : Multiplicative additive mixed FDI attacks

Considering $p_m = 0.5$, which means that multiplicative attacks and additive attacks occur with the same probability, and the control gain K is calculated as

$$K = \begin{bmatrix} 11.5331 & 2.9630 & 0.0745 \\ -0.4644 & 3.0257 & 6.6358 \end{bmatrix}.$$



(a) The tracking performance under only additive attack by using LQR method.

(b) The tracking performance under only additive attack by using the method of this article

Fig. 1. The tracking performance under only additive attack by using both methods.

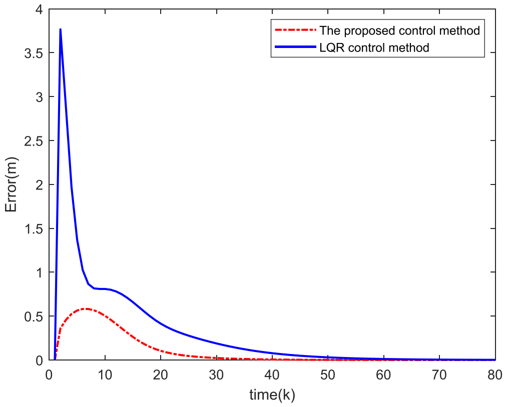
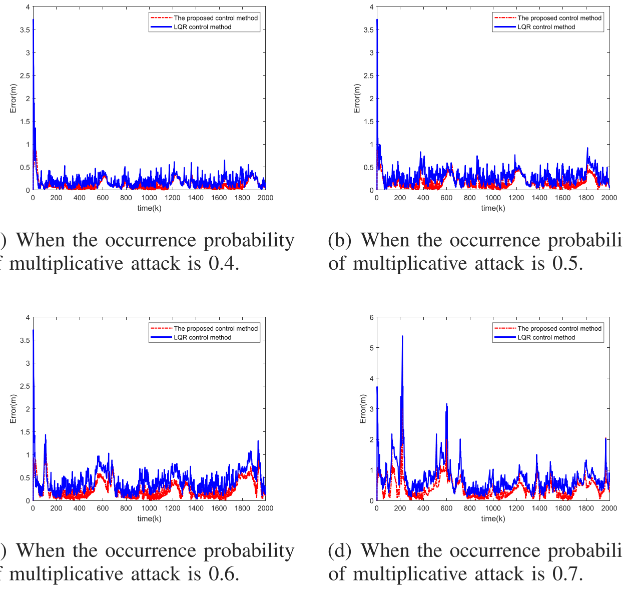


Fig. 2. The tracking errors under only additive attack by using the proposed method and the LQR method.

The eigenvalues of the closed-loop system without multiplicative attacks, that is, the matrix M is an identity matrix, are calculated as -0.1572, 0.3889, and 0.9514, which indicates the stability of the closed-loop system. When multiplicative attacks occur, the eigenvalues of the closed-loop system are 0.7677, 1.238, and 0.9626. It is obvious that the stability of the closed-loop system is no more preserved. For the closed-loop system with LQR, the eigenvalues of the closed-loop system without multiplicative attacks are calculated as 0.8986, 0.7297, and 0.7438. The eigenvalues of the closed-loop system are $0.9484 + 0.0087i$, $0.9484 - 0.0087i$, and 1.1562 under multiplicative attacks occur. Similarly, multiplicative attacks can deteriorate the stability.

In the simulation, different attack probabilities are considered, that is, $p_m = 0.4, 0.5, 0.6, 0.7$. Fig. 3 depicts the norm responses of tracking errors under these different attack probabilities. As seen from these simulation results, the tracking performance is inversely proportion to the multiplicative FDI attack probability, while the proposed control scheme can outperform LQR. Also, when the multiplicative FDI attack probability is 0.7, the tracking error under LQR is almost deteriorated. To further show the effectiveness and advantages of the proposed control scheme, the



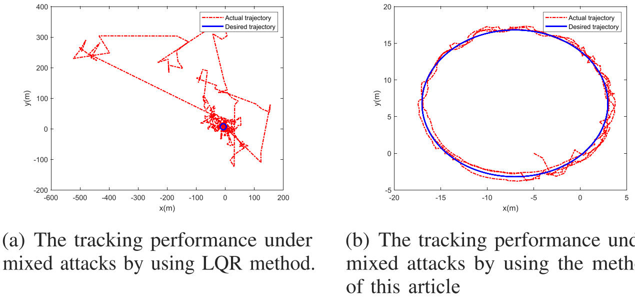
(a) When the occurrence probability of multiplicative attack is 0.4.

(b) When the occurrence probability of multiplicative attack is 0.5.

(c) When the occurrence probability of multiplicative attack is 0.6.

(d) When the occurrence probability of multiplicative attack is 0.7.

Fig. 3. The tracking errors under mixed attacks by using the proposed method and the LQR method.



(a) The tracking performance under mixed attacks by using LQR method.

(b) The tracking performance under mixed attacks by using the method of this article

Fig. 4. The tracking performance under mixed attacks by using both methods.

multiplicative FDI attack probability is set as 0.78. Fig. 4(a) and (b) respectively give the actual trajectories of the mobile robot under LQR and the proposed controller. It is obvious that LQR cannot maintain the tracking performance, but the proposed controller still drive the robot to track the desired trajectory with an allowed tracking error.

V. Conclusion

This article addressed the issue of secure control for CPS subject to actuator false attacks. A generalized attack model was given to describe multiplicative and additive false attacks. Sufficient conditions were proposed to analyze the performance of CPS with a given controller when attacks were described by the design attack model. By using some mathematical operations, conditions were presented to design a secure control scheme, maintaining the desired performance of CPS under both multiplicative and additive false attacks. Finally, simulation results were given to demonstrate the effectiveness of the proposed control scheme.

In the future, a more generalized attack model will be proposed to describe false attacks in accordance with the characteristics of malicious adversaries, and the proactive defense based secure control problem will be investigated to improve the security of CPS under false attacks.

References

[1] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[2] C. Wu, W. Yao, W. Pan, G. Sun, J. Liu, and L. Wu, "Secure control for cyber-physical systems under malicious attacks," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 2, pp. 775–788, Jun. 2022.

[3] W. Qi, Y. Hou, G. Zong, and C. K. Ahn, "Finite-time event-triggered control for semi-Markovian switching cyber-physical systems with FDI attacks and applications," *IEEE Trans. Circuits Syst. I: Regular Papers*, vol. 68, no. 6, pp. 2665–2674, Jun. 2021.

[4] D. Liu and D. Ye, "Pinning-observer-based secure synchronization control for complex dynamical networks subject to DoS attacks," *IEEE Trans. Circuits Syst. I: Regular Papers*, vol. 67, no. 12, pp. 5394–5404, Dec. 2020.

[5] G. Mahadevi, "Location discovery with security in wireless sensor network," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 4, pp. 1528–1533, 2011.

[6] H. Ren, Y. Wang, M. Liu, and H. Li, "An optimal estimation framework of multi-agent systems with random transport protocol," *IEEE Trans. Signal Process.*, vol. 70, pp. 2548–2559, 2022.

[7] C. Wu, W. Pan, G. Sun, J. Liu, and L. Wu, "Learning tracking control for cyber–physical systems," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9151–9163, Jun. 2021.

[8] F. Li, X. Yan, Y. Xie, Z. Sang, and X. Yuan, "A review of cyber-attack methods in cyber-physical power system," in *Proc. IEEE 8th Int. Conf. Adv. Power Syst. Automat. Protection*, 2019, pp. 1335–1339.

[9] S. R. B. Alvee, B. Ahn, T. Kim, Y. Su, Y.-W. Youn, and M.-H. Ryu, "Ransomware attack modeling and artificial intelligence-based ransomware detection for digital substations," in *Proc. IEEE 6th Workshop Electron. Grid*, 2021, pp. 1–5.

[10] J. Ni, F. Duan, and P. Shi, "Fixed-time consensus tracking of multiagent system under DoS attack with event-triggered mechanism," *IEEE Trans. Circuits Syst. I: Regular Papers*, vol. 69, no. 12, pp. 5286–5299, Dec. 2022.

[11] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems–attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Inform.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[12] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. IEEE 47th Annu. Allerton Conf. Commun., Control, Comput.*, 2009, pp. 911–918.

[13] Y. Lu, C. Wu, W. Yao, G. Sun, J. Liu, and L. Wu, "Deep reinforcement learning control of fully-constrained cable-driven parallel robots," *IEEE Trans. Ind. Electron.*, vol. 70, no. 7, pp. 7194–7204, Jul. 2023.

[14] C. Wu, W. Pan, R. Staa, J. Liu, G. Sun, and L. Wu, "Deep reinforcement learning control approach to mitigating actuator attacks," *Automatica*, vol. 152, 2023, Art. no. 110999.

[15] C. Wu, L. Wu, J. Liu, and Z.-P. Jiang, "Active defense-based resilient sliding mode control under denial-of-service attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 237–249, 2020.

[16] X. Lin et al., "Observer-based fixed-time control for permanent magnet synchronous motors with parameter uncertainties," *IEEE Trans. Power Electron.*, vol. 38, no. 4, pp. 4335–4344, Apr. 2023.

[17] C. Wu, X. Li, W. Pan, J. Liu, and L. Wu, "Zero-sum game-based optimal secure control under actuator attacks," *IEEE Trans. Autom. Control*, vol. 66, no. 8, pp. 3773–3780, Aug. 2021.

[18] J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based network intrusion detection systems," *IEEE Trans. Syst., Man, Cybern., Part C. (Appl. Rev.)*, vol. 38, no. 5, pp. 649–659, Sep. 2008.

[19] A.-Y. Lu and G.-H. Yang, "False data injection attacks against state estimation without knowledge of estimators," *IEEE Trans. Autom. Control*, vol. 67, no. 9, pp. 4529–4540, Sep. 2022.

[20] A.-Y. Lu and G.-H. Yang, "Malicious attacks on state estimation against distributed control systems," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3911–3918, Sep. 2020.

[21] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, Mar. 2017.

[22] A.-Y. Lu and G.-H. Yang, "Malicious adversaries against secure state estimation: Sparse sensor attack design," *Automatica*, vol. 136, 2022, Art. no. 110037.

[23] H. Zhao and Y. Niu, "Finite-time sliding mode control of switched systems with one-sided Lipschitz nonlinearity," *J. Franklin Inst.*, vol. 357, no. 16, pp. 11171–11188, 2020.

[24] J. Fu, Y. Lv, and W. Yu, "Robust adaptive time-varying region tracking control of multi-robot systems," *Sci. China Inf. Sci.*, vol. 66, no. 5, pp. 1–2, 2023.

[25] M. Hou, W. Shi, L. Fang, and G. Duan, "Adaptive dynamic surface control of high-order strict feedback nonlinear systems with parameter estimations," *Sci. China Inf. Sci.*, vol. 66, no. 5, 2023, Art. no. 159203.

[26] H. Ren, H. Ma, H. Li, and Z. Wang, "Adaptive fixed-time control of nonlinear mass with actuator faults," *IEEE/CAA J. Automatica Sinica*, vol. 10, no. 5, pp. 1252–1262, May 2023.

[27] S. Song, J. H. Park, B. Zhang, and X. Song, "Event-based adaptive fuzzy fixed-time secure control for nonlinear CPSs against unknown false data injection and backlash-like hysteresis," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 6, pp. 1939–1951, Jun. 2022.

[28] H. Ren, H. Ma, H. Li, and R. Lu, "A disturbance observer based intelligent control for nonstrict-feedback nonlinear systems," *Sci. China Technol. Sci.*, vol. 66, pp. 456–467, 2023.

[29] J. Tian and S. Ma, "Unknown input observer design for one-sided Lipschitz nonlinear continuous-time singular Markovian jump systems," in *Proc. IEEE 12th World Congress Intell. Control Autom.*, 2016, pp. 1920–1925.

[30] C. M. Nguyen, P. N. Pathirana, and H. Trinh, "Robust observer design for uncertain one-sided Lipschitz systems with disturbances," *Int. J. Robust Nonlinear Control*, vol. 28, no. 4, pp. 1366–1380, 2018.

[31] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 5, pp. 779–789, May 2018.

[32] J. Cao, J. Zhou, J. Chen, A. Hu, and M. Hu, "Sliding mode control for discrete-time systems with randomly occurring uncertainties and nonlinearities under hybrid cyber attacks," *Circuits, Syst., Signal Process.*, vol. 40, no. 12, pp. 5864–5885, 2021.

[33] S. Liu, G. Wei, Y. Song, and Y. Liu, "Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks," *Neurocomputing*, vol. 207, pp. 708–716, 2016.

[34] P. Zhu, S. Jin, X. Bu, Z. Hou, and C. Yin, "Model-free adaptive control for a class of MIMO nonlinear cyber-physical systems under false data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 10, no. 1, pp. 467–478, Mar. 2023.

[35] S. Chen, Q. Zhang, D. Lin, and S. Wang, "A class of nonlinear Kalman filters under a generalized measurement model with false data injection attacks," *IEEE Signal Process. Lett.*, vol. 29, pp. 1187–1191, 2022.

[36] A. K. Singh, S. Kumar, N. Kumar, and R. Radhakrishnan, "Bayesian approximation filtering with false data attack on network," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 2, pp. 976–988, Apr. 2022.

[37] G.-D. Hu, "Observers for one-sided Lipschitz non-linear systems," *IMA J. Math. Control Inf.*, vol. 23, no. 4, pp. 395–401, 2006.

[38] M. Abbaszadeh and H. J. Marquez, "Nonlinear observer design for one-sided Lipschitz systems," in *Proc. IEEE Amer. Control Conf.*, 2010, pp. 5284–5289.

[39] X.-K. Liu, S.-Q. Wang, M. Chi, Z.-W. Liu, and Y.-W. Wang, "Resilient secondary control and stability analysis for dc microgrids under mixed cyber attacks," *IEEE Trans. Ind. Electron.*, early access, Apr. 04, 2023, doi: 10.1109/TIE.2023.3262893.

[40] D. Zhao, Z. Wang, G. Wei, and Q.-L. Han, "A dynamic event-triggered approach to observer-based PID security control subject to deception attacks," *Automatica*, vol. 120, 2020, Art. no. 109128.

[41] T. Yang, C. Murguia, M. Kuijper, and D. Nešić, "An unknown input multiobserver approach for estimation and control under adversarial attacks," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 475–486, Mar. 2021.

[42] Y. Ebihara, D. Peaucelle, and D. Arzelier, *S-Variable Approach to LMI-Based Robust Control*. Berlin, Germany: Springer, 2015.

[43] W. Zheng, H.-K. Lam, F. Sun, and S. Wen, "Robust stability analysis and feedback control for uncertain systems with time-delay and external disturbance," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 12, pp. 5065–5077, Dec. 2022.

[44] Y. Wang, Z. Miao, H. Zhong, and Q. Pan, "Simultaneous stabilization and tracking of nonholonomic mobile robots: A Lyapunov-based approach," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 4, pp. 1440–1450, Jul. 2015.

[45] C. Wu, W. Yao, W. Luo, W. Pan, H. Xie, and L. Wu, "A secure robot learning framework for cyber attack scheduling and countermeasure," *IEEE Trans. Robot.*, early access, Jun. 05, 2023, doi: 10.1109/TRO.2023.3275875.

Hongming Zhu received the B.E. degree in electrical and electronic engineering (Electronic Eng. and Communications) from the University of Liverpool, Liverpool, U.K., in 2020, and the M.S. degree in power systems engineering from University College London, London, U.K., in 2021. He is currently working toward the Ph.D. degree in Control Science and Engineering from the Harbin Institute of Technology, Harbin, China. His research interests including reinforcement learning, adaptive dynamic programming, and secure control for cyber-physical systems.

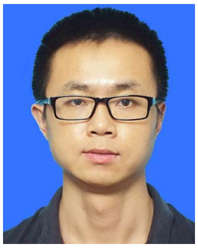
Lezhong Xu received the B.E. degree in mechanical electronic engineering from the College of Mechanical and Electrical Engineering, Northeast Forestry University, Harbin, China, in 2022. He is currently working toward the M.S. degree with the Northeast Forestry University, Harbin. His research interests include intelligent control and cyber-physical systems.

Zeyu Bao was born in 1990. He received the master degree in guidance nagivation and control engineering from Beihang University, Beijing, China, in 2016. He is currently with the Institute of Telecommunication and Navigation Satellites, CAST. His research interests include satellite manufacture and laser communication.

Yifan Liu received the the bachelor's and master's degrees in aircraft design in 2007 and 2009, respectively, from the Harbin Institute of Technology, Harbin, China, where he is currently working toward the Ph.D. degree in control science and engineering. His research interests include model-based systems engineering (MBSE) and fault diagnosis.

Liyuan Yin received the B.S. degree in detection guidance and control technology and the M.S. degree in control science and engineering from Shenyang Aerospace University, Shenyang, China, in 2017 and 2020, respectively. He is currently working toward the Ph.D. degree in control science and engineering with the Harbin Institute of Technology, Harbin, China His research interests include reinforcement learning, adaptive dynamic programming, and secure control for cyber-physical systems.

Weiran Yao (Member, IEEE) received the bachelors (with Hons.) degree, the masters degree, and the doctors degree in aeronautical and astronautical science and technology from the Harbin Institute of Technology (HIT), Harbin, China, in 2013, 2015, and 2020, respectively. From 2017 to 2018, he was a visiting Ph.D. student with the Department of Mechanical and Industrial Engineering, University of Toronto, Toronto, ON, Canada. He is currently an Assistant Professor with HIT. His research interests include unmanned vehicles, multirobot mission planning, and multiagent control systems.



Chengwei Wu (Member, IEEE) received the Ph.D. degree in engineering from the Harbin Institute of Technology, Harbin, China, 2021. From July 2015 to December 2015, he was a Research Assistant with the Department of Mechanical Engineering, The Hong Kong Polytechnic University, Hong Kong. From 2019 to 2021, he was a joint-Ph.D. Student with the Department of Cognitive Robotics, Delft University of Technology, Delft, The Netherlands. He is currently an Assistant Professor with the Harbin Institute of Technology. His research interests include reinforcement learning and cyber-physical systems.

Ligang Wu (Fellow, IEEE) received the B.S. degree in automation, the M.E. degree in navigation guidance and control, and the Ph.D. degree in control theory and control engineering from the Harbin Institute of Technology, Harbin, China, in 2001, 2003, and 2006, respectively. From 2006 to 2007, he was a Research Associate with the Department of Mechanical Engineering, The University of Hong Kong, Hong Kong. From 2007 to 2008, he was a Senior Research Associate with the Department of Mathematics, City University of Hong Kong, Hong Kong. From 2012 to 2013, he was a Research Associate with the Department of Electrical and Electronic Engineering, Imperial College London, London, U.K. In 2008, he joined the Harbin Institute of Technology, China, as an Associate Professor, and then promoted to a Full Professor in 2012. He has authored or coauthored seven research monographs and more than 170 research papers in international referred journals. His research interests include switched systems, stochastic systems, computational and intelligent systems, sliding mode control, and advanced control techniques for power electronic systems. Prof. Wu is an Associate Editor for a number of journals, including IEEE TRANSACTIONS ON AUTOMATIC CONTROL, IEEE/ASME TRANSACTIONS ON MECHATRONICS, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, *Information Sciences, Signal Processing,* and *IET Control Theory and Applications.* He is an Associate Editor for the Conference Editorial Board, IEEE Control Systems Society.