Covert Attack Detection and Secure Control for Cyber Physical Systems

Xianghua Wang, Ali Zolghadri, Changqing Wang

Covert Attack Detection and Secure Control for Cyber Physical Systems

Xianghua Wang, *Member, IEEE,* Ali Zolghadri, *Senior Member, IEEE,* Changqing Wang

***Abstract*—The problem addressed in this paper is that of monitoring and secure control in cyber physical systems subject to cyber covert attacks. In this scenario, the attacker can manipulate sensor measurements and control actions while bypassing the classical monitoring schemes. Firstly, attack detection is investigated by constructing signal generators in both cyber and physical layers, whose output is injected into the transmission network to reveal the covert attacks. After the attack has been detected, the nominal output feedback controller is switched into a secure controller based on adaptive observer to ensure an output tracking performance level. The adaptive observer is used to suppress (and not to estimate) the attack signals, hence the control effect does not depend on the estimation precision. Moreover, there is no assumption on the boundedness of the attack signals. Finally, numerical simulations are provided to show the effectiveness of the proposed scheme.**

***Index Terms*—Cyber physical systems, secure control, covert attacks, attack detection.**

I. Introduction

CYBER-Physical Systems (CPSs) are engineered systems with deep integration of computation, communication and networking, physical processes, and control systems. CPSs are set to change the shape of our daily lives as they concern many technological areas, including aerospace, automotive, energy, chemical industry, transportation, or health care. Monitoring and secure control of CPSs have spurred on substantial research activities during the last decade. Researches have been developed along several major lines, from both control-oriented and information/communication perspectives. Much effort has been devoted to cyber attack detection and secure control. See for example [1] and [2] for a recent survey.

Cyber attacks can be classified into two main categories: denial of service (DoS) attacks and deception attacks, which encompass replay attacks, covert attacks, zero dynamics attacks, and more [3]. A covert attacker possesses the capability to assess the impact of their actions in a manner that the dynamics of the controlled system under attack would appear unchanged from the nominal case [4]. Consequently, detecting covert attacks using conventional methods is highly challenging, and only a limited number of studies on this topic can be found in the literature. These methods can be categorized into two classes. The first class, known as moving target-based methods, introduces elements such as a switched auxiliary system [5], linear time-varying external dynamics [6], or modulation matrices [7] to prevent the attacker from accurately identifying the plant dynamics. Nevertheless, these methods are effective only when operating under the assumption that the attacker remains unaware of the introduced matrices or dynamics. An alternative approach, presented in [8], involves a dual time-varying coding detection scheme. In this scheme, both the measured output signals and control input signals are encoded before transmission over the network and subsequently decoded upon reception by the next nodes. However, this approach necessitates a complex setup, requiring synchronous knowledge of the time-varying coding matrices in both the cyber and physical layers. It also assumes that the attacker cannot accurately distinguish between the time-varying coding matrices. The other class consists of distributed model-based methods [9], [10], which are primarily suitable for large-scale systems featuring interconnected plants. These methods rely on information from adjacent plants to detect attacks. Consequently, they are not applicable to single-plant systems, which are the focus of this paper.

In the realm of secure control, research on resilient control against covert attacks remains relatively sparse. Notably, in [9], a resilient control approach based on attack isolation was developed for large-scale systems facing covert attacks. This approach employs a two-stage fixed-time observer to enhance system resilience. In [10], the attack detection scheme was enhanced to estimate the actions of an attacker. Subsequently, an accommodation scheme was introduced to mitigate or neutralize the abnormal behavior exhibited by interconnected systems under covert attacks. It's worth noting that in [9], [10], the considered plant is assumed to be free from disturbances and noises. In [11], a method was introduced to counteract covert attacks by generating redundant control sequences, which were randomly selected on the actuator side to conceal the exploited control action. However, this approach needs a high computational cost. Fauser and Zhang [12] used frequency hopping spread spectrum to nullify the attack's influence on the system but required two attack detection filters to reveal the actual attack, resulting in both high computational cost and the absence of an attack signal estimate.

Given this overall picture, it seems that finding viable solutions to the problem of covert attacks detection and subsequent secure control remains an open problem. This paper addresses this issue by first presenting a procedure for covert attack detection, using signal generators placed in both the cyber and physical layers capable of generating and injecting signals into the transmission network. Subsequently, an output feedback

X. Wang is with the School of Artificial Intelligence, Beijing University of Posts and Telecommunications, Beijing, China, XianghuaWang@bupt.edu.cn. The corresponding author.

A. Zolghadri is with the CNRS-IMS lab, University of Bordeaux, F-33400 Talence, France, ali.zolghadri@ims-bordeaux.fr

W. Wang is with the School of Automation, Northwestern Polytechnical University, Xi'an, China, wangcq@nwpu.edu.cn

secure control scheme, based on an adaptive observer, is proposed to enable the system to operate effectively even under attack conditions, ensuring a certain level of output tracking performance. The main contributions can be summarized as follows:

1) Regarding attack detection, we propose a method that revolves around the construction of signal generators in both the cyber and physical layers. These generators are tasked with generating and inserting external signals into the transmission network as soon as the CPS begins operation. These additional signals have no impact on the system's performance under nominal conditions (no attacks). However, they are designed to mislead potential adversaries and lead them to form an incorrect system model. As a result, the residual crosses a predefined threshold, revealing the presence of covert attacks. It's important to note that this approach differs from the moving target-based method [8], which relies on rapidly altering the system dynamics to prevent the adversary from accurately recognizing the system model.
2) Regarding subsequent secure control, we propose an original method designed to deal with covert attacks effectively. This approach is built upon an adaptive observer, which plays a pivotal role in ensuring output tracking performance. It's important to note that the primary function of the adaptive observer is to overcome and suppress the effects of attacks, rather than estimating state or attack signals. Consequently, the scheme is not reliant on observer performance, leading to a reduction in computational cost compared to [11], [12]. Furthermore, unlike [9], [10], our proposed scheme is applicable to systems subject to disturbances and noise.

The paper is organized as follows. Section II is devoted to system description under covert attacks. Section III presents our main results, including attack detection and secure control. A numerical example is provided in Section IV and some concluding remarks are given in Section V.

Notations: $\mathbf{I}_r$ is an identity matrix of dimension r. $\mathbf{0}$ is a matrix or vector with appropriate dimension and its all entries are 0. For a vector $x \in \mathbb{R}^n$, $\|x\| = \sqrt{x^T x}$. For a matrix W, $\mathrm{He}(W) = W + W^T$, $\star$ denotes the symmetric part of a matrix and $\mathrm{Trace}(W)$ is the trace of W. S_n is a diagonal matrix of dimension n whose diagonal elements are all $s \neq 0$ and $s \neq -1$.

II. Problem Formulation and Preliminary

This section starts by presenting preliminary knowledge about the plant dynamics, the nominal controller, and the proposed signal generators. Subsequently, we conduct an analysis of system performance under normal conditions before introducing the attack scenario.

A. System description

The cyber physical systems consist of two layers: physical layer and cyber layer, as shown in Fig. 1. The plant is in

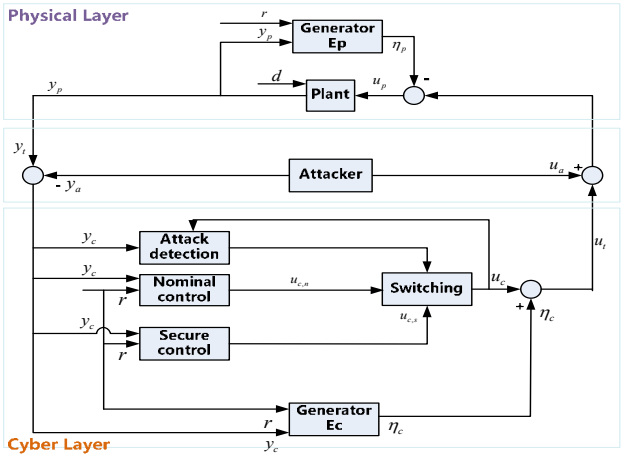

Fig. 1. Block diagram for attack detection and secure control.

the physical layer, which is considered to be continuous-time linear time invariant (LTI) described by

$$\dot{x}_p = Ax_p + Bu_p + Ed, \;\; y_p = Cx_p \tag{1}$$

where $x_p \in \mathbb{R}^n$ is the state vector, $u_p \in \mathbb{R}^m$ is the control input, $y_p \in \mathbb{R}^p$ is the measured output, $d \in \mathbb{R}^q$ is the unknown and bounded disturbance vector, A, B, C and E are matrices of appropriate dimensions.

For the plant (1), the following assumptions are made:

Assumption 1: It is assumed that the couple (A, B) is controllable, and (A, C) is observable.

Assumption 2: $\mathrm{rank}(CB) = \mathrm{rank}(B)$.

Assumption 3: The invariant zeros of the triple (A, B, C) lie in $\mathcal{C}_-$, $\mathcal{C}_-$ denotes the left complex plane.

Remark 1: Assumption 2 (namely the system (1) satisfies the matching condition) and Assumption 3 (namely the system (1) is minimum-phase) are sufficient and necessary for sliding mode observer and unknown input observer [13].

The controller is in the cyber layer. As shown in Fig. 1, y_c is the output signal received by the controller, u_c is the control signal generated by the controller and defined by

$$u_c = \begin{cases} u_{c,n}, & 0 \leq t < T_d \\ u_{c,s}, & t \geq T_d \end{cases} \tag{2}$$

where T_d is the time when the attack is detected and which will be given in Section III-A, and $u_{c,n}$ is the nominal controller whose expression is

$$\dot{\hat{x}}_p = A\hat{x}_p + Bu_c + L_n\tilde{y}_c, \tilde{y}_c = y_c - C\hat{x}_p \tag{3}$$

$$u_{c,n} = K_n\hat{x}_p + r \tag{4}$$

where r is a reference command signal which acts on the closed-loop dynamics to generate y_{ref}

$$\dot{x}_r = A_c x_r + Br, \;\; y_{ref} = Cx_r \tag{5}$$

where $A_c = A + BK_n$, L_n and K_n are design matrices given later in (17). $u_{c,s}$ is the secure controller and will be developed in Section III-B.

$\mathcal{E}_p$ and $\mathcal{E}_c$ are the proposed signal generators in the physical and cyber layers respectively, and are activated at the beginning of the system operation. The dynamics of signal generators $\mathcal{E}_c$ and $\mathcal{E}_p$ are given by

$$\begin{array}{rcl}\dot{\xi}_c &=& A_d\xi_c + BS_m r + L_n S_p y_c \\ \eta_c &=& K_n\xi_c + S_m r\end{array} \tag{6}$$

and

$$\begin{array}{rcl}\dot{\xi}_p &=& A_d\xi_p + BS_m r + L_n S_p y_p \\ \eta_p &=& K_n\xi_p + S_m r\end{array} \tag{7}$$

where $A_d = A + BK_n - L_nC$, S_m and S_p are design parameters and from Notations, the initial values are chosen as $\xi_c(0) = \xi_p(0) = \hat{x}_p(0)$. In the nominal case, $u_c = u_{c,n}$ and from (3)-(4) it follows

$$u_{c,n} = [K_n(\lambda I - A_d)^{-1}B + I]r + K_n(\lambda I - A_d)^{-1}L_n y_c \tag{8}$$

where λ is the Laplace operator. From (6), it follows

$$\eta_c = s[K_n(\lambda I - A_d)^{-1}B + I]r + sK_n(\lambda I - A_d)^{-1}L_n y_c \tag{9}$$

By comparing (8) with (9), it is clear that

$$\eta_c = su_{c,n} \tag{10}$$

The objective is twofold:

- to detect the covert attack. In this work, the observer (3) is also used for attack detection which is a classical observer-based method and the detection mechanism is
  - if $\|\tilde{y}_c\| > \gamma_s\|d\|$ where $\tilde{y}_c$ is from (3), then an attack has occurred;
  - otherwise, it is judged that there are no cyber attacks.
- to design u_c in (2) such that

$$\|y_p - y_{ref}\| \le \gamma_s\|d\| \tag{11}$$

where γ_s is some desired output tracking performance level.

B. Performance analysis for attack-free case

In the following, the closed-loop system performance in the nominal case (attack-free case) will be discussed.

Denote the signals propagated through the networks as y_t and u_t, then from Fig. 1, it follows

$$y_t = y_p, u_t = u_c + \eta_c \tag{12}$$

When there are no cyber attacks, namely $y_a = 0$ and $u_a = 0$, the controller input y_c and the plant input u_p are respectively

$$y_c = y_t, u_p = u_t - \eta_p \tag{13}$$

Combine (12) with (13) to get $y_c = y_t = y_p$, which when substituted into (6) and (7), it follows $\eta_c = \eta_p$. Again from (12) and (13), we get $u_p = u_c + \eta_c - \eta_p = u_c = u_{c,n}$.

Denote $\tilde{x}_p = x_p - \hat{x}_p$, and subtract (3) from (1) (using $u_p = u_c$ and $y_c = y_p$) to get

$$\dot{\tilde{x}}_p = A_o\tilde{x}_p + Ed, \tilde{y}_c = C\tilde{x}_p \tag{14}$$

where $A_o = A - L_nC$.

Define $e_p = x_p - x_r$ and subtract (5) from (1) with the use of $u_p = u_c = u_{c,n}$ and (4) to get

$$\dot{e}_p = A_c e_p - BK_n\tilde{x}_p + Ed, y_p - y_{ref} = Ce_p \tag{15}$$

By combining (14) with (15), we get

$$\begin{array}{l}\left[\begin{array}{c}\dot{e}_p \\ \dot{\tilde{x}}_p\end{array}\right] = \underbrace{\left[\begin{array}{cc}A_c & -BK_n \\ \mathbf{0} & A_o\end{array}\right]}_{A_n}\left[\begin{array}{c}e_p \\ \tilde{x}_p\end{array}\right] + \underbrace{\left[\begin{array}{c}E \\ E\end{array}\right]}_{E_n}d \\ \left[\begin{array}{c}y_p - y_{ref} \\ \tilde{y}_c\end{array}\right] = \underbrace{\left[\begin{array}{cc}C & \mathbf{0} \\ \mathbf{0} & C\end{array}\right]}_{C_n}\left[\begin{array}{c}e_p \\ \tilde{x}_p\end{array}\right]\end{array} \tag{16}$$

By virtue of Bounded Real Lemma [14], for a given $\gamma_s > 0$, if there exist matrices K_n, L_n, and a symmetric positive definite (s.p.d.) matrix $P_n = \text{diag}\{P_c, P_o\}$ with $P_c = P_c^T$, $P_o = P_o^T$ such that

$$\left[\begin{array}{cc}A_n^TP_n + P_nA_n + C_n^TC_n & P_nE_n \\ \star & -\gamma_s^2\mathbf{I}_q\end{array}\right] < \mathbf{0} \tag{17}$$

then $\|y_p - y_{ref}\| \le \gamma_s\|d\|$ (hence the acceptable performance (11) is ensured) and $\|\tilde{y}_c\| \le \gamma_s\|d\|$ (hence there are no false alarms for the attack-free case).

Using the structures of A_n, P_n, E_n and C_n, the inequality (17) becomes

$$\left[\begin{array}{ccc}\Pi_1 & -P_cBK_n & P_cE \\ \star & \Pi_2 & P_oE \\ \star & \star & -\gamma_s^2\mathbf{I}_q\end{array}\right] < \mathbf{0} \tag{18}$$

where $\Pi_1 = P_cA + A^TP_c + P_cBK_n + K_n^TB^TP_c + C^TC$, $\Pi_2 = P_oA + A^TP_o - P_oL_nC - C^TL_n^TP_o + C^TC$. Pre-multiplying and post-multiplying both sides of (18) with $\text{diag}\{P_c^{-1}, \mathbf{I}_n, \mathbf{I}_q\}$ and using Schur complement [15], (18) is equivalent to the following inequality

$$\begin{array}{l}\left[\begin{array}{cccc}\Theta_1 & \mathbf{0} & E & P_c^{-1}C^T \\ \star & \Theta_2 & P_oE & \mathbf{0} \\ \star & \star & -\gamma_s^2\mathbf{I}_q & \mathbf{0} \\ \star & \star & \star & -\mathbf{I}_p\end{array}\right] \\ +\text{He}\left\{\left[\begin{array}{c}-BK_n \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{0}\end{array}\right][\mathbf{0}\ \mathbf{I}_n\ \mathbf{0}\ \mathbf{0}]\right\} < \mathbf{0}\end{array} \tag{19}$$

where $\Theta_1 = AP_c^{-1} + BK_nP_c^{-1} + P_c^{-1}A^T + P_c^{-1}K_n^TB^T$, $\Theta_2 = P_oA + A^TP_o - P_oL_nC - C^TL_n^TP_o + C^TC$. Now, from the Young's inequality [16], it follows that

$$\begin{array}{rl}&\text{He}\left\{\left[\begin{array}{c}-BK_n \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{0}\end{array}\right][\mathbf{0}\ \mathbf{I}_n\ \mathbf{0}\ \mathbf{0}]\right\} \\ \le\ & \gamma_a[-P_c^{-1}K_n^TB^T\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}]^TP_c[-P_c^{-1}K_n^TB^T\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}] \\ & +\gamma_a^{-1}[\mathbf{0}\ \mathbf{I}_n\ \mathbf{0}\ \mathbf{0}]^TP_c[\mathbf{0}\ \mathbf{I}_n\ \mathbf{0}\ \mathbf{0}]\end{array} \tag{20}$$

where $0 < \gamma_a < 1$. Substitute (20) into (19) and use Schur complement [15] again to get

$$\begin{bmatrix} \Theta_1 & \mathbf{0} & E & P_c^{-1}C^T & -BK_nP_c^{-1} & \mathbf{0} \\ \star & \Theta_2 & P_oE & \mathbf{0} & \mathbf{0} & \mathbf{I}_n \\ \star & \star & -\gamma_s^2\mathbf{I}_q & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \star & \star & \star & -\mathbf{I}_p & \mathbf{0} & \mathbf{0} \\ \star & \star & \star & \star & -\gamma_a^{-1}P_c^{-1} & \mathbf{0} \\ \star & \star & \star & \star & \star & -\gamma_aP_c^{-1} \end{bmatrix} < \mathbf{0} \tag{21}$$

Define $\hat{P}_c = P_c^{-1}$, $\hat{K}_n = K_nP_c^{-1}$ and $\hat{L}_n = P_oL_n$, then (21) is linear with respect to $\hat{P}_c$, $\hat{K}_n$, $\hat{L}_n$, and P_o and an LMI solver (e.g. LMI toolbox of MATLAB) can be used to solve it. Then $K_n = \hat{K}_nP_c$, and $L_n = P_o^{-1}\hat{L}_n$.

Remark 2: It can be seen from above that the introduction of signal generators $\mathcal{E}_p$ and $\mathcal{E}_c$ will neither affect the nominal operation nor trigger a false alarm.

Remark 3: From (18), it follows $P_cA_c+A_c^TP_c < \mathbf{0}$, $P_oA_o+A_o^TP_o < \mathbf{0}$ and

$$\begin{bmatrix} P_oA_o + A_o^TP_o + C^TC & P_oE \\ E^TP_o & -\gamma_s^2\mathbf{I}_p \end{bmatrix} < \mathbf{0} \tag{22}$$

which implies $\|C(\lambda\mathbf{I}_n - A_o)^{-1}E\| \le \gamma_s$.

III. Main Results

In this section, the main results including attack detection and secure control are given. In order to derive the main results, the following lemma is firstly introduced.

Lemma 1: [17] For a system in the form of (1), there exist a s.p.d. matrix P, and matrices L, K such that

$$(A - LC)^TP + P(A - LC) < \mathbf{0},\ B^TP = KC$$

if and only if Assumption 2 and Assumption 3 hold.

In the following, a detection scheme is firstly presented to reveal the covert attack. Then, a secure controller is designed such that (11) can be achieved.

A. Attack Detection

The covert attacks operate in two phases.

In Phase 1, the attacker seizes the network signals u_t and y_t and uses them to establish a model of the plant. In this phase, the attack signals u_a and y_a have not yet been injected into the network, and the nominal controller is adopted, namely $u_c = u_{c,n}$. From (10) and (12), it follows that $y_t = y_p$ and $u_t = u_c + \eta_c = \alpha u_c$ with $\alpha = s + 1$. As stated after (13), in this case, $u_p = u_c$, hence $u_p = \alpha^{-1}u_t$, and when substituted into (1) yields

$$\dot{x}_p = Ax_p + \alpha^{-1}Bu_t + Ed,\ y_t = Cx_p \tag{23}$$

As in [8], the covert agent is sophisticated, and has access to the transmitted signals u_t and y_t, and perfect knowledge of the disturbance-free and noise-free plant model [18]. Therefore, from (23) the covert agent can use u_t and y_t to establish a model of the plant as (some system identification technique may be used to estimate them):

$$\dot{x}_a = Ax_a + \alpha^{-1}Bu_a,\ y_a = Cx_a \tag{24}$$

where $u_a \in \mathbb{R}^m$ is the covert agent's control input, $y_a \in \mathbb{R}^p$ is the output signal of the covert agent.

In Phase 2, the covert attack is carried out, and define T_a as the time when this happens. The covert misappropriation is performed by combining two aspects: one is adding the covert controller signal u_a into u_t, and the other is subtracting the covert agent output y_a from y_t, hence u_p (the actual control input signal of the plant) and y_c (the actual output signal received by the controller) in (13) become respectively

$$u_p = u_t + u_a - \eta_p; \tag{25}$$

and

$$y_c = y_t - y_a. \tag{26}$$

From (1), (12) and (24), (25) and (26) can be rewritten as

$$u_p = u_c + u_a + \eta_c - \eta_p, y_c = Cx_p - Cx_a \tag{27}$$

In the following, we will show with signal generators $\mathcal{E}_p$ and $\mathcal{E}_c$, the attack will be uncovered.

Subtract (3) from (1) and use (27) to get

$$\begin{aligned} \dot{\tilde{x}}_p &= A_o\tilde{x}_p + Bu_a + Ed + L_nCx_a + B(\eta_c - \eta_p), \\ \tilde{y}_c &= C\tilde{x}_p - Cx_a \end{aligned} \tag{28}$$

where $\eta_c - \eta_p = K_n(\xi_c - \xi_p)$ and from (6)-(7), it follows

$$\dot{\xi}_c - \dot{\xi}_p = A_d(\xi_c - \xi_p) - L_nS_pCx_a \tag{29}$$

Define $X = [\tilde{x}_p^T\ (\xi_c - \xi_p)^T\ x_a^T]^T$, and augment (24), (28) with (29) to get

$$\dot{X} = A_xX + B_xu_a + E_xd, \tilde{y}_c = C_xX \tag{30}$$

where $C_x = \begin{bmatrix} C & \mathbf{0} & -C \end{bmatrix}$, $E_x = \begin{bmatrix} E^T & \mathbf{0} & \mathbf{0} \end{bmatrix}^T$,

$$A_x = \begin{bmatrix} A_o & BK_n & L_nC \\ \mathbf{0} & A_d & -L_nS_pC \\ \mathbf{0} & \mathbf{0} & A \end{bmatrix}, B_x = \begin{bmatrix} B \\ \mathbf{0} \\ B\alpha^{-1} \end{bmatrix}.$$

The corresponding transfer function is $\tilde{y}_c = W_a'(\lambda)u_a + C(\lambda\mathbf{I}_n - A_o)^{-1}Ed$, and from Remark 3 $\|C(\lambda\mathbf{I}_n - A_o)^{-1}Ed\| \le \gamma_s\|d\|$, $W_a'(\lambda) = (s/\alpha)C(\lambda\mathbf{I}_n - A)^{-1}B - sC(\lambda\mathbf{I}_n - A_o)^{-1}BK_n(\lambda\mathbf{I}_n - A_d)^{-1}L_nC(\lambda\mathbf{I}_n - A)^{-1}B$. When $s \neq 0$ and $s \neq -1$ (when $s = -1$, $\alpha = 0$), $W_a'(\lambda) \neq 0$, and in this case, there exists a time $T_d \ge T_a$ such that for $t \ge T_d$, $\|\tilde{y}_c(t)\| > \gamma_s\|d\|$ and then an alarm unveiling an attack will be triggered and the attack detection time is T_d.

To better show the effectiveness on attack detection of the proposed signal generators, an analysis on the performance without signal generators is conducted here. Without signal generators $\mathcal{E}_c$ and $\mathcal{E}_p$, in Phase 1, the signals propagated through the networks namely y_t and u_t are $y_t = y_p$ and $u_t = u_c$. Since the attack signal u_a has not been injected into the network, the control signal received by the plant is $u_p = u_t = u_c$. Hence an approximated model of the plant can be established by the covert agent as follows:

$$\dot{x}_a = Ax_a + Bu_a,\ y_a = Cx_a \tag{31}$$

In Phase 2, without the signal generator, $\eta_c = \eta_p = 0$, (27) becomes $u_p = u_c + u_a$ and $y_c = Cx_p - Cx_a$, and then (28) becomes

$$\dot{\tilde{x}}_p = A_o\tilde{x}_p + Bu_a + Ed + L_nCx_a, \tilde{y}_c = C\tilde{x}_p - Cx_a \tag{32}$$

Combine (31) with (32) to get

$$\begin{bmatrix} \dot{\tilde{x}}_p \\ \dot{x}_a \end{bmatrix} = \begin{bmatrix} A_o & L_nC \\ \mathbf{0} & A \end{bmatrix} \begin{bmatrix} \tilde{x}_p \\ x_a \end{bmatrix} + \begin{bmatrix} E \\ \mathbf{0} \end{bmatrix} d + \begin{bmatrix} B \\ B \end{bmatrix} u_a,$$
$$\tilde{y}_c = \begin{bmatrix} C & -C \end{bmatrix} \begin{bmatrix} \tilde{x}_p \\ x_a \end{bmatrix}$$

and the transfer function is $\tilde{y}_c = C(\lambda \mathbf{I}_n - A_o)^{-1}Ed + W_a(\lambda)u_a$ where

$$\begin{aligned} W_a(\lambda) &= \begin{bmatrix} C & -C \end{bmatrix} \left(\lambda \mathbf{I}_{2n} - \begin{bmatrix} A_o & L_nC \\ \mathbf{0} & A \end{bmatrix} \right)^{-1} \begin{bmatrix} B \\ B \end{bmatrix} \\ &= C(\lambda \mathbf{I}_n - A_o)^{-1}[(\lambda \mathbf{I}_n - A)(\lambda \mathbf{I}_n - A)^{-1} \\ &+ L_nC(\lambda \mathbf{I}_n - A)^{-1}]B - C(\lambda \mathbf{I}_n - A)^{-1}B \\ &= \mathbf{0} \end{aligned}$$

hence $\tilde{y}_c$ can be rewritten as

$$\tilde{y}_c = C(\lambda \mathbf{I}_n - A_o)^{-1}Ed \tag{33}$$

From Remark 3, it follows that $\|\tilde{y}_c\| \leq \gamma_s \|d\|$. Hence such attacks easily evade classical anomaly detectors and security defense. As already mentioned, this is because covert attacker can calculate the effect (namely y_a) of attack signal u_a on the measured plant output y_p and then mitigate it by injecting $-y_a$ into y_p. As a consequence, the signal received by the controller will appear unchanged from the nominal case.

Remark 4: To unmask the attacker, we propose to insert external signals η_c and η_p from (6) and (7) into the network at the beginning of system operation as shown in Fig. 1. This operation confounds the adversary, leading to establish an erroneous system model. It's worth noting that this approach differs from the moving target-based method [8], which relies on rapidly altering system dynamics to prevent the adversary from accurately recognizing the system model.

B. Secure Control

In this section a secure controller based on an adaptive observer is proposed to replace the nominal controller as soon as a covert attack is detected. This controller will ensure the output tracking performance (11).

Before designing the secure controller, the following proposition is firstly given.

Proposition 1: The system (30) satisfies

- (A_x, B_x, C_x) is minimum phase;
- $\text{rank}(C_xB_x) = \text{rank}(B_x)$.

Proof: The proof is reported in Appendix A. ■

The secure controller is designed as

$$u_{c,s} = K_n\hat{x}_p + r + \bar{u}_c, \bar{u}_c = -\hat{u}_a - K_x\hat{X} \tag{34}$$

where r is from the reference model (5), $\hat{x}_p$ is from (3), $K_x = [-K_n \ K_n \ 0]$, K_n satisfies (17), $\hat{X}$ and $\hat{u}_a$ are from the following observer

$$\dot{\hat{X}} = A_x\hat{X} + B_x\hat{u}_a + L_xe_{y,c} \tag{35a}$$
$$e_{y,c} = \tilde{y}_c - C_x\hat{X} \tag{35b}$$
$$\hat{u}_a(t) = K_1\hat{u}_a(t-\tau) + K_2e_{y,c} \tag{35c}$$

where L_x, K_1 and K_2 are design matrices, $\tau > 0$ is called the 'learning interval'.

Let $\tilde{X} = X - \hat{X}$ and $\tilde{u}_a = u_a - \hat{u}_a$, then the error dynamics is given by subtracting (35) from (30)

$$\dot{\tilde{X}} = (A_x - L_xC_x)\tilde{X} + E_xd + B_x\tilde{u}_a, \ e_{y,c} = C_x\tilde{X} \tag{36}$$

After the attack is detected (for $t \geq T_d$), from (2), $u_c = u_{c,s}$. Combine (27) with (34), then

$$u_p = K_n\hat{x}_p + r - K_x\hat{X} + \tilde{u}_a + \eta_c - \eta_p \tag{37}$$

Substitute (37) into (1) and the closed-loop system is given by

$$\dot{x}_p = A_cx_p + BK_x\tilde{x} + B\tilde{u}_a + Ed + Br \tag{38}$$

Subtract (5) from (38) to get

$$\dot{e}_p = A_ce_p + BK_x\tilde{X} + B\tilde{u}_a + Ed \tag{39}$$

Define $\xi = \begin{bmatrix} \tilde{X} \\ e_p \end{bmatrix}$ and combine (36) with (39) to get

$$\dot{\xi} = (A_\xi - L_\xi C_\xi)\xi + E_\xi d + B_\xi \tilde{u}_a, \ e_{y,c} = C_\xi \xi \tag{40}$$

where

$$\begin{aligned} A_\xi &= \begin{bmatrix} A_x & \mathbf{0} \\ BK_x & A_c \end{bmatrix}, L_\xi = \begin{bmatrix} L_x \\ \mathbf{0} \end{bmatrix}, E_\xi = \begin{bmatrix} E_x \\ E \end{bmatrix}, \\ B_\xi &= \begin{bmatrix} B_x \\ B \end{bmatrix}, C_\xi = \begin{bmatrix} C_x & \mathbf{0} \end{bmatrix}. \end{aligned} \tag{41}$$

Remark 5: From the structure of (41), it is clear that $\text{rank}(C_\xi B_\xi) = \text{rank}(C_xB_x)$ and $\text{rank}(B_\xi) = \text{rank}(B_x)$, which when combined with Proposition 1, it follows that $\text{rank}(C_\xi B_\xi) = \text{rank}(B_\xi)$. Again from the structure of (41), the Rosenbrock matrix of (A_ξ, B_ξ, C_ξ) is

$$\mathcal{R}_\xi = \begin{bmatrix} \lambda \mathbf{I}_{3n} - A_x & \mathbf{0} & B_x \\ -BK_x & \lambda \mathbf{I}_n - A_c & B \\ Cx & \mathbf{0} & \mathbf{0} \end{bmatrix} \tag{42}$$

Define

$$S_R = \begin{bmatrix} \mathbf{I}_{3n} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_n \\ \mathbf{0} & \mathbf{I}_m & \mathbf{0} \end{bmatrix}, S_L = \begin{bmatrix} \mathbf{I}_{3n} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_p \\ \mathbf{0} & \mathbf{I}_n & \mathbf{0} \end{bmatrix} \tag{43}$$

and then

$$\begin{aligned} &\text{rank}(\mathcal{R}_\xi) = \text{rank}(S_L\mathcal{R}_\xi S_R) \\ &= \left[\begin{array}{cc|c} \lambda \mathbf{I}_{3n} - A_x & B_x & \mathbf{0} \\ Cx & \mathbf{0} & \mathbf{0} \\ \hline -BK_x & B & \lambda \mathbf{I}_n - A_c \end{array}\right] \end{aligned} \tag{44}$$

From Proposition 1, it is known that (A_ξ, B_ξ, C_ξ) is minimum phase.

Proposition 2: From Remark 5, there exist a s.p.d. matrix P_ξ, matrices L_ξ and K_ξ such that

$$(A_\xi - L_\xi C_\xi)^T P_\xi + P_\xi(A_\xi - L_\xi C_\xi) < 0, \tag{45a}$$
$$B_\xi^T P_\xi = K_\xi C_\xi \tag{45b}$$

The proof of Proposition 2 is directly from Lemma 1.

Then we have the following main result.

Theorem 1: The proposed secure controller (34)-(35) can ensure the acceptable performance (11) if

- there exist matrices L_ξ, K_ξ and a s.p.d. matrix P_ξ such that
$$\Omega_\xi = \begin{bmatrix} \Psi_\xi & P_\xi E_\xi \\ E_\xi^T P_\xi & -(\gamma_s^2-\gamma_f^2)\mathbf{I} \end{bmatrix} < 0 \quad (46)$$
and (45b) are satisfied simultaneously, where $\Psi_\xi = (A_\xi - L_\xi C_\xi)^T P_\xi + P_\xi(A_\xi - L_\xi C_\xi) + \begin{bmatrix} \mathbf{0} & \mathbf{I}_n \end{bmatrix}^T C^T C \begin{bmatrix} \mathbf{0} & \mathbf{I}_n \end{bmatrix}$, $0<\gamma_f<\gamma_s$,
- $$K_2 = K_\xi \quad (47)$$
- K_1 is chosen as
$$K_1 = k_1\mathbf{I} \text{ and } 0 < k_1 < \frac{1}{\sqrt{\gamma+1}} < 1 \quad (48)$$
where $0<\gamma<1$ is an arbitrary constant,
- τ is selected appropriately such that
$$\|\Lambda_\tau\| \le k_f \quad (49)$$
where $\Lambda_\tau = u_a(t) - K_1 u_a(t-\tau)$, $k_f>0$ is an arbitrarily small constant.

Proof: It follows from (35c) that

$$\begin{aligned} \tilde{u}_a(t) &= u_a(t) - \hat{u}_a(t) \\ &= u_a(t) - K_1\hat{u}_a(t-\tau) - K_2 e_{y,c} \\ &= u_a(t) - K_1 u_a(t-\tau) + K_1\tilde{u}_a(t-\tau) - K_2 e_{y,c} \\ &= \Lambda_\tau + K_1\tilde{u}_a(t-\tau) - K_2 e_{y,c} \end{aligned} \quad (50)$$

Construct a positive function as

$$V = \xi^{\mathrm{T}} P_\xi \xi + \int_{t-\tau}^{t} \tilde{u}_a^{\mathrm{T}}(\omega)\tilde{u}_a(\omega)d\omega \quad (51)$$

where P_ξ is from (46), and differentiate V with the use of (40), then

$$\begin{aligned} \dot{V} &= \xi^{\mathrm{T}}\left[(A_\xi - L_\xi C_\xi)^{\mathrm{T}} P_\xi + P_\xi(A_\xi - L_\xi C_\xi)\right]\xi + \\ &\quad 2\xi^{\mathrm{T}} P_\xi E_\xi d + 2\xi^{\mathrm{T}} P_\xi B_\xi \tilde{u}_a + \tilde{u}_a^{\mathrm{T}}(t)\tilde{u}_a(t) \\ &\quad -\tilde{u}_a^{\mathrm{T}}(t-\tau)\tilde{u}_a(t-\tau) \end{aligned} \quad (52)$$

Let $Term1 = 2\xi^{\mathrm{T}} P_\xi B_\xi \tilde{u}_a + \tilde{u}_a^{\mathrm{T}}(t)\tilde{u}_a(t)$, and use (45b), (47) and (50) to get

$$\begin{aligned} & Term1 \\ =\ & 2\xi^{\mathrm{T}} C_\xi^T K_\xi^T(\Lambda_\tau + K_1\tilde{u}_a(t-\tau) - K_2 e_{y,c}) + (\Lambda_\tau \\ & + K_1\tilde{u}_a(t-\tau) - K_2 e_{y,c})^T(\Lambda_\tau + K_1\tilde{u}_a(t-\tau) - K_2 e_{y,c}) \\ =\ & 2e_{y,c}^T K_\xi^T(\Lambda_\tau + K_1\tilde{u}_a(t-\tau) - K_2 e_{y,c}) + (\Lambda_\tau + K_1 \\ & \tilde{u}_a(t-\tau) - K_2 e_{y,c})^T(\Lambda_\tau + K_1\tilde{u}_a(t-\tau) - K_2 e_{y,c}) \\ =\ & -e_{y,c}^T K_2^T K_2 e_{y,c} + \underbrace{\Lambda_\tau^T K_1\tilde{u}_a(t-\tau) + \tilde{u}_a^T(t-\tau)K_1^T\Lambda_\tau}_{Term2} \\ & + \Lambda_\tau^T\Lambda_\tau + \tilde{u}_a^T(t-\tau)K_1^T K_1\tilde{u}_a(t-\tau) \end{aligned} \quad (53)$$

From the Young's inequality [16], it follows that

$$Term2 \le \tfrac{1}{\gamma}\Lambda_\tau^{\mathrm{T}}\Lambda_\tau + \gamma\tilde{u}_a^{\mathrm{T}}(t-\tau)K_1^{\mathrm{T}}K_1\tilde{u}_a(t-\tau), \quad (54)$$

where $0<\gamma<1$. By substituting (54) and (53) into (52), and using (48), $\dot{V}$ can be further written as

$$\begin{aligned} \dot{V} &\le \xi^{\mathrm{T}}\left[(A_\xi - L_\xi C_\xi)^{\mathrm{T}} P_\xi + P_\xi(A_\xi - L_\xi C_\xi)\right]\xi + \\ &\quad 2\xi^{\mathrm{T}} P_\xi E_\xi d - e_{y,c}^T K_2^T K_2 e_{y,c} + \Lambda_\tau^{\mathrm{T}}(\mathbf{I} + 1/\gamma\mathbf{I})\Lambda_\tau \\ &\quad +\tilde{u}_a^{\mathrm{T}}(t-\tau)(\gamma K_1^{\mathrm{T}}K_1 + K_1^{\mathrm{T}}K_1 - \mathbf{I})\tilde{u}_a(t-\tau) \\ &\le \xi^{\mathrm{T}}\left[(A_\xi - L_\xi C_\xi)^{\mathrm{T}} P_\xi + P_\xi(A_\xi - L_\xi C_\xi)\right]\xi \\ &\quad +2\xi^{\mathrm{T}} P_\xi E_\xi d + (1+1/\gamma)k_f^2 \end{aligned}$$

Since k_f can be arbitrarily small, there must exist $0<\gamma_f<\gamma_s$ such that $(1+1/\gamma)k_f^2 = \gamma_f^2 d^T d$.

Define $W = \dot{V} + \xi^T \begin{bmatrix} \mathbf{0} \\ \mathbf{I}_n \end{bmatrix} C^T \underbrace{C\begin{bmatrix} \mathbf{0} & \mathbf{I}_n \end{bmatrix}\xi}_{y_p - y_{ref}} - \gamma_s^2 d^T d$ and it follows that $W = \begin{bmatrix} \xi^T & d^T \end{bmatrix}\Omega_\xi \begin{bmatrix} \xi \\ d \end{bmatrix}$, where Ω_ξ is from (46). Since $\Omega_\xi < 0$, $W<0$. There are two cases: if $\dot{V}\ge 0$, then $\|y_p - y_{ref}\| \le \gamma_s\|d\|$; if $\dot{V}<0$, then V will decrease until $\dot{V}\ge 0$ holds. Hence $\|y_p - y_{ref}\| \le \gamma_s\|d\|$ can be ensured. Here completes the proof of Theorem 1. ■

Remark 6: With the proposed secure controller (34)-(35), the output tracking performance $\|y_p - y_{ref}\| \le \gamma_s\|d\|$ can be achieved. It is noted that the adaptive observer is used to suppress the effect of attacks, not to provide the estimates of states and attack signals. Hence the estimation precision has no influences on the control effect, different, for example, from the observer-based scheme reported in [19]. Moreover, there is no assumption on the amplitude of the attack signal u_a, as for example in [20] where the attack signal was assumed to be bounded.

Remark 7: Define a new variable $\bar{L}_\xi = P_\xi L_\xi$, then (46) can be transformed into an LMI with respect to the variables P_ξ and $\bar{L}_\xi$ as follows:

$$\Omega_\xi = \begin{bmatrix} \mathrm{He}(P_\xi A_\xi - \bar{L}_\xi C_\xi) + C* & P_\xi E_\xi \\ E_\xi^T P_\xi & -(\gamma_s^2-\gamma_f^2)\mathbf{I} \end{bmatrix} < 0 \quad (55)$$

where $C* = \begin{bmatrix} \mathbf{0} & \mathbf{I}_n \end{bmatrix}^T C^T C \begin{bmatrix} \mathbf{0} & \mathbf{I}_n \end{bmatrix}$. However, it is not a trivial work to find a systematic solution satisfying (55) and (45b) simultaneously. To solve this difficult problem, similar to [17], we rewrite linear equation (45b) as

$$\mathrm{Trace}[(B_\xi^T P_\xi - K_\xi C_\xi)^T(B_\xi^T P_\xi - K_\xi C_\xi)] = 0 \quad (56)$$

Further, we introduce the following condition

$$(B_\xi^T P_\xi - K_\xi C_\xi)^T(B_\xi^T P_\xi - K_\xi C_\xi) < \varepsilon I \quad (57)$$

where ε is a small enough positive scalar. By Schur complement [15], (57) is equivalent to

$$\begin{bmatrix} -\varepsilon\mathbf{I}_{3n} & B_\xi^T P_\xi - K_\xi C_\xi \\ \star & -\mathbf{I}_{3n} \end{bmatrix} < 0 \quad (58)$$

which is an LMI with respect to variable P_ξ and K_ξ. Now, standard LMI toolbox in Matlab can be used to solve (55) and (58). The feasibilty of (55) and (58) is ensured in Proposition 2.

IV. Numerical Example

In this section, simulations will be conducted to verify the effectiveness of the proposed scheme.

A. Example and simulation conditions

We consider the continuous-time linearized model of the F-404 engine [21], described as $\dot{x} = Ax + Ed(t)$ where $d(t) = 0.001\sin(t) + 0.002\sin(2t)$,

$$A = \begin{bmatrix} -1.46 & 0 & 0.248 \\ 0.1643 & -0.4 & -0.3788 \\ 0.3107 & 0 & -2.23 \end{bmatrix}, E = \begin{bmatrix} 0.2 \\ 0.8 \\ 0 \end{bmatrix}.$$

Assume that the input and output matrices are $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$; the measurement noise $\nu(t)$ is the white noise vector, the attack signal is formulated as $u_a = \begin{bmatrix} 0.7316e^{0.0127t} \\ 0.01\sin(t) \end{bmatrix}$ which starts at $T_a = 15s$. The initial states of the plant and the attacker are $x_p(0) = [-1\ 1\ 1]^T$ and $x_a(0) = [0\ 0\ 0]^T$, respectively. The reference command is $r = [1\ 1]^T$.

The simulations are done for the following four cases:

Case 1 Covert attacks have not compromised the plant;

Case 2 Covert attacks compromise the plant without the signal generator;

Case 3 Covert attacks compromise the plant with the signal generator;

Case 4 Covert attacks have been detected, and the secure controller is operating.

B. Simulation parameters

The design parameters are chosen as $\tau = 0.001$ (which is the simulation step), $s = 2$, $\gamma_s = 1$,

$$L_n = \begin{bmatrix} 14.07 & 163.48 \\ 60.28 & 653.48 \\ 0.85 & -0.14 \end{bmatrix}, K_2 = \begin{bmatrix} 738.44 & -180.32 \\ -180.32 & 53.02 \end{bmatrix},$$
$$K_1 = 0.9988\mathbf{I}_2, K_n = \begin{bmatrix} -72.92 & -0.38 & -0.34 \\ -0.37 & -74.66 & 0.37 \end{bmatrix},$$
$$L_x = \begin{bmatrix} 860.27 & -147.13 \\ -486.29 & 373.18 \\ -5.86 & 1.33 \\ -1874.23 & 632.24 \\ 482.72 & 564.16 \\ -24.15 & 6.16 \\ 914.44 & -132.97 \\ -253.55 & 429.37 \\ 12.31 & -3.00 \end{bmatrix}. \tag{59}$$

C. Simulation results

Simulation results for the four cases are presented in Fig. 2-Fig. 5. The simulation plots including the system outputs $y_{p,i}, i = 1, 2$, the controller inputs $y_{c,i}, i = 1, 2$, the controller outputs $u_{c,i}, i = 1, 2$, the system inputs $u_{p,i}, i = 1, 2$, the evaluation function $\|\tilde{y}_c\|$, the output tracking error $\|y_p - y_{ref}\|$ and threshold $\gamma_s\|d\|$.

The simulation results for Case 1 are presented in Fig. 2, and it is clear that $y_p = y_c$, $u_p = u_c$, $|\tilde{y}_c\| \leq \gamma_s\|d\|$ and $\|y_p - y_{ref}\| \leq \gamma_s\|d\|$. Hence the nominal controller (8) can guarantee the acceptable performance (11) and there are no false alarms.

The simulation results for Case 2 are presented in Fig. 3. Comparing with Fig. 2, it can be seen that the controller inputs $y_{c,i}, i = 1, 2$ and the controller outputs $u_{c,i}, i = 1, 2$ have no changes, hence $|\tilde{y}_c\| \leq \gamma_s\|d\|$ namely a missing alarm occurs (covert attacks are masked); but the system outputs $y_{p,i}, i = 1, 2$ and the system inputs $u_{p,i}, i = 1, 2$ undergo substantial changes for $t \geq T_a$ hence $\|y_p - y_{ref}\| > \gamma_s\|d\|$ for $t > T_a$ and the acceptable performance (11) cannot be ensured.

To reveal covert attacks, the signal generators are constructed in Case 3 whose simulation curves correspond to Fig. 4. Comparing Fig. 4 to Fig. 3, it is clear that both the controller inputs $y_{c,i}, i = 1, 2$ and the controller outputs $u_{c,i}, i = 1, 2$ change substantially for $t \geq T_a$; $|\tilde{y}_c\| > \gamma_s\|d\|$ for $t > T_d = 15.01s$ (namely covert attacks are unmasked); however $\|y_p - y_{ref}\| > \gamma_s\|d\|$ since the nominal controller is still used.

In Case 4, the proposed secure controller is adopted and simulation plots are presented in Fig. 5, where $\|y_p - y_{ref}\| \leq \gamma_s\|d\|$, which shows the effectiveness of the proposed secure controller.

V. Conclusion

In this paper, an active secure control scheme including attack detection and secure control has been proposed. It has been shown that covert attacks cannot be detected with the classical methods since the signals received by the controller undergo no changes before and after covert attacks. In order to unmask such attacks, signal generators are constructed in both layers, and judicious extra signals have been inserted into the network as soon as the Cyber-Physical System (CPS) begins operation. A secure controller, based on an adaptive observer, has been designed to maintain a certain level of tracking performance even in the presence of attacks. The learning observer's estimation precision does not impact control effectiveness; its role is to mitigate the impact of covert attacks. The paper also includes numerical simulations that demonstrate the effectiveness of the proposed scheme. Future research will explore managing the transition between nominal and secure controllers, consider more complex control performance indicators, and system modeling. These topics are currently under investigation.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61973197 and the Shaanxi Provincial Natural Science Basic Research Program Project under Grant 2019JLZ-06.

Appendix

The proof of Proposition 1

The invariant zeros of (A_x, B_x, C_x) are given by the values of λ that make its Rosenbrock matrix (denoted by $\mathcal{R}_x := \begin{bmatrix} \lambda\mathbf{I}_{3n} - A_x & B_x \\ C_x & \mathbf{0} \end{bmatrix}$) lose rank [13]. Using the partitions in (30), it follows that

$$\mathcal{R}_x = \begin{bmatrix} \lambda\mathbf{I}_n - A_o & -BK_n & -L_nC & B \\ \mathbf{0} & \lambda\mathbf{I}_n - A_d & L_nS_pC & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \lambda\mathbf{I}_n - A & B\alpha^{-1} \\ C & \mathbf{0} & -C & \mathbf{0} \end{bmatrix} \tag{60}$$

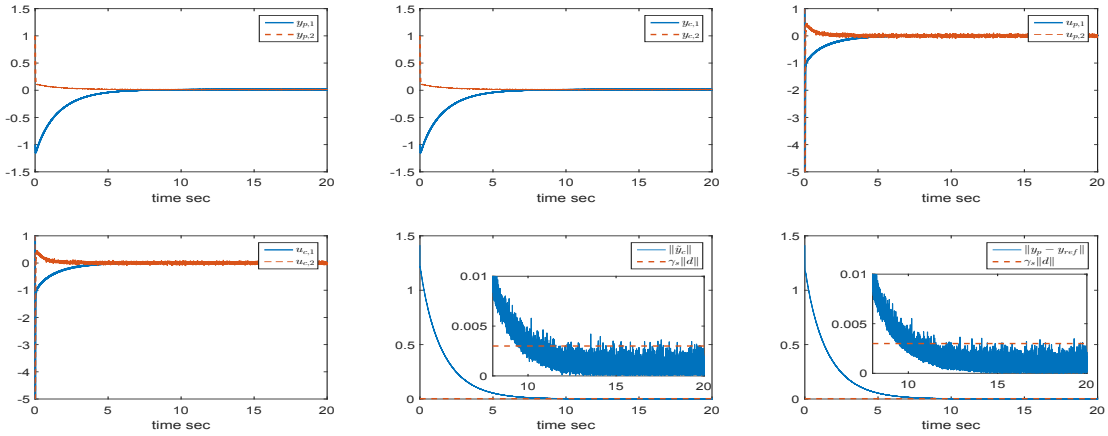

Fig. 2. Simulation curves for Case 1.

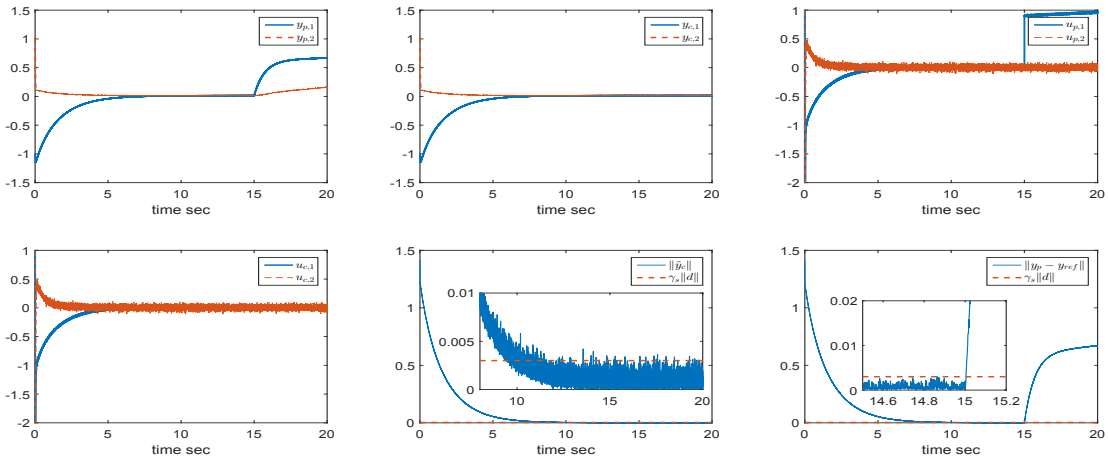

Fig. 3. Simulation curves for Case 2.

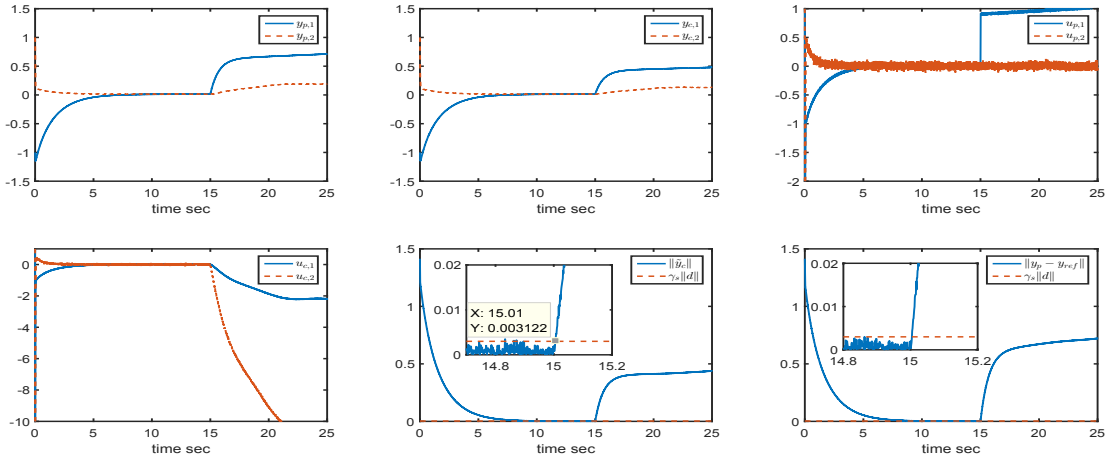

Fig. 4. Simulation curves for Case 3.

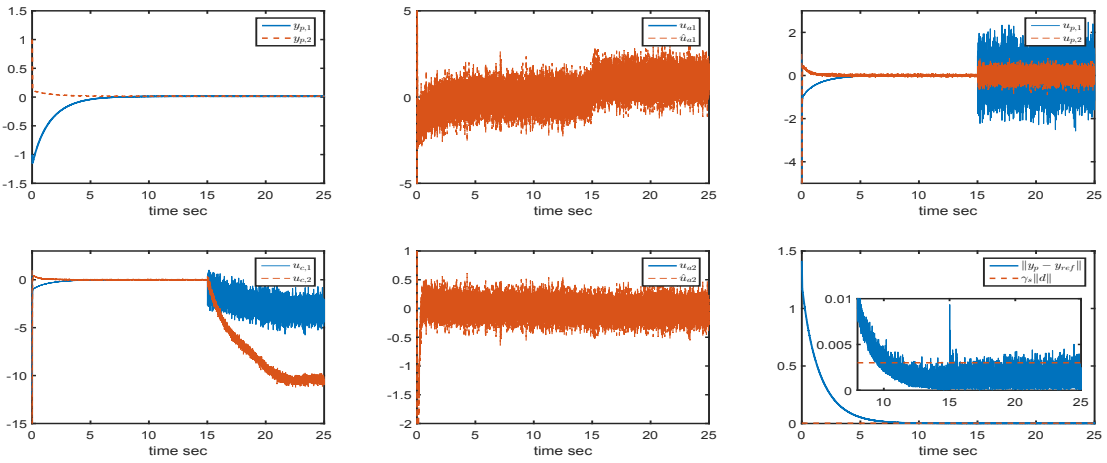

Fig. 5. Simulation curves for Case 4.

Define $T_R^1 = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ \mathbf{I}_n & \mathbf{0} & \mathbf{I}_n & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_m \end{bmatrix}$,

$T_R^2 = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_n & \mathbf{0} \\ \mathbf{0} & K_n\alpha/s & \mathbf{0} & \mathbf{I}_m \end{bmatrix}$, $T_R^3 = \begin{bmatrix} \mathbf{I}_n & -1/s\mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_n & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_m \end{bmatrix}$, $T_L^1 = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ -\mathbf{I}_n & \mathbf{0} & \mathbf{I}_n & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_p \end{bmatrix}$,

$T_L^2 = \begin{bmatrix} \mathbf{I}_n & 1/s\mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_n & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_p \end{bmatrix}$, $T_L^3 = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_n & L_n \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_p \end{bmatrix}$, $T_L^4 = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{0} & sL_n \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_n & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_p \end{bmatrix}$

then

$$\begin{aligned} & \operatorname{rank}(\mathcal{R}_x) \\ = \ & \operatorname{rank}(T_L^4 T_L^3 T_L^2 T_L^1 \mathcal{R}_x T_R^1 T_R^2 T_R^3) \\ = \ & \operatorname{rank}\left(\left[\begin{array}{cc|cc} \lambda\mathbf{I}_n - A_o & \mathbf{0} & \mathbf{0} & B \\ sL_nC & \lambda\mathbf{I}_n - A_c & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \lambda\mathbf{I}_n - A & -Bs/\alpha \\ \mathbf{0} & \mathbf{0} & -C & \mathbf{0} \end{array}\right]\right) \end{aligned}$$

From Assumption 3, $\begin{bmatrix} \lambda\mathbf{I}_n - A & -Bs/\alpha \\ -C & \mathbf{0} \end{bmatrix}$ is full of column rank for any λ that lies in $\mathcal{C}_+$ namely the right complex plane. From Remark 3, it is known that the values of λ that make $\lambda\mathbf{I}_n - A_o$ and $\lambda\mathbf{I}_n - A_c$ lose rank are both lie in $\mathcal{C}_-$ namely the left complex plane. Hence (A_x, B_x, C_x) is minimum phase. From $C_xB_x = (s/\alpha)CB$ and Assumption 2, it is known that when $s \neq 0$, $\operatorname{rank}(C_xB_x) = \operatorname{rank}(B_x)$. □

References

[1] S. Tan, J. M. Guerrero, P. Xie, *et al*. "Brief Survey on Attack Detection Methods for Cyber-Physical Systems," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5329–5339, 2020.

[2] D. Ding, Q. L. Han, X. Ge, J. Wang. "Secure State Estimation and Control of Cyber-Physical Systems: A Survey," *IEEE Trans. Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 176–190, 2021.

[3] D. Mikhaylenko, P. Zhang. "Stealthy local covert attacks on cyber-physical systems," *IEEE Trans. Automatic Control*, vol. 67, no. 12, pp. 6778–6785, 2022.

[4] R. S. Smith. "Covert misappropriation of networked control systems: Presenting a feedback structure," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 82–92, 2015.

[5] C. Schellenberger, P. Zhang. "Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system," *Proc. the 56th IEEE Conference on Decision and Control (CDC),* Melbourne, Australia, 2017, pp. 1374–1379.

[6] S. Weerakkody, B. Sinopoli. "Detecting integrity attacks on control systems using a moving target approach," *Proc. the 54th IEEE Conference on Decision and Control (CDC),* Osaka, Japan, 2015, pp. 5820–5826.

[7] A. Hoehn, P. Zhang. "Detection of covert attacks and zero dynamics attacks in cyber-physical systems," *Proc. 2016 American Control Conference (ACC),* Boston, MA, USA, 2016, pp. 302–307.

[8] Z. Wu, E. Tian, H. Chen. "Covert Attack Detection for LFC Systems of Electric Vehicles: A Dual Time-Varying Coding Method," *IEEE/ASME Trans. Mechatronics*, vol. 28, no. 2, pp. 681–691, 2023.

[9] D. Zhao, Y. Lv, J. Zhou, *et al*. "Attack-isolation-based resilient control of large-scale systems against collusive attacks," *IEEE Trans. Network Science and Engineering*, vol. 9, no. 4, pp. 2857–2869, 2022.

[10] A. Barboni, T. Parisini. "Towards distributed accommodation of covert attacks in interconnected systems," *Proc. the 59th IEEE Conference on Decision and Control (CDC),* Jeju, Korea (South), 2020, pp. 5731–5736.

[11] F. Tedesco, D. Famularo, G. Franze. "A resilient control strategy for networked multi-agent systems subject to covert attacks," *Transactions of the Institute of Measurement and Control*, no. 01423312211021295, 2021.

[12] M. Fauser, P. Zhang. "Resilience and detection of cyber-physical systems to covert attacks by exploiting Frequency Hopping Spread Spectrum," *Proc. 2021 American Control Conference (ACC),* online, 2021, pp. 4631–4636.

[13] C. P. Tan, F. Crusca, M. Aldeen. "Extended results on robust state estimation and fault detection," *Automatica*, vol. 44, no. 8, pp. 2027–2033, 2008.

[14] J. K. Goyal, S. Aggarwal, P. R. Sahoo, *et al*. "Design of Robust PID Controller using Static Output Feedback framework," *IFAC-PapersOnLine*, vol. 53, no. 1, pp. 13–18, 2020.

[15] J. Lan, R. J. Patton. "Integrated fault estimation and fault-tolerant control for uncertain Lipschitz nonlinear systems," *Int. J. Robust and Nonlinear Control*, vol. 27, no. 5, pp. 761–780, 2017.

[16] T. Yucelen, A. J. Calise. "Derivative-free model reference adaptive control," *J. Guidance, Control, and Dynamics*, vol. 34, no. 4, pp. 933–950, 2011.
[17] Q. Jia, W. Chen, Y. Zhang, H. Li. "Integrated design of fault reconstruction and fault-tolerant control against actuator faults using learning observers," *Int. J. Systems Science*, vol. 47, no. 16, pp. 3749–3761, 2016.
[18] F. Hou, J. Sun. "Covert attacks against output tracking control of cyber-physical systems," *Proc. the 43rd Annual Conference of the IEEE Industrial Electronics Society (IECON 2017)*, Beijing, China, 2017, pp. 5743–5748.
[19] S. B. Rebai, H. Voos, M. Darouach. "Attack-tolerant control and observer-based trajectory tracking for Cyber-Physical Systems," *European J. Control*, vol. 47, pp. 30–36, 2019.
[20] A. Barboni, H. Rezaee, F. Boem, *et al*. "Detection of covert cyber-attacks in interconnected systems: A distributed model-based approach," *IEEE Trans. Automatic Control*, vol. 65, no. 9, pp. 3728–3741, 2020.
[21] X. Ge, Q. L. Han, M. Zhong, *et al*. "Distributed Krein space-based attack detection over sensor networks under deception attacks," *Automatica*, vol. 109, no. 108557, 2019.

Xianghua Wang received the B.E. degree in Automation from Northwestern Polytechnical University, Xi'an, China, in 2010 and the Ph.D. degree in Mechanical System and Control from Peking University, Beijing, China, in 2015. She is currently an associate professor at Beijing University of Posts and Telecommunications. Her current research interests include fault diagnosis, fault tolerant control, guidance and control. She authored or co-authored 1 book and more than 60 papers.

Ali Zolghadri received his PhD from the University of Bordeaux, France C and has been a Full Professor of Control Systems Engineering there since 2003. His current research interests are centered around autonomy, resilience and safety/(cyber)security of cyber-physical systems. He is member of International Technical Committees "SafeProcess" and "Aerospace" of IFAC C IEEE senior member, and TC member of EuroGNC (Council of European Aerospace societies). He has served as IPC member for various international conferences, and has delivered a number of plenary lectures and other invited talks at venues worldwide. He is an Associate Editor of the "Journal of the Franklin Institute" (Elsevier, USA) and "Complex Engineering Systems" journal C and Editorial Board member of "Aerospace Science and Engineering", MDPI (Switzerland). He is author/co-author of more than 260 publications in archive journals, refereed conference proceedings and technical book chapters, and co-holder of 15 patents in aerospace. He is the recipient of CNRS Medal of Innovation 2016 which rewards C considering all fields and subfields of research C "outstanding scientific research with innovative applications in the technological and societal fields".

Changqing Wang received the B.E. degree in Mechanical Design and Automation from Northwestern Polytechnical University, Xi'an, China, in 1996 and the Ph.D. degree in System Analysis and Control from Moscow Power Engineering Institute, Moscow, Russia, in 2006. His is currently a professor at Northwestern Polytechnical University. His current research directions include fault-tolerant control, navigation, and control. He has authored or co authored 1 book and more than 40 papers.