Resilient Control of Cyber-Physical System Using Nonlinear Encoding Signal Against System Integrity Attacks

Youngjun Joo, *Member, IEEE*, Zhihua Qu, *Fellow, IEEE*, and Toru Namerikawa, *Senior Member, IEEE*

***Abstract*—In this paper, we propose an attack resilient control structure for a cyber-physical system (CPS) to enhance the CPS security against stealthy system integrity attacks that manipulate the state of the physical plant while undetected. With the help of nonlinear encoding/decoding components, the proposed structure can detect stealthy attacks and preserve the nominal performance without considering attacks. Meanwhile, for avoiding the eavesdropping of transmitted signals used to synchronize encoding/decoding components between the physical and cyber layers, the chaotic oscillators are employed for the secure communication. The resilience against the malicious attacks and the robustness under the time delay and nonlinear components of the proposed CPS structure are investigated in view of input-to-state stable (ISS) framework. Simulations for Quadruple-Tank Process are performed to validate the performance of the proposed method.**

***Index Terms*—attack resilient control, chaotic oscillator, cyber-physical system, system integrity attack**

I. Introduction

With the progress of computing and communication technologies, diverse IT infrastructures across the different system layers and heterogeneous physical plants are integrated to improve efficiency. Such a cyber-physical framework, called as a cyber-physical system (CPS), has been applied to many industrial fields including the smart grids, health-care systems, and autonomous vehicles [1]–[3]. However, by increasing the complexity of the network, the vulnerability of CPS from malicious attackers is escalated. For example, it has been reported that such attacks caused severe damage to critical infrastructure. The Natanz uranium enrichment facility in Iran was infected by Stuxnet malware. Infected programmable logic controllers (PLC) damaged around $1,000$ centrifuges by increasing their rotational speed while the recorded data was transmitted to legitimate controllers for hiding those changes from operators [4]. In 2015, cyber attacks on the Ukraine power grid compromised three regional distribution companies and it led to a six-hour blackout. Adversaries gathered information on valid credentials via the BlackEnergy 3 malware, manipulated the Supervisory Control and Data Acquisition (SCADA) systems, and interrupted reports of outages [5].

Although numerous cyber attack scenarios including DoS, random, replay, and bias injection attacks have been studied [6], [7], they become more dexterous and, sometimes, spend lots of time and effort to inflict critical damage on physical components. Based on information about the physical plant, stealthy system integrity attack scenarios by compromising actuators and sensors for manipulating the state of the plant while evading attack detection components have been actively studied. Attack strategies for electric power grids and their prevention have been investigated in [8]–[10] and it has been extended to dynamical discrete-time systems [11]–[14]. The works in [15], [16] presented stealthy attack strategies for continuous-time systems based on the frequency domain approach. Since attack vectors are designed by intelligent adversaries for deceiving the anomaly of CPS, their detection is hard to accomplish by the classical fault detection approaches [17]. For protecting CPS against such attacks, active attack detection methods such as a control input redesign technique using a physical watermarking [18], [19] and a moving target approach by adding additional dynamics [20] have been discussed. These techniques may increase the installation cost or degrade the control performance during normal operations (absent of cyber attacks). To cope with these shortcomings, an approach of coding the control input or sensor output with a scaling factor to modify system matrices has been presented [21], [22]. While this approach represents an effort of hiding system information, a patient attacker can decode the information based on system identification techniques. Finally, for multi-agent systems, a robust control design against attacks is developed [23]–[25] using competitive interaction to ensure both robustness against attacks and nominal performance.

This paper deals with attack-aware control problems for CPS under stealthy system integrity attacks. The main technical developments and contributions are: 1) the class of stealthy system integrity attack strategy, which drives the physical plant to an unsafe state without being detected, is identified; 2) by embedding encoding/decoding components of chaotic signals, an attack-aware control structure is presented to detect any system integrity attack and to preserve the nominal control performance in the absence of attacks; 3) both resilience against attacks and robustness with respect to time delay are explicitly established using the input-to-state stable (ISS) framework.

The rest of this paper is as follows: Section II introduces

This work is supported in part by US National Science Foundation under grants ECCS-1927994 and ECCS-1308928, by US Department of Energy's awards DE-EE0009152, DE-EE0009028, DE-EE0007998, DE-EE0007327 and DE-EE0006340, by US Department of Transportation's award DTRT13-G-UTC51, and by a grant from Florida Center for Cybersecurity.

Y. Joo is with the Advanced Robotics Lab., CTO Division, LG Electronics, Seoul, 06772, South Korea (e-mail: youngjun.joo@lge.com).

Z. Qu is with the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32816 USA (e-mail: qu@ucf.edu).

T. Namerikawa is with the Department of System Design Engineering, Keio University, Kanagawa 223-8522, Japan (e-mail: namerikawa@sd.keio.ac.jp).

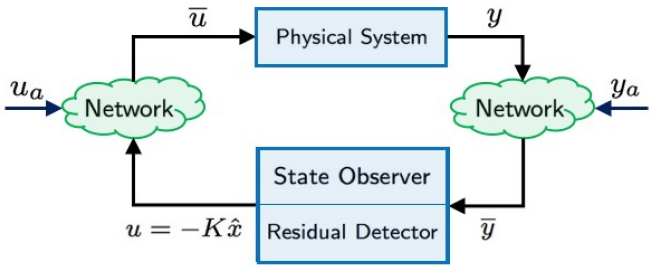

Fig. 1. CPS configuration of networked control system

the CPS configuration and the system integrity attack strategy. In Section III, the resilient CPS structure and its robustness are presented. Section IV further investigates the effect of time delay and the security of the communication network. Simulations for Quadruple-Tank Process are performed to validate the performance of the proposed method in Section V. Finally, we conclude this paper in Section VI.

Notations: For matrix A, A^T and A^{-1} denote the transpose and the inverse of A, and $\lambda_{\min}(A)$ and $\lambda_{\max}(A)$ represent the smallest and largest eigenvalues of A, respectively. I_n and $0_{m\times n}$ denote the $n\times n$ identity and $m\times n$ zero matrices, respectively. Superscript or subscript would be omitted if there is no danger of confusion.

II. CPS and System Integrity Attacks

In this section, a cyber-physical system (CPS) configuration is used to represent a dynamic system controlled over communication network, and the standard approach of using measurement-based residual test to verify the overall system integrity is introduced as the baseline. An intelligent attacker who has the information of the plant model can launch the so-called *system integrity attack* [6], [7], [11]–[13], [15], [16], a coordinated input-output attack by injecting appropriately designed simultaneous attack vectors into both control input and output measurement channels. It is shown that such an attack could arbitrarily manipulate the state of the system while passing the test of any output-measurement residual-based attack detection. Detection as well as resilience of the overall control under system integrity attacks are the focus of this paper, and we begin by discussing attack scenarios.

A. Cyber-Physical System Configuration

The CPS configuration, depicted in Fig. 1, is composed of a physical plant, a remote monitoring/control station (including a state observer, a residual detector, and an observer-based feedback control), and their communication network. In this paper, the class of linear time-invariant plants is considered:

$$\dot{x} = Ax + B\overline{u}, \qquad y = Cx, \tag{1}$$

where $x \in \mathbb{R}^n$ is the plant state, $\overline{u} \in \mathbb{R}^m$ is the actual control signal received at the plant, and $y \in \mathbb{R}^p$ is the plant output. The triplet (A,B,C) is assumed to be controllable and observable.

At the control station, the observer-based state feedback control is given by

$$\dot{\hat{x}} = A\hat{x} + Bu + L(\overline{y} - \hat{y}), \qquad \hat{y} = C\hat{x}, \qquad u = -K\hat{x}, \tag{2}$$

where $u \in \mathbb{R}^m$ is the control input designed, $\overline{y} \in \mathbb{R}^p$ is the output measurement received, $\hat{x} \in \mathbb{R}^n$ is the state estimate, and $\hat{y} \in \mathbb{R}^p$ is the output estimate. It is assumed that gain matrices K and L are chosen such that $(A-BK)$ and $(A-LC)$ are Hurwitz and the desired performance is achieved under the nominal operation (i.e., $\overline{u} = u$ and $\overline{y} = y$).

A baseline detection algorithm is implemented to monitor the plant behavior at the controller side for detecting the abnormality of the system. Using the information of output residual $z = (\overline{y} - \hat{y})$, any of standard fault detectors such as those in [17] can be employed to determine the operational status according to the following test:

$$\begin{cases} \|Wz\| \le \mu: & \text{normal operation} \\ \|Wz\| > \mu: & \text{abnormal operation} \end{cases}, \tag{3}$$

where W is an invertible weighting matrix, and $\mu \ge 0$ is the threshold to be chosen by the control center staff.

If an attacker gains access to the communication network, both the control input and measurement output may be corrupted. Accordingly, the plant input and the measurement vector are in general denoted as $\overline{u} = u + u_a$ and $\overline{y} = y + y_a$ where $u_a \in \mathbb{R}^m$ and $y_a \in \mathbb{R}^p$ are the input and output attack vectors, respectively. The class of perfectly stealthy attacks will be investigated in the next subsection.

B. Perfect Stealthy Attacks of System Integrity

Resilience of control systems needs to be investigated for various attack scenarios, including DoS, replay attack, and false data injection attacks [6], [7]. The following class of system integrity attacks is arguably the worst kind.

Assumption 1: An attacker capable of launching the system integrity attack is assumed to have the full information of matrices A, B, and C in model (1) and to have gained access to the communication network to inject u_a and y_a.

Compared to those attack models in [6], [7], [11]–[13], [15], [16], assumption 1 does not necessarily involve any real-time information of the plant state, or the control input, or any other information at the control station (*e.g.,* K and L). Consider the following nominal system of (1) and (2) absent of attack (*i.e.,* $u_a = y_a = 0$):

$$\begin{aligned} \dot{x}_n &= Ax_n + Bu_n, & u_n &= -K\hat{x}_n, & y_n &= Cx_n, \\ \dot{\hat{x}}_n &= A\hat{x}_n + Bu_n + Lz_n, & z_n &= y_n - \hat{y}_n, & \hat{y}_n &= C\hat{x}_n. \end{aligned} \tag{4}$$

where $x_n/\hat{x}_n$, u_n, $y_n/\hat{y}_n$, and z_n are the plant/control state, input, plant/control output, and output residual of the nominal system, respectively. Then, the state of the system can be decomposed into the nominal state and the perturbation induced by the attack vectors as $e_a = x - x_n$, $\hat{e}_a = \hat{x} - \hat{x}_n$, and $z_a = z - z_n$.

Definition 1: An attack is said to be *stealthy* if the residual detector (3) fails to detect its presence (*i.e.,* $\|Wz(t)\| \le \mu$). In addition, the attack is said to be *perfectly stealthy* if it is stealthy with $z_a(t) = 0$.

With respect to the baseline detection algorithm (3), the following lemma provides a perfect stealthy attack strategy for continuous-time linear systems in the form of (1).

Lemma 1: Consider the CPS in the form of (1), (2), and (3). Under assumption 1, the system integrity attack is perfect stealthy if the attack vectors u_a and y_a are generated by

$$\begin{aligned} \dot{x}_a &= Ax_a + Bu_a, & x_a(t_0) &= 0, \\ u_a &= -K_a x_a + Hy + r_a, & y_a &= -Cx_a, \end{aligned} \tag{5}$$

where $x_a \in \mathbb{R}^n$ is the state of the attack model, K_a and H are any matrices, and $r_a \in \mathbb{R}^m$ is any exogenous injection (with $r_a(t) = 0$ for $t \in [0, t_0]$ and for some starting time t_0).

Proof: Given the attack model (5), the overall perturbed system becomes

$$\begin{aligned} \dot{x} &= (A - BK + BHC)x + BK(x - \hat{x}) - BK_a x_a + Br_a, \\ \dot{\hat{x}} &= (A - BK)\hat{x} + LC(x - \hat{x}) - LCx_a, \\ \dot{e}_a &= (A - BK)e_a + BK(e_a - \hat{e}_a) - BK_a x_a + BHCx + Br_a, \\ \dot{\hat{e}}_a &= (A - BK)\hat{e}_a + LC(e_a - \hat{e}_a) - LCx_a, \\ \dot{x}_a &= (A - BK_a)x_a + BHCx + Br_a, \\ z_a &= C(e_a - \hat{e}_a - x_a), \end{aligned}$$

in which $e_a(t) = \hat{e}_a(t) = 0$ and $z_a(t) = 0$ for $t \in [0, t_0]$. Applying the state transformation $w = e_a - \hat{e}_a - x_a$, we have the following transformed state equation as

$$\dot{w} = (A - LC)w, \qquad z_a = Cw.$$

Since $w(t_0) = 0$ and $(A - LC)$ is Hurwitz, $w(t) = 0$ and $z_a(t) = 0$ for all $t \in [0, \infty)$. The latter says that $z(t) = z_n(t)$ for all $t \in [0, \infty)$; that is, the measurement residual remains unchanged in the presence of system integrity attack in the form of (5), which concludes the proof. ■

Implementation and impacts of perfect stealthy attacks depend upon *a priori* knowledge about the CPS. If strategy (5) is implemented with $H = 0$, the attack requires only information of system matrices. This case is an open-loop attack, or simply a bad data attack. Exogenous injection r_a can be used to change the equilibrium point of the plant state x and, should the attacker intend to make the plant state become unbounded, K_a can be selected such that $(A - BK_a)$ is unstable (in which case the attack vectors of u_a and y_a become unbounded). In order to make the dynamics of the overall system unstable without using an unstable attack model, strategy (5) can be implemented with $H \neq 0$ being chosen such that matrix $(A - BK + BHC)$ is unstable. In the latter case, the attacker needs to know not only system matrices but also real-time measurement of the plant output. On the other hand, among various system integrity attacks, the zero dynamics attack has been actively researched in literature [21], [26]. It aims to keep $y = y_n$ (*i.e.,* in view of strategy (5), the attack design is reduced to find an input attack vector $u_a = -K_a x_a$ so as to excite the unstable part of zero dynamics while $y = y_n$) whereas the objective of the system integrity attack in Lemma 1 is $z = z_n$, and thus the former is a subclass of the latter.

The above analysis shows that, by adopting the perfect stealthy attack strategy (5), the attacker can not only change the steady state value but also manipulate the dynamic response of the physical plant while evading any residual-based detection. It is worth noting that attack strategy (5) generalizes the discrete-time strategies proposed in [12] and, in the noisy setting, it has similar properties as those in [12].

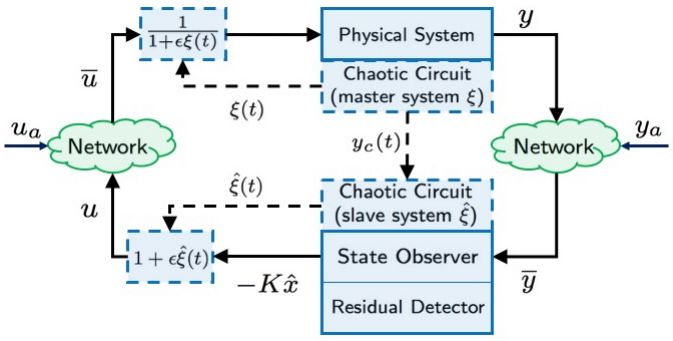

Fig. 2. Protection of CPS by embedding nonlinear components

III. Resilient Control by Nonlinear Dynamic Encoding/Decoding

This section provides an attack-aware control structure to detect various suspicious operations including the system integrity attack while achieving the attack resilience and the nominal control performance. At the control station side, the control input is encoded by a time-varying function generated by a nonlinear circuit, transmitted via the communication network, and, at the plant side, decoded using another nonlinear circuit. Moreover, to prevent eavesdropping, the nonlinear circuits used in encoding/decoding are chosen to be chaotic oscillators with a synchronization signal securely communicated via a separate network. It will be shown that the system integrity attack can be effectively detected by the proposed structure and that the overall system is resilient against attacks.

A. Embedment of Nonlinear Dynamic Components

As shown in Fig. 2, standard attack detection algorithms can be enhanced by using nonlinear encoding/decoding components, which are two chaotic oscillators embedded into CPS and linked through a separate scalar secure communication. The chaotic oscillator at the plant site is the master circuit, and the other at the control station serves as the slave[1]. This scheme is completely scalable for networked physical systems as the master signal can be multi-cast to all physical subsystems equipped with their own slaves. Securing a scalar signal is much easier to accomplish than attempting to secure all or some of the control and output signals (of higher dimensions and at different locations).

The proposed resilient CPS structure is composed of a physical plant given by

$$\dot{x} = Ax + \frac{1}{1 + \varepsilon\xi} B\overline{u}, \qquad y = Cx, \qquad \overline{u} = u + u_a, \tag{6}$$

where ε is a positive design constant (to ensure that $\varepsilon|\xi| \leq 0.5$), $\xi \in \mathbb{R}$ is the *dynamic decoding signal* generated by the master chaotic circuit (to be defined subsequently), and an observer-based state feedback control designed as

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + \frac{1}{1 + \varepsilon\hat{\xi}} Bu + L(\overline{y} - \hat{y}), \\ u &= -[1 + \varepsilon\hat{\xi}]K\hat{x}, \qquad \hat{y} = C\hat{x}, \qquad \overline{y} = y + y_a, \end{aligned} \tag{7}$$

[1] Alternatively, the master circuit could also be placed at the control station.

where $\hat{\xi} \in \mathbb{R}$ is the *dynamic encoding signal* generated by the slave circuit, and $\varepsilon|\hat{\xi}| \leq 0.5$. The dynamic encoding/decoding signal pair and their nonlinear embedment into system/control equations (6) and (7) are the key of the proposed resilient control design against attacks.

The output of the master circuit is sent as the *circuit synchronization signal* y_c to the slave circuit(s) in order to synchronize their corresponding states. Upon achieving synchronization (*i.e.,* as $\lim_{t\to\infty}|\xi(t)-\hat{\xi}(t)| \to 0$), the proposed resilient CPS of (6) and (7) recovers the nominal performance of the original linear CPS of (1) and (2). Instead of the proposed structure in (6), a method of encoding the input matrix as $\tilde{B} = \alpha B$ with a secured scaling factor α has been discussed [21]. But, a patient attacker can easily eavesdrop and decode such information by using a system identification technique. On the other hand, outputs of chaotic circuits cannot be decoded (or synchronized) without the full knowledge of its specific class and associated internal parameters; and without the real-time information of such nonlinear signals, sophisticated attackers cannot imitate the plant behavior properly or deceive the residual detector. To further enhance robustness, circuit synchronization signal y_c could be sent through a communication channel (e.g., using a software defined network) separate from the communication network transmitting the control and output vectors of the physical plant. In short, the proposed robustification prevents anyone from decoding the dynamic coded control signal except for the intended receiver.

B. Choices of Circuits and Dynamic Signals

In Fig. 2, the master/slave pair can be chosen to be any of various types of chaotic oscillators, as long as they can be synchronized using an output feedback. Chua's circuit is one such candidate and, in the rest of the paper, it is used as the master and slave circuits since it is easy to implement [27]–[29]. Specifically, the master circuit is composed of inductor L_1, two resistors R_1 and R_2, two capacitors C_1 and C_2, and a nonlinear element $g(\cdot)$. Its dynamic equations are given by

$$\begin{aligned} C_1\dot{v}_1 &= \frac{1}{R_1}(v_2 - v_1) - g(v_1), \\ C_2\dot{v}_2 &= \frac{1}{R_1}(v_1 - v_2) + I, \\ L_1\dot{I} &= -v_2 - R_2 I, \qquad\qquad y_c = v_1, \end{aligned} \tag{8}$$

where $v_1 \in \mathbb{R}$, $v_2 \in \mathbb{R}$, and $I \in \mathbb{R}$ are the voltage across C_1, the voltage across C_2, and the current through L_1, respectively,

$$g(v_1) = \begin{cases} \overline{d}v_1 + (\overline{d} - \underline{d})E & \text{if } v_1 \leq -E, \\ \underline{d}v_1 & \text{if } |v_1| < E, \\ \overline{d}v_1 + (\underline{d} - \overline{d})E & \text{if } v_1 \geq E, \end{cases} \tag{9}$$

and $\underline{d} < -1/(R_1 + R_2) < \overline{d} < 0$ and $E > 0$ are constants. Similarly, the slave circuit is described as

$$\begin{aligned} C_1\dot{\hat{v}}_1 &= \frac{1}{R_1}(\hat{v}_2 - \hat{v}_1) - g(\hat{v}_1) + l_c(y_c - \hat{y}_c), \\ C_2\dot{\hat{v}}_2 &= \frac{1}{R_1}(\hat{v}_1 - \hat{v}_2) + \hat{I}, \\ L_1\dot{\hat{I}} &= -\hat{v}_2 - R_2\hat{I}, \qquad\qquad \hat{y}_c = \hat{v}_1, \end{aligned} \tag{10}$$

where $l_c > 0$ is the coupling gain to be chosen, $\hat{v}_1 \in \mathbb{R}$, $\hat{v}_2 \in \mathbb{R}$, and $\hat{I} \in \mathbb{R}$ are the estimates of v_1, v_2, and I, respectively. Defining the corresponding estimation error variables as $\tilde{v}_1 = v_1 - \hat{v}_1$, $\tilde{v}_2 = v_2 - \hat{v}_2$, and $\tilde{I} = I - \hat{I}$, we have the following error system:

$$\begin{aligned} C_1\dot{\tilde{v}}_1 &= \frac{1}{R_1}(\tilde{v}_2 - \tilde{v}_1) - \{g(v_1) - g(\hat{v}_1)\} - l_c\tilde{v}_1, \\ C_2\dot{\tilde{v}}_2 &= \frac{1}{R_1}(\tilde{v}_1 - \tilde{v}_2) + \tilde{I}, \\ L_1\dot{\tilde{I}} &= -\tilde{v}_2 - R_2\tilde{I}. \end{aligned} \tag{11}$$

While Chua's circuits have been studied in terms of their uniform boundedness [27], [28] and convergence [29], the following lemma provides the specific results needed for the subsequently development.

Lemma 2: Consider the circuit dynamics in (8) and (10). Then, design parameters R_1, R_2, L_1, C_1, C_2, $\underline{d}$, $\overline{d}$, and E and initial conditions of the circuit can be chosen such that all the master circuit variables are both chaotic and uniformly bounded as, denoting $x_c = [v_1\ v_2\ I]^T$,

$$\|x_c(t)\| \leq M_c. \tag{12}$$

where M_c is a positive constant. Furthermore, if gain l_c is chosen such that

$$l_c \geq (1/R_1) - \underline{d} + \beta \tag{13}$$

for some $\beta > 0$, then the circuit error system (11) is exponentially stable, and the circuit state estimate is bounded as

$$\|\hat{x}_c(t)\| \leq M_c + M_1\|\tilde{x}_c(t_0)\|e^{-\alpha_c t}, \tag{14}$$

where $\hat{x}_c = [\hat{v}_1\ \hat{v}_2\ \hat{I}]^T$, $\tilde{x}_c = x_c - \hat{x}_c$,

$$\alpha_c = \min\left\{\frac{2\beta}{C_1}, \frac{1}{R_1C_2}, \frac{2R_2}{L_1}\right\}, \quad M_1 = \sqrt{\frac{\max\{C_1, C_2, L_1\}}{\min\{C_1, C_2, L_1\}}}.$$

Proof: Uniform boundedness under appropriate choices of initial conditions and design parameters have been shown in [27], [28]. To show exponential convergence of synchronization error system (11), consider quadratic Lyapunov function

$$V_c = \frac{1}{2}\left[C_1\tilde{v}_1^2 + C_2\tilde{v}_2^2 + L_1\tilde{I}^2\right]. \tag{15}$$

It follows from (13) that

$$\dot{V}_c \leq -\beta\tilde{v}_1^2 - \frac{1}{2R_1}\tilde{v}_2^2 - R_2\tilde{I}^2 \leq -\alpha_c V_c, \tag{16}$$

which yields

$$\|\tilde{x}_c(t)\| \leq M_1\|\tilde{x}_c(t_0)\|e^{-\alpha_c t}. \tag{17}$$

Recalling the definition of $\tilde{x}_c$ yields the bound on $\hat{x}_c$, which completes the proof. ■

Upon choosing chaotic circuits and understanding their properties of uniform boundedness and synchronization, we can make choices of dynamic signals. As mentioned before, dynamic synchronization signal should be the output of the master circuit, i.e., $y_c = v_1$. The pair of dynamic encoding and decoding signals has multiple choices, in particular,

$$\xi = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 I, \quad \hat{\xi} = \lambda_1\hat{v}_1 + \lambda_2\hat{v}_2 + \lambda_3\hat{I}, \tag{18}$$

where $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$. Special cases of such choices include:

- $\xi = v_1$ (and $\hat{\xi} = \hat{v}_1$);
- $\xi = v_2$ (and $\hat{\xi} = \hat{v}_2$);
- $\xi = I$ (and $\hat{\xi} = \hat{I}$).

Upon making any specific choices of dynamic signals in the form of (18), we need to choose ε to satisfy the requirements $\varepsilon|\xi| \leq 0.5$ and $\varepsilon|\hat{\xi}| \leq 0.5$. This can be done by providing estimates of initial conditions $x_c(t_0)$ and $\hat{x}_c(t_0)$ and by determining the value of ε using (12) and (14). In the next section, impact and performance of incorporating these dynamic signals into the CPS configuration will be analyzed.

C. Performance and Robustness

Dynamics of plant (6) and control station (7) can be expressed as

$$\begin{aligned} \dot{x} &= (A-BK)x + BKe + \frac{\varepsilon\tilde{\xi}}{1+\varepsilon\xi}BK(x-e) + \frac{1}{1+\varepsilon\xi}Bu_a, \\ \dot{e} &= (A-LC)e + \frac{\varepsilon\tilde{\xi}}{1+\varepsilon\xi}BK(x-e) + \frac{1}{1+\varepsilon\xi}Bu_a - Ly_a, \end{aligned} \tag{19}$$

where $e = x - \hat{x}$ is the plant state estimation error, and $\tilde{\xi} = \xi - \hat{\xi}$ is the error between decoding and encoding signals. From the baseline design for gain matrices K and L, there exist positive definite matrices P_s and P_o such that $(A-BK)^T P_s + P_s(A-BK) = -2I$ and $(A-LC)^T P_o + P_o(A-LC) = -2I$.

The proposed resilient CPS structure utilizes dynamic encoding/decoding signals ξ and $\hat{\xi}$ in the form of (18) which, as being illustrated in this paper, involves two Chus's circuits (8) and (10). The following theorem provides not only the nominal performance in the presence of nonlinear dynamic components but also robustness against attacks.

Theorem 1: Consider system (19) whose dynamic signals are defined by (18), (8), and (10). If gain l_c is chosen according to (13), then the system has the following properties:

- Global asymptotic stability and exponential convergence when $u_a = 0$ and $y_a = 0$
- Input-to-state stability (ISS) with respect to attack vectors u_a and y_a.

Proof: It follows from (18), Hölder's inequality, and (17) that $\left|\tilde{\xi}\right| \leq \|\tilde{x}_c\| \leq M_1\|\tilde{x}_c(t_0)\|e^{-\alpha_c t}$. Consider the Lyapunov function: given V_c in (15) and for some $c_e > 2\|P_sBK\|^2$, $V_s = V_c + x^T P_s x + c_e e^T P_o e$. It follows from (16) that

$$\begin{aligned} \dot{V}_s &\leq -\alpha_c V_c - 2\|x\|^2 - 2c_e\|e\|^2 + 2x^T P_s BKe \\ &\quad + \frac{2\varepsilon\tilde{\xi}}{1+\varepsilon\xi}x^T P_s BK(x-e) + \frac{2c_e\varepsilon\tilde{\xi}}{1+\varepsilon\xi}e^T P_o BK(x-e) \\ &\quad + \frac{2}{1+\varepsilon\xi}x^T P_s Bu_a + \frac{2c_e}{1+\varepsilon\xi}e^T P_o Bu_a - 2c_e e^T P_o Ly_a \\ &\leq -\lambda_s V_s + M_2\|\tilde{x}_c(t_0)\|e^{-\alpha_c t}V_s + M_3\|u_a\|^2 + M_4\|y_a\|^2, \end{aligned} \tag{20}$$

where $\lambda_s = \min\left\{\alpha_c, \lambda_{max}^{-1}(P_s), (c_e - 2\|P_sBK\|^2)/(c_e\lambda_{max}(P_o))\right\}$, $M_2 = 2\varepsilon M_1 \max\left\{\frac{3\|P_sBK\|+c_e\|P_oBK\|}{\lambda_{max}(P_s)}, \frac{\|P_sBK\|+3c_e\|P_oBK\|}{c_e\lambda_{max}(P_o)}\right\}$, $M_3 = 8(\|P_sB\|^2 + c_e\|P_oB\|^2)$, and $M_4 = 2c_e\|P_oL\|^2$.

For the case that there is no attack, we know from (20) that

$$w(t) \triangleq \dot{V}_s + \lambda_s V_s - M_2\|\tilde{x}_c(t_0)\|e^{-\alpha_c t}V_s \leq 0.$$

Dividing V_s on both side of the equation and then multiplying dt yields

$$\frac{1}{V_s}dV_s + [\lambda_s - M_2\|\tilde{x}_c(t_0)\|e^{-\alpha_c t}]dt = \frac{w(t)}{V_s}dt.$$

Integrating both sides of the equation and invoking the fact that $w(t)/V_s < 0$ yield

$$\log V_s(t) - \log V_s(t_0) \leq -\lambda_s(t-t_0) + \frac{M_2}{\alpha_c}e^{-\alpha_c t_0}\|\tilde{x}_c(t_0)\|,$$

and hence

$$V_s(t) \leq V_s(t_0)e^{\frac{M_2}{\alpha_c}e^{-\alpha_c t_0}\|\tilde{x}_c(t_0)\|}e^{-\lambda_s(t-t_0)},$$

which shows global asymptotic stability and exponential convergence.

We can conclude ISS directly by noting that both u_a and y_a are additive terms to the linear time-varying differential inequality given by (20). ■

The robustness property established in the above theorem provides the basis for us to investigate whether perfect stealthy attacks can now be prevented by incorporating the proposed embedment of chaotic circuits and dynamic signals, which is the topic of the subsequent subsection.

D. Detection of System Integrity Attacks

From the perspective of attack detection, dynamic signals $\xi(t)$ and $\hat{\xi}(t)$ can also be viewed as the probing signals whose net effect is null if the system is not under attack and the two chaotic circuits have already been synchronized. The following theorem presents the performance of the active attack detection method under the proposed CPS structure.

Theorem 2: Consider system (6) and (7) whose dynamic signals are defined by (18), (8), and (10). Then, under the system integrity attack in the form of (5), the perfect stealthy attack is detected by the residual-based attack detector (3).

Proof: Consider the following nominal system of (6) and (7) in the absence of attacks as

$$\begin{aligned} \dot{x}_n &= (A-BK)x_n + BK(x_n - \hat{x}_n) + \frac{\varepsilon\tilde{\xi}}{1+\varepsilon\xi}BK\hat{x}_n, \\ \dot{\hat{x}}_n &= (A-BK)\hat{x}_n + LC(x_n - \hat{x}_n), \quad z_n = C(x_n - \hat{x}_n). \end{aligned}$$

Then, with variables $e_a = x - x_n$, $\hat{e}_a = \hat{x} - \hat{x}_n$, and $z_a = z - z_n$, the perturbed system affected by the attack (5) is computed as

$$\begin{aligned} \dot{e}_a &= Ae_a - \frac{1+\varepsilon\hat{\xi}}{1+\varepsilon\xi}BK\hat{e}_a + \frac{1}{1+\varepsilon\xi}Bu_a, \\ \dot{\hat{e}}_a &= (A-BK)\hat{e}_a + LC(e_a - \hat{e}_a) + Ly_a, \\ \dot{w} &= (A-LC)w + \frac{\varepsilon\tilde{\xi}}{1+\varepsilon\xi}BK\hat{e}_a - \frac{\varepsilon\xi}{1+\varepsilon\xi}Bu_a, \quad z_a = Cw, \end{aligned}$$

where $w = e_a - \hat{e}_a - x_a$.

After achieving synchronization of two circuits (*i.e.,* $\tilde{\xi} = 0$), the perturbed measurement residual z_a is calculated as

$$z_a(t) = -C\int_{t_0}^{t}\frac{\varepsilon\xi(\eta)}{1+\varepsilon\xi(\eta)}e^{(A-LC)(t-\eta)}Bu_a(\eta)d\eta.$$

Hence, it is obvious that z_a equals to zero only if there is no attack (*i.e.,* $u_a = 0$). ■

Practically, the threshold μ is selected as a positive value due to model uncertainties and measurement noises. Thus, to improve the attack detection performance, the designer needs to select the larger ε to exceed the threshold μ since the magnitude of z_a increases as ε increases. In a similar manner, the proposed CPS structure is also applicable to detect other types of stealthy attack strategies since it is difficult to generate the attack vectors u_a and y_a to compensate the effect of cyber attacks without information on ξ and $\hat{\xi}$. For instance, the objective of the stealthy attack strategy in [11] is to induce large perturbations on the physical plant while causing slight variations on z_a. But, the proposed one can amplify the magnitude of z_a by increasing ε to find out such stealthy attacks.

IV. Robustness Against Communication Delay

It is well known that the remote control by communicating data under various physical and cyber components induces several side effects such as communication delay and information loss [30], [31]. Such effects are inevitable and may lead to performance degradation and even instability of the closed-loop system. In this section, we explore the robustness regarding the time delay and the secure communication structure for preventing the eavesdropping attack. For the ease of presentation, we make the following assumption (which can be removed by extending the analysis to accounting for multiple and possibly unknown delays).

Assumption 2: The time delays in the communication network between the physical plant and its monitoring/control station are the same and known[2].

Now, we present the following CPS model with the master and slave Chua's circuits as

$$\begin{aligned}
\dot{x}(t) &= Ax(t) + \frac{1}{1+\varepsilon\xi(t-\tau)}B\{u(t-\tau)+u_a(t)\},\\
\dot{\hat{x}}(t) &= A\hat{x}(t) + \frac{1}{1+\varepsilon\hat{\xi}(t-\tau)}Bu(t-\tau)\\
&\quad + L\{y(t-\tau)-\hat{y}(t-\tau)+y_a(t)\},\\
u(t) &= -\{1+\varepsilon\hat{\xi}(t)\}K\hat{x}(t), \quad y(t)=Cx(t),\ \hat{y}(t)=C\hat{x}(t)
\end{aligned} \tag{21}$$

and

$$\begin{aligned}
C_1\dot{v}_1(t) &= \frac{1}{R_1}\{v_2(t)-v_1(t)\} - g(v_1(t)),\\
C_2\dot{v}_2(t) &= \frac{1}{R_1}\{v_1(t)-v_2(t)\} + I(t),\\
L_1\dot{I}(t) &= -v_2(t) - R_2 I(t), \qquad y_c(t) = v_1(t),\\
C_1\dot{\hat{v}}_1(t) &= \frac{1}{R_1}\{\hat{v}_2(t)-\hat{v}_1(t)\} - g(\hat{v}_1(t))\\
&\quad + l_c\{y_c(t-\tau)-\hat{y}_c(t-\tau)\},\\
C_2\dot{\hat{v}}_2(t) &= \frac{1}{R_1}\{\hat{v}_1(t)-\hat{v}_2(t)\} + \hat{I}(t),\\
L_1\dot{\hat{I}}(t) &= -\hat{v}_2(t) - R_2\hat{I}(t), \qquad \hat{y}_c(t) = \hat{v}_1(t),
\end{aligned} \tag{22}$$

[2]Communication delays are known for devices equipped with such timing techniques such as GPS or the precision time protocol (PTP) [32], [33].

where $\tau \geq 0$ is the communication time delay. For the completeness of the solution, let $\chi(t) = \phi(t)$ for some initial condition $\phi(t)$ and $t \in [-\tau, 0]$ where $\chi^T(t) = [x^T(t), \hat{x}^T(t), v_1(t), v_2(t), I(t), \hat{v}_1(t), \hat{v}_2(t), \hat{I}(t)]^T$. The robustness of the proposed CPS structure regarding the time delay is discussed in the following theorem.

Theorem 3: Consider system (21) whose dynamic signals are defined by (18) and (22). If gain l_c is chosen according to (13) and communication time delay τ is satisfied that $\tau < \min\{\alpha_c/\alpha_d,\ \lambda_d/(\alpha_1+\alpha_2+14)\}$ where

$$\alpha_d = \frac{l_c}{C_1}\left\{\frac{1}{C_1^2}\left(\frac{1}{R_1}-\underline{d}\right)^2 + \frac{1}{C_1C_2R_1^2}+1\right\} + \frac{l_c^2}{C_1}\left(\frac{1}{C_1^2}+1\right),$$

$$\lambda_d = \min\left\{\alpha_c', \frac{1}{2\lambda_{\max}(P_s)}, \frac{1}{4\lambda_{\max}(P_o)}\right\}, \quad \alpha_c' = \alpha_c - \tau\alpha_d,$$

$$\begin{aligned}
\alpha_1 &= \frac{9\|P_sBKA\|^2}{(\lambda_{\min}(P_s))^2} + \frac{9\|A\|^2}{8\lambda_{\min}(P_s)\lambda_{\min}(P_o)} + \frac{32\|P_sBK\|^2\|P_oBKA\|^2}{\lambda_{\min}(P_s)\lambda_{\min}(P_o)}\\
&\quad + \frac{4\|P_oBKA\|^2}{(\lambda_{\min}(P_o))^2} + \frac{\|P_oLCA\|^2}{(\lambda_{\min}(P_o))^2},\\
\alpha_2 &= \frac{9\|P_sBKBK\|^2}{(\lambda_{\min}(P_s))^2} + \frac{9\|BK\|^2}{8\lambda_{\min}(P_s)\lambda_{\min}(P_o)} + \frac{9\|LC\|^2}{8\lambda_{\min}(P_s)\lambda_{\min}(P_o)}\\
&\quad + \frac{32\|P_sBK\|^2\|P_oBKBK\|^2}{\lambda_{\min}(P_s)\lambda_{\min}(P_o)} + \frac{4\|P_oBKBK\|^2}{(\lambda_{\min}(P_o))^2} + \frac{4\|P_oBKLC\|^2}{(\lambda_{\min}(P_o))^2}\\
&\quad + \frac{32\|P_sBK\|^2\|P_oBKLC\|^2}{\lambda_{\min}(P_s)\lambda_{\min}(P_o)} + \frac{4\|P_oBKLC\|^2}{(\lambda_{\min}(P_o))} + \frac{\|P_oLCLC\|^2}{(\lambda_{\min}(P_o))},
\end{aligned}$$

then the system has the following properties:

- Global exponential stability when $u_a = 0$ and $y_a = 0$
- Input-to-state stability (ISS) with respect to attack vectors u_a and y_a.

Proof: With the relation that $\chi(t-\tau) = \chi(t) - \int_{-\tau}^{0}\dot{\chi}(t+\eta)d\eta$, system (21) and (22) can be rewritten as

$$\begin{aligned}
\dot{x}(t) &= (A-BK)x(t) + BKe(t) + \frac{1}{1+\varepsilon\xi(t-\tau)}Bu_a(t)\\
&\quad + \frac{\varepsilon\tilde{\xi}(t-\tau)}{1+\varepsilon\xi(t-\tau)}BK\{x(t)-e(t)\}\\
&\quad + \frac{1+\varepsilon\hat{\xi}(t-\tau)}{1+\varepsilon\xi(t-\tau)}BK\int_{-\tau}^{0}\dot{x}(t+\eta)-\dot{e}(t+\eta)d\eta,\\
\dot{e}(t) &= (A-LC)e(t) + \frac{1}{1+\varepsilon\xi(t-\tau)}Bu_a(t) - Ly_a(t)\\
&\quad + \frac{\varepsilon\tilde{\xi}(t-\tau)}{1+\varepsilon\xi(t-\tau)}BK\{x(t)-e(t)\}\\
&\quad - \frac{\varepsilon\tilde{\xi}(t-\tau)}{1+\varepsilon\xi(t-\tau)}BK\int_{-\tau}^{0}\dot{x}(t+\eta)-\dot{e}(t+\eta)d\eta\\
&\quad + LC\int_{-\tau}^{0}\dot{e}(t+\eta)d\eta
\end{aligned} \tag{23}$$

and

$$\begin{aligned}
C_1\dot{\tilde{v}}_1(t) &= \frac{1}{R_1}\{\tilde{v}_2(t)-\tilde{v}_1(t)\} - \{g(v_1(t)) - g(\hat{v}_1(t))\}\\
&\quad - l_c\tilde{v}_1(t) + l_c\int_{-\tau}^{0}\dot{\tilde{v}}_1(t+\eta)d\eta,\\
C_2\dot{\tilde{v}}_2(t) &= \frac{1}{R_1}\{\tilde{v}_1(t)-\tilde{v}_2(t)\} + \tilde{I}(t),\\
L_1\dot{\tilde{I}}(t) &= -\tilde{v}_2(t) - R_2\tilde{I}(t),
\end{aligned} \tag{24}$$

in which $\zeta(t) = \phi_d(t)$ for some initial condition $\phi_d(t)$ and $t \in [-2\tau, 0]$ where $\zeta^T(t) = [\tilde{v}_1(t), \tilde{v}_2(t), \tilde{I}(t), x^T(t), e^T(t)]^T$.

We first prove that, in the presence of the time delay, the master and slave circuits are also exponentially synchronized each other. Consider the Lyapunov function V_c in (15). It follows that

$$\begin{aligned}\dot{V}_c(t) \quad \leq \quad & -\alpha_c V_c(t) + \frac{l_c}{C_1}\int_{-\tau}^{0} \gamma_1 V_c(t) + V_c(t+\eta)d\eta \\ & + \frac{l_c^2}{C_1}\int_{-\tau}^{0} \gamma_2 V_c(t) + V_c(t+\eta-\tau)d\eta,\end{aligned}$$

where $\gamma_1 = \left\{ \frac{1}{C_1^2}\left(\frac{1}{R_1} - \underline{d}\right)^2 + \frac{1}{C_1 C_2 R_1^2} \right\}$, $\gamma_2 = \frac{1}{C_1^2}$. Following the Lyapunov-Razumikhin approach [34], assume that $V_c(\eta) \leq V_c(t)$ for $t - 2\tau \leq \eta \leq t$. Then, we have $\dot{V}_c(t) \leq -\alpha_c V_c(t) + \tau\alpha_d V_c(t) \leq -\alpha_c' V_c(t)$. where $\alpha_c' = \alpha_c - \tau\alpha_d$. Hence, it follows from $\tau < \alpha_c/\alpha_d$ that $\|\tilde{x}_c(t)\| \leq M_1 \|\tilde{x}_c(t_0)\| e^{-\alpha_c' t}$.

Now, we prove the main part of theorem. Let the Lyapunov function be $V_s = V_c + x^T P_s x + c_e e^T P_o e$ where c_e is some positive constant which will be defined later. Then, with the inequality $\|\tilde{\xi}(t)\| \leq M_1 \|\tilde{x}_c(t_0)\| e^{-\alpha_c' t}$, following a similar procedure in the proof of Theorem 1 and assuming that $V_s(\eta) \leq V_s(t)$ for $t - 2\tau \leq \eta \leq t$, we have

$$\begin{aligned}\dot{V}_s(t) \quad \leq \quad & -\lambda_d' V_s(t) + M_2' \|\tilde{x}_c(t_0)\| e^{-\alpha_c' t} V_s(t) + M_3 \|u_a(t)\|^2 \\ & + M_4 \|y_a(t)\|^2 + M_5 \left\| \int_{-\tau}^{0} u_a(t+\eta)d\eta \right\|^2 \\ & + M_6 \left\| \int_{-\tau}^{0} y_a(t+\eta)d\eta \right\|^2, \qquad (25)\end{aligned}$$

where $\lambda_d' = \lambda_d - \tau(\alpha_1 + \alpha_2 + 14)$, $c_e = 8\|P_s BK\|^2$, $M_2' = M_2 e^{\alpha_c'\tau}$, $M_5 = 24c_e\|P_o LCB\|^2$, and $M_6 = 18\|P_s BKL\|^2 + 24c_e\|P_o BKL\|^2 + 6c_e\|P_o LCL\|^2$. For the case that there is no attack ($u_a(t) = y_a(t) = 0$), it follows that

$$V_s(t) \leq V_s(t_0) e^{\frac{M_2'}{\alpha_c'} e^{-\alpha_c' t_0} \|\tilde{x}_c(t_0)\|} e^{-\lambda_d'(t-t_0)},$$

which shows global exponential stability.

We can also conclude that system is ISS with respect to u_a and y_a from the linear time-varying differential inequality given by (25). ■

Theorem 3 indicates that the CPS structure is robust under the small time delay τ and the result of Theorem 1 is recovered as τ decreases to zero. Moreover, it is remarkable that, in the presence of τ, the selection of the large coupling gain l_c for achieving the fast synchronization speed may result in the instability of the closed-loop system since it decreases the upper bound of τ and destabilizes the error system (24) between two Chua's circuits.

V. Simulation Verification

To validate the proposed attack detection method, simulations for Quadruple-Tank Process [35] are carried out. With the linearized system model[3], consider the proposed CPS structure (6) and (7) with $\xi = v_1$ and $\hat{\xi} = \hat{v}_1$,

$$A = \begin{bmatrix} -0.0159 & 0 & 0.0419 & 0 \\ 0 & -0.0111 & 0 & 0.0333 \\ 0 & 0 & -0.0419 & 0 \\ 0 & 0 & 0 & -0.0333 \end{bmatrix},$$

$$B = \begin{bmatrix} 0.0833 & 0 \\ 0 & 0.0628 \\ 0 & 0.0479 \\ 0.0312 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0 \end{bmatrix},$$

$$K = \begin{bmatrix} 0.3315 & 0.0274 & 0.1528 & 0.0174 \\ 0.0480 & 0.3369 & 0.0296 & 0.1613 \end{bmatrix},$$

$$L = \begin{bmatrix} 1.4841 & -0.1160 & 6.5596 & -2.1720 \\ -0.3335 & 1.3702 & -5.5018 & 6.3243 \end{bmatrix}^T.$$

The parameters of two Chua's circuits are as follows:

$$L_1 = 0.2,\ R_1 = 1.5,\ R_2 = 0.005,\ C_1 = 0.1,\ C_2 = 2,$$
$$\underline{d} = -4,\ \overline{d} = -0.1,\ E = 1,\ l_c = 20.$$

[3]For detailed system parameters, see [35]

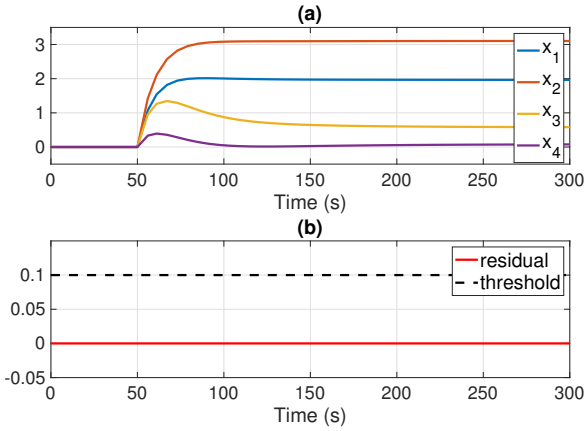

Fig. 3. Simulation results of the standard configuration: (a) plant state x, (b) residual $\|Wz\|$ and threshold μ

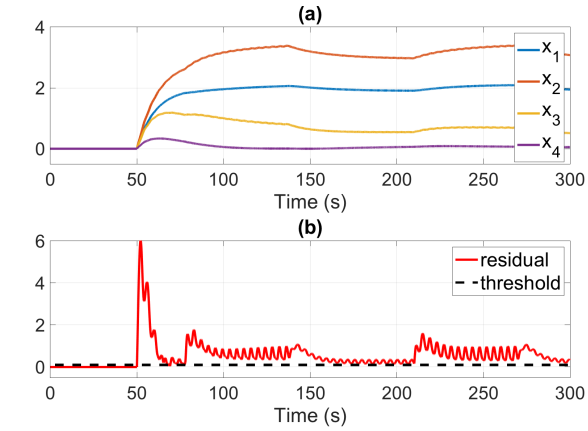

Fig. 4. Simulation results of the proposed configuration: (a) plant state x, (b) residual $\|Wz\|$ and threshold μ

From the behavior of Chua's circuit with given parameters, the scaling constant $\varepsilon = 0.04$ is chosen such that $|\varepsilon\xi| < 0.5$ and $|\varepsilon\hat{\xi}| < 0.5$. In addition, the parameters of residual detector are selected as $W = 100 \cdot \mathrm{I}_2$ and $\mu = 0.1$. The attack gain matrix

$$K_a = \begin{bmatrix} 1.3922 & -0.0030 & 0.3270 & -0.0052 \\ 0.0561 & 1.4015 & 0.0121 & 0.3456 \end{bmatrix}$$

and the injection input $r_a(t) = \begin{bmatrix} 3 & 5 \end{bmatrix}^T$ for $t \geq 50$ are chosen to change the dynamic response of the physical plant.

Fig. 3 shows simulation results for the linear CPS structure under the system integrity attack. As can be seen in Fig. 3 (a), the state of the physical plant deviates from the desired one without being detected. In other words, the measurement residual between the measurement and observer output remains zero and the residual detector is not activated as shown in Fig. 3 (b). On the other hand, simulation results for the proposed resilient CPS structure are shown in Fig. 4. By virtue of encoding/decoding components, the residual shows the oscillating behavior and, thus, the residual detector is triggered. From the above simulation results, we confirm that the proposed method can detect the system integrity attack even though the conventional CPS fails to detect.

VI. Conclusion

In this paper, we dealt with attack-aware control problems of a cyber-physical system (CPS) under intelligent adversaries. For system integrity attack strategies, we proposed an active attack detection resilient CPS structure by embedding nonlinear encoding/decoding components to protect information on the CPS model and transmitted signals. In addition, for avoiding the eavesdropping, Chua's circuits are employed to guarantee the secure communication between the physical and cyber layers. The robustness of the proposed CPS structure regarding nonlinear time-varying components and the communication time delay is investigated based on input-to-state stable (ISS) framework.

References

[1] E. A. Lee, "Cyber physical systems: design challenges", *11th IEEE Symposium on Object Oriented Real-Time Distributed Computing*, pp. 363-369, 2008.

[2] K. D. Kim and P. R. Kumar, "Cyber-physical systems: a perspective at the centennial", *Proc. IEEE*, vol. 100, pp. 1287-1308, 2012.

[3] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey", *IET Cyber-physical systems: theory and applications*, vol. 1, no. 1, pp. 13-27, 2016.

[4] D. P. Fidler, "Was stuxnet an act war? decoding a cyberattack", *IEEE Security & Privacy*, vol. 9, no. 4, pp. 56-59, 2011.

[5] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: implications for false data injection attacks", *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317-3318, 2017.

[6] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries", *Automatica*, vol. 51, pp. 135-148, 2015.

[7] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security - a survey", *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802-1831, 2017.

[8] T. Irita and T. Namerikawa, "Detection of Replay Attack on Smart Grid with Code Signal and Bargaining Game", in *Proc. Amer. Control Conf.*, Seattle, WA, USA, May 2017, pp. 2112-2117.

[9] A. Gusrialdi and Z. Qu, "Smart Grid Security: Attacks and Defenses," in *Smart Grid Control: An Overview and Research Opportunities*, Jakob Stoustrup, Anuradha Annaswamy, Aranya Chakrabortty, and Zhihua Qu (Eds.), Springer Verlag, 2018.

[10] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An Attack-Resilient Cooperative Control Strategy of Multiple Distributed Generators in Distribution Networks," *IEEE Trans. Smart Grid*, vol.7, no.6, pp.2923-2932, 2016.

[11] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks", *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2618-2624, 2016.

[12] T. Shinohara and T. Namerikawa, "Manipulative Zero-Stealthy Attacks in Cyber-Physical Systems: Existence Space of Feasible Attack Objectives", in *Proc. IEEE Conf. Control Technol. Appl.*, Kohala Coast, HI, USA, Aug. 2017, pp. 1123-1128.

[13] Y. Chen, S. Kar, and J. M. Moura, "Optimal attack strategies subject to detection constraints against cyber-physical systems", *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 1157-1168, 2018.

[14] T. Shinohara, T. Namerikawa, and Z. Qu, "Resilient Reinforcement in Secure State Estimation against Sensor Attacks with a priori Information", *IEEE Trans. Autom. Control*, vol. 64, no. 12, pp. 5024-5038, 2019.

[15] R. S. Smith, "A decoupled feedback structure for covertly appropriating networked control systems", *in Proc. IFAC*, Milano, Italy, Aug. 2011, pp. 90-95.

[16] R. S. Smith, "Covert misappropriation of networked control systems", *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 82-92, 2015.

[17] S. X. Ding, *Model-based fault diagnosis technique: design schemes, algorithm, and tools*, Springer Science & Business Media, 2008.

[18] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor output", *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 93-109, 2015.

[19] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: active defense of networked cyber-physical systems", *Proc. IEEE*, vol. 105, no. 2, pp. 219-240, 2017.

[20] S. Weerakkody and B. Sinopoli, "Detecting integrity attacks on control systems using a moving target approach", in *Proc. IEEE Conf. Decision and Control*, Osaka, Japan, Dec. 2015, pp. 5820-5826.t

[21] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems", in *Proc. 50th Annu. Allerton Conf.*, Monticello, IL, USA, Oct. 2012, pp. 1806-1813.

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

[23] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Competitive Interaction Design of Cooperative Systems Against Attacks," *IEEE Trans. Autom. Control*, vol. 63, no. 9, pp. 3159-3166, 2018.

[24] A. Gusrialdi, Z. Qu and M. A. Simaan, "Game Theoretical Designs of Resilient Cooperative Systems," in *European Control Conf.*, Linz, Austria, Jul. 2015, pp. 1699-1705.

[25] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Robust Design of Cooperative Systems Against Attacks," in *Proc. Amer. Control Conf.*, Portland, OR, USA, Jun. 2014, pp. 1462-1468.

[26] G. Park, C. Lee, H. Shim, Y. Eun, and K. H. Johansson, "Stealthy adversaries against uncertain cyber-physical systems: threat of robust zero-dynamics attack", *IEEE Trans. Autom. Control*, vol. 64, no. 12, pp. 4907-4919, 2019.

[27] T. Matsumoto, "A chaotic attractor from Chua's circuit", *IEEE Trans. Circuits Syst.*, vol. 31, no. 12, pp. 1055-1058, 1984.

[28] T. Matsumoto, L. O. Chua, and M. Komuro, "The double scroll", *IEEE Trans. Circuits Syst.*, vol. 32, no. 8, pp. 798-818, 1985.

[29] V. Siderskiy and V. Kapila, "Parameter Matching using Adaptive Synchronization of Two Chua's Oscillators", in *Proc. Amer. Control Conf.*, Portland, OR, USA, Jun. 2014, pp. 5620-5626.

[30] P. F. Hokayem and M. W. Spong, "Bilateral teleoperation: an historical survey", *Automatica*, vol. 42, no. 12, pp. 2035-2057, 2006.

[31] P. J. Antsaklis, B. Goodwine, V. Gupta, M. J. McCourt, Y. Wnag, P. Wu, M. Xia, H. yu, and F. Zhu, "Control of cyberphysical systems using passivity and dissipativity based methods", *Eur. J. Control*, vol. 19, no. 5, pp. 379-388, 2013.

[32] *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, IEEE 1588-2008, 2008.

[33] K. Correll, N. Barendt, and M. Branicky, "Design considerations for software only implementations of the IEEE 1588 Precision Time Protocol", *Proc. Conf. IEEE 1588*, 2005.

[34] J. H. Su, "Further results on the robust stability of linear systems with a single time delay", *Syst. Contr. Lett.*, vol. 23, no. 5, pp. 375-379, 1994.

[35] K. H. Johansson, "The quadruple-tank process: A multivariable laboratory process with an adjustable zero", *IEEE Trans. Control Syst. Technol.*, vol. 8, no. 3, pp. 456-465, 2000.