Mitigating Attacks With Nonlinear Dynamics on Actuators in Cyber-Physical Mechatronic Systems

Mohammad Al Janaideh, Eman Hammad, Abdallah Farraj, and Deepa Kundur

***Abstract*—The impact and mitigation of false data injection (FDI) attacks with nonlinear dynamics targeting actuators in cyber-physical mechatronic systems (CPMSs) is investigated in this paper. Actuators in mechatronic systems exhibit vulnerabilities to inputs with well-known nonlinearities (e.g., backlash, deadzone, and saturation), where the nonlinear dynamics can affect the actuators' performance. A mitigation approach is proposed based on the retrospective cost-based adaptive control to stabilize and regulate the CPMS under such FDI cyberattack. Since mechatronic systems are implemented with actuators of different dynamical properties, this paper considers systems of linear and nonlinear dynamics. Simulation results demonstrate how the proposed adaptive control system achieves internal model control with the dynamics of the actuator systems and the nonlinearities of the backlash, deadzone, and saturation attacks. Results further show that the controller inverts and rejects the effects of attacks with unknown nonlinearities.**

***Index Terms*—Adaptive control, attack mitigation, cyberattacks, mechatronic cyber-physical systems (CPSs), nonlinear dynamics.**

I. Introduction

CYBER-PHYSICAL systems (CPSs) are complex systems that integrate sensors, communication networks, actuators, and control schemes with conventional physical systems [1]. Integration of sensory and cyber-enabled control into traditional physical systems greatly enhances operation and resilience by facilitating situational awareness, distributed algorithms, and control. Many CPSs contain mechatronic subsystems and are thus denoted as cyber-physical mechatronic systems (CPMSs). Examples of CPMSs include smart transportation, complex manufacturing, and integrated biomedical robotics [2], [3]. As CPMSs grow in complexity, their reliable operation requires adaptive control designs that are responsive to changing physical environments and increasingly advanced cyberthreats.

The benefits of integrating communication and cyber-enabled intelligence into mechatronic systems are accompanied by an increased risk of cyberattacks on the system with negative consequences. The confidentiality-integrity-availability framework is commonly used to classify the different threats that target information. However, this framework is adjusted for the context of CPMS, where the integrity and availability of measurements and control commands are of utmost importance. Thus, in CPMS, we consider the I-A-C framework. In the case of cyberattacks targeting integrity, the adversary infiltrates communicated data (sensory measurements with control commands) to impact system operation in a stealthy manner. Examples of cyberattacks targeting information integrity include false data injection (FDI) attacks that are the focus of this paper due to their potential sever impact on CPMS operation [4]–[7]. Attacks on availability often materialize as denial-of-service (DoS) attacks targeting communication channels; here, an adversary interrupts cyber network operation to cause either communication link failure or excessive delay and results in preventing the timely exchange of information amongst sensors, actuators, and control systems. Finally, in attacks on confidentiality, an unauthorized adversary would accesses and breach system data.

Cyberattacks on CPMS can lead to system malfunctioning, safety or instability problems, financial losses for system operators, and/or unlawful gains for intruders. The traditional first-lines of defense against cyberthreats includes security controls, such as intrusion detection, intrusion prevention, traffic filtering, and encryption. However, recent cyber security studies have shown that cyberthreats targeting CPMS are advanced, persistent, and complex and are likely to bypass these lines of defenses (e.g., *advanced and stealthy* attacks). Thus, approaches to CPMS security have shifted from attack prevention to attack mitigation via control. Moreover, FDI threats have been gaining much attention as such adverse actions manipulate the structure of the data delivery system to insert fabricated information in the data stream while bypassing bad data detection filters. FDI attack models in the literature assume an adversary with some knowledge (full or partial) of the system state and dynamics.

Mitigating attacks on CPMS usually rely on employing state-estimation methods within a closed-loop control system, see for example [8]–[11]. Such methods use estimation in closed-loop control to detect changes in the system dynamics or control

Manuscript received August 9, 2018; revised December 14, 2018; accepted January 29, 2019. Date of publication February 18, 2019; date of current version September 3, 2019. Paper no. TII-18-2084. *(Corresponding author: Mohammad Al Janaideh.)*

M. Al Janaideh is with the Department of Mechanical Engineering, Memorial University, St. John's, NL A1B 3X5, Canada (e-mail: maljanaideh@mun.ca).

E. Hammad, A. Farraj, and D. Kundur are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: ehammad@ece.utoronto.ca; abdallah@ece.utoronto.ca; dkundur@ece.utoronto.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2019.2899933

algorithm, and then propose a technique to reject the dynamics of cyberattacks. For example, in [9], a smooth variable structure filter was used in a closed-loop control system to estimate the states of the system and to identify system parameters. This filter considered the estimation error to detect changes in the system parameters. A state observer is proposed in [10] to detect changes in system dynamics and an adaptive filter with an adaptive law are employed to stabilize the system dynamics. Also, a Luenberger observer has been developed in [11] to identify attacks on actuators and sensors in a linear dynamical system that includes a state feedback control system. It can be observed that the performance of these methods is strongly limited by the estimation. Hence, to address the shortcoming of previous approaches, the proposed adaptive control system is designed to stabilize the system dynamics without requiring the estimation of state dynamics.

Moreover, we consider DoS attacks that can result in time-delays in system measurements and/or control commands. Time-delays in CPMS affect the dynamics and degrade the performance and this may cause high oscillations and instability [13]. For example, unavoidable time-delays negatively impact the performance between master and slave robots in teleoperating CPSs, where the existence of even a small time-delay may lead to instability of control systems. Furthermore, time-delays affect vehicle-to-vehicle communication in vehicle control systems [14]. Hence, to ensure reliable and practical control implementation for CPMS, these control systems must be designed considering information delays and uncertainties. Hence, this highlights the importance of considering cyberattacks causing time-delays in CPMSs' control design.

A CPMS is considered in this paper where communication links exist between select sensors, control, and actuators. CPMSs have been widely used in different smart, self-adapting, intelligent manufacturing, and mechatronic systems. An effective CPMS model of mechatronic systems [15]–[17] enables the investigation of their vulnerabilities, controller design, and mitigation strategies to successfully remediate the impact of cyberattacks that target system weaknesses. A number of studies propose identification techniques, adaptive control systems, and disturbance observers, see, for example, [18]–[23].

The current literature, however, lacks a robust understanding of the impact of cyberattacks on CPMSs with nonlinear dynamics. Thus, the aim of this paper is to establish a framework for cyber security studies on mechatronic systems. We focus on mitigating FDI attacks that introduce nonlinear dynamics to the input of actuators in closed-loop systems. Retrospective cost-based adaptive control (RCAC) has been effectively used in a variety of control applications to regulate unknown linear and nonlinear systems; see, for example, [24]–[26]. This method relies on knowledge of the first Markov parameter of the state-space model of the system. Hence, we propose the RCAC [27] within our framework to reject the effects of FDI attacks injecting nonlinear dynamics into the actuator.

The main contributions of this paper are as follows:

1) We present a framework to model closed-loop CPMSs under cyberthreats and reactive mitigation. Specifically, we consider FDI attacks that inject dynamics in actuator inputs of CPMSs and adaptive control mechanisms for mitigation.
2) We formulate FDI attacks on actuator inputs that exhibit nonlinear dynamics including backlash, saturation, and deadzone, which affect system performance.
3) We propose a novel approach to address CPMSs FDI attacks for different nonlinearities; this paper shows that the internal model principle control approach of the RCAC can reject cyberattacks with nonlinear dynamics on a class of mechatronic systems.

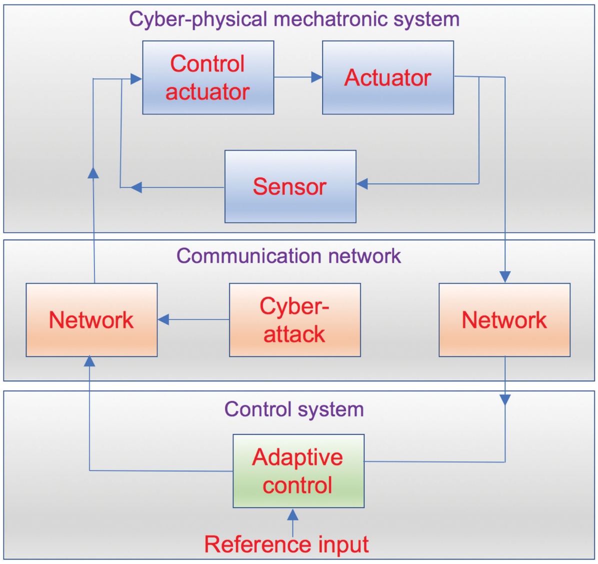


Fig. 1. CPMS is controlled and monitored by a control system through a communication network.

The rest of the paper is organized as follows: Section II formulates the problem and presents the CPMS threat model. This section introduces the mechatronic CPS and the nonlinear dynamic attacks model. Section III proposes and studies the RCAC adaptive control paradigm for FDI attack mitigation. This section presents the internal model control principle to explain the technique of the RCAC control to reject attacks. Sections IV and V numerically investigate the performance of the proposed mitigation control framework for different case studies. Section VI shows the Application to a mechatronic system. Finally, conclusions and final remarks are presented in Section VII.

II. Problem Formulation

This section presents a cyber-physical model of a generic mechatronic system where communication links exist between sensors, actuators, and the control systems, as shown in Fig. 1. This system characterizes a class of intelligent mechatronic systems in manufacturing and industrial automation [16]. As discussed previously, the integration of communication technologies within the closed-loop system increases its susceptibility to cyberthreats by increasing the attack surface, hence enhancing vulnerabilities that can be exploited by malicious adversaries. We assert, however, that CPMSs also enable the abstraction of cross-domain functionalities and analysis, and

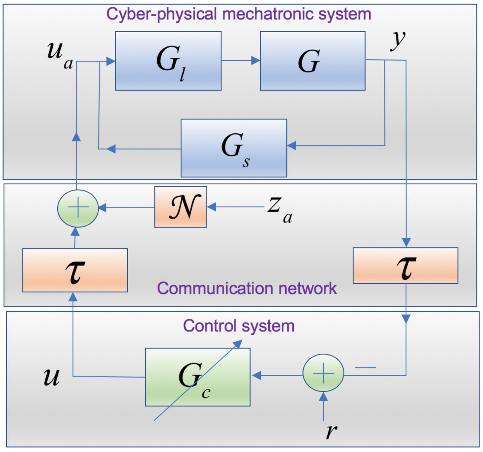


Fig. 2. Closed-loop system for CPMS shown in Fig. 1 with cyberattack of $\mathcal{N}$ and input z_a, adaptive control G_c, and communication links with delay of $\mathcal{T}$. The signal u_a drives the mechatronic system that is modeled with transfer functions of G_l (control system), G (actuator dynamics), and G_s (sensor dynamics) in a closed-loop system. The mechatronic system is operated by the command signal r through the communication links.

have the potential to tractably treat uncertainties introduced by system components, such as communication systems under attack. Furthermore, CPMSs modeling facilitates hierarchical multiagent centralized and distributed control approaches, allowing for complex coordination and collaboration amongst system agents. Although a wide range of cyber events may target a CPMSs of interest, in this paper, we focus on a relevant class of FDI attacks on actuator systems.

A. Mechatronic Cyber-Physical System

The threat model considered in this paper, considers an actuator that is vulnerable to inputs with deadzone, saturation, and backlash nonlinearities. These input nonlinearities, discussed in Section II-C, affect the performance of the actuator and may cause instability to the closed-loop system and oscillations in the output. Furthermore, the threat model considers a class of FDI attacks that is designed to exploit the actuator's vulnerability to inputs with nonlinearities, as will be further elaborated analytically in the following section. The control signal drives the actuator through a communication link (that is often targeted and exploited by cyberattacks). Hence, the threat model considers an adversary with adequate resources and system access that enable him/her to generate and inject deadzone, saturation, or backlash nonlinearities at the actuator input. Furthermore, we also assume a delay in the communication network, and that the tracking error due to the delay is bounded.

B. Modeling

In this section, we present a mathematical model of an overall CPMS under attack, as shown in Fig. 2. The mechatronic system is modeled with discrete transfer functions of $G_l(z)$ to represent the control system, $G(z)$ to represent the actuator dynamics, and $G_s(z)$ to represent sensor dynamics in a closed-loop system. In this paper, we assume $G_s(z) = 1$. As depicted in Fig. 2, the system under consideration is comprised of a single agent with dynamics represented by

$$x(k+1) = Ax(k) + Bu_a(k-\mathcal{T}) \tag{1}$$

$$u_a(k-\mathcal{T}) = \mathcal{N}[z_a](k) + u(k) \tag{2}$$

$$y(k) = Cx(k-\mathcal{T}) \tag{3}$$

$$e(k) = r(k) - y(k) \tag{4}$$

where $u_a(k) \in \mathbb{R}$ is input signal that drives the actuator, $e(k) \in \mathbb{R}$ is the tracking error, $A \in \mathbb{R}^{n\times n}$ is the state matrix, $B \in \mathbb{R}^n$ is the input matrix, $C \in \mathbb{R}^{1\times n}$ is output matrix, $r(k) \in \mathbb{R}$ is the command input, $z_a \in \mathbb{R}$ is the input signal that drives the attack system to generate the nonlinearity on the actuator, $\mathcal{N}[z_a] : \mathbb{R} \longrightarrow \mathbb{R}$, where $||\mathcal{N}[z_a]||_\infty \le \beta_a$, where β_a is positive constant, and $\mathcal{T}$ represents a time delay in the loop. One objective within this model is to develop a controller that can mitigate the impact of cyberattacks on the closed-loop mechatronics system with the communication delay $\mathcal{T}$ in the feedback sensor. It is important to mention that while our attack model and approach are consistent to that of prior art on cyber-physical actuator attacks [21], [20], we focus on novel attacks exploiting nonlinear dynamics vulnerabilities in actuators. In this paper, we consider discrete-time models since different mechatronic systems are operated by data acquisition systems that consider discrete time in real-time systems.

C. Nonlinear Dynamic Attacks Model

This paper considers three possible cyberattacks that exploit nonlinear dynamics on actuators in CPMSs to affect system performance. These nonlinear dynamics cause inaccuracies and oscillations in the motion control systems, and this may lead to instability of closed-loop systems [28]–[31]. In this paper, we assume that the attacks are unknown to system defenders. The following attack model is adopted:

$$u_a(k-\mathcal{T}) = u(k) + \eta(k) \tag{5}$$

where $\eta(k)$ is the output of a nonlinear dynamic model.

1) Backlash Nonlinearity Attack: Backlash nonlinearity is one of the most important nonlinear dynamics that limit and affect the performance of position and velocity control in industrial robots, smart mechatronic systems, and automation [34]. This nonlinearity includes a threshold or gap that affects the motion in mechanical systems. When this gap exists in the dynamical systems, the motion of these systems becomes completely autonomous and unknown. The command signal is shifted by this gap when it increases and decreases. This causes high steady-state errors and inaccuracies in precision motion systems. In a closed-loop system, the gap of the backlash nonlinearity leads to energy storage in a closed-loop system, which can yield instability and oscillations in the output of mechatronic systems. Such effects degrade the performance of different actuators, such as smart material-based actuators, that are used in applications including semiconductor manufacturing. The output of the backlash nonlinear model of the attack system can be defined as

$$\mathcal{N}(k) = \mathcal{A}_B[z_a](k) \tag{6}$$

where $\mathcal{A}_B[z_a](k) = b_\rho(k)$, and, for $k > 1$

$$b_\rho(k) = \max\{z_a(k) - \rho, \min\{z_a(k) + \rho, b_\rho(k-1)\}\} \tag{7}$$

where $b_\rho(1) = \max\{z_a(1) - \rho, \min\{z_a(1) + \rho, 0\}\}$, ρ is a positive threshold that represents the gap, and κ is a positive constant that regulates the slope of the increasing $(z_a(k) - \rho)$ and decreasing $(z_a(k) + \rho)$ curves.

2) Deadzone Nonlinearity Attack: The deadzone nonlinearity is a nonlinearity in which the motion system cannot respond to the command signal until this command reaches a specific value, which is the deadzone threshold. This kind of nonlinearity can refer to a threshold (deadzone) in which output of the system becomes zero when the command signal crosses certain limiting value. Deadzone severely limits the performance of motion control systems, and is a nonlinearity that affects the performance of actuators, such as valves and dc servo motors. The output of the deadzone model of the attack system is expressed as

$$\mathcal{N}(k) = \mathcal{A}_D[z_a](k) \tag{8}$$

where

$$\mathcal{A}_D[z_a](k) = \max\{z_a(k) - \sigma, \min\{z_a(k) + \sigma, 0\}\} \tag{9}$$

where σ is a positive constant.

3) Saturation Nonlinearity Attack: Saturation is a nonlinearity in which the output of the system is proportional to input in limited range that is determined by a threshold. Once the input exceeds the threshold, the output of the actuator becomes constant and does not change till the input becomes less that the positive threshold in case of increasing or more than the negative threshold in case of decreasing. It is known that the saturation nonlinearity limits the amplitude of the control signal, which may cause high tracking errors in the actuator output. The output of the saturation nonlinear model of the attack system is described as

$$\mathcal{N}(k) = \mathcal{A}_S[z_a](k) \tag{10}$$

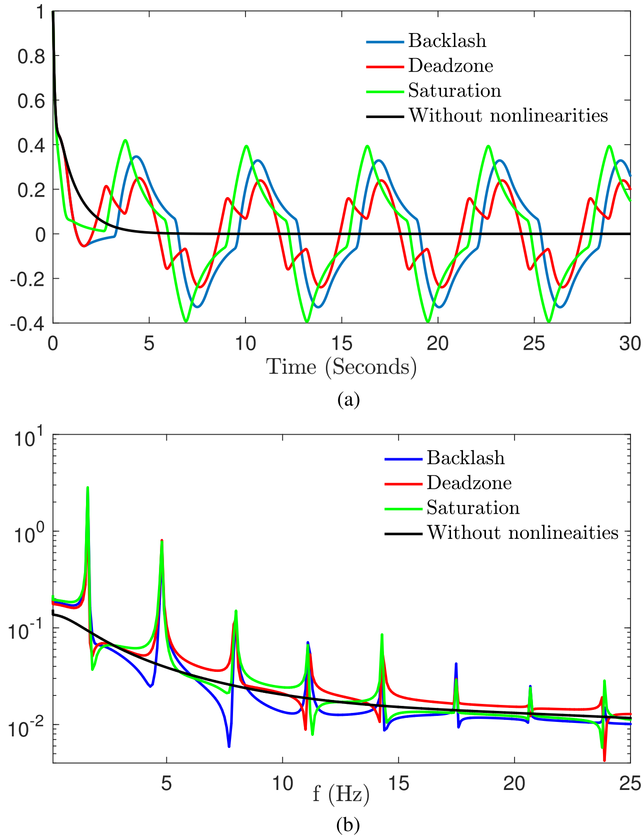
where

$$\mathcal{A}_S[z_a](k) = \begin{cases} \kappa, & \text{if} \quad z_a(k) \geq \kappa \\ z_a(k), & \text{if} \quad -\kappa \leq z_a(k) \leq \kappa \\ -\kappa, & \text{if} \quad z_a(k) \leq \kappa \end{cases} \tag{11}$$

where κ is a positive constant.

D. Example 1

This paper focuses on mitigating FDI attacks that introduce nonlinear dynamics on the input of actuators in closed-loop systems. In this section, we present a motivating example to show how system performance of these actuators is degraded by nonlinear dynamics. The dynamics of these actuators can be modeled using a spring-mass system (second-order system). This system can be considered as a standard model for a class of actuators in motion control systems [32] and [33]. These actuators include, for example, piezoceramic actuators [36], magnetostrictive actuators [57], and reluctance actuators [58].



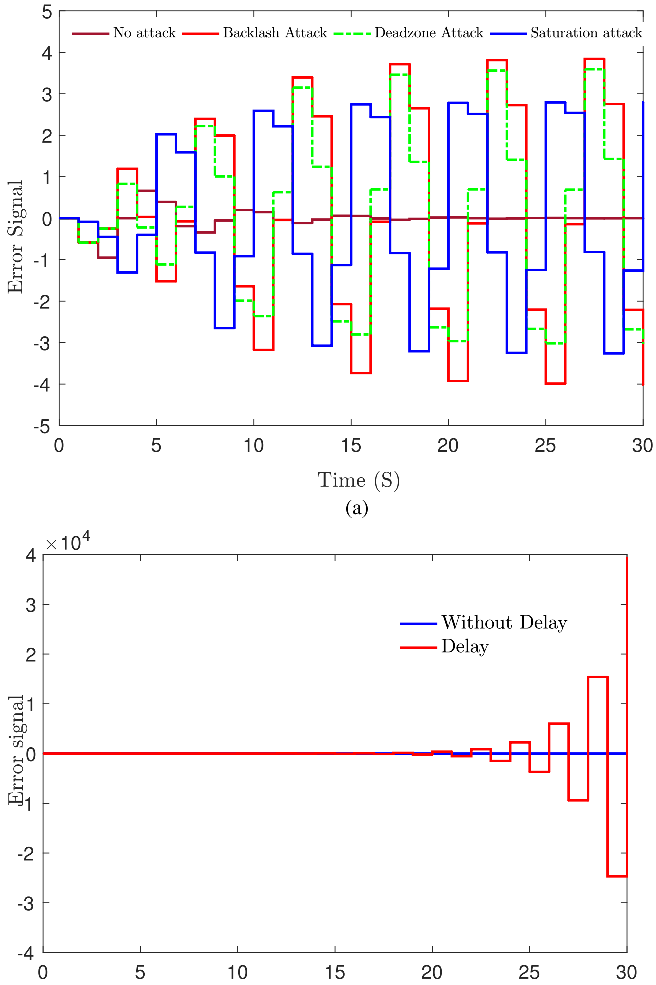
(a)

(b)

Fig. 3. (a) Tracking error of a closed-loop system with the transfer function that consists of 1 kg mass, 1.3 N· s/m damping, and 1 N/m spring constant with a PID controller of 1 proportional gain, 0.05 derivative gain, 1.4 integral gain, and filter coefficient 100. (b) DFT of the output in (a) with and without the backlash, deadzone, and saturation nonlinearities.

In this example, we consider the command signal of $r(k) = 1$. The attack model driven with $z_a(k) = \sin(0.2\pi k)$, backlash nonlinearity (7) of $\rho = 0.5$, deadzone nonlinearity (9) of $\sigma = 0.5$, and saturation nonlinearity (11) of $\kappa = 0.5$. We use mass of 1 kg, damping of 1.3 N· s/m, and spring constant of 1 N/m to present the dynamic of a stable actuator system. A PID controller of proportional gain 1, derivative gain 0.05, integral gain 1.4, and filter coefficient 100. The PID control system is one of the most well-known control systems that are used in the industry [37], [38]. The tracking error in the output of the actuator model with and without the nonlinearities when the command signal $u(t) = 1$ are shown in Fig. 3(a). Fig. 3(b) shows the discrete Fourier transform (DFT) of the tracking error of the actuator output with and without the backlash, deadzone, and saturation nonlinearities.

The example shows different harmonic components in the output of the actuator due to the input nonlinearities. These harmonics that appear over different excitation frequencies cause oscillations in the output of the actuators. Such oscillations lead to high inaccuracies and may cause instability for the actuators in mechatronic systems, see, for example, [39]–[41].



(a)

(b)

Fig. 4. Command-following tracking error e. (a) Tracking error due to FDI attacks with backlash, deadzone, and saturation nonlinearities. (b) Tracking error due to the delay.

E. Example 2

This example includes a CPMS characterized with the second-order system of

$$G(z) = \frac{z - 0.5}{(z - 0.6)(z - 0.8)} \tag{12}$$

a feedback controller of

$$G_l(z) = \frac{-1.617z^2 + 2.251z - 0.8179}{z^3 - 0.3877z^2 - 0.991z + 1.23} \tag{13}$$

a time delay of $\mathcal{T} = 3$, and a command signal of $r(k) = \sin(0.2\pi k)$. The harmonic input is used to cover the state of the system over different input values. The attack model is driven with $z_a(k) = \sin(\pi k)$ and backlash nonlinearity (7) of $\rho = 0.5$, deadzone nonlinearity (9) of $\sigma = 0.5$, and saturation nonlinearity (11) of $\kappa = 0.5$. Fig. 4(a) shows the error with the attacks and without delay. Fig. 4(b) shows the errors with the attacks and with the delay. It is obvious that the attacks with nonlinear dynamics cause high oscillations and inaccuracies for the closed-loop system, and the delay in the closed-loop systems may causes instability with the nonlinear attacks. Then, in order to stabilize CPMSs with such cyberattacks and delays, it is essential to consider an adaptive control system that can stabilize the closed-loop system against different unknown nonlinear attacks with delays.

III. Adaptive Control for FDI Attacks Mitigation

In this section, we present the RCAC adaptive control that is used in this paper to reject the FDI attacks on CPMSs. Then, we present the internal model control principle in order to investigate the mechanism that the RCAC uses to reject the attacks.

A. Adaptive Control

RCAC is a new discrete control algorithm that uses the concept of retrospectively optimized control, where the past controller coefficients used to reoptimized to enhance the control signal [27], [35]. This adaptive control system, proposed in [43]–[48], obtains the new control signal based on the history and the performance of the previous control signal. This control technique has shown excellent performance in stabilizing different closed-loop systems.

Let the RCAC adaptive controller of order n_c be expressed as

$$u(k) = \sum_{i=1}^{n_c} M_i(k)u(k-i) + \sum_{i=1}^{n_c} N_i(k)e(k-i) \tag{14}$$

where, for all $i = 1, \ldots, n_c$, $M_i(k) \in \mathbb{R}$ and $N_i(k) \in \mathbb{R}$. The control (14) can be expressed as

$$u(k) = \theta(k)\phi(k-1)$$

where

$$\theta(k) \triangleq \begin{bmatrix} M_1(k) \cdots M_{n_c}(k) & N_1(k) \cdots N_{n_c}(k) \end{bmatrix}$$

is the controller gain matrix, and the regressor vector $\phi(k)$ is given by

$$\phi(k-1) \triangleq [u(k-1) \cdots u(k-n_c) \quad e(k-1) \cdots e(k-n_c)]^{\mathrm{T}}.$$

The transfer function matrix of the controller $G_{c,k}(z)$ is

$$G_{c,k}(z) = \frac{N_1(k)z^{n_c-1} + N_2(k)z^{n_c-2} + \cdots + N_{n_c}(k)}{z^{n_c} - M_1(k)z^{n_c-1} + \cdots + M_{n_c-1}(k)z + M_{n_c}(k)}.$$

For $i \geq 1$, define the Markov parameter

$$H_i \triangleq CA^{i-1}B$$

and let ℓ be a positive integer. Then, for all $k \geq \ell$

$$x(k) = A^{\ell}x(k-\ell) + \sum_{i=1}^{\ell} A^{i-1}B\mathcal{N}((u(k-i))) \tag{15}$$

where $\mathcal{N}$ represents the nonlinear dynamics of the attacks on the actuator system. The nonlinear dynamics include backlash, saturation, or deadzone nonlinearities. Thus, the tracking error is

$$e(k) = CA^{\ell}x(k-\ell) - r(k) + \bar{H}\bar{U}(k-1) \tag{16}$$

where

$$\bar{H} \triangleq \begin{bmatrix} H_1 \cdots & H_{\ell} \end{bmatrix} \in \mathbb{R}^{1\times\ell}$$

and

$$\bar{U}(k-1) \triangleq \begin{bmatrix} \mathcal{N}\big((u(k-1))\big) \\ \vdots \\ \mathcal{N}\big((u(k-\ell))\big) \end{bmatrix}.$$

We rearrange the columns of $\bar{H}$ and the components of $\bar{U}(k-1)$ and partition the resulting matrix and vector so that

$$\bar{H}\bar{U}(k-1) = \mathcal{H}'U'(k-1) + \mathcal{H}U(k-1) \tag{17}$$

where $\mathcal{H}' \in \mathbb{R}^{1\times(\ell-l_U)}$, $\mathcal{H} \in \mathbb{R}^{1\times l_U}$, $U'(k-1) \in \mathbb{R}^{\ell-l_U}$, and $U(k-1) \in \mathbb{R}^{l_U}$. Then, we rewrite (16) as

$$e(k) = \mathcal{S}(k) + \mathcal{H}U(k-1) \tag{18}$$

where

$$\mathcal{S}(k) \triangleq CA^{\ell}x(k-\ell) - r(k) + \mathcal{H}'U'(k-1). \tag{19}$$

Furthermore, for $j = 1,\ldots,s$, we rewrite (18) with a delay of k_j time steps, where $0 \le k_1 \le k_2 \le \cdots \le k_s$, in the form

$$e(k-k_j) = \mathcal{S}_j(k-k_j) + \mathcal{H}_j U_j(k-k_j-1). \tag{20}$$

Thus, (19) becomes

$$\mathcal{S}_j(k-k_j) \triangleq CA^{\ell}x(k-k_j-\ell) + \mathcal{H}'_j U'_j(k-k_j-1).$$

Then, (17) can be written as

$$\bar{H}\bar{U}(k-k_j-1) = \mathcal{H}'_j U'_j(k-k_j-1) + \mathcal{H}_j U_j(k-k_j-1)$$

where $\mathcal{H}'_j \in \mathbb{R}^{1\times(\ell-l_{U_j})}$, $\mathcal{H}_j \in \mathbb{R}^{1\times l_{U_j}}$, $U'_j(k-k_j-1) \in \mathbb{R}^{\ell-l_{U_j}}$, and $U_j(k-k_j-1) \in \mathbb{R}^{l_{U_j}}$. Now, by stacking

$$e(k-k_1),\ldots,e(k-k_s)$$

we define the *extended performance* as

$$E(k) \triangleq \begin{bmatrix} e(k-k_1) \\ \vdots \\ e(k-k_s) \end{bmatrix} \in \mathbb{R}^{s}. \tag{21}$$

Therefore

$$E(k) \triangleq \tilde{\mathcal{S}}(k) + \tilde{\mathcal{H}}\tilde{U}(k-1) \tag{22}$$

where

$$\tilde{\mathcal{S}}(k) \triangleq \begin{bmatrix} \mathcal{S}_1(k-k_1) \\ \vdots \\ \mathcal{S}_s(k-k_s) \end{bmatrix} \in \mathbb{R}^{s}.$$

Also, $\tilde{U}(k-1)$ has the form

$$\tilde{U}(k-1) \triangleq \begin{bmatrix} \mathcal{N}\big(u(k-q_1)\big) \\ \vdots \\ \mathcal{N}\big(u(k-q_{l_{\tilde{U}}})\big) \end{bmatrix} \in \mathbb{R}^{l_{\tilde{U}}}$$

where, for $i = 1,\ldots,l_{\tilde{U}}$, $k_1 \le q_i \le k_s + \ell$, and $\tilde{\mathcal{H}} \in \mathbb{R}^{s\times l_{\tilde{U}}}$ is constructed according to the structure of $\tilde{U}(k-1)$. The vector $\tilde{U}(k-1)$ is formed by stacking

$$U_1(k-k_1-1),\ldots,U_s(k-k_s-1)$$

and removing copies of repeated components. Next, for $j = 1,\ldots,s$, we define the *retrospective performance*

$$\hat{e}_j(k-k_j) \triangleq \mathcal{S}_j(k-k_j) + \mathcal{H}_j\hat{U}_j(k-k_j-1) \tag{23}$$

where the past controls $U_j(k-k_j-1)$ in (20) are replaced by the retrospective controls $\hat{U}_j(k-k_j-1)$. In analogy with (21), the *extended retrospective performance* for (23) is defined as

$$\hat{E}(k) \triangleq \begin{bmatrix} \hat{e}_1(k-k_1) \\ \vdots \\ \hat{e}_s(k-k_s) \end{bmatrix} \in \mathbb{R}^{s}$$

and thus is given by

$$\hat{E}(k) = \tilde{\mathcal{S}}(k) + \tilde{\mathcal{H}}\hat{\tilde{U}}(k-1) \tag{24}$$

where the components of $\hat{\tilde{U}}(k-1) \in \mathbb{R}^{l_{\tilde{U}}}$ are the components of

$$\hat{U}_1(k-k_1-1),\ldots,\hat{U}_s(k-k_s-1)$$

ordered in the same way as the components of $\tilde{U}(k-1)$. Subtracting (22) from (24) yields

$$\hat{E}(k) = E(k) - \tilde{\mathcal{H}}\tilde{U}(k-1) + \tilde{\mathcal{H}}\hat{\tilde{U}}(k-1). \tag{25}$$

Finally, we define the *retrospective cost function*

$$\mathcal{Q}(\hat{\tilde{U}}(k-1),k) \triangleq \hat{E}^{\mathrm{T}}(k)R(k)\hat{E}(k) \tag{26}$$

where $R(k) \in \mathbb{R}^{s\times s}$ is a positive-definite performance weighting. The goal is to determine refined controls $\hat{\tilde{U}}(k-1)$ that, when applied to the system, will provide better performance than the controls $U(k)$. The refined control values $\hat{\tilde{U}}(k-1)$ are subsequently used to update the controller. In addition, to ensure that (26) has a global minimizer, the following regularized cost is used

$$\begin{aligned}\bar{\mathcal{Q}}(\hat{\tilde{U}}(k-1),k) \triangleq\ & \hat{E}^{\mathrm{T}}(k)R(k)\hat{E}(k) \\ & + \eta(k)\hat{\tilde{U}}^{\mathrm{T}}(k-1)\hat{\tilde{U}}(k-1)\end{aligned} \tag{27}$$

where $\eta(k) \ge 0$. Substituting (25) into (27) yields

$$\begin{aligned}\bar{\mathcal{Q}}(\hat{\tilde{U}}(k-1),k) = & \hat{\tilde{U}}(k-1)^{\mathrm{T}}\mathcal{A}(k)\hat{\tilde{U}}(k-1) \\ & + \mathcal{B}(k)\hat{\tilde{U}}(k-1) + \mathcal{C}(k)\end{aligned} \tag{28}$$

where

$$\begin{aligned}\mathcal{A}(k) &\triangleq \tilde{\mathcal{H}}^{\mathrm{T}}R(k)\tilde{\mathcal{H}} + \eta(k)I_{l_{\tilde{U}}} \\ \mathcal{B}(k) &\triangleq 2\tilde{\mathcal{H}}^{\mathrm{T}}R(k)[E(k) - \tilde{\mathcal{H}}\tilde{U}(k-1)] \\ \mathcal{C}(k) &\triangleq E^{\mathrm{T}}(k)R(k)E(k) - 2E^{\mathrm{T}}(k)R(k)\tilde{\mathcal{H}}\tilde{U}(k-1) \\ &\quad + \tilde{U}^{\mathrm{T}}(k-1)\tilde{\mathcal{H}}^{\mathrm{T}}R(k)\tilde{\mathcal{H}}\tilde{U}(k-1).\end{aligned}$$

If either $\tilde{\mathcal{H}}$ has full column rank or $\eta(k) > 0$, then $\mathcal{A}(k)$ is positive definite. In this case, $\bar{J}(\hat{\tilde{U}}(k-1), k)$ has the unique global minimizer

$$\hat{\tilde{U}}(k-1) = -\frac{1}{2}\mathcal{A}^{-1}(k)\mathcal{B}(k). \tag{29}$$

Then, we define the cumulative cost function as

$$\begin{aligned}\mathcal{Q}_R(\theta, k) \triangleq \sum_{i=2}^{k} \|\phi^{\mathrm{T}}(i-2)\theta^{\mathrm{T}}(k) - \hat{u}^{\mathrm{T}}(i-1)\|^2 \\ + (\theta(k) - \theta_0)P_0^{-1}(\theta(k) - \theta_0)^{\mathrm{T}}\end{aligned} \tag{30}$$

where $\| \cdot \|$ is the Euclidean norm. Minimizing (30) yields

$$\begin{aligned}\theta^{\mathrm{T}}(k) &= \theta^{\mathrm{T}}(k-1) + P(k-1)\phi(k-2) \\ &\quad [\phi^{\mathrm{T}}(k-1)P(k-1)\phi(k-2)] \\ &\quad + [\phi^{\mathrm{T}}(k-2)\theta^{\mathrm{T}}(k-1) - \hat{u}^{\mathrm{T}}(k-1)].\end{aligned}$$

The error covariance is updated by

$$\begin{aligned}P(k) &= P(k-1) - P(k-1)\phi(k-2) \\ &\quad [\phi^{\mathrm{T}}(k-2)P(k-1)\phi(k-1) + 1]^{-1} \\ &\quad \phi^{\mathrm{T}}(k-2)P(k-1).\end{aligned}$$

The error covariance matrix is $P(0) = \alpha I_{2n_c}$, where α is a positive constant. The next section shows that the proposed controller achieves internal model principle control in the presence of cyberattacks with nonlinear dynamics.

B. Internal Model Control Principle

This section presents the internal model control principle with attacks in CPMSs presented in Fig. 2. Consider the closed-loop system shown in Fig. 2 with the harmonic command of $r(k) = \mathrm{Re}\{A_r(e^{j\Omega})\}$, where A_r is a complex number and Ω is the command frequency. For analysis only, the main harmonic component is used in the closed-loop system for the phase-shift calculations. The transfer function $G_{\mathcal{T}}$ is used to present the harmonic component of the delay. $G_{\mathrm{c},J}$ is the transfer function of the RCAC adaptive controller at the steady state J. The transfer function $A_{\mathcal{N}}$ is used to present the main harmonic component in the nonlinearity of the attack. The attack $A_{\mathcal{N}}$ is unknown and inserted in the closed-loop system of Fig. 2. Then, we examine the magnitude and phase of

$$G_{ur}(e^{j\Omega}) \triangleq \frac{G_{\mathrm{c},J}(e^{j\Omega})}{1 + G_{\mathcal{T}}G_{\mathcal{T}}A_{\mathcal{N}}G_{\mathcal{A}}G_{\mathrm{c},J}(e^{j\Omega})} \tag{31}$$

where

$$G_{\mathcal{A}} \triangleq \frac{GG_l}{1 + GG_l} \tag{32}$$

and

$$G_{ry}(e^{j\Omega}) \triangleq \frac{A_{\mathcal{N}}G_{\mathcal{T}}G_{\mathcal{A}}}{1 + G_{\mathcal{T}}G_{\mathcal{T}}A_{\mathcal{N}}G_{\mathcal{A}}G_{\mathrm{c},J}(e^{j\Omega})}. \tag{33}$$

The magnitude $|G_{ur}(e^{j\Omega})|$ reveals whether the controller $G_{\mathrm{c},J}(e^{j\Omega})$ provides high magnitude at the command frequencies and their harmonics introduced by the attacks and closed-loop system delay. The phase $\angle G_{ur}(e^{j\Omega})$ shows whether $G_{\mathrm{c},J}(e^{j\Omega})$ compensates the phase shift provided by the attacks at the command frequency. To regulate the command-following error e to 0 at the frequency Ω, it follows from:

$$r(k) = G_{ur}(e^{j\Omega})G_{ry}(e^{j\Omega})r(k) \tag{34}$$

that

$$G(e^{j\Omega})G_{ur}(e^{j\Omega}) = 1. \tag{35}$$

The gain and phase of G_{ur}, therefore, must satisfy

$$|G_{ur}(e^{j\Omega})| = \frac{1}{|G_{uy}(e^{j\Omega})|} \tag{36}$$

$$\angle G_{ur}(e^{j\Omega}) = -\angle G_{uy}(e^{j\Omega}). \tag{37}$$

The above-mentioned analysis is used in the next section to show that the RCAC adaptive control achieves internal model control principle with attacks in CPMSs.

IV. Numerical Results

In this section, the RCAC adaptive controller is used to reject the effects of the backlash, deadzone, and saturation attacks on actuators in the CPMSs. We use the discrete transfer of (12) with uncertainties given by

$$G(z) = \frac{z - 0.3}{(z - 0.5)(z - 0.9)} \tag{38}$$

and the feedback controller of (13). We inject attacks with backlash, deadzone, and saturation nonlinearities as follows.

A. Time Delay

The capability of the RCAC adaptive controller to stabilize closed-loop systems with constant delay is examined. This section ignores the cyberattacks, then $z_a(k) = 0$ and $\mathcal{N} = 0$. The CPMS is characterized with the linear plant (38) and the feedback controller (13) with the command signal of $r(k) = \sin(0.2\pi k)$ and $\mathcal{T} = 3$ steps and $\mathcal{T} = 6$ steps as communication delays in the network. Fig. 5 shows the simulation results with the RCAC adaptive controller of $\alpha = 0.1$ and $n_c = 3$. At $t = 300$ s and $\mathcal{T} = 3$, the adaptive control system is

$$G_c(z) = \frac{-0.3527z^20 + .3132z - 0.3232}{z^3 + 0.8195z^2 - 0.5567z + 0.7369} \tag{39}$$

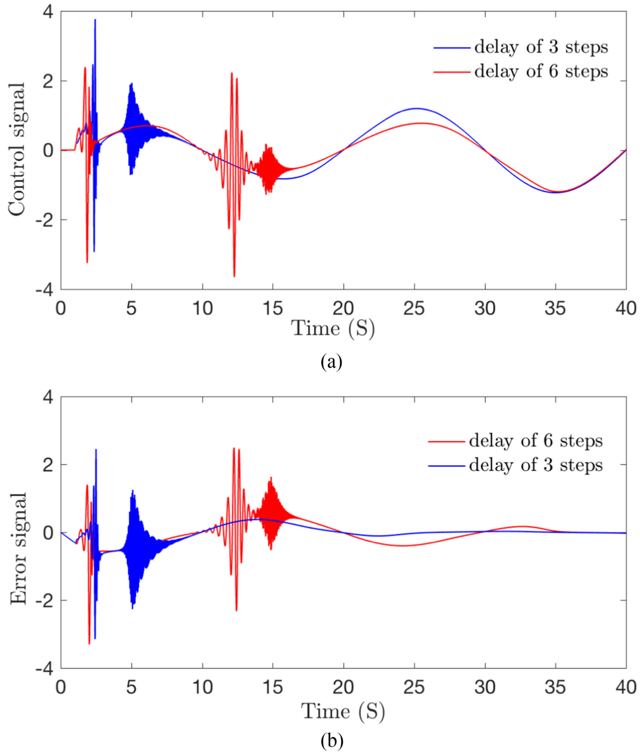
and at $\mathcal{T} = 6$ the adaptive control system is

$$G_c(z) = \frac{-0.4430z^20 + 0.2549z - 0.0249}{z^3 + 0.7088z^2 + 0.1593z + 0.1315}. \tag{40}$$

We conclude that the RCAC can stabilize closed-loop systems that include uncertainties in the linear dynamics with bounded delays.

B. Mitigating Attacks With Backlash Nonlinearities

In this section, the linear dynamic system (38) and the feedback controller (13) are used to represent a CPMS. We use the command signal $r(k) = \sin(0.2\pi k)$, the attack model with



(a)

(b)

Fig. 5. Simulation results of the closed-loop system in Fig. 2 with the actuator system (38), control system (13), the adaptive control system (39) for $\mathcal{T} = 3$, and (40) for $\mathcal{T} = 6$. (a) RCAC control signal. (b) Tracking error.

$z_a(k) = \sin(0.2\pi k)$, backlash nonlinearity (7) of $\rho = 0.5$, and $\mathcal{T} = 3$ as a communication delay in the network. The controller is activated at 150 s. We use $n_c = 3$ and $\alpha = 0.1$. The RCAC adaptive controller G_c at 300 s is

$$G_c(z) = \frac{-0.5728z^2 - 0.0513z + 0.4211}{z^3 + 0.5237z^2 + 0.3310z + 0.0971}. \tag{41}$$

Fig. 6(a)–(e) shows the simulation results for $\mathcal{T} = 3$ and Fig. 6(f)–(h) shows the simulation results for $\mathcal{T} = 6$. The adaptive controller with $\mathcal{T} = 6$ is

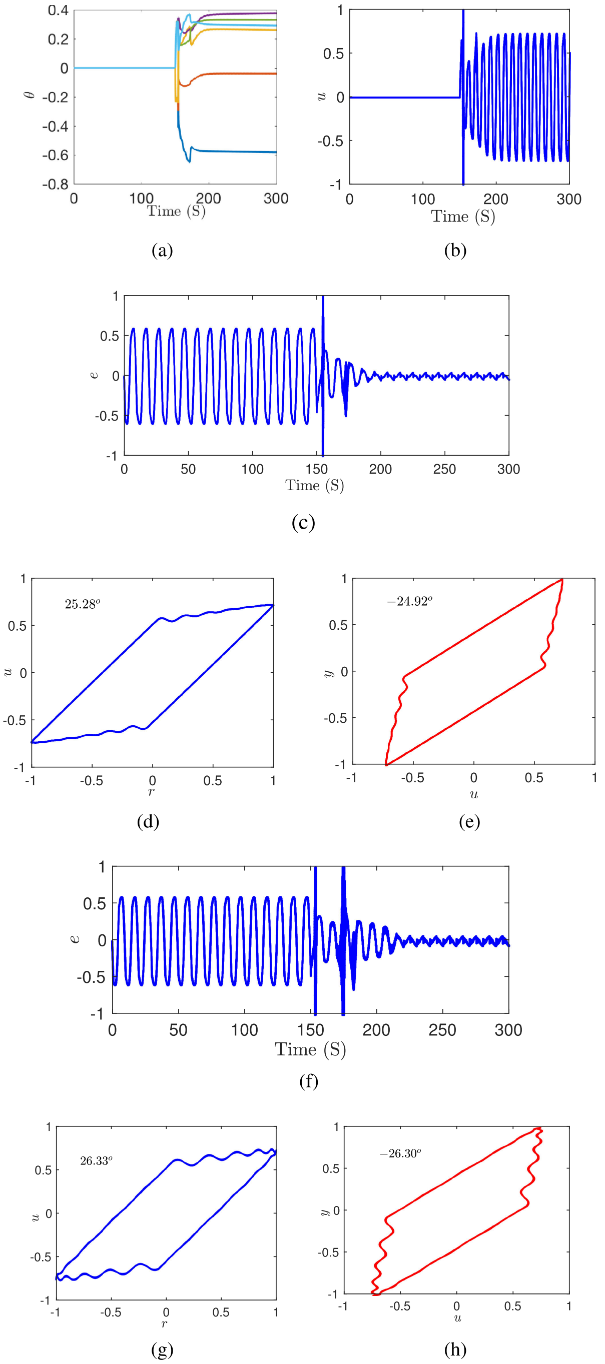
$$G_c(z) = \frac{-0.5825z^2 - 0.2599z - 0.0395}{z^3 + 0.3767z^2 + 0.3310z + 0.2914}. \tag{42}$$

The results show that the adaptive controller rejects the backlash attack and stabilizes the closed-loop system. At $t = 300$, Fig. 6(d) shows phase shift of 25.28° between the control signal $u(k)$ and the output $y(k)$, and Fig. 6(e) shows phase shift of −24.92° between the command signal $r(k)$ and the control signal $u(k)$. Fig. 6(g)–(h) shows similar results.

C. Mitigating Attacks With Deadzone Nonlinearities

The simulation of the previous section is used with deadzone nonlinearity (9) of $\sigma = 0.5$. We consider the command signal of $r(k) = \sin(0.2\pi k)$, the attack model with $z_a(k) = \sin(0.2\pi k)$, and $\mathcal{T} = 3$ as a communication delay in the network. The controller is activated at 150 s. The RCAC adaptive controller with $\alpha = 0.1$ and $n_c = 3$ at 300 s is

$$G_c(z) = \frac{-0.0714z^2 - 0.1187z - 0.1558}{z^3 + 0.6159z^2 - 0.5022z + 0.8846}. \tag{43}$$



(a)

(b)

(c)

(d)

(e)

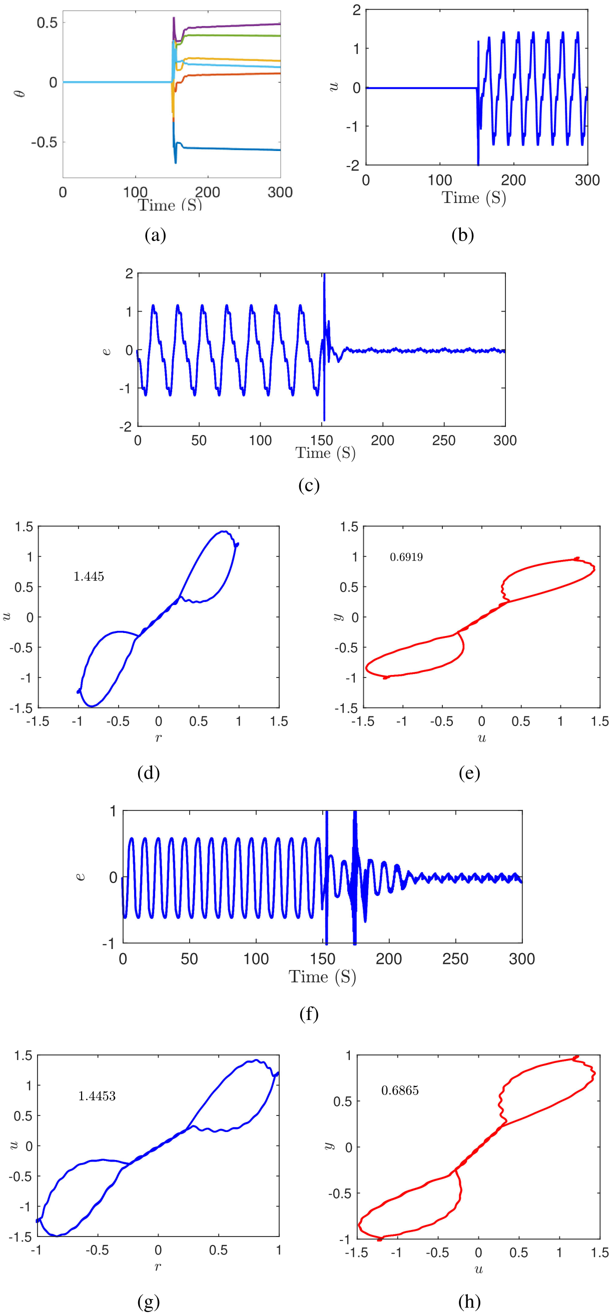
(f)

(g)

(h)

Fig. 6. Mitigating attacks with backlash nonlinearities. (a) Evolution of the controller coefficients $\theta(k)$. (b) Control signal $u(k)$. (c) Tracking error $e(k)$. (d) Command signal $r(k)$ versus the control signal $u(k)$. (e) Control signal $u(k)$ versus the output signal $y(k)$. (f) Tracking error $e(k)$. (g) Command signal $r(k)$ versus the control signal $u(k)$. (h) Control signal $u(k)$ versus the output signal $y(k)$. Simulation results are shown for (a)–(e) $\mathcal{T} = 3$ and (f)–(h) $\mathcal{T} = 6$.

Fig. 7(a)–(e) shows the simulation results for $\mathcal{T} = 3$ and Fig. 7(f)–(h) shows the simulation results for $\mathcal{T} = 6$. The



(a) (b) (c) (d) (e) (f) (g) (h)

Fig. 7. Mitigating attacks with deadzone nonlinearities. (a) Evolution of the controller coefficients $\theta(k)$. (b) Control signal $u(k)$. (c) Tracking error $e(k)$. (d) Command signal $r(k)$ versus the control signal $u(k)$. (e) Control signal $u(k)$ versus the output signal $y(k)$. (f) Tracking error $e(k)$. (g) Command signal $r(k)$ versus the control signal $u(k)$. (h) Control signal $u(k)$ versus the output signal $y(k)$. Simulation results are shown for (a)–(e) $\mathcal{T} = 3$ and (f)–(h) $\mathcal{T} = 6$.

adaptive controller with for $\mathcal{T} = 6$ is

$$G_c(z) = \frac{-0.5678z^2 + 0.1784z + 0.4857}{z^3 + 0.4857z^2 + 0.3876z + 0.1260}. \tag{44}$$

The results show that the adaptive controller rejects the deadzone nonlinearity attack and stabilizes the closed-loop system. At $t = 300$, Fig. 7(d) shows a gain of 1.445 between the control signal $u(k)$ and the output $y(k)$, and Fig. 7(e) shows a gain of 0.6919 between the command signal $r(k)$ and the control signal $u(k)$. Fig. 7(g)–(h) show similar results.

D. Mitigating Attacks With Saturation Nonlinearities

The simulation of the previous section is used with the saturation nonlinearity (11) of $\kappa = 0.5$. We consider the command signal of $r(k) = \sin(0.2\pi k)$, the attack model of $z_a(k) = \sin(0.2\pi k)$, and $\mathcal{T} = 3$ as a communication delay in the network. The controller is activated at 150 s. The RCAC adaptive controller with $\alpha = 0.1$ and $n_c = 3$ at 300 s is

$$G_c(z) = \frac{-0.5180z^2 + 0.2135z + 0.0288}{z^3 + 0.7824z^2 - 0.0353z + 0.2522}. \tag{45}$$

Fig. 8(a)–(e) shows the simulation results for $\mathcal{T} = 3$, and Fig. 8(f)–(h) shows the simulation results with $\mathcal{T} = 6$. The adaptive controller for $\mathcal{T} = 6$ is

$$G_c(z) = \frac{-0.6487z^2 + 0.0971z + 0.3705}{z^3 + 0.6535z^2 + 0.3497z - 0.0042}. \tag{46}$$

Similarly, the adaptive control effectively rejects this type of FDI attack and stabilizes the closed-loop control system. At $t = 300$, Fig. 8(d) shows phase shift of 5.1476° between the control signal u and the output y, and Fig. 8(e) shows phase shift of $-4.493°$ between the command signal r and the control signal u. Fig. 8(g) and (h) shows similar results.

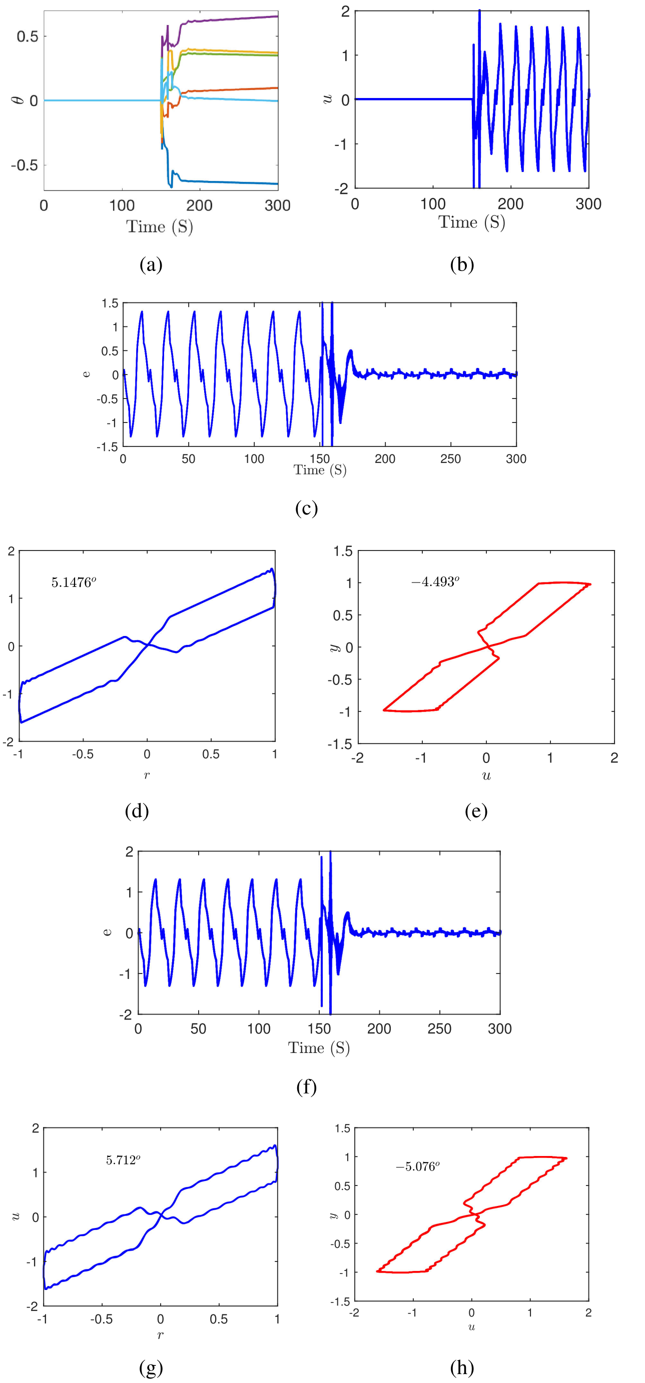
V. Mitigating Attacks With Uncertainties in the Actuator System

In this section, the FDI attacks on actuators that show nonlinear dynamics in their outputs are studied. These actuators are characterized with the Hammerstein system shown in Fig. 9. This system, which consists of a nonlinear model followed by a linear system, has been widely used to represent the nonlinear dynamics of different mechatronic systems, such as piezoceramics, magnetostrictive actuators, and shape-memory-alloy actuators [38]–[42]. These actuators have been recently used in different micro/nanopositioning control systems. The most well-known nonlinearity that affects the performance of these actuators is the hysteresis nonlinearity [42]. In this section, we focus on the mitigating attacks on actuator systems that show hysteresis uncertainties in their dynamics.

The following Hammerstein model of a Prandtl–Ishlinskii hysteresis model and linear dynamic system of (38) is used. This model has been employed recently to model the nonlinear dynamics of different piezoceramic and magnetostrictive actuators [54] and [55]. The output of the model is

$$\mathcal{H}[v](k) = \sum_{i=1}^{n} g_i \mathcal{F}_i[v](k) \tag{47}$$

where g_i are positive weights and $\mathcal{F}_i[v](k)$ is the output of the backlash operator with the threshold ρ_i. We used three backlash operators $n = 3$ with weights and thresholds of $g_1 = 0.37$, $\rho_1 = 0$, $g_2 = 0.27$, $\rho_2 = 0.15$, $g_3 = 0.37$, and $\rho_3 = 0.25$. The



(a) (b) (c) (d) (e) (f) (g) (h)

Fig. 8. Mitigating attacks with saturation nonlinearities. (a) Evolution of the controller coefficients $\theta(k)$. (b) Control signal $u(k)$. (c) Tracking error $e(k)$. (d) Command signal $r(k)$ versus the control signal $u(k)$. (e) Control signal $u(k)$ versus the output signal $y(k)$, (f) Tracking error $e(k)$. (g) Command signal $r(k)$ versus the control signal $u(k)$. (h) Control signal $u(k)$ versus the output signal $y(k)$. Simulation results are shown for (a)–(e) $\mathcal{T} = 3$ and (f)–(h) $\mathcal{T} = 6$.

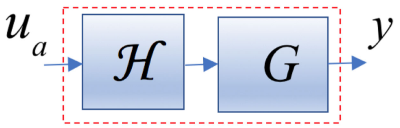


Fig. 9. Hammerstein system for the actuator system.

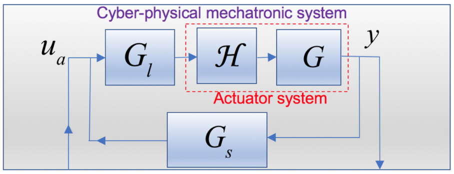


Fig. 10. Closed-loop system with a Hammerstein system for the actuator system.

simulation of Sections IV.B, IV.C, and IV.D with this Hammerstein system is shown in the closed-loop system in Fig. 10. The RCAC adaptive controller with $\alpha = 1$ and $n_c = 3$ at 300 s for the deadzone attack is

$$G_c(z) = \frac{-0.5767z^2 - 0.0115z + 0.3090}{z^3 + 0.5895z^2 + 0.1578z + 0.2519}. \tag{48}$$

Fig. 11(a)–(c) shows the simulation results. For the saturation attack the adaptive controller at 300 s is

$$G_c(z) = \frac{-0.9817z^2 + 0.4542z + 0.3255}{z^3 + 1.0591z^2 + 0.7453z + 0.7352}. \tag{49}$$

Fig. 11(d)–(f) shows the simulation results. For the backlash attack the adaptive controller at 300 s is

$$G_c(z) = \frac{-0.5598z^2 - 0.007z + 0.2966}{z^3 + 0.6095z^2 + 0.1464z + 0.2433}. \tag{50}$$

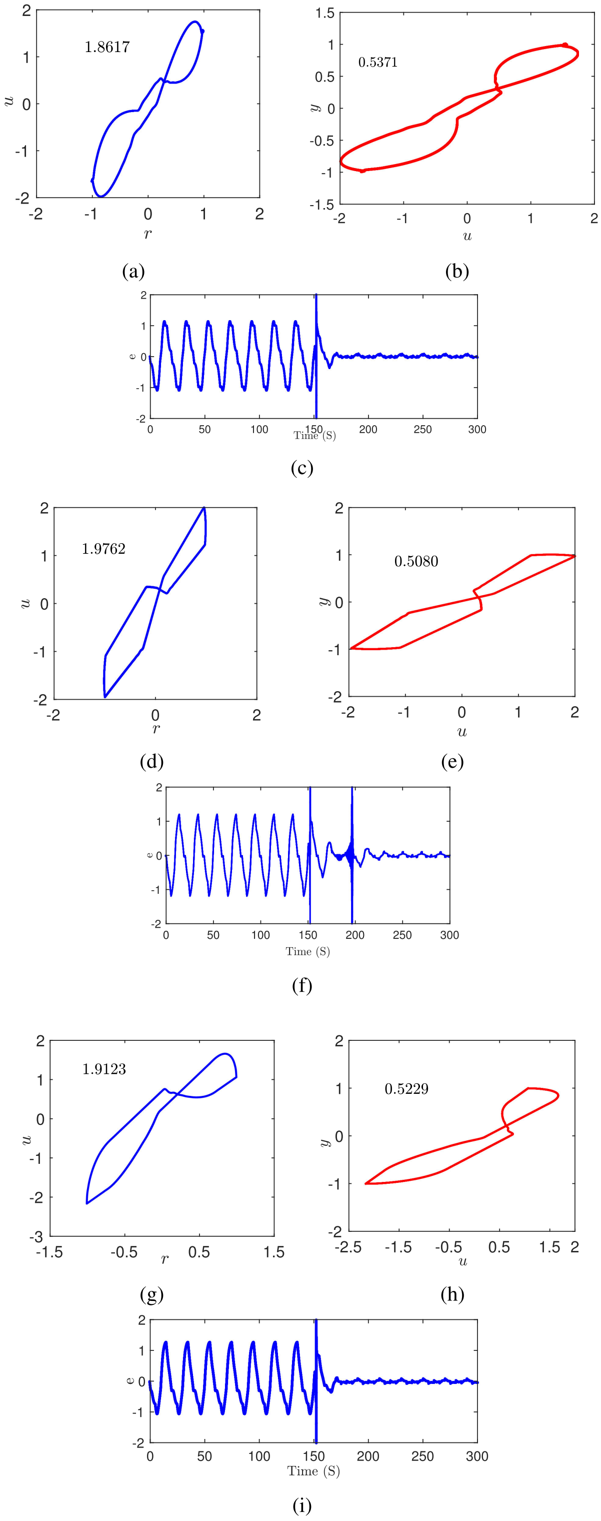
The results show that the RCAC adaptive controller rejects the attacks and stabilizes the closed-loop system.

VI. Application to a Mechatronic System

In this section, we apply the attacks with backlash, deadzone, and saturation nonlinearities on a CPMS that represents a microgripper system [56]. This microgripper has been integrated in microrobots to provide micrometers motion for micromanipulation and pick-and-place tasks. The relationship between the input voltage (V) and the output displacement (μ m) of the microgripper is expressed as [56]

$$G(z) = \frac{0.925z + 0.3952}{z^2 + 0.5384z + 0.2828}. \tag{51}$$

To represent the microgripper system with attacks, Fig. 2 is used with a proportional-integrator controller in $G_l(z)$, the linear dynamic model (51), and $\mathcal{T} = 3$ for the communication delay in the network. The microgripper system is operated with the command signal of $r(k) = \sin(0.2\pi k)$, the attack model of $z_a(k) = \sin(0.2\pi k)$, backlash nonlinearity (7) of $\rho = 0.5$, deadzone nonlinearity (9) of $\sigma = 0.5$, and saturation nonlinearity (11) of $\kappa = 0.5$. For the RCAC adaptive controller, we use $n_c = 6$ and $\alpha = 0.23$. The controller is activated at 100 s. Fig. 12 shows the simulation results. In this section, a FDI attack with unknown nonlinear dynamics for a microgripper system is presented. The results show that the adaptive controller rejects the impact of the backlash, deadzone, and saturation nonlinearities.



(a) (b)

(c)

(d) (e)

(f)

(g) (h)

(i)

Fig. 11. Mitigating attacks for Hammerstein system (9) and (38) with attacks of deadzone nonlinearities: (a) Command signal $r(k)$ versus the control signal $u(k)$; (b) control signal $u(k)$ versus the output signal $y(k)$; and (c) tracking error $e(k)$. Mitigating attacks for Hammerstein system (9) and (38) with attacks of saturation nonlinearities: (d) Command signal $r(k)$ versus the control signal $u(k)$; (e) control signal $u(k)$ versus the output signal $y(k)$; and (f) tracking error $e(k)$. Mitigating attacks for Hammerstein system (9) and (38) with attacks of backlash nonlinearities: (g) Command signal $r(k)$ versus the control signal $u(k)$; (h) control signal $u(k)$ versus the output signal $y(k)$; and (i) tracking error $e(k)$.

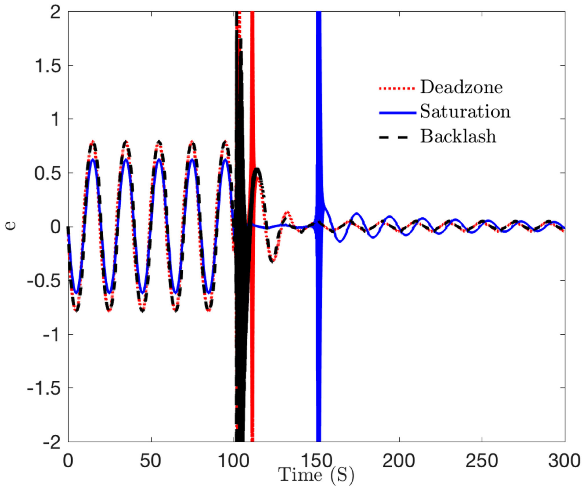


Fig. 12. Tracking error $e(k)$ of the microgripper system (51) with command signal $r(k) = \sin(0.2\pi k)$ and the attack model of $z_a(k) = \sin(0.2\pi k)$ backlash nonlinearity (7) of $\rho = 0.5$, deadzone nonlinearity (9) of $\sigma = 0.5$, and saturation nonlinearity (11) of $\kappa = 0.5$. The communication delay in the network is $\mathcal{T} = 3$.

VII. Conclusion

This paper addresses the problem of reactive mitigation against FDI attacks that exploit nonlinear dynamics of CPMSs. These nonlinear dynamics include the backlash, deadzone, and saturation nonlinearities. The attacks of backlash, deadzone, and saturation nonlinearities degrade the performance of mechatronic actuators, and causes high oscillation and inaccuracies in the output responses. The adaptive control is used to reject the effects of these attacks. Specifically, the RCAC adaptive controller rejects the effects of cyberattacks that include nonlinear dynamics on mechatronic actuators. The proposed framework employs a closed-loop system constructed with an actuator, local control, a feedback signal, and communication links that result in time delays. The adaptive controller is demonstrated to perfectly reject the effect of backlash, deadzone, and saturation nonlinearities. The RCAC adaptive controller acts as internal model control and inverts the effects of the attacks on the dynamics. The results show promise in the application of RCAC to stabilize and control CPMSs under cyberattacks.

References

[1] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[2] L. Monostori *et al.*, "Cyber-physical systems in manufacturing," *CIRP Ann.*, vol. 65, no. 2, pp. 621–641, 2016.

[3] A. Takacs, P. Galambos, P. Pausits, I. Rudas, and T. Haidegger, "Nonlinear soft tissue models and force control for medical cyber-physical systems," in *Proc. Int. Conf. Syst., Man, Cybern.*, 2015, pp. 1520–1525.

[4] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[5] K. Zetter, "A cyberattack has caused confirmed physical damage for the second time ever," *Wired Mag.*, 2016.

[6] R. Lee, A. Assante, and C. Tim, "Analysis of the cyber attack on the Ukrainian power grid," *SANS Ind. Control Syst.*, pp. 1–29, Mar. 2016.

[7] K. Hamedani, L. Liu, A. Rachad, J. Wu, and Y. Yi, "Reservoir computing meets smart grids: Attack detection using delayed feedback networks," *IEEE Trans. Ind. Inform.*, vol. 14, no. 2, pp. 734–743, Feb. 2018.

[8] D. Ding, Q. Han, Y. Xiang, X. Ge, and X. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018.

[9] F. Fei *et al.*, "Cross-layer retrofitting of UAVs against cyber-physical attacks," in *Proc. Int. Conf. Robot. Autom.*, 2018, pp. 550–557.

[10] X. Huang and J. Dong, "Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks," *IEEE Trans. Cybernet.*, vol. 48, no. 12, pp. 3432–3439, Dec. 2018.

[11] A. Lu and G. Yang, "Secure Luenberger-like observers for cyberphysical systems under sparse actuator and sensor attacks," *Automatica*, vol. 98, pp. 124–129, 2018.

[12] J. Yan, Y. Wan, X. Luo, C. Chen, C. Hua, and X. Guan, "Formation control of teleoperating cyber-physical system with time delay and actuator saturation," *IEEE Trans. Control Syst. Technol.*, vol. 26, no. 4, pp. 1458–1467, Jul. 2018.

[13] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.

[14] L. Zhang, J. Sun, and G. Orosz, "Hierarchical design of connected cruise control in the presence of information delays and uncertain vehicle dynamics," *IEEE Trans. Control Syst. Technol.*, vol. 26, no. 1, pp. 139–150, Jan. 2018.

[15] L. Wang, M. Torngren, and M. Onori, "Current status and advancement of cyberphysical systems in manufacturing," *J. Manuf. Syst.*, vol. 37, pp. 517–527, 2015.

[16] P. Hehenberger, H. Thomas, and J. Torry-Smith, "From mechatronic systems to cyber-physical systems: Demands for a new design methodology," in *Mechatronic Futures*. Cham, Switzerland: Springer, 2016, pp. 147–163.

[17] P. Leitaao, A. Colombo, and S. Karnouskos, "Industrial automation based on cyber-physical systems technologies: Prototype implementations and Challenges," *Comput. Ind.*, vol. 81, pp. 11–25, Sep. 2016.

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

[19] D. Ding, Z. Wang, D. Ho, and G. Wei, "Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks," *IEEE Trans. Cybernet.*, vol. 47, no. 8, pp. 1936–1947, Aug. 2017.

[20] X. Jin, W. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 6058–6064, Nov. 2017.

[21] T. Yucelen, W. Haddad, and E. Feron, "Adaptive control architectures for mitigating sensor attacks in cyber-physical systems," *Cyber-Phys. Syst.*, vol. 2, pp. 24–52, 2016.

[22] X. Huang and J. Dong, "Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks," *IEEE Trans. Cybernet.*, vol. 48, no. 12, pp. 3432–3439, Dec. 2018.

[23] Z. Guo, D. Shi, K. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, Mar. 2017.

[24] M. Al Janaideh and D. Bernstein, "Adaptive control of uncertain Hammerstein systems with hysteretic nonlinearities," *Proc. Decision Control*, Los Angeles, CA, 2014, pp. 545–550.

[25] Y. Rahman, A. Xie, J. Hoagg, and D. Bernstein, "A tutorial and overview of retrospective cost adaptive control," in *Proc. Conf. Amer. Control Conf.*, Boston, MA, USA, 2016, pp. 3386–3409.

[26] M. Al Janaideh and D. Bernstein, "Adaptive control of Hammerstein systems with unknown input nonlinearity and partially modeled linear dynamics," *Int. J. Control Autom. Syst.*, vol. 14, pp. 957–966, 2016.

[27] Y. Rahman, A. Xie, and D. Bernstein, "Retrospective cost adaptive control: Pole placement, frequency response, and connections with LQG control," *IEEE Control Syst. Mag.*, vol. 37, no. 5, pp. 28–69, Oct. 2017.

[28] H. Khalil, *Nonlinear Systems*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1996.

[29] M. Krstic, I. Kanellakopoulos, and P. Kokotovic, *Nonlinear and Adaptive Control Design*. New York, NY, USA: Wiley, 1995.

[30] A. Cavallo, C. Natale, S. Pirozzi, and C. Visone, "Limit cycles in control systems employing smart actuators with hysteresis," *IEEE/ASME Trans. Mechatronics*, vol. 10, no. 2, pp. 172–180, Apr. 2005.

[31] J. Slotine and W. Li, *Applied Nonlinear Control*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1991.

[32] O. Kouhei, M. Shibata, and T. Murakami, "Motion control for advanced mechatronics," *IEEE/ASME Trans. Mechatronics*, vol. 1, no. 1, pp. 56–67, Mar. 1996.

[33] C. W. de Silva, *Mechatronics: An Integrated Approach*. Boca Raton, FL, USA: CRC Press, 2004.

[34] M. Nordin and G. Per-Olof, "Controlling mechanical systems with backlash—a survey," *Automatica*, vol. 38, pp. 1633–1649, 2002.

[35] Y. Rahman and D. Bernstein, "Adaptive control of plants that are practically impossible to control by fixed-gain control laws," in *Proc. IEEE Conf. Decis. Control*, Las Vegas, NV, USA, 2016, pp. 383–388.

[36] S. Khadraoui, M. Rakotondrabe, and P. Lutz, "Interval modeling and robust control of piezoelectric microactuators," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 2, pp. 486–494, Mar. 2012.

[37] K. Astrom, T. Johan, and K. Astrom, *Advanced PID Control*. Research Triangle Park, NC, USA: ISA, 2006.

[38] K. Astrom and T. Johan, "The future of PID control," *Control Eng. Pract.*, vol. 9, pp. 1163–1175, 2001.

[39] J. Voros, "Modeling and identification of systems with backlash," *Automatica*, vol. 46, pp. 369–374, 2010.

[40] N. Hieu, S. Odomari, T. Yoshida, T. Senjyu, and A. Yona, "Nonlinear adaptive control of ultrasonic motors considering dead-zone," *IEEE Trans. Ind. Inform.*, vol. 9, no. 4, pp. 1847–1854, Nov. 2013.

[41] R. Mantri, A. Saberi, and V. Venkatasubramanian, "Stability analysis of continuous time planar systems with state saturation nonlinearity," *IEEE Trans. Circuits Syst.*, vol. 45, no. 9, pp. 989–993, Sep. 1998.

[42] D. S. Bernstein, "Ivory ghost," *IEEE Control Syst. Mag.*, vol. 27, no. 5, pp. 16–17, Oct. 2007.

[43] A. D'Amato, A. Ali, A. Ridley, and D. Bernstein, "Retrospective cost optimization for adaptive state estimation, input estimation, and model refinement," *Procedia Comput. Sci.*, vol. 18, pp. 1919–1928, 2013.

[44] J. Yan, A. D'Amato, E. Sumer, J. Hoagg, and D. Bernstein, "Adaptive control of uncertain Hammerstein systems with monotonic input nonlinearities using auxiliary nonlinearities," in *Proc. IEEE Conf. Decis. Control*, 2012, pp. 4811–4816.

[45] J. Yan and D. Bernstein, "Minimum modelling retrospective cost adaptive control of uncertain Hammerstein systems using auxiliary nonlinearities," *Int. J. Control*, vol. 87, , pp. 483–505, 2014.

[46] M. Yu and D. Bernstein, "Retrospective cost subsystem estimation and smoothing for linear systems with structured uncertainty," *J. Aerosp. Inf. Syst.*, vol. 15, pp. 566–584, 2018.

[47] M. Al Janaideh and D. Bernstein, "Adaptive control of Hammerstein systems with unknown Prandtl–Ishlinskii hysteresis," *J. Syst. Control Eng.*, vol. 229, pp. 149–157, 2015.

[48] F. Sobolic and D. Bernstein, "Retrospective cost adaptive control with concurrent closed-loop identification of time-varying nonminimum-phase zeros," in *Proc. IEEE Decis. Control Conf.*, 2018, pp. 371–376.

[49] R, Gorbet, K. Morris, and D. Wang, "Passivity-based stability and control of hysteresis in smart actuators," *IEEE Trans. Control Syst. Technol.*, vol. 9, no. 1, pp. 5–16, Jan. 2001.

[50] J. Nealis and R. Smith, "Model-based robust control design for magnetostrictive transducers operating in hysteretic and nonlinear regimes," *IEEE Trans. Control Syst. Technol.*, vol. 15, no. 1, pp. 22–39, Jan. 2007.

[51] M. Al Janaideh and D. Bernstein, "Inversion-free adaptive control of uncertain systems with shape-memory-alloy actuation," in *Proc. Am. Control Conf.*, 2013, pp. 3579–3584.

[52] X. Tan and J. Baras, "Modeling and control of hysteresis in magnetostrictive actuators," *Automatica*, vol. 40, pp. 1469–1480, 2004.

[53] M. Al Janaideh, M. Rakotondrabe, and X. Tan, "Hysteresis in smart mechatronic systems: Modeling, identification, and control," *IEEE/ASME Trans. Mechatronics*, vol. 21, no. 1, pp. 1–3, Feb. 2016.

[54] M. Al Janaideh and O. Aljanaideh, "Further results on open-loop compensation of rate-dependent hysteresis in a magnetostrictive actuator with the Prandtl–Ishlinskii model," *Mech. Syst. Signal Process.*, vol. 104, pp. 835–850, 2018.

[55] M. Al Janaideh, M. Rakotondrabe, I. Al-Darabsah, and O. Aljanaideh, "Internal model-based feedback control design for inversion-free feedforward rate-dependent hysteresis compensation of piezoelectric cantilever actuator," *Control Eng. Pract.*, vol. 72, pp. 29–41, 2018.

[56] M. Rakotondrabe and I. Ivan, "Development and force/position control of a new hybrid thermo-piezoelectric microgripper dedicated to micromanipulation tasks," *IEEE Trans. Autom. Sci. Eng.*, vol. 8, no. 4, pp. 824–834, Oct. 2011.

[57] D. Davino, C. Natale, S. Pirozzi, and C. Visone, "Phenomenological dynamic model of a magnetostrictive actuator," *Phys. B, Condensed Matter*, vol. 343, pp. 112–116, 2004.

[58] A. Katalenic, H. Butler, and P. Van Den Bosch, "High-precision force control of short-stroke reluctance actuators with an air gap observer," *IEEE/ASME Trans. Mechatronics*, vol. 21, no. 5, pp. 2431–2439, Oct. 2016.

Authors' photographs and biographies not available at the time of publication.