An Adaptive Control Architecture for Mitigating Sensor and Actuator Attacks in Cyber-Physical Systems

Xu Jin, *Student Member, IEEE*, Wassim M. Haddad, *Fellow, IEEE*, and Tansel Yucelen, *Member, IEEE*

***Abstract*—Recent technological advances in communications and computation have spurred a broad interest in control law architectures involving the monitoring, coordination, integration, and operation of sensing, computing, and communication components that tightly interact with the physical processes that they control. These systems are known as cyber-physical systems and due to their use of open computation and communication platform architectures, controlled cyber-physical systems are vulnerable to adversarial attacks. In this technical note, we propose a novel adaptive control architecture for addressing security and safety in cyber-physical systems. Specifically, we develop an adaptive controller that guarantees uniform ultimate boundedness of the closed-loop dynamical system in the face of adversarial sensor and actuator attacks that are time-varying and partial asymptotic stability when the sensor and actuator attacks are time-invariant. Finally, we provide a numerical example to illustrate the efficacy of the proposed adaptive control architecture.**

***Index Terms*—Actuator attacks, adaptive control, cyber-physical systems, partial asymptotic stability, sensor attacks, uniform ultimate boundedness.**

I. Introduction

The design and implementation of control law architectures for modeling and controlling complex dynamical systems is a nontrivial control engineering task involving the consideration and operation of computing and communication components interacting with the physical system to be controlled. These complex dynamical systems merge the cyber-world of computing and communications with the physical world, and are known as *cyber-physical systems* (see [1] and the references therein). Cyber-physical systems are characterized by a large number of highly coupled heterogeneous dynamic network components and have become ubiquitous in the control of complex dynamical systems given the recent advances in embedded sensor, computation, and communication technologies. Such systems include safety-critical aerospace systems, power systems, communications systems, network systems, transportation systems, large-scale manufacturing systems, integrative biological systems, economic systems, process control systems, and health-care systems, to name but a few examples.

In all of the aforementioned applications, reliable system analysis and decentralized control system design, with integrated verification and validation, are essential for providing high system performance and reconfigurable system operation in the presence of system uncertainties and system component failures. Even though cyber-physical systems are transforming the way we are interacting with the physical world, they introduce several grand research challenges. In particular, the complex, large-scale heterogeneous architectures and components that are pervasive in cyber-physical systems demands system robustness, resiliency, reliability, safety, and security for addressing the constantly changing and reconfiguring dynamics of these systems whose computation, information, and control processing is tightly coupled with the physical process. And given that a wide range of cyber-physical systems involve the use of open communication and computation platform architectures, they are vulnerable to adversarial cyber-attacks that can have drastic societal ramifications.

In particular, attackers can gain access to sensing and actuation computing platforms and manipulate system measurement data and control input commands to severely compromise system performance and integrity, and hence, security and safety in cyber-physical systems is of paramount importance. In contrast to classical estimation and control problems, wherein physical system variables cannot be measured directly due to sensor noise and are typically assumed to fluctuate about their true value, controlled systems with measurement and actuation devices that are hijacked and controlled by an adversarial entity that actively engages to maximally degrade system information and control require new and novel control algorithms to recover system performance.

Cyber-physical system security involving information security and detection in adversarial environments have been considered in the literature [2]–[21], with early approaches focusing on classical fault detection, isolation, and recovery schemes (see, for example, [2]–[4] and the references therein). In this technical note, we build on the solid foundation of adaptive control theory to develop new adaptive control architectures that can foil malicious sensor and actuator attacks. Specifically, we develop an adaptive controller for mitigating time-varying and time-invariant, state-dependent sensor and actuator attacks. We show that the proposed controller guarantees uniform ultimate boundedness of the closed-loop dynamical system when the adversarial sensor and actuator attacks are time-varying and partial asymptotic stability when the sensor and actuator attacks are time-invariant. Finally, we discuss the practicality of the proposed approach and provide a numerical example involving the lateral directional dynamics of an aircraft to illustrate the efficacy of the proposed adaptive control architecture.

II. Notation and Problem Formulation

The notation used in this technical note is fairly standard. Specifically, $\mathbb{R}$ denotes the set of real numbers, $\mathbb{R}^n$ denotes the set of $n \times 1$ real column vectors, $\mathbb{R}^{n\times m}$ denotes the set of $n \times m$ real matrices, $(\cdot)^{\mathrm{T}}$ denotes the transpose operator, $(\cdot)^{-1}$ denotes the inverse operator, $\det(\cdot)$ denotes the determinant operator, $\|\cdot\|_1$ denotes the

Manuscript received April 4, 2016; revised September 6, 2016 and December 20, 2016; accepted January 6, 2017. Date of publication January 11, 2017; date of current version October 25, 2017. This work was supported in part by the Air Force Office of Scientific Research under Grant FA9550-16-1-0100. Recommended by Associate Editor H. Lin.

X. Jin and W. M. Haddad are with the School of Aerospace Engineering Georgia Institute of Technology, Atlanta, GA 30332, USA (e-mail: xu.jin@gatech.edu; wm.haddad@aerospace.gatech.edu).

T. Yucelen is with the Department of Mechanical Engineering University of South Florida, Tampa, FL 33620, USA (e-mail: yucelen@usf.edu).

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/TAC.2017.2652127

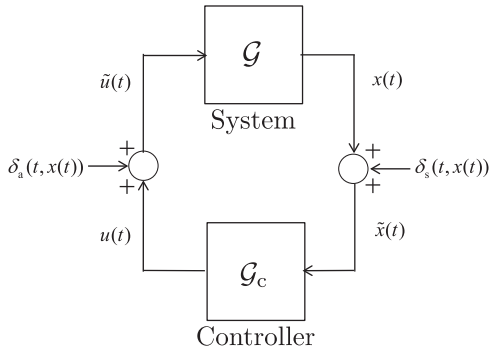

Fig. 1. Closed-loop dynamical system in the presence of sensor and actuator attacks.

absolute sum norm, $\|\cdot\|_2$ denotes the Euclidian norm, and $\|\cdot\|_{\rm F}$ denotes the Frobenius matrix norm. Furthermore, we write $\lambda_{\min}(A)$ (respectively, $\lambda_{\max}(A)$) for the minimum (respectively, maximum) eigenvalue of the matrix A, $\mathrm{spec}(A)$ for the spectrum of the matrix A including multiplicity, and $\underline{x}$ (respectively, $\overline{x}$) for the lower bound (respectively, upper bound) of a bounded signal; that is, for $x(t) \in \mathbb{R}^n$, $t \geq 0$, $\underline{x} \leq \|x(t)\|_2$, $t \geq 0$ (respectively, $\|x(t)\|_2 \leq \overline{x}$, $t \geq 0$), and for $X(t) \in \mathbb{R}^{p\times m}$, $t \geq 0$, $\underline{x} \leq \|X(t)\|_{\rm F}$, $t \geq 0$ (respectively, $\|X(t)\|_{\rm F} \leq \overline{x}$, $t \geq 0$). Finally, for $y \in \mathbb{R}^n$, y_i denotes the ith component of y.

In this technical note, we consider linear dynamical systems $\mathscr{G}$ of the form

$$\dot{x}(t) = Ax(t) + Bu(t), \quad x(0) = x_0, \quad t \geq 0 \tag{1}$$

where $x(t) \in \mathbb{R}^n$, $t \geq 0$, is the state vector, $u(t) \in \mathbb{R}^m$, $t \geq 0$, is the control input, and $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times m}$ are known system matrices. We assume that the pair (A, B) is controllable and the control input $u(\cdot)$ is restricted to the class of admissible controls consisting of measurable functions such that $u(t) \in \mathbb{R}^m$, $t \geq 0$. In addition, we assume that the compromised system state

$$\tilde{x}(t) = x(t) + \delta_{\rm s}(t, x(t)), \quad t \geq 0 \tag{2}$$

is available for feedback, where $\tilde{x}(t) \in \mathbb{R}^n$, $t \geq 0$, and $\delta_{\rm s} : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ captures sensor attacks. In particular, if $\delta_{\rm s}(\cdot,\cdot)$ is nonzero, then the uncompromised state vector $x(t)$, $t \geq 0$, is corrupted with a faulty (or malicious) signal $\delta_{\rm s}(\cdot,\cdot)$. Alternatively, if $\delta_{\rm s}(t,x) \equiv 0$, then $\tilde{x}(t) = x(t)$, $t \geq 0$, and the uncompromised state vector is available for feedback. Furthermore, we assume that the control input is also compromised and is given by

$$\tilde{u}(t) = u(t) + \delta_{\rm a}(t, x(t)), \quad t \geq 0 \tag{3}$$

where $\tilde{u}(t) \in \mathbb{R}^m$, $t \geq 0$, and $\delta_{\rm a} : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^m$ captures actuator attacks. In particular, if $\delta_{\rm a}(\cdot,\cdot)$ is nonzero, then the uncompromised control signal $u(t)$, $t \geq 0$, is corrupted with a faulty (or malicious) signal $\delta_{\rm a}(\cdot,\cdot)$. Alternatively, if $\delta_{\rm a}(t,x) \equiv 0$, then $\tilde{u}(t) = u(t)$, $t \geq 0$, and the control signal is uncompromised; see Fig. 1.

Since (A, B) is controllable, there exists a feedback gain matrix $K \in \mathbb{R}^{m\times n}$ such that $A_{\rm r} \triangleq A + BK$ is Hurwitz. In this case, it follows from converse Lyapunov theory [22] that for every positive definite matrix $R \in \mathbb{R}^{n\times n}$, there exists a unique positive-definite $P \in \mathbb{R}^{n\times n}$ satisfying

$$0 = A_{\rm r}^{\rm T} P + P A_{\rm r} + R. \tag{4}$$

For $\delta_{\rm s}(t, x(t)) \neq 0$, $t \geq 0$, and $\delta_{\rm a}(t, x(t)) \neq 0$, $t \geq 0$, our objective is to design a controller $\mathscr{G}_{\rm c}$ of the form

$$u(t) = K\tilde{x}(t) + v(t), \quad t \geq 0 \tag{5}$$

where $v(t) \in \mathbb{R}^m$, $t \geq 0$, is a corrective signal that suppresses or counteracts the effect of state-dependent sensor and actuator attacks $\delta_{\rm s}(t, x(t))$, $t \geq 0$, and $\delta_{\rm a}(t, x(t))$, $t \geq 0$, to asymptotically (or approximately) recover the ideal system performance achieved when the uncompromised state vector is available for feedback and control signal is uncompromised.

III. Adaptive Ultimate Boundedness and Stabilization for State-Dependent Sensor and Actuator Attacks

In this section, we design the corrective signal $v(t)$, $t \geq 0$, in (5) to achieve adaptive ultimate boundedness and stabilization in the presence of state-dependent sensor and actuator attacks. We assume that the sensor attack in (2) is parameterized as $\delta_{\rm s}(t, x(t)) = w(t)x(t)$, $t \geq 0$, where $w(t) \in \mathbb{R}$, $t \geq 0$, is an *unknown* time-varying weight such that $\|w(t)\|_2 \leq \overline{w}$, $t \geq 0$, and $\|\dot{w}(t)\|_2 \leq \overline{\dot{w}}$, $t \geq 0$, with *unknown* bounds $\overline{w}$ and $\overline{\dot{w}}$. In this case, we assume that $w(t) > -1$, $t \geq 0$, in order to construct a feasible corrective signal $v(t)$, $t \geq 0$, since $w(t) \equiv -1$ results in $\tilde{x}(t) \equiv 0$, and hence, it is not possible to construct $v(t)$, $t \geq 0$, to asymptotically recover the ideal system performance.

Furthermore, we assume that the actuator attack in (3) can be parameterized as $\delta_{\rm a}(t, x(t)) = W^{\rm T}(t)\varphi(x(t))$, $t \geq 0$, where $W(t) \in \mathbb{R}^{p\times m}$, $t \geq 0$, is an *unknown* time-varying weighting matrix and $\varphi(x(t)) \in \mathbb{R}^p$, $t \geq 0$, is a nonlinear function with a known structure and with $x(t)$, $t \geq 0$, in general being unknown. Since the uncompromised state vector $x(t)$, $t \geq 0$, is not available for feedback, we rewrite

$$W^{\rm T}(t)\varphi(x(t)) = W^{\rm T}(t)\varphi(\tilde{x}(t)) + \sigma(t, x(t)), \quad t \geq 0 \tag{6}$$

where $\sigma(t, x(t)) \in \mathbb{R}^m$, $t \geq 0$, is *unknown* and bounded, that is, $\|\sigma(t, x(t))\|_2 \leq \bar{\sigma}$, $t \geq 0$, and where $\bar{\sigma} > 0$ is *unknown*. Note that assuming that $\|\sigma(t, x(t))\|_2 \leq \bar{\sigma}$, $t \geq 0$, is without loss of generality since a worst-case actuator attack will lead to actuator amplitude saturation in practice. Therefore, (1) can be equivalently written as

$$\dot{x}(t) = Ax(t) + B\Big[u(t) + W^{\rm T}(t)\varphi(\tilde{x}(t)) + \sigma(t, x(t))\Big], \quad x(0) = x_0, \quad t \geq 0. \tag{7}$$

To achieve system ultimate boundedness in the face of time-varying, state-dependent sensor and actuator attacks, we use the corrective signal given by

$$v(t) = -\hat{\mu}(t)K\tilde{x}(t) - \hat{W}^{\rm T}(t)\varphi(\tilde{x}(t) - \hat{\sigma}(t)\mathrm{sgn}_{\rm v}(B^{\rm T}P\tilde{x}(t)), \quad t \geq 0 \tag{8}$$

where, for $y \in \mathbb{R}^n$, $\mathrm{sgn}_{\rm v}(y) \triangleq [\mathrm{sgn}(y_1), \ldots, \mathrm{sgn}(y_n)]^{\rm T}$, $\mathrm{sgn}(\alpha) \triangleq \frac{\alpha}{|\alpha|}$, $\alpha \neq 0$, and $\mathrm{sgn}(0) \triangleq 0$, and

$$\dot{\hat{\mu}}(t) = \gamma \mathrm{Proj}\big[\hat{\mu}(t),\ \tilde{x}^{\rm T}(t)PBK\tilde{x}(t)\big],\ \hat{\mu}(0) = \hat{\mu}_0, \quad t \geq 0, \tag{9}$$

$$\dot{\hat{W}}(t) = \eta \mathrm{Proj}_{\rm m}\big[\hat{W}(t),\ \varphi(\tilde{x}(t))\tilde{x}^{\rm T}(t)PB\big],\ \hat{W}(0) = \hat{W}_0, \tag{10}$$

$$\dot{\hat{\sigma}}(t) = \nu \mathrm{Proj}\big[\hat{\sigma}(t),\ \|\tilde{x}^{\rm T}(t)PB\|_1\big],\ \hat{\sigma}(0) = \hat{\sigma}_0 \tag{11}$$

where $\hat{\mu}(t) \in \mathbb{R}$, $t \geq 0$, is the estimate of $\mu(t) \triangleq w(t)(1 + w(t))^{-1} \in \mathbb{R}$, $t \geq 0$, that depends on the sensor uncertainty $w(t)$, $t \geq 0$, $\hat{W}(t) \in \mathbb{R}^{p\times m}$, $t \geq 0$, is the estimate of the parametric uncertainty $W(t)$, $t \geq 0$, $\hat{\sigma}(t) \in \mathbb{R}$, $t \geq 0$, is the estimate of the unknown bound $\bar{\sigma}$, $\gamma \in \mathbb{R}$, $\eta \in \mathbb{R}$, and $\nu \in \mathbb{R}$ are positive design gains, and $\mathrm{Proj} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ is the projection operator. Specifically, for a continuously differentiable

convex function $\phi : \mathbb{R}^n \to \mathbb{R}$ given by $\phi(\theta) \triangleq \frac{(\varepsilon_\theta+1)\theta^{\mathrm{T}}\theta-\theta_{\max}^2}{\varepsilon_\theta\theta_{\max}^2}$, where $\theta_{\max} \in \mathbb{R}$ is a *projection norm bound* imposed on $\theta \in \mathbb{R}^n$ and $\varepsilon_\theta > 0$ is a *projection tolerance bound*, the *projection operator* $\mathrm{Proj} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ is defined by

$$\mathrm{Proj}(\theta, y) \triangleq \begin{cases} y, & \text{if } \phi(\theta) < 0, \\ y, & \text{if } \phi(\theta) \geq 0 \text{ and } \phi'(\theta)y \leq 0, \\ y - \frac{\phi'^{\mathrm{T}}(\theta)\phi'(\theta)y}{\phi'(\theta)\phi'^{\mathrm{T}}(\theta)}\phi(\theta), & \text{if } \phi(\theta) \geq 0 \text{ and } \phi'(\theta)y > 0 \end{cases} \tag{12}$$

where $y \in \mathbb{R}^n$. Note that it follows from the definition of the projection operator that $(\theta - \theta^*)^{\mathrm{T}}(\mathrm{Proj}(\theta, y) - y) \leq 0, \theta^* \in \mathbb{R}^n$ [23]. Furthermore, $\mathrm{Proj}_{\mathrm{m}} : \mathbb{R}^{n\times m} \times \mathbb{R}^{n\times m} \to \mathbb{R}^{n\times m}$ defines a generalization of the projection operator to matrices wherein

$$\begin{aligned}\mathrm{Proj}_{\mathrm{m}}(\Theta, Y) = {} & (\mathrm{Proj}(\mathrm{col}_1(\Theta), \mathrm{col}_1(Y))), \ldots, \\ & \mathrm{Proj}(\mathrm{col}_m(\Theta), \mathrm{col}_m(Y)))\end{aligned} \tag{13}$$

where $\Theta \in \mathbb{R}^{n\times m}$, $Y \in \mathbb{R}^{n\times m}$, and $\mathrm{col}_i(\cdot)$ denotes the ith column operator. In this case, for a given $\Theta^* \in \mathbb{R}^{n\times m}$, it follows from (12) that

$$\begin{aligned}&\mathrm{tr}[(\Theta-\Theta^*)^{\mathrm{T}}(\mathrm{Proj}_{\mathrm{m}}(\Theta-Y)-Y)] \\ &= \sum_{i=1}^{m}[\mathrm{col}_i(\Theta-\Theta^*)^{\mathrm{T}}(\mathrm{Proj}(\mathrm{col}_i(\Theta), \mathrm{col}_i(Y))-\mathrm{col}_i(Y))] \leq 0\end{aligned} \tag{14}$$

holds. In this technical note, we assume that the projection norm bound imposed on each column of $\Theta \in \mathbb{R}^{n\times m}$ is $\theta_{\max}$.

Next, define $\mu_\lambda(t) \triangleq \tilde{\mu}(t)\lambda^{\frac{1}{2}}(t)$, $t \geq 0$, $W_\lambda(t) \triangleq \tilde{W}(t)\lambda^{\frac{1}{2}}(t)$, $t \geq 0$, and $\sigma_\lambda(t) \triangleq \tilde{\sigma}(t)\lambda^{\frac{1}{2}}(t)$, $t \geq 0$, with $\tilde{\mu}(t) \triangleq \mu(t) - \hat{\mu}(t)$, $t \geq 0$, $\tilde{W}(t) \triangleq W(t) - \hat{W}(t)$, $t \geq 0$, $\tilde{\sigma}(t) \triangleq \bar{\sigma} - \hat{\sigma}(t)$, $t \geq 0$, and $\lambda(t) \triangleq \big(1 + w(t)\big)^{-1}$, $t \geq 0$. Since $w(t) > -1$, note that $\mu(t)$, $t \geq 0$, and $\lambda(t)$, $t \geq 0$, are well-defined and $\lambda(t) > 0$, $t \geq 0$. For the statement of the next result, note that

$$\begin{aligned}\dot{x}(t) = {} & A_{\mathrm{r}}x(t) + \mu_\lambda(t)\lambda^{-\frac{1}{2}}(t)BK\tilde{x}(t) + BW_\lambda^{\mathrm{T}}(t)\lambda^{-\frac{1}{2}}(t)\varphi(\tilde{x}(t)) \\ & + B(\sigma(t, x(t)) - \hat{\sigma}(t)\mathrm{sgn}_{\mathrm{v}}(B^{\mathrm{T}}P\tilde{x}(t))), \\ & x(0) = x_0, \quad t \geq 0,\end{aligned} \tag{15}$$

$$\begin{aligned}\dot{\mu}_\lambda(t) = {} & [\dot{\mu}(t) - \gamma\mathrm{Proj}\big(\hat{\mu}(t),\ \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big)]\lambda^{\frac{1}{2}}(t) \\ & + \frac{1}{2}\mu_\lambda(t)\dot{\lambda}(t)\lambda^{-1}(t), \quad \mu_\lambda(0) = \mu_{\lambda 0},\end{aligned} \tag{16}$$

$$\begin{aligned}\dot{W}_\lambda(t) = {} & [\dot{W}(t) - \eta\mathrm{Proj}_{\mathrm{m}}\big(\hat{W}(t), \varphi(\tilde{x}(t))\tilde{x}^{\mathrm{T}}(t)PB\big)]\lambda^{\frac{1}{2}}(t) \\ & + \frac{1}{2}W_\lambda(t)\dot{\lambda}(t)\lambda^{-1}(t), \quad W_\lambda(0) = W_{\lambda 0},\end{aligned} \tag{17}$$

$$\begin{aligned}\dot{\sigma}_\lambda(t) = {} & [-\nu\mathrm{Proj}\big(\hat{\sigma}(t),\ ||\tilde{x}^{\mathrm{T}}(t)BP||_1\big)]\lambda^{\frac{1}{2}}(t) \\ & + \frac{1}{2}\sigma_\lambda(t)\dot{\lambda}(t)\lambda^{-1}(t), \quad \sigma_\lambda(0) = \sigma_{\lambda 0}.\end{aligned} \tag{18}$$

Theorem 3.1: Consider the linear dynamical system $\mathscr{G}$ given by (1) with time-varying, state-dependent sensor and actuator attacks given by (2) and (3), respectively, where $\|w(t)\|_2 \leq \overline{w}$, $t \geq 0$, $\|\dot{w}(t)\|_2 \leq \overline{\dot{w}}$, $t \geq 0$, $\|W(t)\|_{\mathrm{F}} \leq \overline{W}$, $t \geq 0$, $\|\dot{W}(t)\|_{\mathrm{F}} \leq \overline{\dot{W}}$, $t \geq 0$, and $\|\sigma(t, x(t))\|_2 \leq \overline{\sigma}$, $t \geq 0$. Then, with the controller $\mathscr{G}_{\mathrm{c}}$ given by (5) and the corrective signal $v(t)$, $t \geq 0$, given by (8), the closed-loop system given by (15)–(18) is uniformly bounded for all $\big(x_0, \mu_{\lambda 0}, W_{\lambda 0}, \sigma_{\lambda 0}\big) \in \mathbb{R}^n \times \mathbb{R} \times \mathbb{R}^{p\times m} \times \mathbb{R}$ with the ultimate bounds

$$\begin{aligned}\|x(t)\|_2 \leq {} & \Bigg[\frac{1}{\lambda_{\min}(P)}[\lambda_{\max}(P)d_1^{-1}d_2 \\ & + \gamma^{-1}\overline{\lambda}\big(\overline{\mu} + \hat{\mu}_{\max}\big)^2 + \eta^{-1}\overline{\lambda}\big(\overline{W} + \hat{W}_{\max}\big)^2 \\ & + \nu^{-1}\overline{\lambda}\big(\overline{\sigma} + \hat{\sigma}_{\max}\big)^2]\Bigg]^{\frac{1}{2}}, \quad t \geq T,\end{aligned} \tag{19}$$

$$\begin{aligned}|\mu_\lambda(t)| \leq {} & [\gamma\lambda_{\max}(P)d_1^{-1}d_2 + \overline{\lambda}\big(\overline{\mu} + \hat{\mu}_{\max}\big)^2 \\ & + \gamma\eta^{-1}\overline{\lambda}\big(\overline{W} + \hat{W}_{\max}\big)^2 \\ & + \gamma\nu^{-1}\overline{\lambda}\big(\overline{\sigma} + \hat{\sigma}_{\max}\big)^2]^{\frac{1}{2}}, \quad t \geq T,\end{aligned} \tag{20}$$

$$\begin{aligned}\|W_\lambda(t)\|_{\mathrm{F}} \leq {} & [\eta\lambda_{\max}(P)d_1^{-1}d_2 + \eta\gamma^{-1}\overline{\lambda}\big(\overline{\mu} + \hat{\mu}_{\max}\big)^2 \\ & + \overline{\lambda}\big(\overline{W} + \hat{W}_{\max}\big)^2 \\ & + \eta\nu^{-1}\overline{\lambda}\big(\overline{\sigma} + \hat{\sigma}_{\max}\big)^2]^{\frac{1}{2}}, \quad t \geq T,\end{aligned} \tag{21}$$

$$\begin{aligned}|\sigma_\lambda(t)| \leq {} & [\nu\lambda_{\max}(P)d_1^{-1}d_2 + \nu\gamma^{-1}\overline{\lambda}\big(\overline{\mu} + \hat{\mu}_{\max}\big)^2 \\ & + \nu\eta^{-1}\overline{\lambda}\big(\overline{W} + \hat{W}_{\max}\big)^2 + \overline{\lambda}\big(\overline{\sigma} + \hat{\sigma}_{\max}\big)^2]^{\frac{1}{2}}, \\ & t \geq T\end{aligned} \tag{22}$$

where $T > 0$, $d_1 \triangleq \lambda_{\min}(R)$, $d_2 \triangleq \gamma^{-1}[2\big(\overline{\mu} + \hat{\mu}_{\max}\big)\overline{\dot{\mu}}\overline{\lambda} + \big(\overline{\mu} + \hat{\mu}_{\max}\big)^2\overline{\dot{\lambda}}] + \eta^{-1}[2\big(\overline{W} + \hat{W}_{\max}\big)\overline{\dot{W}}\overline{\lambda} + \big(\overline{W} + \hat{W}_{\max}\big)^2\overline{\dot{\lambda}}] + \nu^{-1}[\big(\overline{\sigma} + \hat{\sigma}_{\max}\big)^2\overline{\dot{\lambda}}]$, and $\hat{\mu}_{\max} \in \mathbb{R}$, $\hat{W}_{\max} \in \mathbb{R}$, and $\hat{\sigma}_{\max} \in \mathbb{R}$ are projection norm bounds.

Proof: To show boundedness of the closed-loop system given by (15)–(18), consider the Lyapunov-like function given by

$$V\big(x, \mu_\lambda, W_\lambda, \sigma_\lambda\big) = x^{\mathrm{T}}Px + \gamma^{-1}\mu_\lambda^2 + \eta^{-1}\mathrm{tr}(W_\lambda^{\mathrm{T}}W_\lambda) + \nu^{-1}\sigma_\lambda^2 \tag{23}$$

where P satisfies (4). Note that $V(0, 0, 0, 0) = 0$, $V\big(x, \mu_\lambda, W_\lambda, \sigma_\lambda\big) > 0$ for all $\big(x, \mu_\lambda, W_\lambda, \sigma_\lambda\big) \neq (0, 0, 0, 0)$, and $V\big(x, \mu_\lambda, W_\lambda, \sigma_\lambda\big)$ is radially unbounded. The time derivative of (23) along the closed-loop system trajectories of (15)–(18) is given by

$$\begin{aligned}&\dot{V}\big(x(t), \mu_\lambda(t), W_\lambda(t), \sigma_\lambda(t)\big) \\ &\quad = -x^{\mathrm{T}}(t)Rx(t) + 2\mu_\lambda(t)\lambda^{-\frac{1}{2}}(t)x^{\mathrm{T}}(t)PBK\tilde{x}(t) \\ &\qquad + 2\gamma^{-1}\mu_\lambda(t)[\dot{\mu}(t) - \gamma\mathrm{Proj}\big(\hat{\mu}(t), \\ &\qquad \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big)]\lambda^{\frac{1}{2}}(t) \\ &\qquad + \gamma^{-1}\mu_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t) + 2x^{\mathrm{T}}(t)PB\phi_\lambda(t)\lambda^{-\frac{1}{2}}(t) \\ &\qquad + 2\mathrm{tr}[W_\lambda^{\mathrm{T}}(t)\lambda^{-\frac{1}{2}}(t)\varphi(\tilde{x}(t))x^{\mathrm{T}}(t)PB] \\ &\qquad + 2\eta^{-1}\mathrm{tr}[W_\lambda^{\mathrm{T}}(t)[\dot{W}(t) \\ &\qquad - \eta\mathrm{Proj}_{\mathrm{m}}\big(\hat{W}(t),\ \varphi(\tilde{x}(t))\tilde{x}^{\mathrm{T}}(t)PB\big)]\lambda^{\frac{1}{2}}(t)] \\ &\qquad + \eta^{-1}\mathrm{tr}(W_\lambda^{\mathrm{T}}(t)W_\lambda(t))\dot{\lambda}(t)\lambda^{-1}(t) \\ &\qquad + 2x^{\mathrm{T}}(t)PB(\sigma(t, x(t)) - \hat{\sigma}(t)\mathrm{sgn}_{\mathrm{v}}(B^{\mathrm{T}}P\tilde{x}(t))) \\ &\qquad + 2\nu^{-1}\sigma_\lambda(t)[-\nu\mathrm{Proj}\big(\hat{\sigma}(t),\ \|\tilde{x}^{\mathrm{T}}(t)BP\|_1\big)]\lambda^{\frac{1}{2}}(t) \\ &\qquad + \nu^{-1}\sigma_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t).\end{aligned} \tag{24}$$

Now, using

$$\begin{aligned}
&2x^{\mathrm{T}}(t)PB(\sigma(t,x(t))-\hat{\sigma}(t)\mathrm{sgn}_{\mathrm{v}}(B^{\mathrm{T}}P\tilde{x}(t)))\\
&\quad=2\tilde{x}^{\mathrm{T}}(t)PB\sigma(t,x(t))\lambda(t)\\
&\qquad-2\tilde{x}^{\mathrm{T}}(t)PB\hat{\sigma}(t)\lambda(t)\mathrm{sgn}_{\mathrm{v}}(B^{\mathrm{T}}P\tilde{x}(t))\\
&\quad\le 2\|\tilde{x}^{\mathrm{T}}(t)PB\|_1\overline{\sigma}\lambda(t)-2\|\tilde{x}^{\mathrm{T}}(t)PB\|_1\hat{\sigma}(t)\lambda(t)\\
&\quad=2\|\tilde{x}^{\mathrm{T}}(t)PB\|_1\sigma_\lambda(t)\lambda^{\frac{1}{2}}(t),\ \ t\ge 0 \qquad (25)
\end{aligned}$$

it follows from (24) that

$$\begin{aligned}
&\dot{V}\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big)\\
&\le -x^{\mathrm{T}}(t)Rx(t)+2\mu_\lambda(t)\lambda^{\frac{1}{2}}(t)\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\\
&\quad+\gamma^{-1}\mu_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t)+2\gamma^{-1}\mu_\lambda(t)[\dot{\mu}(t)\\
&\qquad-\gamma\mathrm{Proj}\big(\hat{\mu}(t),\ \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big)]\lambda^{\frac{1}{2}}(t)\\
&\quad+2\mathrm{tr}[W_\lambda^{\mathrm{T}}(t)\lambda^{\frac{1}{2}}(t)\varphi(\tilde{x}(t))\tilde{x}^{\mathrm{T}}(t)PB]\\
&\quad+2\eta^{-1}\mathrm{tr}[W_\lambda(t)[\dot{W}(t)\\
&\qquad-\eta\mathrm{Proj}_{\mathrm{m}}\big(\hat{W}(t),\ \varphi(\tilde{x}(t))\tilde{x}^{\mathrm{T}}(t)PB\big)]\lambda^{\frac{1}{2}}(t)]\\
&\quad+\eta^{-1}\mathrm{tr}(W_\lambda^{\mathrm{T}}(t)W_\lambda(t))\dot{\lambda}(t)\lambda^{-1}(t)\\
&\quad+2\|\tilde{x}^{\mathrm{T}}(t)BP\|_1\sigma_\lambda(t)\lambda^{\frac{1}{2}}(t)\\
&\quad+2\nu^{-1}\sigma_\lambda(t)[-\nu\mathrm{Proj}\big(\hat{\sigma}(t),\ \|\tilde{x}^{\mathrm{T}}(t)BP\|_1\big)]\lambda^{\frac{1}{2}}(t)\\
&\quad+\nu^{-1}\sigma_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t),\ \ t\ge 0 \qquad (26)
\end{aligned}$$

where we used the fact that $x(t)=\lambda(t)\tilde{x}(t)$, $t\ge 0$.

Next, for $t\ge 0$, using

$$\begin{aligned}
&\mu_\lambda(t)\lambda^{\frac{1}{2}}(t)\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\\
&\quad-\mu_\lambda(t)\lambda^{\frac{1}{2}}(t)\mathrm{Proj}\big(\hat{\mu}(t),\ \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big)\\
&\qquad=\lambda(t)\big(\hat{\mu}(t)-\mu(t)\big)[\mathrm{Proj}\big(\hat{\mu}(t),\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big)\\
&\qquad\quad-\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)]\le 0, \qquad (27)
\end{aligned}$$

$$\begin{aligned}
&\mathrm{tr}[W_\lambda(t)\lambda^{\frac{1}{2}}(t)\varphi(\tilde{x}(t))\tilde{x}^{\mathrm{T}}(t)PB]\\
&\quad-\eta^{-1}\mathrm{tr}[W_\lambda(t)[\eta\mathrm{Proj}_{\mathrm{m}}[\hat{W}(t),\ \varphi(\tilde{x}(t))\tilde{x}^{\mathrm{T}}(t)PB]]\lambda^{\frac{1}{2}}(t)]\le 0, \qquad (28)
\end{aligned}$$

$$\begin{aligned}
&2\|\tilde{x}^{\mathrm{T}}(t)BP\|_1\sigma_\lambda(t)\lambda^{\frac{1}{2}}(t)+2\nu^{-1}\sigma_\lambda(t)\\
&\quad\cdot[-\nu\mathrm{Proj}\big(\hat{\sigma}(t),\ \|\tilde{x}^{\mathrm{T}}(t)BP\|_1\big)]\lambda^{\frac{1}{2}}(t)\le 0 \qquad (29)
\end{aligned}$$

it follows from (26) that

$$\begin{aligned}
&\dot{V}\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big)\\
&\le -x^{\mathrm{T}}(t)Rx(t)+2\gamma^{-1}\mu_\lambda(t)\dot{\mu}(t)+\gamma^{-1}\mu_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t)\\
&\quad+2\eta^{-1}\mathrm{tr}[W_\lambda^{\mathrm{T}}(t)\dot{W}_\lambda(t)]+\eta^{-1}\mathrm{tr}[W_\lambda^{\mathrm{T}}(t)W_\lambda(t)\dot{\lambda}(t)\lambda^{-1}(t)]\\
&\quad+\nu^{-1}\sigma_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t)\\
&\le -d_1\|x(t)\|_2^2+d_2,\quad t\ge 0 \qquad (30)
\end{aligned}$$

and hence, $\dot{V}\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big)<0$ outside of the compact set

$$\begin{aligned}
\mathscr{D}_{\mathrm{c}}\triangleq\Big\{&\big(x,\mu_\lambda,W_\lambda,\sigma_\lambda\big)\in\mathbb{R}^n\times\mathbb{R}\times\mathbb{R}^{p\times m}\times\mathbb{R}:\\
&\|x\|_2\le\vartheta_1,\ \ |\mu_\lambda|\le\vartheta_2,\\
&\|W_\lambda\|_{\mathrm{F}}\le\vartheta_3,\ \text{and}\ \ |\sigma_\lambda|\le\vartheta_4\Big\} \qquad (31)
\end{aligned}$$

where $\vartheta_1\triangleq\sqrt{d_2/d_1}$, $\vartheta_2\triangleq\overline{\lambda}^{\frac{1}{2}}\big(\overline{\mu}+\hat{\mu}_{\max}\big)$, $\vartheta_3\triangleq\overline{\lambda}^{\frac{1}{2}}\big(\overline{W}+\hat{W}_{\max}\big)$, and $\vartheta_4\triangleq\overline{\lambda}^{\frac{1}{2}}\big(\overline{\sigma}+\hat{\sigma}_{\max}\big)$. This proves uniform boundedness of the solution $\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big)$ of the closed-loop system given by (15)–(18) for all $\big(x_0,\mu_{\lambda0},W_{\lambda0},\sigma_{\lambda0}\big)\in\mathbb{R}^n\times\mathbb{R}\times\mathbb{R}^{p\times m}\times\mathbb{R}$ [22].

To show the ultimate bounds for $x(t)$, $t\ge T$, $\mu_\lambda(t)$, $t\ge T$, $W_\lambda(t)$, $t\ge T$, and $\sigma_\lambda(t)$, $t\ge T$, given by (19)–(22), note that, for $t\ge T$

$$\begin{aligned}
&\lambda_{\min}(P)\|x(t)\|_2^2+\gamma^{-1}|\mu_\lambda(t)|^2\\
&\qquad+\eta^{-1}\|W_\lambda(t)\|_{\mathrm{F}}^2+\nu^{-1}|\sigma_\lambda(t)|^2\le\upsilon_{\max} \qquad (32)
\end{aligned}$$

where $\upsilon_{\max}\triangleq\lambda_{\min}(P)\vartheta_1^2+\gamma^{-1}\vartheta_2^2+\eta^{-1}\vartheta_3^2+\nu^{-1}\vartheta_4^2$. It now follows from (32) that $\|x(t)\|_2^2\le\frac{\upsilon_{\max}}{\lambda_{\min}(P)}$, $t\ge T$, $|\mu_\lambda(t)|^2\le\gamma\upsilon_{\max}$, $t\ge T$, $\|W_\lambda(t)\|_{\mathrm{F}}^2\le\eta\upsilon_{\max}$, $t\ge T$, and $|\sigma_\lambda(t)|^2\le\nu\upsilon_{\max}$, $t\ge T$. The result is now immediate. ■

Remark 3.1: Theorem 3.1 assumes that $w(t)>-1$, $t\ge 0$. This assumption implies that $\lambda(t)>0$, $t\ge 0$. As long as the sign of $\lambda(t)$ is known, Theorem 3.1 can be used to address the case where $\lambda(t)<0$, $t\ge 0$. The assumption $w(t)>-1$, $t\ge 0$, can be relaxed by utilizing tools from [24] that can allow $\lambda(t)$ to have any sign as long as $w(t)\ne-1$ under the assumption that its sign is a priori known.

Note that the controller $u(t)$, $t\ge 0$, given by (5) is discontinuous because of the presence of the signum function $\mathrm{sgn}_{\mathrm{v}}(\cdot)$ in the controller architecture. This discontinuity can lead to a chattering phenomenon, which is undesirable in practice. In order to reduce or eliminate the chattering effect, a smooth function can be implemented instead of the signum function [25]; that is, we replace $\mathrm{sgn}_{\mathrm{v}}(\cdot)$ by $\tanh_{\mathrm{v}}(\cdot)$, where, for $y\in\mathbb{R}^n$, $\tanh_{\mathrm{v}}(y)\triangleq[\tanh(y_1),\ldots,\tanh(y_n)]^{\mathrm{T}}$. Note that ([25])

$$0\le|\alpha|-\alpha\tanh\left(\frac{\alpha}{\varepsilon}\right)\le c_0\varepsilon,\qquad\alpha\in\mathbb{R} \qquad (33)$$

where $\varepsilon>0$ is a design constant and c_0 satisfies $c_0=e^{-(c_0+1)}$, and hence, $c_0=0.2785$. Thus, we modify (8) as

$$\begin{aligned}
v(t)=\ &-\hat{\mu}(t)K\tilde{x}(t)-\hat{W}^{\mathrm{T}}(t)\varphi(\tilde{x}(t))\\
&-\hat{\sigma}(t)\tanh_{\mathrm{v}}\left(\frac{B^{\mathrm{T}}P\tilde{x}(t)\hat{\sigma}(t)}{\varepsilon}\right),\quad t\ge 0. \qquad (34)
\end{aligned}$$

In this case, (25) becomes

$$\begin{aligned}
&2x^{\mathrm{T}}(t)PB\left[\sigma(t,x(t))-\hat{\sigma}(t)\tanh_{\mathrm{v}}\left(\frac{B^{\mathrm{T}}P\tilde{x}(t)\hat{\sigma}(t)}{\varepsilon}\right)\right]\\
&\quad\le 2\|\tilde{x}^{\mathrm{T}}(t)PB\|_1\overline{\sigma}\lambda(t)\\
&\qquad-2\tilde{x}^{\mathrm{T}}(t)PB\hat{\sigma}(t)\lambda(t)\tanh_{\mathrm{v}}\left(\frac{B^{\mathrm{T}}P\tilde{x}(t)\hat{\sigma}(t)}{\varepsilon}\right)\\
&\quad=2\|\tilde{x}^{\mathrm{T}}(t)PB\|_1\tilde{\sigma}(t)\lambda(t)\\
&\qquad+\sum_{i=1}^{m}2\lambda(t)\Bigg[|(\tilde{x}^{\mathrm{T}}(t)PB)_i\hat{\sigma}(t)|\\
&\qquad-(\tilde{x}^{\mathrm{T}}(t)PB)_i\hat{\sigma}(t)\tanh_{\mathrm{v}}\left(\frac{(\tilde{x}^{\mathrm{T}}(t)PB)_i\hat{\sigma}(t)}{\varepsilon}\right)\Bigg]\\
&\quad\le 2\|\tilde{x}^{\mathrm{T}}(t)PB\|_1\sigma_\lambda(t)\lambda^{\frac{1}{2}}(t)+2m\overline{\lambda}c_0\varepsilon,\quad t\ge 0. \qquad (35)
\end{aligned}$$

Now, it follows from (30) that

$$\begin{aligned}\dot{V}\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big)&\\ \le -x^{\mathrm{T}}(t)Rx(t)+2\gamma^{-1}\mu_\lambda(t)\dot{\mu}(t)&\\ +\gamma^{-1}\mu_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t)+2\eta^{-1}\mathrm{tr}[W_\lambda^{\mathrm{T}}(t)\dot{W}_\lambda(t)]&\\ +\eta^{-1}\mathrm{tr}[W_\lambda^{\mathrm{T}}(t)W_\lambda(t)\dot{\lambda}(t)\lambda^{-1}(t)]&\\ +\nu^{-1}\sigma_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t)+2m\overline{\lambda}c_0\varepsilon&\\ \le -d_1\|x(t)\|_2^2+d_3,\quad t\ge 0 \qquad (36)\end{aligned}$$

where $d_3 \triangleq \gamma^{-1}[2\big(\overline{\mu}+\hat{\mu}_{\max}\big)\overline{\mu\lambda}+\big(\overline{\mu}+\hat{\mu}_{\max}\big)^2\overline{\dot{\lambda}}]+\eta^{-1}[2\big(\overline{W}+\hat{W}_{\max}\big)\overline{\dot{W}\,\lambda}+\big(\overline{W}+\hat{W}_{\max}\big)^2\overline{\dot{\lambda}}]+\nu^{-1}[\big(\overline{\sigma}+\hat{\sigma}_{\max}\big)^2\overline{\dot{\lambda}}]+2m\overline{\lambda}c_0\varepsilon$. Hence, $\dot{V}\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big)<0$ outside of the compact set

$$\begin{aligned}\Omega_{\mathrm{c}} \triangleq \Big\{\big(x,\mu_\lambda,W_\lambda,\sigma_\lambda\big)\in\mathbb{R}^n\times\mathbb{R}\times\mathbb{R}^{p\times m}\times\mathbb{R}:\ \|x\|_2\le\vartheta_1,&\\ |\mu_\lambda|\le\vartheta_2,\ \|W_\lambda\|_{\mathrm{F}}\le\vartheta_3,\ \text{and}\ |\sigma_\lambda|\le\vartheta_4\Big\} \qquad (37)\end{aligned}$$

where $\vartheta_1 \triangleq \sqrt{d_3/d_1}$, $\vartheta_2 \triangleq \overline{\lambda}^{\frac{1}{2}}\big(\overline{\mu}+\hat{\mu}_{\max}\big)$, $\vartheta_3 \triangleq \overline{\lambda}^{\frac{1}{2}}\big(\overline{W}+\hat{W}_{\max}\big)$, and $\vartheta_4 \triangleq \overline{\lambda}^{\frac{1}{2}}\big(\overline{\sigma}+\hat{\sigma}_{\max}\big)$. This proves uniform boundedness of the solution $\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big)$ of the closed-loop system given by (15)–(18) for all $\big(x_0,\mu_{\lambda0},W_{\lambda0},\sigma_{\lambda0}\big)\in\mathbb{R}^n\times\mathbb{R}\times\mathbb{R}^{p\times m}\times\mathbb{R}$. Ultimate boundedness follows using similar arguments as in the proof of Theorem 3.1.

Remark 3.2: In arriving at Theorem 3.1 we assumed that $\|\sigma(t,x(t))\|_2\le\bar{\sigma},\ t\ge0$, where $\bar{\sigma}>0$ is unknown. Alternatively, we can assume that $\sigma(t,x(t))$ satisfies the Lipschitz condition $\|\sigma(t,x(t))\|_2\le\bar{\sigma}\|\tilde{x}(t)\|_2,\ t\ge0$, where $\bar{\sigma}>0$ is an *unknown* Lipschitz constant. In this case, it can be shown that Theorem 3.1 holds with

$$\begin{aligned}v(t)=&-\hat{\mu}(t)K\tilde{x}(t)-\hat{W}^{\mathrm{T}}(t)\varphi(\tilde{x}(t))\\ &-\hat{\sigma}(t)\|\tilde{x}(t)\|_2\mathrm{sgn}_{\mathrm{v}}(B^{\mathrm{T}}P\tilde{x}(t)),\quad t\ge0 \qquad (38)\end{aligned}$$

and with (11) and (18) replaced by

$$\dot{\hat{\sigma}}(t)=\ \nu\mathrm{Proj}\big[\hat{\sigma}(t),\ \|\tilde{x}(t)\|_2\|\tilde{x}^{\mathrm{T}}(t)PB\|_1\big],\ \hat{\sigma}(0)=\hat{\sigma}_0, \qquad (39)$$

$$\begin{aligned}\dot{\sigma}_\lambda(t)=\ &[-\nu\mathrm{Proj}\big(\hat{\sigma}(t),\ \|\tilde{x}(t)\|_2\|\tilde{x}^{\mathrm{T}}(t)BP\|_1\big)]\lambda^{\frac{1}{2}}(t)\\ &+\frac{1}{2}\sigma_\lambda(t)\dot{\lambda}(t)\lambda^{-1}(t),\quad \sigma_\lambda(0)=\sigma_{\lambda0}. \qquad (40)\end{aligned}$$

Next, we specialize Theorem 3.1 to the case where the sensor and actuator attacks on the system are time-invariant. In particular, we assume that the compromised system state is given by

$$\tilde{x}(t)=\ x(t)+\delta_{\mathrm{s}}(x(t)),\quad t\ge0 \qquad (41)$$

and is available for feedback, where $\tilde{x}(t)\in\mathbb{R}^n,\ t\ge0$, and $\delta_{\mathrm{s}}:\mathbb{R}^n\to\mathbb{R}^n$ captures sensor attacks. Furthermore, we assume that the control input is also compromised and is given by

$$\tilde{u}(t)=\ u(t)+\delta_{\mathrm{a}}(x(t)),\quad t\ge0 \qquad (42)$$

where $\tilde{u}(t)\in\mathbb{R}^m,\ t\ge0$, and $\delta_{\mathrm{a}}:\mathbb{R}^n\to\mathbb{R}^m$ captures actuator attacks. Moreover, we assume that the sensor attack in (41) is parameterized as $\delta_{\mathrm{s}}(x(t))=wx(t),\ t\ge0$, where $w\in\mathbb{R}$ is an *unknown* weight such that $\|w\|_2\le\overline{w}$ with *unknown* bound $\overline{w}$. In addition, we assume that the actuator attack in (42) is parameterized as $\delta_{\mathrm{a}}(x(t))=W^{\mathrm{T}}\varphi(x(t)),\ t\ge0$, where $W\in\mathbb{R}^{p\times m}$ is an *unknown* weighting matrix and $\varphi(x(t))\in\mathbb{R}^p,\ t\ge0$, is a nonlinear function with a known structure and with $x(t),\ t\ge0$, in general being unknown. In this case, (6) becomes

$$W^{\mathrm{T}}\varphi(x(t))=W^{\mathrm{T}}\varphi(\tilde{x}(t))+\sigma(x(t)),\ \ t\ge0 \qquad (43)$$

where $\sigma(x(t))\in\mathbb{R}^m,\ t\ge0$, is *unknown* and bounded, that is, $\|\sigma(x(t))\|_2\le\bar{\sigma},\ t\ge0$, and where $\bar{\sigma}>0$ is *unknown*. Therefore, (1) can be equivalently written as

$$\begin{aligned}\dot{x}(t)=\ Ax(t)+B\Big[u(t)+W^{\mathrm{T}}\varphi(\tilde{x}(t))+\sigma(x(t))\Big],&\\ x(0)=x_0,\quad t\ge0. \qquad (44)\end{aligned}$$

Next, define $\mu_\lambda(t)\triangleq\tilde{\mu}(t)\lambda^{\frac{1}{2}},\ t\ge0$, $W_\lambda(t)\triangleq\tilde{W}(t)\lambda^{\frac{1}{2}},\ t\ge0$, and $\sigma_\lambda(t)\triangleq\tilde{\sigma}(t)\lambda^{\frac{1}{2}},\ t\ge0$, with $\tilde{\mu}(t)\triangleq\mu-\hat{\mu}(t),\ t\ge0$, $\tilde{W}(t)\triangleq W-\hat{W}(t),\ t\ge0$, $\tilde{\sigma}(t)\triangleq\bar{\sigma}-\hat{\sigma}(t),\ t\ge0$, and $\lambda\triangleq\big(1+w\big)^{-1}$. For the statement of the next result, note that

$$\begin{aligned}\dot{x}(t)=\ &A_{\mathrm{r}}x(t)+\mu_\lambda(t)\lambda^{-\frac{1}{2}}BK\tilde{x}(t)+BW_\lambda^{\mathrm{T}}(t)\lambda^{-\frac{1}{2}}\varphi(\tilde{x}(t))\\ &+B(\sigma(x(t))-\hat{\sigma}(t)\mathrm{sgn}(B^{\mathrm{T}}P\tilde{x}(t))),\\ &x(0)=x_0,\quad t\ge0, \qquad (45)\end{aligned}$$

$$\dot{\mu}_\lambda(t)=\ -\gamma\mathrm{Proj}\big(\hat{\mu}(t),\ \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big)\lambda^{\frac{1}{2}},\quad \mu_\lambda(0)=\mu_{\lambda0}, \qquad (46)$$

$$\begin{aligned}\dot{W}_\lambda(t)=\ &-\eta\mathrm{Proj}_{\mathrm{m}}\big(\hat{W}(t),\ \varphi(\tilde{x}(t))\tilde{x}^{\mathrm{T}}(t)PB\big)\lambda^{\frac{1}{2}},\\ &W_\lambda(0)=W_{\lambda0}, \qquad (47)\end{aligned}$$

$$\dot{\sigma}_\lambda(t)=\ -\nu\mathrm{Proj}\big(\hat{\sigma}(t),\ ||\tilde{x}^{\mathrm{T}}(t)BP||_1\big)\lambda^{\frac{1}{2}},\quad \sigma_\lambda(0)=\sigma_{\lambda0}. \qquad (48)$$

Theorem 3.2: Consider the linear dynamical system $\mathscr{G}$ given by (1) with time-invariant, state-dependent sensor and actuator attacks given by (41) and (42), respectively, where $\|w\|_2\le\overline{w},\ t\ge0$, $\|W\|_{\mathrm{F}}\le\overline{W},\ t\ge0$, and $\|\sigma(x(t))\|_2\le\overline{\sigma},\ t\ge0$. Then, with the controller $\mathscr{G}_{\mathrm{c}}$ given by (5) and the corrective signal $v(t),\ t\ge0$, given by (8), the closed-loop system given by (45)–(48) is Lyapunov stable for all $\big(x_0,\mu_{\lambda0},W_{\lambda0},\sigma_{\lambda0}\big)\in\mathbb{R}^n\times\mathbb{R}\times\mathbb{R}^{p\times m}\times\mathbb{R}$ and $\lim_{t\to\infty}x(t)=0$.

Proof: Since the sensor and actuator attacks are time-invariant, it follows that $\overline{\dot{\mu}}=0$, $\overline{\dot{\lambda}}=0$, and $\overline{\dot{W}}=0$, and hence, d_2 in Theorem 3.1 given by $d_2=\gamma^{-1}[2\big(\overline{\mu}+\hat{\mu}_{\max}\big)\overline{\dot{\mu}\lambda}+\big(\overline{\mu}+\hat{\mu}_{\max}\big)^2\overline{\dot{\lambda}}]+\eta^{-1}[2\big(\overline{W}+\hat{W}_{\max}\big)\overline{\dot{W}\,\lambda}+\big(\overline{W}+\hat{W}_{\max}\big)^2\overline{\dot{\lambda}}]+\nu^{-1}[\big(\overline{\sigma}+\hat{\sigma}_{\max}\big)^2\overline{\dot{\lambda}}]=0$. In this case, with the Lyapunov function candidate $V\big(x,\mu_\lambda,W_\lambda,\sigma_\lambda\big)$ given by (23), using similar arguments as in the proof of Theorem 3.1 it follows that

$$\begin{aligned}\dot{V}\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big)\ &\le\ -x^{\mathrm{T}}(t)Rx(t)\\ &\le\ -d_1\|x(t)\|_2^2,\quad t\ge0 \qquad (49)\end{aligned}$$

which shows that the closed-loop system given by (45)–(48) is Lyapunov stable for all $\big(x_0,\mu_{\lambda0},W_{\lambda0},\sigma_{\lambda0}\big)\in\mathbb{R}^n\times\mathbb{R}\times\mathbb{R}^{p\times m}\times\mathbb{R}$.

Finally, with $W_1\big(x,\mu_\lambda,W_\lambda,\sigma_\lambda\big)=W_2\big(x,\mu_\lambda,W_\lambda,\sigma_\lambda\big)=V\big(x,\mu_\lambda,W_\lambda,\sigma_\lambda\big)$ and $W\big(x,\mu_\lambda,W_\lambda,\sigma_\lambda\big)=x^{\mathrm{T}}Rx$, it follows from Theorem 2.5 of [26] that $\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big)\to\mathscr{R}$ as $t\to\infty$, where $\mathscr{R}\triangleq\{\big(x,\mu_\lambda,W_\lambda,\sigma_\lambda\big)\colon W\big(x,\mu_\lambda,W_\lambda,\sigma_\lambda\big)=0\}=\{\big(x,\mu_\lambda,W_\lambda,\sigma_\lambda\big)\colon x=0\}$. In particular, note that

$$\begin{aligned}\dot{W}\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big)&=2x^{\mathrm{T}}(t)R\dot{x}(t)\\ =\ &2x^{\mathrm{T}}(t)R[A_{\mathrm{r}}x(t)+\mu_\lambda(t)\lambda^{-\frac{1}{2}}BK\tilde{x}(t)+B\phi_\lambda(t)\lambda^{-\frac{1}{2}}\\ &+BW_\lambda^{\mathrm{T}}(t)\lambda^{-\frac{1}{2}}\varphi(\tilde{x}(t))+B(\sigma(x(t))-\hat{\sigma}(t)\mathrm{sgn}(B^{\mathrm{T}}P\tilde{x}(t)))]\end{aligned}$$

is bounded for all $t\ge0$, and hence, all conditions of Theorem 2.5 of [26] are satisfied proving that $x(t)\to0$ as $t\to0$. ■

Remark 3.3: It is important to note that since $\dot{V}\big(x(t),\mu_\lambda(t),W_\lambda(t),\sigma_\lambda(t)\big),\ t\ge0$, is not continuously differentiable, a standard proof involving Barbalat's lemma does not hold in proving partial asymptotic stability in Theorem 3.2. Consequently, Theorem 3.2 requires the more general result given by [26, Theorem 2.5].

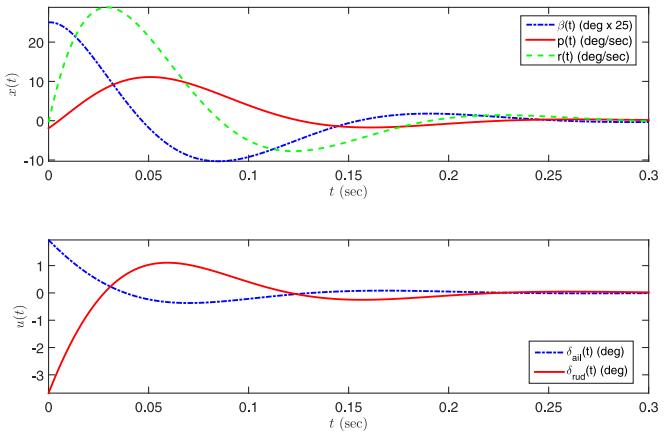

Fig. 2. Nominal system performance of the lateral directional dynamics of the aircraft given by (50) when the state vector $x(t)$, $t \geq 0$, is available for feedback and the control signal is uncompromised.

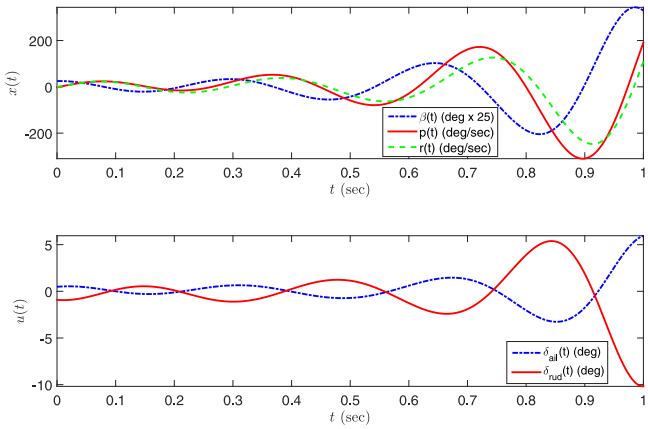

Fig. 3. System performance of the lateral directional dynamics of the aircraft given by (50) in the presence of time-varying and state-dependent sensor and actuator attacks without any corrective signal (i.e., $v(t) \equiv 0$) in (34).

IV. Illustrative Numerical Example

To illustrate the key ideas presented in this technical note, we consider a dynamical system representing the lateral directional dynamics of an aircraft adopted from [24, p. 136] given by

$$\begin{bmatrix} \dot{\beta}(t) \\ \dot{p}(t) \\ \dot{r}(t) \end{bmatrix} = \begin{bmatrix} -0.025 & 0.104 & -0.994 \\ 574.7 & 0 & 0 \\ 16.20 & 0 & 0 \end{bmatrix} \begin{bmatrix} \beta(t) \\ p(t) \\ r(t) \end{bmatrix} + \begin{bmatrix} 0.122 & -0.276 \\ -53.61 & 33.25 \\ 195.5 & -529.4 \end{bmatrix} u(t), \quad t \geq 0 \tag{50}$$

where $[\beta(0),\ p(0),\ r(0)]^{\mathrm{T}} = [1,\ -2,\ -1]^{\mathrm{T}}$ and with state feedback control gain

$$K = \begin{bmatrix} 2.053 & 0.079 & -0.045 \\ -3.823 & -0.128 & 0.102 \end{bmatrix}, \tag{51}$$

where the state vector $x(t) = \big[\beta(t),\ p(t),\ r(t)\big]^{\mathrm{T}}$, $t \geq 0$, contains the sideslip angle in deg, the roll rate in deg/s, and the yaw rate in deg/s, respectively, and the control input $u(t) = \big[\delta_{\mathrm{ail}}(t),\ \delta_{\mathrm{rud}}(t)\big]^{\mathrm{T}}$, $t \geq 0$, contains the aileron command in deg and the rudder command in deg, respectively. The nominal performance of this dynamical system is shown in Fig. 2.

To illustrate the results of Theorem 3.1 with (8) replaced by (34) consider the time-varying, state-dependent sensor and actuator attacks given by (2) and (3), respectively, with $w(t) = -\big(0.75 + 0.15\sin(2.5t)\big)$, $t \geq 0$, and $\delta_{\mathrm{a}}(t, x(t)) = [1, \quad 1]^{\mathrm{T}} 0.5\cos(2.5t) + [0.1\cos(2t), \quad 0.5\sin(t)]^{\mathrm{T}} 0.2\sin(\beta(t))\cos(p(t))$, $t \geq 0$. The system performance of the controller $\mathscr{G}_{\mathrm{c}}$ given by (5) without any corrective action (i.e., $v(t) \equiv 0$) results in an unstable closed-loop system and is shown in Fig. 3.

To design the proposed corrective signal given by (34), (10)–(11), we set $\gamma = 0.8$, $\xi = 0.8$, $\eta = 0.8$, $\nu = 0.8$, and $R = I_3$. Alternatively, a more methodical selection using a convex optimization approach [27] can be used to select the design parameters. The system performance of the controller given by (5) with the proposed corrective signal is depicted in Fig. 4. This shows that the proposed adaptive control architecture achieves satisfactory system performance in the face of time-varying, state-dependent sensor and actuator attacks.

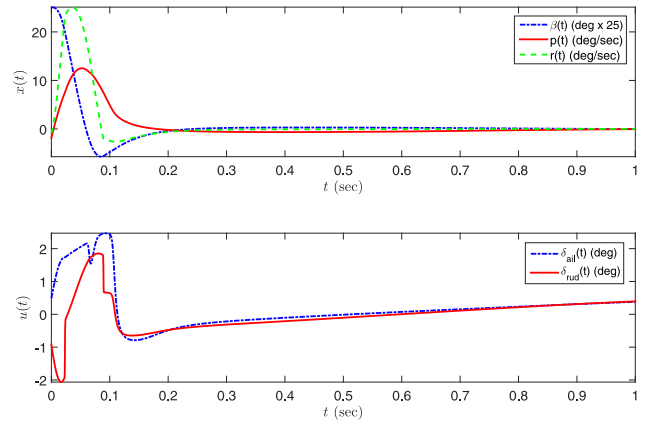

Fig. 4. System performance of the lateral directional dynamics of the aircraft given by (50) in the presence of time-varying and state-dependent sensor and actuator attacks with the proposed corrective signal given by (34), (10)–(11) with $\gamma = 0.8$, $\xi = 0.8$, $\eta = 0.8$, $\nu = 0.8$, and $R = I_3$.

V. Conclusion

In this technical note, we developed an adaptive framework for the control design of cyber-physical systems in the presence of simultaneous adversarial sensor and actuator attacks. The adaptive control framework addresses the fundamental issues of adaptation, controller complexity, and security in controlled cyber-physical systems. In future research, we will extend the proposed framework to develop reliable hybrid-adaptive control architectures for cyber-physical systems involving system nonlinearities and system modeling uncertainty, with integrated verification and validation, for providing robust system performance and reconfigurable system operation in the presence of system uncertainties, component failures, and adversarial attacks. In addition, we will consider cyber-physical systems with communication dropouts and time delays.

References

[1] P. Antsaklis, "Goals and challenges in cyber-physical systems research," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3117–3119, 2014.

[2] M.-A. Massoumnia, G. C. Verghese, and A. S. Willsky, "Failure detection and identification," *IEEE Trans. Autom. Control*, vol. 34, no. 3, pp. 316–321, 1989.

[3] M. Blanke and J. Schröder, *Diagnosis and Fault-Tolerant Control*. New York: Springer, 2006, vol. 691.
[4] I. Hwang, S. Kim, Y. Kim, and C. E. Seah, "A survey of fault detection, isolation, and reconfiguration methods," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 3, pp. 636–653, 2010.
[5] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proc. IEEE*, vol. 95, no. 1, pp. 163–187, 2007.
[6] A. Gupta, C. Langbort, and T. Basar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. IEEE Conf. Decision and Control*, 2010, pp. 1096–1101.
[7] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems—Part I: Models and fundamental limitations," *arXiv preprint arXiv:1202.6144*, 2012.
[8] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems—Part II: Centralized and distributed monitor design," *arXiv preprint arXiv:1202.6049*, 2012.
[9] 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, 2013.
[10] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, 2012.
[11] J. Weimer, N. Bezzo, M. Pajic, G. J. Pappas, O. Sokolsky, and I. Lee, "Resilient parameter-invariant control with application to vehicle cruise control," in *Control of Cyber-Physical Systems*. New York: Springer, 2013, pp. 197–216.
[12] K. C. Sou, H. Sandberg, and K. H. Johansson, "On the exact solution to a smart grid cyber-security analysis problem," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 856–865, 2013.
[13] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.
[14] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.
[15] K. G. Vamvoudakis, J. P. Hespanha, B. Sinopoli, and Y. Mo, "Detection in adversarial environments," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3209–3223, 2014.
[16] N. Bezzo, J. Weimer, M. Pajic, O. Sokolsky, G. J. Pappas, and I. Lee, "Attack resilient state estimation for autonomous robotic systems," *Proc. IEEE/RSJ Int. Conf. Intelligent Robots and Systems*, pp. 3692–3698, 2014.
[17] J. Park, R. Ivanov, J. Weimer, M. Pajic, and I. Lee, "Sensor attack detection in the presence of transient faults," *Proc. ACM/IEEE 6th Int. Conf. Cyber-Physical Systems*, pp. 1–10, 2015.
[18] M. Pajic, P. Tabuada, I. Lee, and G. J. Pappas, "Attack-resilient state estimation in the presence of noise," *Proc. 54th IEEE Conf. Decision and Control*, pp. 5827–5832, 2015.
[19] R. Mitchell and R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Trans. Reliability*, vol. 62, no. 1, pp. 199–210, 2013.
[20] 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.
[21] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, 2012.
[22] W. M. Haddad and V. Chellaboina, *Nonlinear Dynamical Systems and Control: A Lyapunov-Based Approach*. Princeton, NJ: Princeton University Press, 2008.
[23] J.-B. Pomet and L. Praly, "Adaptive nonlinear regulation: Estimation from the Lyapunov equation," *IEEE Trans. Autom. Control*, vol. 37, no. 6, pp. 729–740, 1992.
[24] E. Lavretsky and K. Wise, *Robust and Adaptive Control With Aerospace Applications*. New York: Springer, 2012.
[25] M. M. Polycarpou and P. A. Ioannou, "A robust adaptive nonlinear control design," *Automatica*, vol. 32, no. 3, pp. 423–427, 1996.
[26] W. M. Haddad, V. Chellaboina, and S. G. Nersesov, *Impulsive and Hybrid Dynamical Systems: Stability, Dissipativity, and Control*. Princeton, NJ: Princeton University Press, 2006.
[27] M. L. Fravolini, T. Yucelen, and G. Campa, "Set theoretic performance verification of low-frequency learning adaptive controllers," *Int. J. Adapt. Control and Signal Process.*, vol. 29, no. 10, pp. 1243–1258, 2015.