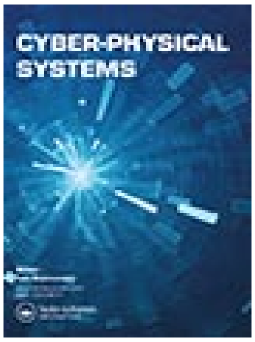

Taylor & Francis
Taylor & Francis Group

Cyber-Physical Systems

ISSN: 2333-5777 (Print) 2333-5785 (Online) Journal homepage: http://www.tandfonline.com/loi/tcyb20

Adaptive control architectures for mitigating sensor attacks in cyber-physical systems

Tansel Yucelen, Wassim M. Haddad & Eric M. Feron

To cite this article: Tansel Yucelen, Wassim M. Haddad & Eric M. Feron (2016): Adaptive control architectures for mitigating sensor attacks in cyber-physical systems, Cyber-Physical Systems, DOI: 10.1080/23335777.2016.1244562

To link to this article: http://dx.doi.org/10.1080/23335777.2016.1244562

Published online: 19 Oct 2016.

CYBER-PHYSICAL SYSTEMS, 2016
http://dx.doi.org/10.1080/23335777.2016.1244562

Taylor & Francis
Taylor & Francis Group

Adaptive control architectures for mitigating sensor attacks in cyber-physical systems

Tansel Yucelen[a], Wassim M. Haddad[b] and Eric M. Feron[b]

[a]Department of Mechanical Engineering, University of South Florida, Tampa, FL, USA; [b]School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA, USA

ABSTRACT

The accuracy of sensor measurements is critical to the design of high-performance control systems since sensor uncertainties can significantly deteriorate achievable closed-loop dynamical system performance. Sensor uncertainty can arise due to low sensor quality, sensor failure or detrimental environmental conditions. For example, relatively cheap sensor suites are used for low-cost, small-scale unmanned vehicle applications that can result in inaccurate sensor measurements. Alternatively, sensor measurements can also be corrupted by malicious attacks if dynamical systems are controlled through large-scale, multilayered communication networks as is the case in cyber-physical systems. This paper presents several adaptive control architectures for stabilisation of linear dynamical systems in the presence of sensor uncertainty and sensor attacks. Specifically, we propose new and novel adaptive controllers for state-independent and state-dependent sensor uncertainties. In particular, we show that the proposed controllers guarantee asymptotic stability of the closed-loop dynamical system when the sensor uncertainties are time-invariant and uniform ultimate boundedness when the uncertainties are time-varying. We further discuss the practicality of the proposed approaches and provide several numerical examples to illustrate the efficacy of the proposed adaptive control architectures.

ARTICLE HISTORY
Received 11 March 2016
Accepted 26 September 2016

KEYWORDS
Linear dynamical systems; sensor attacks; adaptive control; asymptotic stability; uniform ultimate boundedness; cyber-physical systems

1. Introduction

The design and implementation of control law architectures for modelling and controlling complex, large-scale network dynamical systems is a nontrivial control engineering task involving the consideration and operation of computing and communication components interacting with the physical and biological processes to be controlled. These collections of complex, large-scale multilayered dynamical networks merge the cyberworld of computing and communications with the physical and biological worlds, and are known as *cyber-physical systems* (see [1] and the references therein). Cyber-physical systems are characterised by a large number of highly coupled heterogeneous dynamic network components and have become ubiquitous in the control of large-scale, complex dynamical systems given the recent advances in embedded sensor, computation, and communication technologies. Such systems include safety-critical aerospace systems, power systems, communications

CONTACT Tansel Yucelen ✉ yucelen@usf.edu

systems, network systems, transportation systems, large-scale manufacturing systems, integrative biological systems, economic systems, ecological systems, process control systems and health care systems.

In the aforementioned applications, the system computation and information processing is strongly integrated with the physical processes and it has virtually become impossible to identify whether the dynamical system behaviour is the result of the system computations (i.e. the computer programs), the governing physical laws or the tight integration of both working in unison. This is the case, for example, in cooperative control of unmanned air vehicles and autonomous underwater vehicles for combat, surveillance and reconnaissance; distributed reconfigurable sensor networks for managing power levels of wireless networks; air and ground transportation systems for air traffic control and payload transport and traffic management; swarms of air vehicle formations for command and control between heterogeneous air vehicles; and congestion control in communication networks for routing the flow of information through multilayered networks.

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 computing platforms and manipulate system measurement data 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 devices that are hijacked and controlled by an adversarial entity that actively engages to maximally degrade system information require adaptive control algorithms to recover system performance.

Cyber-physical security involving information security and detection in adversarial environments have been considered in the literature.[2–13] In particular, early approaches are focused on classical fault detection, isolation, and recovery schemes (see, for example, [2,3] and references therein). Specifically, sensor measurements are compared with an analytical model of the dynamical system by forming a residual signal and analysing this signal to determine if a fault has occurred. However, in practice it is difficult to identify a single residual signal per failure mode, and as the number of failure modes increase this becomes prohibitive. In addition, a common underlying assumption of the classical fault detection, isolation and recovery schemes is that all dynamical system signals remain bounded during the fault detection process, which is not a valid assumption; especially if the adversarial attacks are state-dependent (see, for example, the problem given in Section 5.2 addressing the lateral directional dynamics of an aircraft).

More recently, the authors in [4] consider the problem of control and estimation in a networked system with communication links subject to disturbances, which correspond to packet losses. The disturbance model is assumed to follow a particular stochastic process (typically a Bernoulli process), which does not necessarily capture the behaviour of an attacker. The authors in [5] consider a model in which the attacker plans to maximise a certain cost; however, their results are limited to one-dimensional systems. In [6–8], the authors consider the fundamental limitations of attack detection and identification methods for linear systems. For the particular case of power networks, their approach is computationally expensive and is not linked to the controller design.

In [9], adversarial attacks on actuator and sensors are modelled as disturbances. However, the control methodology presented cannot handle situations where more than half of the sensors are compromised and the set of attacked nodes change over time. In [10], the authors consider the problem of sensor attacks under the assumption that a bounded subset of the sensors is corrupted. However, as in [5], their results are limited to one-dimensional systems. Finally, sensor attacks based on steady-state operation models are presented in [11–13]. However, these results fail to exploit the constraints imposed by the system dynamics and are limited to smart grid models.

In this paper, we present several adaptive control architectures for stabilisation of linear dynamical systems in the presence of sensor attacks. Unlike the other approaches cited above, the proposed architectures do not require boundedness of all of the compromised closed-loop system signals. Furthermore, the proposed approach can account for sensor attacks that can corrupt all available sensor measurements and we do not assume that the sensor attacks are constrained to a particular model. In addition, we can address both transient and steady-state stability and performance. Specifically, we present new adaptive control architectures for state-independent and state-dependent sensor uncertainties under realistic assumptions. The proposed controllers guarantee asymptotic stability of the closed-loop dynamical system when the sensor uncertainties are time-invariant and guarantee uniform ultimate boundedness when the uncertainties are time-varying. We further discuss the practicality of the proposed approaches and provide several numerical examples to illustrate the proposed framework.

Although our proposed adaptive control architectures build on the solid foundation of adaptive control theory, they significantly go beyond classical adaptive control architectures (see, for example, [14–19]). Specifically, since the class of uncertainties considered in this paper originates from sensor attacks resulting from devices that are hijacked and controlled by an adversarial entity, we require new and novel adaptive controller frameworks as compared to classical adaptive control architectures that focus on the class of uncertainties originating from parametric uncertainty and system nonlinearities. Finally, although we only consider stabilisation of linear dynamical systems to elucidate our proposed adaptive control approach for mitigating sensor attacks, the proposed framework can be readily extended to address command following problems as well as system nonlinearities.

The contents of the paper are as follows. In Section 2, we present the problem formulation for adaptive stabilisation of linear dynamical systems in the presence of sensor attacks. In Section 3, we develop an adaptive controller architecture for addressing state-independent sensor uncertainties, whereas Section 4 extends this architecture to address state-dependent sensor uncertainties. In Section 5, we provide several illustrative numerical examples that highlight the proposed adaptive stabilisation framework. Finally, in Section 6, we present conclusions and highlight some recommendations for future research.

The notation used in this paper 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 and $\|\cdot\|_2$ denotes the Euclidian norm. Furthermore, we write $\lambda_{\min}(A)$ (resp., $\lambda_{\max}(A)$) for the minimum (resp., maximum) eigenvalue of the Hermitian matrix A, $\mathrm{spec}(A)$ for the spectrum of the Hermitian matrix

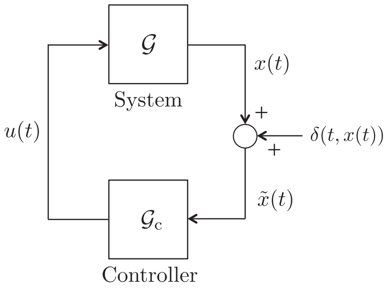

Figure 1. Closed-loop dynamical system in the presence of sensor attacks.

A including multiplicity and $\underline{x}$ (resp., $\overline{x}$) for the lower bound (resp., upper bound) of a bounded signal $x(t) \in \mathbb{R}^n$, $t \geq 0$, that is, $\underline{x} \leq \|x(t)\|_2$, $t \geq 0$ (resp., $\|x(t)\|_2 \leq \overline{x}$, $t \geq 0$).

2. Problem formulation

Consider the linear dynamical system $\mathcal{G}$ given by

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

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

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

is available for feedback, where $\tilde{x}(t) \in \mathbb{R}^n$, $t \geq 0$ and $\delta : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ capture sensor attacks. In particular, if $\delta(\cdot,\cdot)$ is nonzero, then the uncompromised state vector $x(t)$, $t \geq 0$, is corrupted with a faulty (or malicious) signal $\delta(\cdot,\cdot)$. Alternatively, if $\delta(t, x) \equiv 0$ is zero, then $\tilde{x}(t) = x(t)$, $t \geq 0$, and the uncompromised state vector is available for feedback; see Figure 1.

Since (A, B) is controllable, there exists a feedback gain matrix $K \in \mathbb{R}^{m\times n}$ that asymptotically stabilises the linear dynamical system $\mathcal{G}$ when the state vector is available for feedback, that is,

$$\dot{x}(t) = A_r x(t), \quad x(0) = x_0, \quad t \geq 0, \tag{3}$$

where $A_r \triangleq A + BK$ is Hurwitz. In this case, it follows from converse Lyapunov theory [20] 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

$$0 = A_r^{\mathrm{T}} P + P A_r + R. \tag{4}$$

For $\delta(t, x(t)) \neq 0$, $t \geq 0$, our objective is to design a controller $\mathcal{G}_c$ 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 $\delta(t, x(t))$, $t \geq 0$, to asymptotically (or approximately) recover the ideal system performance achieved when the state vector is available for feedback.

Even though, for simplicity of exposition, we consider a linear dynamical system $\mathcal{G}$ given by (1) and a linear controller $\mathcal{G}_\mathrm{c}$ given by (5), the results in this paper can be readily extended to the case where $\mathcal{G}$ and $\mathcal{G}_\mathrm{c}$ are given by

$$\dot{x}(t) = f(x(t)) + G(x(t))u(t), \quad x(0) = x_0, \quad t \geq 0, \tag{6}$$

$$u(t) = \phi(\tilde{x}(t)) + v(t), \tag{7}$$

where $f : \mathbb{R}^n \to \mathbb{R}^n$, $f(0) = 0$, $G : \mathbb{R}^n \to \mathbb{R}^{n \times m}$, and $\phi : \mathbb{R}^n \to \mathbb{R}^m$. In this case, we assume that $\phi(\tilde{x})$ asymptotically stabilises $\mathcal{G}$ when the uncompromised state vector is available for feedback, that is, the zero solution $x(t) \equiv 0$ of (6) with $u(t) = \phi(x(t))$ and $v(t) \equiv 0$ is asymptotically stable. In this case, there exists a continuously differentiable function $V : \mathbb{R}^n \to \mathbb{R}$ and a function $l : \mathbb{R}^n \to \mathbb{R}^p$ such that $V(0) = 0$, $l(0) = 0$, and

$$0 = V'(x) f_\mathrm{r}(x) + l^\mathrm{T}(x) l(x), \tag{8}$$

where $V'(x) \triangleq \partial V / \partial x$, $f_\mathrm{r}(x) \triangleq f(x) + G(x)\phi(x)$, and $l^\mathrm{T}(x) l(x) > 0$, $x \neq 0$. A similar construction can be used to extend the framework to command following.

In this paper, we design the corrective signal $v(t)$, $t \geq 0$, in (5) for two important classes of sensor uncertainties; namely, state-independent and state-dependent sensor uncertainties. Specifically, for state-independent sensor uncertainties, $\tilde{x}(t)$, $t \geq 0$, in (2) takes the form

$$\tilde{x}(t) = x(t) + \delta(t), \tag{9}$$

where $\delta(t) \in \mathbb{R}^n$, $t \geq 0$, is an *unknown* bounded time-varying disturbance such that $\|\delta(t)\|_2 \leq \overline{\delta}$, $t \geq 0$. For state-dependent sensor uncertainties, we consider

$$\tilde{x}(t) = x(t) + \delta(t, x(t)), \tag{10}$$

with the parameterisation $\delta(t, x(t)) = w(t)x(t)$, where $w(t) \in \mathbb{R}$, $t \geq 0$, is an *unknown* bounded time-varying weight with bounded rate of change such that $\|w(t)\|_2 \leq \overline{w}$, $t \geq 0$, and $\|\dot{w}(t)\|_2 \leq \overline{\dot{w}}$, $t \geq 0$. 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.

Remark 1: In the case where the parameterisation $\delta(t, x(t)) = w(t)x(t)$ does not hold, one can consider a neural network universal function approximator [21] to parameterise $\delta(t, x(t))$ on a compact subset of $\mathbb{R}^n$. For details of such a parameterisation; see, for example, [21].

3. Adaptive stabilisation for state-independent sensor attacks

In this section, we design the corrective signal $v(t)$, $t \geq 0$, in (5) to achieve adaptive stabilisation in the presence of state-independent sensor uncertainties. In particular, we first consider the case where the sensor uncertainty in (9) is time-invariant, that is, $\delta(t) \equiv \delta$, $t \geq 0$ and then we generalise our results to the time-varying sensor uncertainty case.

3.1. Time-invariant, state-independent sensor attacks

In this subsection, we assume that the sensor uncertainty in (9) is time-invariant, that is, $\delta(t) \equiv \delta$, $t \geq 0$ and we consider the controller $\mathcal{G}_{\mathrm{c}}$ in (5) with the corrective signal given by

$$v(t) = -K\hat{\delta}(t), \tag{11}$$

where

$$\dot{\hat{\delta}}(t) = -\gamma A^{\mathrm{T}}\tilde{P}\big(\tilde{x}(t) - \hat{x}(t) - \hat{\delta}(t)\big), \quad \hat{\delta}(0) = \hat{\delta}_0, \quad t \geq 0, \tag{12}$$

$$\dot{\hat{x}}(t) = A_{\mathrm{r}}\hat{x}(t) + \big(\gamma A^{\mathrm{T}}\tilde{P} + L\big)\big(\tilde{x}(t) - \hat{x}(t) - \hat{\delta}(t)\big), \quad \hat{x}(0) = \hat{x}_0, \quad t \geq 0, \tag{13}$$

$\hat{\delta}(t) \in \mathbb{R}^n$, $t \geq 0$, is the estimate of the sensor uncertainty δ, $\hat{x}(t) \in \mathbb{R}^n$, $t \geq 0$, is the state estimate of the compromised state vector $x(t)$, $t \geq 0$, $\gamma \in \mathbb{R}$ is a positive design gain, and $L \in \mathbb{R}^{n\times n}$ is the gain matrix for the state estimator dynamics (13) and is such that $A_{\mathrm{r}} - L$ is Hurwitz. Since $A_{\mathrm{r}} - L$ is Hurwitz, it follows from converse Lyapunov theory [20] that there exists a unique positive-definite $\tilde{P} \in \mathbb{R}^{n\times n}$ satisfying

$$0 = \big(A_{\mathrm{r}} - L\big)^{\mathrm{T}}\tilde{P} + \tilde{P}\big(A_{\mathrm{r}} - L\big) + \tilde{R}, \tag{14}$$

for a given positive-definite matrix $\tilde{R} \in \mathbb{R}^{n\times n}$.

For the statement of the next theorem, define $e(t) \triangleq \tilde{x}(t) - \hat{x}(t) - \hat{\delta}(t)$, $t \geq 0$, and $\tilde{\delta}(t) \triangleq \delta - \hat{\delta}(t)$, $t \geq 0$, and note that

$$\dot{e}(t) = \big(A_{\mathrm{r}} - L\big)e(t) - A\tilde{\delta}(t), \quad e(0) = e_0, \quad t \geq 0, \tag{15}$$

$$\dot{\tilde{\delta}}(t) = \gamma A^{\mathrm{T}}\tilde{P}e(t), \quad \tilde{\delta}(0) = \tilde{\delta}_0, \quad t \geq 0. \tag{16}$$

Theorem 1: *Consider the linear dynamical system $\mathcal{G}$ given by (1) with state-independent sensor uncertainty given by (9), where $\delta(t) \equiv \delta$, $t \geq 0$, and assume that* $\det(A) \neq 0$. *Then, with the controller $\mathcal{G}_{\mathrm{c}}$ given by (5) and the corrective signal $v(t)$, $t \geq 0$, given by (11), the zero solution $\big(e(t), \tilde{\delta}(t)\big) \equiv (0, 0)$ of the closed-loop system given by (15) and (16) is Lyapunov stable for all $\big(e_0, \tilde{\delta}_0\big) \in \mathbb{R}^n \times \mathbb{R}^n$ and* $\lim_{t\to\infty} e(t) = 0$ *and* $\lim_{t\to\infty} \tilde{\delta}(t) = 0$.

Proof: To show Lyapunov stability of the closed-loop system given by (15) and (16), consider the Lyapunov function candidate given by

$$V\big(e, \tilde{\delta}\big) = e^{\mathrm{T}}\tilde{P}e + \gamma^{-1}\tilde{\delta}^{\mathrm{T}}\tilde{\delta}, \tag{17}$$

where $\tilde{P}$ satisfies (14). Note that $V(0, 0) = 0$, $V\big(e, \tilde{\delta}\big) > 0$ for all $\big(e, \tilde{\delta}\big) \neq (0, 0)$ and $V\big(e, \tilde{\delta}\big)$ is radially unbounded. The time derivative of (17) along the closed-loop system trajectories of (15) and (16) is given by

$$\begin{aligned}\dot{V}\big(e(t),\tilde{\delta}(t)\big) &= 2e^{\mathrm{T}}(t)\tilde{P}\big[\big(A_{\mathrm{r}}-L\big)e(t)-A\tilde{\delta}(t)\big]+2\tilde{\delta}^{\mathrm{T}}(t)A^{\mathrm{T}}\tilde{P}e(t)\\ &= e^{\mathrm{T}}(t)\big[\big(A_{\mathrm{r}}-L\big)^{\mathrm{T}}\tilde{P}+\tilde{P}\big(A_{\mathrm{r}}-L\big)\big]e(t)\\ &= -e^{\mathrm{T}}(t)\tilde{R}e(t)\\ &\leq\ 0,\quad t\geq 0,\end{aligned}\tag{18}$$

and hence, the closed-loop system given by (15) and (16) is Lyapunov stable for all $\big(e_0,\tilde{\delta}_0\big)\in\mathbb{R}^n\times\mathbb{R}^n$.

To show $\lim_{t\to\infty}e(t)=0$, note that

$$\ddot{V}\big(e(t),\tilde{\delta}(t)\big)=-2e^{\mathrm{T}}(t)\tilde{R}\Big(\big(A_{\mathrm{r}}-L\big)e(t)-A\tilde{\delta}(t)\Big)\tag{19}$$

is bounded for all $t\geq 0$ since $\big(e(t),\tilde{\delta}(t)\big)$ is bounded for all $t\geq 0$. Thus, $\dot{V}\big(e(t),\tilde{\delta}(t)\big)$, $t\geq 0$, is uniformly continuous in t. Now, it follows from Barbalat's lemma [[20], p. 211] that $\lim_{t\to\infty}\dot{V}\big(e(t),\tilde{\delta}(t)\big)=0$, and hence, $\lim_{t\to\infty}e(t)=0$.

Finally, to show $\lim_{t\to\infty}\tilde{\delta}(t)=0$, define $\mathcal{R}\triangleq\big\{(e,\tilde{\delta}\in\mathbb{R}^n\times\mathbb{R}^n:\dot{V}\big(e,\tilde{\delta}\big)=0\big\}$ and let $\mathcal{M}$ be the largest invariant set contained in $\mathcal{R}$. In this case, it follows from (15) that $A\tilde{\delta}=0$, and hence, $\tilde{\delta}=0$ since $\det(A)\neq 0$. Thus, $\big(e(t),\tilde{\delta}(t)\big)\to\mathcal{M}=\big\{(0,0)\big\}$ as $t\to\infty$. □

Remark 2: It follows from (1) and (11) that

$$\dot{x}(t)=A_{\mathrm{r}}x(t)+BK\tilde{\delta}(t),\quad x(0)=x_0,\quad t\geq 0,\tag{20}$$

which, using the boundedness of $\tilde{\delta}(t)$, $t\geq 0$, implies that $x(t)$ is bounded for all $t\geq 0$. Hence, using (9), $\tilde{x}(t)$ is bounded for all $t\geq 0$. Furthermore, since $e(t)=\tilde{x}(t)-\hat{x}(t)-\hat{\delta}(t)$, $t\geq 0$, and the signals $e(t)$, $t\geq 0$, $\tilde{x}(t)$, $t\geq 0$, and $\hat{\delta}(t)$, $t\geq 0$, are bounded, it follows that $\hat{x}(t)$, $t\geq 0$, is bounded.

Remark 3: Since, by Theorem 1, $\lim_{t\to\infty}\tilde{\delta}(t)=0$, it follows from (20) that $\lim_{t\to\infty}x(t)=0$. In addition, $\lim_{t\to\infty}e(t)=0$ and $\lim_{t\to\infty}\tilde{\delta}(t)=0$ imply $\lim_{t\to\infty}\big(x(t)-\hat{x}(t)\big)=0$, which shows that the state estimate $\hat{x}(t)$, $t\geq 0$, converges to the uncompromised state vector $x(t)$, $t\geq 0$.

Remark 4: In the case where $\det(A)=0$, it can be shown that the solution $\big(e(t),\tilde{\delta}(t)\big)$ of the closed-loop system given by (15) and (16) is Lyapunov stable for all $\big(e_0,\tilde{\delta}_0\big)\in\mathbb{R}^n\times\mathbb{R}^n$ and $\lim_{t\to\infty}e(t)=0$. In this case, $\lim_{t\to\infty}A\tilde{\delta}(t)=0$, which implies that only a specific subset of $\tilde{\delta}(t)$, $t\geq 0$, converges to zero.

3.2. Time-varying, state-independent sensor attacks

In this subsection, we consider time-varying, state-independent sensor attacks with bounded variation and unbounded rates of change (e.g. an unknown signal corrupted with measurement noise). To address this problem, define $\sigma(t)\triangleq x(t)-\hat{x}(t)$, $t\geq 0$, and consider the augmented system

$$\dot{\xi}(t)=A_{\mathrm{c}}\xi(t)+B_{\mathrm{c}}\delta(t),\quad \xi(0)=\xi_0,\quad t\geq 0,\tag{21}$$

$$z(t)=C_{\mathrm{c}}\xi(t),\tag{22}$$

where $\xi(t) \triangleq \left[\sigma^{\mathrm{T}}(t), \hat{\delta}^{\mathrm{T}}(t)\right]^{\mathrm{T}}$,

$$A_{\mathrm{c}} \triangleq \begin{bmatrix} A_{\mathrm{r}} - \gamma A^{\mathrm{T}}\tilde{P} - L & -BK + \gamma A^{\mathrm{T}}\tilde{P} + L \\ -\gamma A^{\mathrm{T}}\tilde{P} & \gamma A^{\mathrm{T}}\tilde{P} \end{bmatrix}, \tag{23}$$

$$B_{\mathrm{c}} \triangleq \begin{bmatrix} BK - \gamma A^{\mathrm{T}}\tilde{P} - L \\ -\gamma A^{\mathrm{T}}\tilde{P} \end{bmatrix}, \tag{24}$$

$$C_{\mathrm{c}} \triangleq \left[0_n \; I_n\right], \tag{25}$$

with $\det(A) \neq 0$. Note that in the case where $\delta(t) \equiv \delta$, $t \geq 0$, it follows from Theorem 1 that the zero solution $\left(\sigma(t), \tilde{\delta}(t)\right) = \left(0, 0\right)$ is asymptotically stable, and hence, A_{c} is Hurwitz. Thus, in the presence of time-varying sensor attacks with bounded variations and unbounded rates of changes, the controller $\mathcal{G}_{\mathrm{c}}$ given by (5) with the corrective signal given by (11), (12) and (13) yields bounded system solutions. In this case, since the DC gain of the dynamical system given by (21) and (22) is $-C_{\mathrm{c}}A_{\mathrm{c}}^{-1}B_{\mathrm{c}} = I_n$, we can characterise the accuracy of the signal $z(t) = \hat{\delta}(t)$, $t \geq 0$, that can estimate $\delta(t)$, $t \geq 0$, by resorting to classical frequency domain methods.[22,23]

Since asymptotic stability of the solution $\left(e(t), \tilde{\delta}(t)\right)$, $t \geq 0$, is not possible in the presence of time-varying, state-independent sensor uncertainties, we use time-domain methods to characterise the effect of controller design parameters on the ultimate bound of $\left(e(t), \tilde{\delta}(t)\right)$, $t \geq 0$, in the neighbourhood of the equilibrium point $(0, 0)$. For the remainder of this section, without loss of generality, we assume that the time-varying sensor uncertainties are bounded and have bounded rates of change; that is, $\|\delta(t)\|_2 \leq \overline{\delta}$, $t \geq 0$, and $\|\dot{\delta}(t)\|_2 \leq \overline{\dot{\delta}}$, $t \geq 0$.

For the statement of our next result, it is necessary to introduce the projection operator.[24] Specifically, let $\phi : \mathbb{R}^n \rightarrow \mathbb{R}$ be a continuously differentiable convex function 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*. Then, the *projection operator* $\mathrm{Proj} : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ is defined by

$$\mathrm{Proj}(\theta, y) \triangleq \begin{cases} y, & \text{if } \phi(\theta) < 0, \\ y, & \text{if } \phi(\theta) \geq 0 \text{ and } \phi'(\theta)y \leq 0, \\ y - \frac{\phi'^{\mathrm{T}}(\theta)\phi'(\theta)y}{\phi'(\theta)\phi'^{\mathrm{T}}(\theta)}\phi(\theta), & \\ \quad \text{if} \phi(\theta) \geq 0 \text{ and } \phi'(\theta)y > 0, & \end{cases} \tag{26}$$

where $y \in \mathbb{R}^n$. Note that it follows from the definition of the projection operator that $(\theta - \theta^*)^{\mathrm{T}}(\mathrm{Proj}(\theta, y) - y) \leq 0, \theta^* \in \mathbb{R}^n$.

Next, for the controller $\mathcal{G}_{\mathrm{c}}$ given by (5), we use the corrective signal

$$v(t) = -K\hat{\delta}(t), \quad t \geq 0, \tag{27}$$

where

$$\dot{\hat{\delta}}(t) = \gamma\, \mathrm{Proj}\Big(\hat{\delta}(t), -A^{\mathrm{T}}\tilde{P}\big(\tilde{x}(t) - \hat{x}(t) - \hat{\delta}(t)\big)\Big), \quad \hat{\delta}(0) = \hat{\delta}_0, \quad t \geq 0, \tag{28}$$

$$\dot{\hat{x}}(t) = A_{\mathrm{r}}\hat{x}(t) + L\big(\tilde{x}(t) - \hat{x}(t) - \hat{\delta}(t)\big)$$

$$- \gamma\ \mathrm{Proj}\Big(\hat{\delta}(t),\ -A^{\mathrm{T}}\tilde{P}\big(\tilde{x}(t) - \hat{x}(t) - \hat{\delta}(t)\big)\Big), \quad \hat{x}(0) = \hat{x}_0, \quad t \geq 0, \tag{29}$$

with $\tilde{P}$ satisfying (14). For the statement of the next theorem, recall that $e(t) = \tilde{x}(t) - \hat{x}(t) - \hat{\delta}(t)$, $t \geq 0$, and $\tilde{\delta}(t) = \delta(t) - \hat{\delta}(t)$, $t \geq 0$, and note that

$$\dot{e}(t) = \big(A_{\mathrm{r}} - L\big)e(t) - A\tilde{\delta}(t) + \dot{\delta}(t), \quad e(0) = e_0, \quad t \geq 0, \tag{30}$$

$$\dot{\tilde{\delta}}(t) = \dot{\delta}(t) - \gamma\ \mathrm{Proj}\Big(\hat{\delta}(t),\ -A^{\mathrm{T}}\tilde{P}\big(\tilde{x}(t) - \hat{x}(t) - \hat{\delta}(t)\big)\Big), \quad \tilde{\delta}(0) = \tilde{\delta}_0, \quad t \geq 0. \tag{31}$$

Theorem 2: *Consider the linear dynamical system $\mathcal{G}$ given by (1) with state-independent sensor uncertainty given by (9), where $\|\delta(t)\|_2 \leq \overline{\delta}$, $t \geq 0$, and $\|\dot{\delta}(t)\|_2 \leq \overline{\dot{\delta}}$, and assume that $\det(A) \neq 0$. Then, with the controller $\mathcal{G}_{\mathrm{c}}$ given by (5) and the corrective signal $v(t)$, $t \geq 0$, given by (27), the closed-loop system given by (30) and (31) is uniformly bounded for all $\big(e_0, \tilde{\delta}_0\big) \in \mathbb{R}^n \times \mathbb{R}^n$ with the ultimate bounds*

$$\|e(t)\|_2 \leq \left[\frac{\lambda_{\max}(\tilde{P})}{\lambda_{\min}(\tilde{P})}\eta_1^2 + \frac{1}{\gamma\lambda_{\min}(\tilde{P})}\eta_2^2\right]^{\frac{1}{2}}, \quad t \geq T, \tag{32}$$

$$\|\tilde{\delta}(t)\|_2 \leq \left[\gamma\lambda_{\max}(\tilde{P})\eta_1^2 + \eta_2^2\right]^{\frac{1}{2}}, \quad t \geq T, \tag{33}$$

where $\eta_1 \triangleq \frac{1}{\sqrt{d_1}}\left[\frac{d_2}{2\sqrt{d_1}} + \left(\frac{d_2^2}{4d_1} + d_3\right)^{\frac{1}{2}}\right]$, $\eta_2 \triangleq \hat{\delta}_{\max} + \overline{\delta}$, $d_1 \triangleq \lambda_{\min}(\tilde{R})$, $d_2 \triangleq 2\lambda_{\max}(\tilde{P})\overline{\dot{\delta}}$, *and* $d_3 \triangleq 2\gamma^{-1}(\hat{\delta}_{\max} + \overline{\delta})\overline{\dot{\delta}}$.

Proof: To show uniform boundedness of the closed-loop system given by (30) and (31), consider the Lyapunov-like function given by (17) where $\tilde{P}$ satisfies (14). Note that $V(0,0) = 0$, $V\big(e, \tilde{\delta}\big) > 0$ for all $\big(e, \tilde{\delta}\big) \neq (0,0)$, and $V\big(e, \tilde{\delta}\big)$ is radially unbounded. The time derivative of (17) along the closed-loop system trajectories of (30) and (31) is given by

$$\begin{aligned}
\dot{V}\big(e(t), \tilde{\delta}(t)\big) &= -e^{\mathrm{T}}(t)\tilde{R}e(t) - 2e^{\mathrm{T}}(t)\tilde{P}A\tilde{\delta}(t) + 2e^{\mathrm{T}}(t)\tilde{P}\dot{\delta}(t) \\
&\quad -2\tilde{\delta}^{\mathrm{T}}(t)\mathrm{Proj}\big(\hat{\delta}(t),\ -A^{\mathrm{T}}\tilde{P}e(t)\big) + 2\gamma^{-1}\tilde{\delta}^{\mathrm{T}}(t)\dot{\delta}(t) \\
&= -e^{\mathrm{T}}(t)\tilde{R}e(t) + 2e^{\mathrm{T}}(t)\tilde{P}\dot{\delta}(t) + 2\gamma^{-1}\tilde{\delta}^{\mathrm{T}}(t)\dot{\delta}(t) \\
&\quad + 2\big(\hat{\delta}(t) - \delta(t)\big)^{\mathrm{T}}\Big(\mathrm{Proj}\big(\hat{\delta}(t),\ -A^{\mathrm{T}}\tilde{P}e(t)\big) - \big(-A^{\mathrm{T}}\tilde{P}e(t)\big)\Big) \\
&\leq -e^{\mathrm{T}}(t)\tilde{R}e(t) + 2e^{\mathrm{T}}(t)\tilde{P}\dot{\delta}(t) + 2\gamma^{-1}\tilde{\delta}^{\mathrm{T}}(t)\dot{\delta}(t) \\
&\leq -d_1\|e(t)\|_2^2 + d_2\|e(t)\|_2 + d_3 \\
&= -\left[\sqrt{d_1}\|e(t)\|_2 - \frac{d_2}{2\sqrt{d_1}}\right]^2 + \frac{d_2^2}{4d_1} + d_3, \quad t \geq 0,
\end{aligned} \tag{34}$$

and hence, $\dot{V}\big(e(t), \tilde{\delta}(t)\big) < 0$ outside of the compact set

$$\Omega \triangleq \Big\{\big(e, \tilde{\delta}\big) \in \mathbb{R}^n \times \mathbb{R}^n : \|e\|_2 \leq \eta_1 \text{ and } \|\tilde{\delta}\|_2 \leq \eta_2\Big\}. \tag{35}$$

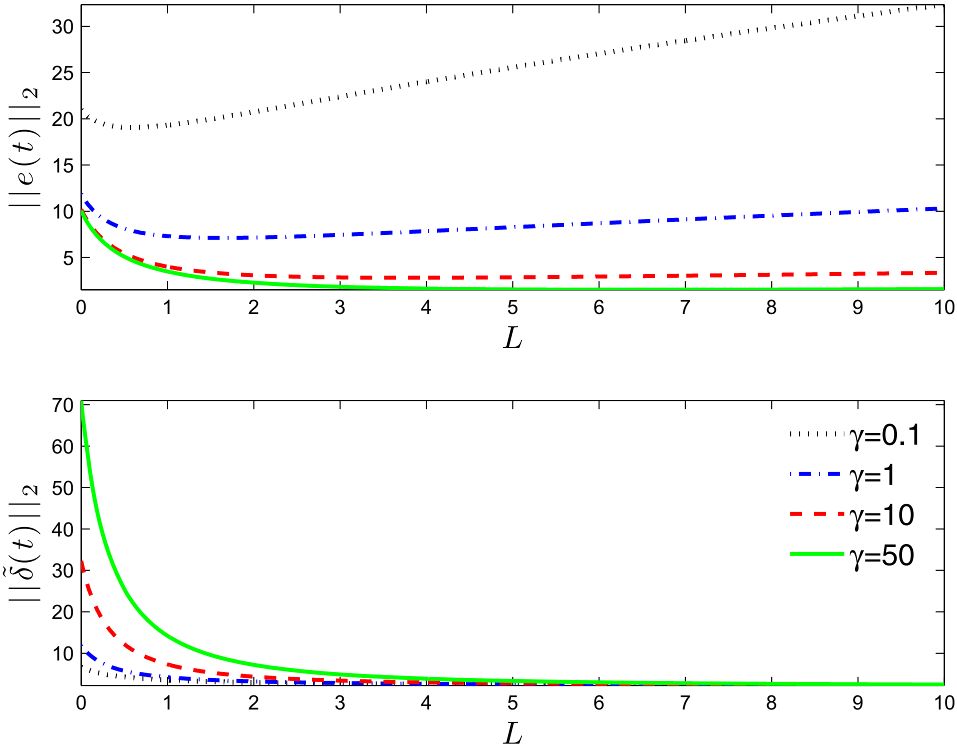

Figure 2. Effect of L and γ on the ultimate bounds given by (32) and (33).

This proves the uniform boundedness of the solution $\left(e(t), \tilde{\delta}(t)\right)$ of the closed-loop system given by (30) and (31) for all $\left(e_0, \tilde{\delta}_0\right) \in \mathbb{R}^n \times \mathbb{R}^n$.[25]

To show the ultimate bounds for $e(t)$, $t \geq T$ and $\tilde{\delta}(t)$, $t \geq T$, given by (32) and (33), respectively, note that $\lambda_{\min}(\tilde{P})\|e(t)\|_2^2 + \gamma^{-1}\|\tilde{\delta}(t)\|_2^2 \leq \lambda_{\max}(\tilde{P})\eta_1^2 + \gamma^{-1}\eta_2^2$, $t \geq T$, or, equivalently, $\lambda_{\min}(\tilde{P})\|e(t)\|_2^2 \leq \lambda_{\max}(\tilde{P})\eta_1^2 + \gamma^{-1}\eta_2^2$, $t \geq T$, and $\gamma^{-1}\|\tilde{\delta}(t)\|_2^2 \leq \lambda_{\max}(\tilde{P})\eta_1^2 + \gamma^{-1}\eta_2^2$, $t \geq T$, which proves (32) and (33).

Remark 5: A similar remark to Remark 2 holds for Theorem 2. Namely, all signals used to construct the controller $\mathcal{G}_c$ given by (5) with the corrective signal defined in (27)–(29) are bounded.

Remark 6: The ultimate bounds given by (32) and (33) characterise how the controller parameters need to be chosen in order to achieve small excursions of $\|e(t)\|_2$ and $\|\tilde{\delta}(t)\|_2$ for $t \geq T$. This is particularly important to obtain accurate estimates for $\hat{x}(t)$, $t \geq T$ and $\hat{\delta}(t)$, $t \geq T$, and also to suppress the effect of $\tilde{\delta}(t)$, $t \geq T$, in (20). To elucidate the effect of controller design parameters on (32) and (33), let $A = 1$ and $B = 1$ in (1), let $K = -1.5$ in (5), let $\bar{\delta} = 1$ and $\bar{\dot{\delta}} = 5$ in (9), let $\tilde{R} = 1$ in (14), and let $\hat{\delta}_{\max} = 1$ in (28). Figure 2 illustrates the effect of $L \in [0, 10]$ in (14) and $\gamma = \{0.1, 1, 10, 50\}$ in (28) on the ultimate bounds given by (32) and (33). Specifically, as expected, increasing both L and γ yields smaller ultimate bounds for $e(t)$, $t \geq T$ and $\tilde{\delta}(t)$, $t \geq T$.

4. Adaptive stabilisation for state-dependent sensor attacks

In this section, we design the corrective signal $v(t)$, $t \geq 0$, in (5) to achieve adaptive stabilisation in the presence of state-dependent sensor attacks. In particular, we first consider the case where the sensor uncertainty in (9) is time-invariant, that is, $\delta(t, x(t)) \equiv \delta(x(t))$, with $\delta(x(t)) = wx(t)$, $t \geq 0$, and then we generalise our results to the time-varying sensor uncertainty case.

4.1. Time-invariant, state-dependent sensor attacks

In this subsection, we assume that the sensor attack in (10) is time-invariant, that is, $\delta(t, x(t)) \equiv \delta(x(t))$, with $\delta(x(t)) = wx(t)$, $t \geq 0$, and consider the controller $\mathcal{G}_{\mathrm{c}}$ in (5) with the corrective signal given by

$$v(t) = -\hat{\mu}(t)K\tilde{x}(t), \quad t \geq 0, \tag{36}$$

where

$$\dot{\hat{\mu}}(t) = \gamma\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t), \quad \hat{\mu}(0) = \hat{\mu}_0, \quad t \geq 0, \tag{37}$$

$\hat{\mu}(t) \in \mathbb{R}$, $t \geq 0$, is the estimate of $\mu \triangleq w(1+w)^{-1} \in \mathbb{R}$ that depends on the sensor uncertainty w, and $\gamma \in \mathbb{R}$ is a positive design gain.

Next, define $\mu_\lambda(t) \triangleq \tilde{\mu}(t)\lambda^{\frac{1}{2}}$, $t \geq 0$, where $\tilde{\mu}(t) \triangleq \mu - \hat{\mu}(t)$, $t \geq 0$ and $\lambda \triangleq (1+w)^{-1} \in \mathbb{R}$. Since $w > -1$, note that μ and λ are well-defined and $\lambda > 0$. For the statement of the next theorem note that

$$\dot{x}(t) = A_{\mathrm{r}}x(t) + \mu_\lambda(t)\lambda^{-\frac{1}{2}}BK\tilde{x}(t), \quad x(0) = x_0, \quad t \geq 0, \tag{38}$$
$$\dot{\mu}_\lambda(t) = -\gamma\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\lambda^{\frac{1}{2}}, \quad \mu_\lambda(0) = \mu_{\lambda 0}, \quad t \geq 0. \tag{39}$$

Theorem 3: *Consider the linear dynamical system $\mathcal{G}$ given by (1) with state-dependent sensor uncertainty given by (10), where $\delta(t, x(t)) \equiv \delta(x(t))$ and $\delta(x(t)) = wx(t)$, $t \geq 0$. Then, with the controller $\mathcal{G}_{\mathrm{c}}$ given by (5) and the corrective signal $v(t)$, $t \geq 0$, given by (36), the zero solution $\big(x(t), \mu_\lambda(t)\big) = \big(0, 0\big)$ of the closed-loop system given by (38) and (39) is Lyapunov stable for all $\big(x_0, \mu_{\lambda 0}\big) \in \mathbb{R}^n \times \mathbb{R}$ and $\lim_{t\to\infty} x(t) = 0$.*

Proof: To show Lyapunov stability of the closed-loop system given by (38) and (39), consider the Lyapunov function candidate given by

$$V\big(x, \mu_\lambda\big) = x^{\mathrm{T}}Px + \gamma^{-1}\mu_\lambda^2, \tag{40}$$

where P satisfies (4). Note that $V(0,0) = 0$, $V\big(x, \mu_\lambda\big) > 0$ for all $\big(x, \mu_\lambda\big) \neq (0, 0)$, and $V\big(x, \mu_\lambda\big)$ is radially unbounded. The time derivative of (40) along the closed-loop system trajectories of (38) and (39) is given by

$$\begin{aligned}
\dot{V}\big(x(t), \mu_\lambda(t)\big) &= -x^{\mathrm{T}}(t)Rx(t) + 2\mu_\lambda(t)\lambda^{-\frac{1}{2}}x^{\mathrm{T}}(t)PBK\tilde{x}(t) \\
&\quad - 2\mu_\lambda(t)\lambda^{\frac{1}{2}}\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t) \\
&= -x^{\mathrm{T}}(t)Rx(t) + 2\mu_\lambda(t)\lambda^{\frac{1}{2}}\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t) \\
&\quad - 2\mu_\lambda(t)\lambda^{\frac{1}{2}}\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)
\end{aligned}$$

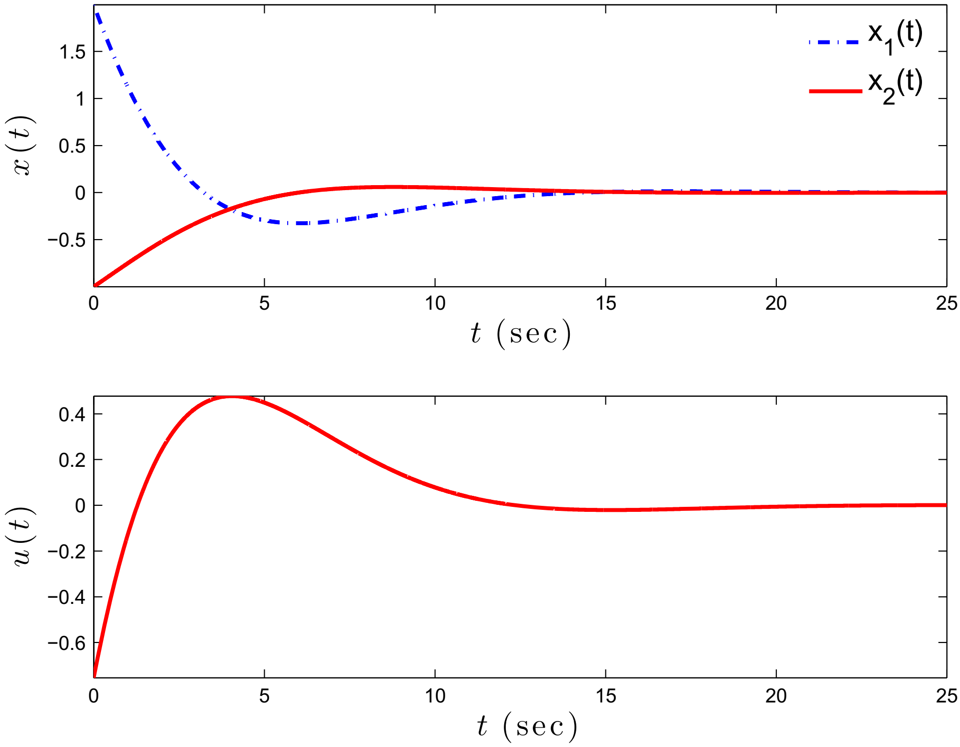

Figure 3. Nominal system performance of the linear dynamical system given by (55) when the state vector $x(t)$, $t \geq 0$, is available for feedback.

$$
\begin{aligned}
&= -x^{\mathrm{T}}(t)Rx(t) \\
&\leq 0, \quad t \geq 0,
\end{aligned} \tag{41}
$$

where we used the fact that $x(t) = \lambda\tilde{x}(t)$, $t \geq 0$, which follows from (10) with $\delta(x(t)) = wx(t)$, $t \geq 0$. Hence, the closed-loop system given by (38) and (39) is Lyapunov stable for all $\big(x_0, \mu_{\lambda 0}\big) \in \mathbb{R}^n \times \mathbb{R}$.

To show $\lim_{t\to\infty} x(t) = 0$, note that

$$\ddot{V}\big(x(t), \mu_\lambda(t)\big) = -2x^{\mathrm{T}}(t)R\Big(A_{\mathrm{r}}x(t) + \mu_\lambda(t)\lambda^{-\frac{1}{2}}BK\tilde{x}(t)\Big) \tag{42}$$

is bounded for all $t \geq 0$ since $\big(x(t), \mu_\lambda(t)\big)$ is bounded for all $t \geq 0$. Thus, $\dot{V}\big(x(t), \mu_\lambda(t)\big)$, $t \geq 0$, is uniformly continuous in t. Now, it follows from Barbalat's lemma [[20], p. 211] that $\lim_{t\to\infty} \dot{V}\big(x(t), \mu_\lambda(t)\big) = 0$, and hence, $\lim_{t\to\infty} x(t) = 0$. □

Remark 7: Since, by Theorem 3 and the fact that $\lambda > 0$, $\mu_\lambda(t)$, $t \geq 0$, is bounded, it follows from the definition of $\mu_\lambda(t)$ that $\tilde{\mu}(t)$ is bounded for all $t \geq 0$. Hence, the estimate $\hat{\mu}(t) \in \mathbb{R}$, $t \geq 0$, used in the corrective signal (36) is bounded.

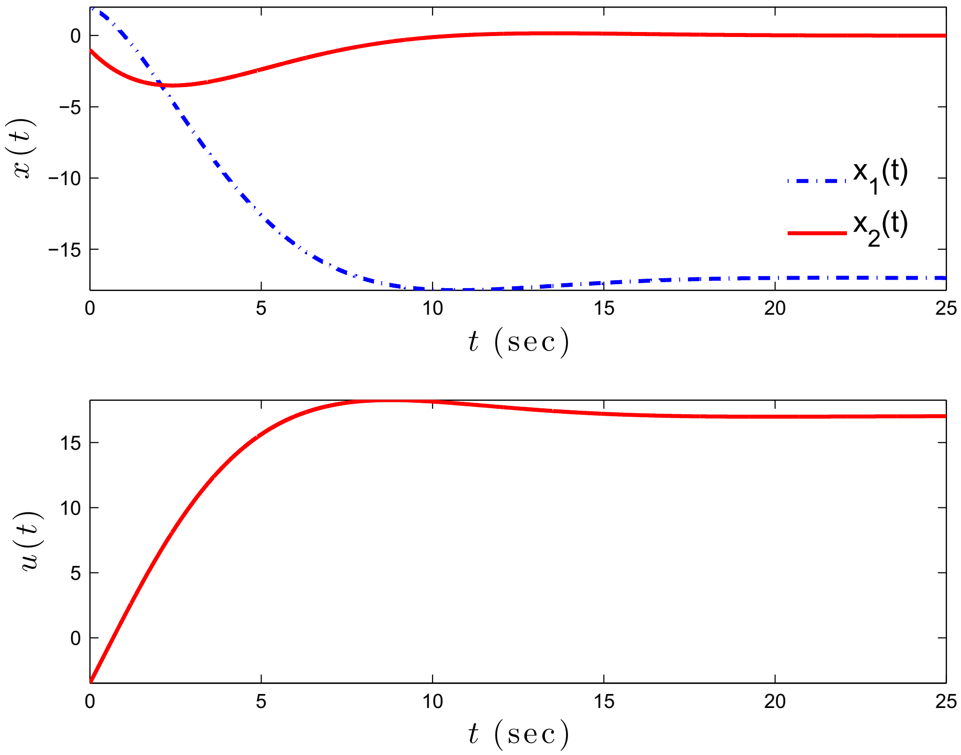

Figure 4. System performance of the linear dynamical system given by (55) in the presence of time-invariant and state-independent sensor attacks without any corrective signal (i.e. $v(t) \equiv 0$) in (5).

4.2. *Time-varying, state-dependent sensor attacks*

In this subsection, we generalise the results of the previous subsection to time-varying state-dependent sensor attacks in (10). To address this case, we use the corrective signal given by

$$v(t) = -\hat{\mu}(t)K\tilde{x}(t), \quad t \geq 0, \tag{43}$$

where

$$\dot{\hat{\mu}}(t) = \gamma \ \mathrm{Proj}\big(\hat{\mu}(t),\ \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big), \quad \hat{\mu}(0) = \hat{\mu}_0, \quad t \geq 0. \tag{44}$$

Next, recall that $\mu_\lambda(t) = \tilde{\mu}(t)\lambda^{\frac{1}{2}}(t)$, $t \geq 0$, with $\tilde{\mu}(t) = \mu(t) - \hat{\mu}(t)$, $t \geq 0$, $\mu(t) = w(t)\big(1 + w(t)\big)^{-1}$, $t \geq 0$, and $\lambda(t) = \big(1 + w(t)\big)^{-1}$, $t \geq 0$. 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

$$\dot{x}(t) = A_{\mathrm{r}}x(t) + \mu_\lambda(t)\lambda^{-\frac{1}{2}}(t)BK\tilde{x}(t), \quad x(0) = x_0, \quad t \geq 0, \tag{45}$$

$$\begin{aligned} \dot{\mu}_\lambda(t) = {} & \Big(\dot{\mu}(t) - \gamma \ \mathrm{Proj}\big(\hat{\mu}(t),\ \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big)\Big)\lambda^{\frac{1}{2}}(t) \\ & + \frac{1}{2}\mu_\lambda(t)\dot{\lambda}(t)\lambda^{-1}(t), \quad \mu_\lambda(0) = \mu_{\lambda 0}, \quad t \geq 0. \end{aligned} \tag{46}$$

Theorem 4: *Consider the linear dynamical system $\mathcal{G}$ given by* (1) *with state-dependent sensor uncertainty given by* (10), *where $\|w(t)\|_2 \leq \overline{w}$, $t \geq 0$, and $\|\dot{w}(t)\|_2 \leq \overline{\dot{w}}$, $t \geq 0$.*

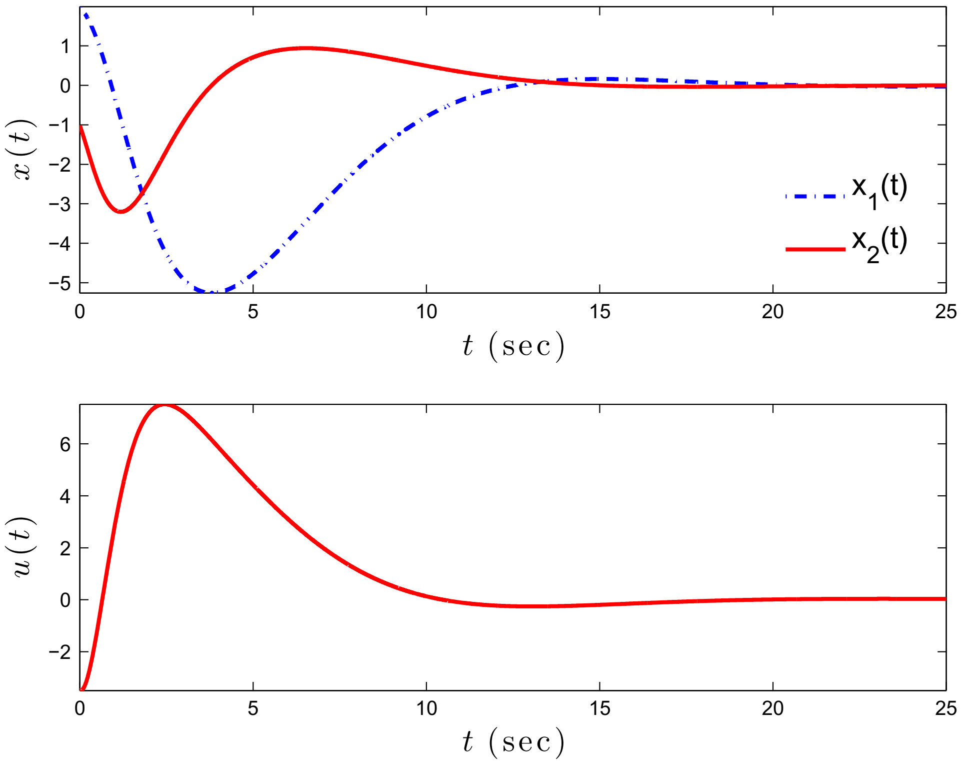

Figure 5. System performance of the linear dynamical system given by (55) in the presence of time-invariant and state-independent sensor attacks with the proposed corrective signal given by (11), (12) and (13) with $\gamma = 5$, $L = 2.5I_2$, and $R = I_2$.

Then, with the controller $\mathcal{G}_c$ *given by* (5) *and the corrective signal* $v(t)$, $t \ge 0$, *given by* (43), *the closed-loop system given by* (45) *and* (46) *is uniformly bounded for all* $\left(x_0, \mu_{\lambda 0}\right) \in \mathbb{R}^n \times \mathbb{R}$ *with the ultimate bounds*

$$\|x(t)\|_2 \le \left[\frac{1}{\lambda_{\min}(P)}\left(\lambda_{\max}(P)d_1^{-1}d_2 + \gamma^{-1}\overline{\lambda}\left(\overline{\mu} + \hat{\mu}_{\max}\right)^2\right)\right]^{\frac{1}{2}}, \quad t \ge T, \tag{47}$$

$$\|\mu_\lambda(t)\|_2 \le \left[\gamma\lambda_{\max}(P)d_1^{-1}d_2 + \overline{\lambda}\left(\overline{\mu} + \hat{\mu}_{\max}\right)^2\right]^{\frac{1}{2}}, \quad t \ge T, \tag{48}$$

where $d_1 \triangleq \lambda_{\min}(R)$ *and* $d_2 \triangleq \gamma^{-1}\left(2\left(\overline{\mu} + \hat{\mu}_{\max}\right)\overline{\dot{\mu}\lambda} + \left(\overline{\mu} + \hat{\mu}_{\max}\right)^2\overline{\dot{\lambda}}\right)$.

Proof: To show uniform boundedness of the closed-loop system given by (45) and (46), consider the Lyapunov-like function given by (40), where P satisfies (4). Note that $V(0,0) = 0$, $V\left(x, \mu_\lambda\right) > 0$ for all $\left(x, \mu_\lambda\right) \neq (0,0)$, and $V\left(x, \mu_\lambda\right)$ is radially unbounded. The time derivative of (40) along the closed-loop system trajectories of (45) and (46) is given by

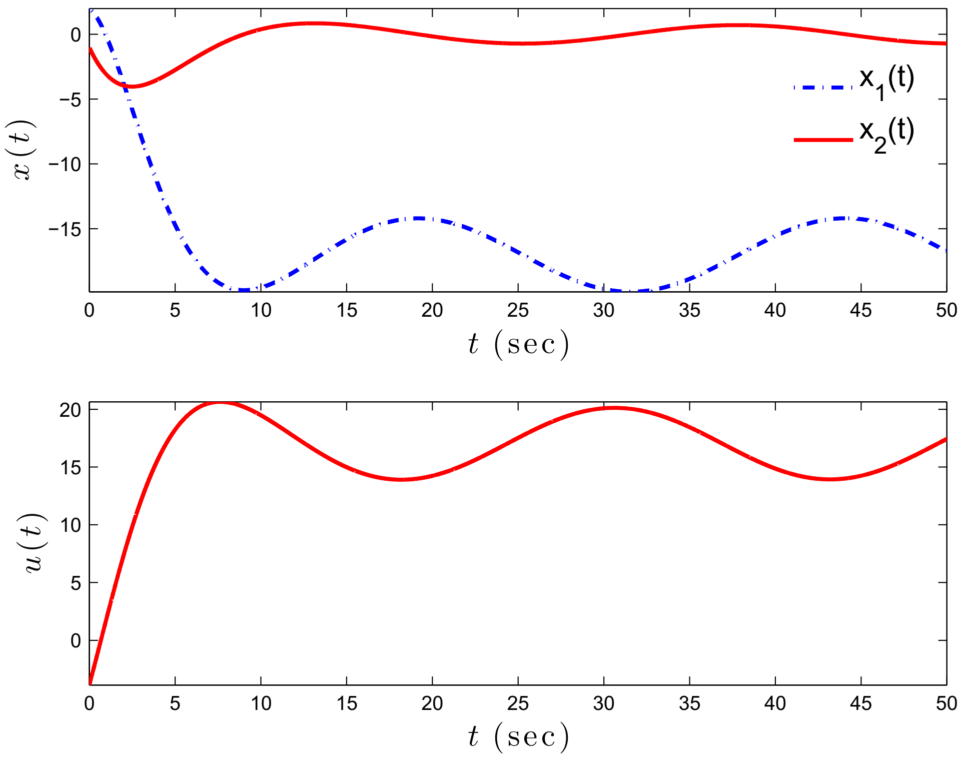

Figure 6. System performance of the linear dynamical system given by (55) in the presence of time-varying and state-independent sensor attacks without any corrective signal (i.e. $v(t) \equiv 0$) in (5).

$$
\begin{aligned}
\dot{V}\big(x(t), \mu_\lambda(t)\big) &= -x^{\mathrm{T}}(t)Rx(t) + 2\mu_\lambda(t)\lambda^{-\frac{1}{2}}(t)x^{\mathrm{T}}(t)PBK\tilde{x}(t) \\
&\quad + 2\gamma^{-1}\mu_\lambda(t)\Big(\dot{\mu}(t) - \gamma \ \mathrm{Proj}\big(\hat{\mu}(t),\ \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big)\Big)\lambda^{\frac{1}{2}}(t) \\
&\quad + \gamma^{-1}\mu_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t) \\
&= -x^{\mathrm{T}}(t)Rx(t) + 2\mu_\lambda(t)\lambda^{\frac{1}{2}}(t)\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t) \\
&\quad + 2\gamma^{-1}\mu_\lambda(t)\Big(\dot{\mu}(t) - \gamma \ \mathrm{Proj}\big(\hat{\mu}(t),\ \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big)\Big)\lambda^{\frac{1}{2}}(t) \\
&\quad + \gamma^{-1}\mu_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t),
\end{aligned}
\tag{49}
$$

where we used the fact that $x(t) = \lambda(t)\tilde{x}(t)$, $t \geq 0$, which follows from (10).

Next, using

$$
\begin{aligned}
&\mu_\lambda(t)\lambda^{\frac{1}{2}}(t)\tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t) - \mu_\lambda(t)\lambda^{\frac{1}{2}}(t)\ \mathrm{Proj}\big(\hat{\mu}(t),\ \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big) \\
&\quad = \lambda(t)\big(\hat{\mu}(t) - \mu(t)\big)\Big(\mathrm{Proj}\big(\hat{\mu}(t), \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\big) - \tilde{x}^{\mathrm{T}}(t)PBK\tilde{x}(t)\Big) \ \leq \ 0,
\end{aligned}
\tag{50}
$$

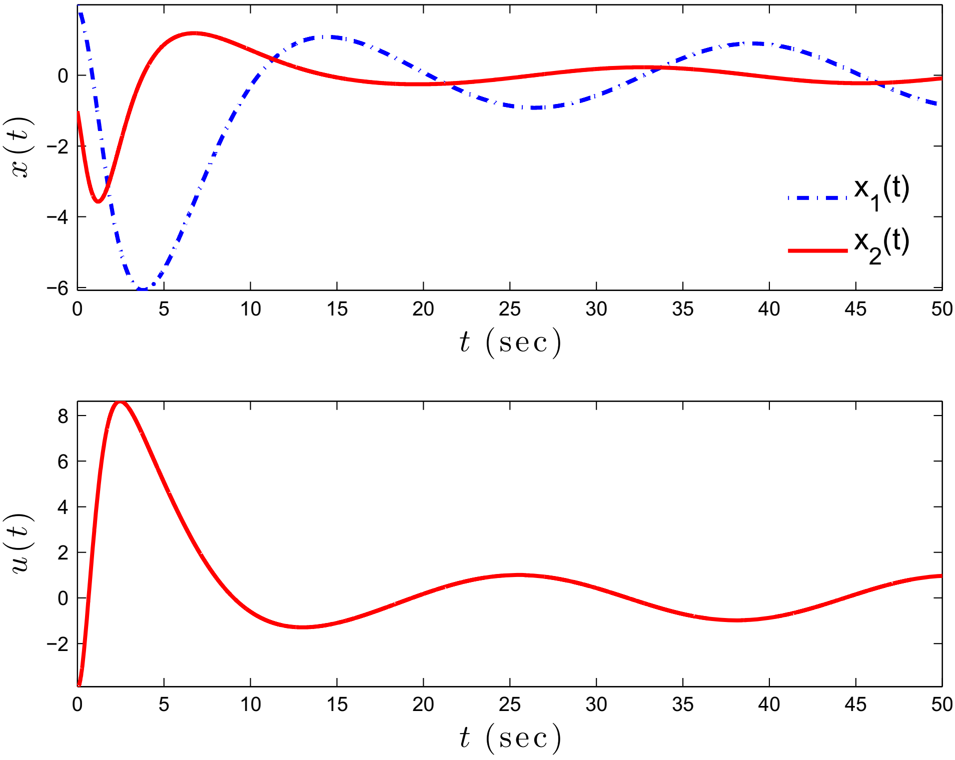

Figure 7. System performance of the linear dynamical system given by (55) in the presence of time-varying and state-independent sensor attacks with the proposed corrective signal given by (27), (28) and (29) with $\gamma = 5$, $L = 2.5I_2$, and $R = I_2$.

it follows from (49) that

$$\begin{aligned}\dot{V}\big(x(t),\mu_\lambda(t)\big) &\le -x^{\mathrm{T}}(t)Rx(t) + 2\gamma^{-1}\mu_\lambda(t)\dot{\mu}(t) + \gamma^{-1}\mu_\lambda^2(t)\dot{\lambda}(t)\lambda^{-1}(t)\\ &\le -d_1\|x(t)\|_2^2 + d_2, \quad t \ge 0,\end{aligned} \tag{51}$$

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

$$\Omega \triangleq \Big\{\big(x,\mu_\lambda\big) \in \mathbb{R}^n \times \mathbb{R}^n : \|x\|_2 \le \eta_1 \text{ and } \|\mu_\lambda\|_2 \le \eta_2\Big\}, \tag{52}$$

where $\eta_1 \triangleq \sqrt{d_2/d_1}$ and $\eta_2 \triangleq \overline{\lambda}^{\frac{1}{2}}\big(\overline{\mu} + \hat{\mu}_{\max}\big)$. This proves uniform boundedness of the solution $\big(x(t),\mu_\lambda(t)\big)$ of the closed-loop system given by (45) and (46) for all $\big(x_0,\mu_{\lambda 0}\big) \in \mathbb{R}^n \times \mathbb{R}$.[25] The remainder of the proof now follows as in the proof of Theorem 2. □

Remark 8: A similar remark to Remark 7 holds for Theorem 4. In particular, it can be shown that the estimate $\hat{\mu}(t) \in \mathbb{R}$, $t \ge 0$, used in the corrective signal given by (43) is bounded.

Remark 9: The ultimate bound given for $x(t)$, $t \ge T$, in (47) characterises the distance between the trajectories of the linear dynamical system $\mathcal{G}$ in (1) and the zero equilibrium point. To see the effect of the positive design gain γ in (44) on the ultimate bound of $x(t)$,

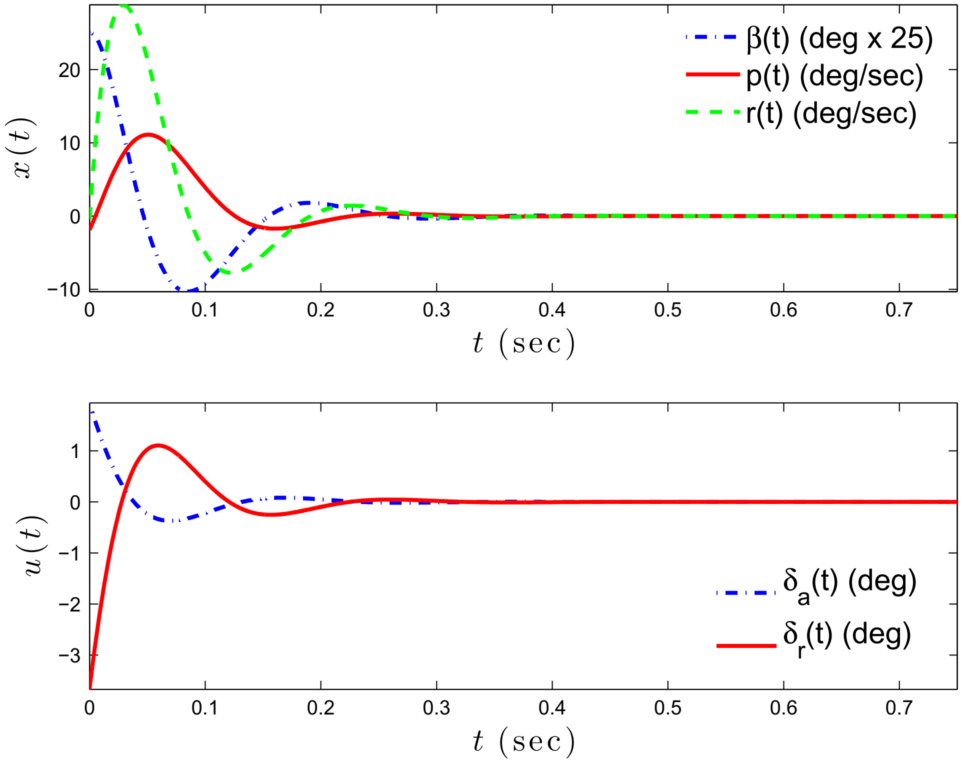

Figure 8. Nominal system performance of the lateral directional dynamics of the aircraft given by (57) when the state vector $x(t)$, $t \geq 0$, is available for feedback.

$t \geq T$, note that (47) can be equivalently written as

$$\|x(t)\|_2 \leq \gamma^{-\frac{1}{2}}\sqrt{d^*}, \quad t \geq T, \tag{53}$$

where

$$d^* \triangleq \frac{1}{\lambda_{\min}(P)}\left(\lambda_{\max}(P)d_1^{-1}\left(2(\overline{\mu}+\hat{\mu}_{\max})\overline{\dot{\mu}\lambda}+(\overline{\mu}+\hat{\mu}_{\max})^2\overline{\dot{\lambda}}\right)+\overline{\lambda}(\overline{\mu}+\hat{\mu}_{\max})^2\right), \tag{54}$$

and hence, increasing γ decreases the ultimate bound on $x(t)$, $t \geq T$. As compared with the results of Theorem 2 for the time-varying, state-independent sensor attack case, the adaptive control architecture in Theorem 4 for the time-varying, state-dependent sensor attack case has the capability to directly guarantee a smaller ultimate bound by increasing the design parameter γ unlike the controller of Theorem 2, where both γ and L need to be tuned simultaneously as discussed in Remark 6.

5. Illustrative numerical examples

In this section, we present two numerical examples to demonstrate the utility and efficacy of the proposed control architectures for stabilisation of linear dynamical systems in the presence of sensor attacks.

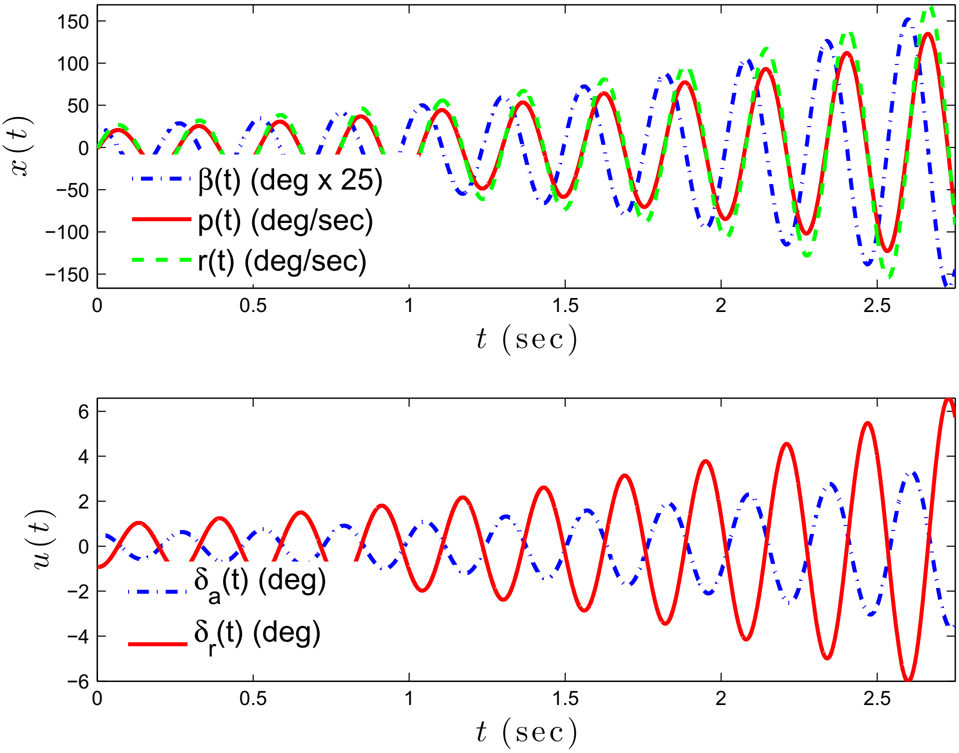

Figure 9. System performance of the lateral directional dynamics of the aircraft given by (57) in the presence of time-invariant and state-dependent sensor attacks without any corrective signal (i.e. $v(t) \equiv 0$) in (5).

5.1. State-independent sensor attacks

To illustrate the key ideas presented in Section 3, consider the unstable linear dynamical system given by

$$\begin{bmatrix}\dot{x}_1(t)\\ \dot{x}_2(t)\end{bmatrix} = \begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}x_1(t)\\ x_2(t)\end{bmatrix} + \begin{bmatrix}0\\ 1\end{bmatrix}u(t), \quad \begin{bmatrix}x_1(0)\\ x_2(0)\end{bmatrix} = \begin{bmatrix}2\\ -1\end{bmatrix}, \quad t \geq 0, \tag{55}$$

with the state feedback control gain

$$K = \left[-1.160, \ -1.565\right], \tag{56}$$

resulting in the nominal system performance (i.e. when the state vector $x(t) = \left[x_1(t), x_2(t)\right]^{\mathrm{T}}$, $t \geq 0$, is available for feedback) given in Figure 3. The closed-loop natural frequency is 0.4 rad/sec and damping ratio is 0.707. To illustrate the results of Theorem 1, consider a time-invariant and state-independent sensor attack given by (9) with $\delta = \left[1, \ 1\right]^{\mathrm{T}}$. The system performance of the controller $\mathcal{G}_{\mathrm{c}}$ given by (5) without any corrective signal (i.e. $v(t) \equiv 0$) is depicted in Figure 4, which clearly results in a nonacceptable system response.

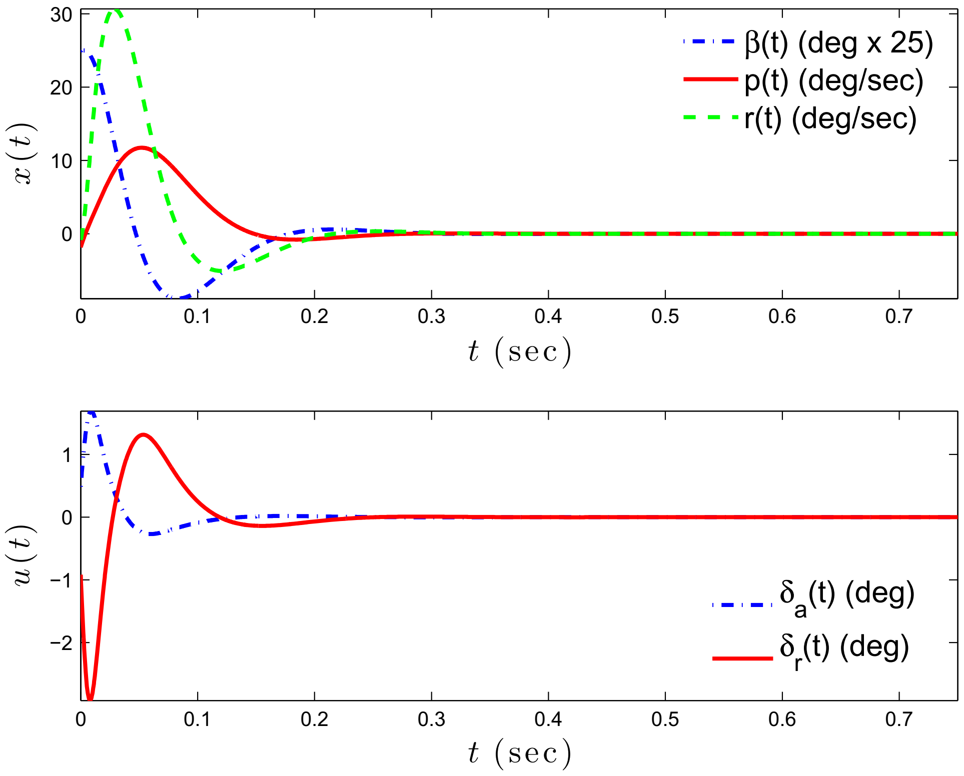

Figure 10. System performance of the lateral directional dynamics of the aircraft given by (57) in the presence of time-invariant and state-dependent sensor attacks with the proposed corrective signal given by (36) and (37) with $\gamma = 10$ and $R = I_3$.

To design the proposed corrective signal (11)–(13), we set $\gamma = 5$, $L = 2.5I_2$ and $R = I_2$. The system performance of the controller $\mathcal{G}_c$ given by (5) with the proposed corrective signal is depicted in Figure 5. As expected from Theorem 1, the proposed control architecture asymptotically stabilises the linear dynamical system given by (55) for this sensor attack.

Next, to illustrate the results of Theorem 2, consider a time-varying and state-independent sensor attack given by (9) with $\delta(t) = \left[1 + 0.25\sin(0.25t),\ 1 + 0.25\cos(0.25t)\right]^{\mathrm{T}}$, $t \geq 0$. For this case, the system performance of the controller $\mathcal{G}_c$ given by (5) without any corrective action is depicted in Figure 6. To design the proposed corrective signal given by (27)–(29), we set $\gamma = 5$, $L = 2.5I_2$ and $R = I_2$. The system performance of the controller $\mathcal{G}_c$ given by (5) with the proposed corrective signal is depicted in Figure 7. This shows the proposed adaptive control architecture recovers the nominal system performance in the face of sensor attacks.

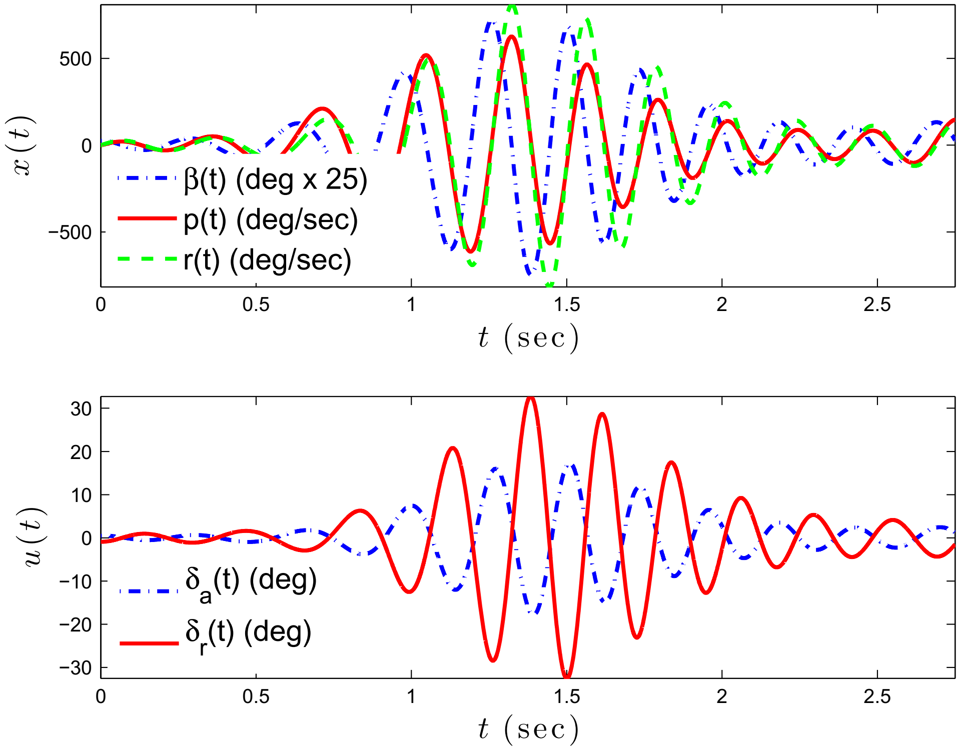

Figure 11. System performance of the lateral directional dynamics of the aircraft given by (57) in the presence of time-varying and state-dependent sensor attacks without any corrective signal (i.e. $v(t) \equiv 0$) in (5).

5.2. State-dependent sensor attacks

To illustrate the key ideas presented in Section 4, we consider a Lyapunov stable linear dynamical system representing the lateral directional dynamics of an aircraft [16] given by

$$\begin{bmatrix}\dot{\beta}(t)\\ \dot{p}(t)\\ \dot{r}(t)\end{bmatrix} = \begin{bmatrix}-0.025 & 0.104 & -0.994\\ 574.7 & 0 & 0\\ 16.20 & 0 & 0\end{bmatrix}\begin{bmatrix}\beta(t)\\ p(t)\\ r(t)\end{bmatrix} + \begin{bmatrix}0.122 & -0.276\\ -53.61 & 33.25\\ 195.5 & -529.4\end{bmatrix}u(t), \quad \begin{bmatrix}\beta(0)\\ p(0)\\ r(0)\end{bmatrix} = \begin{bmatrix}1\\ -2\\ -1\end{bmatrix}, \quad t \geq 0, \tag{57}$$

with state feedback control gain

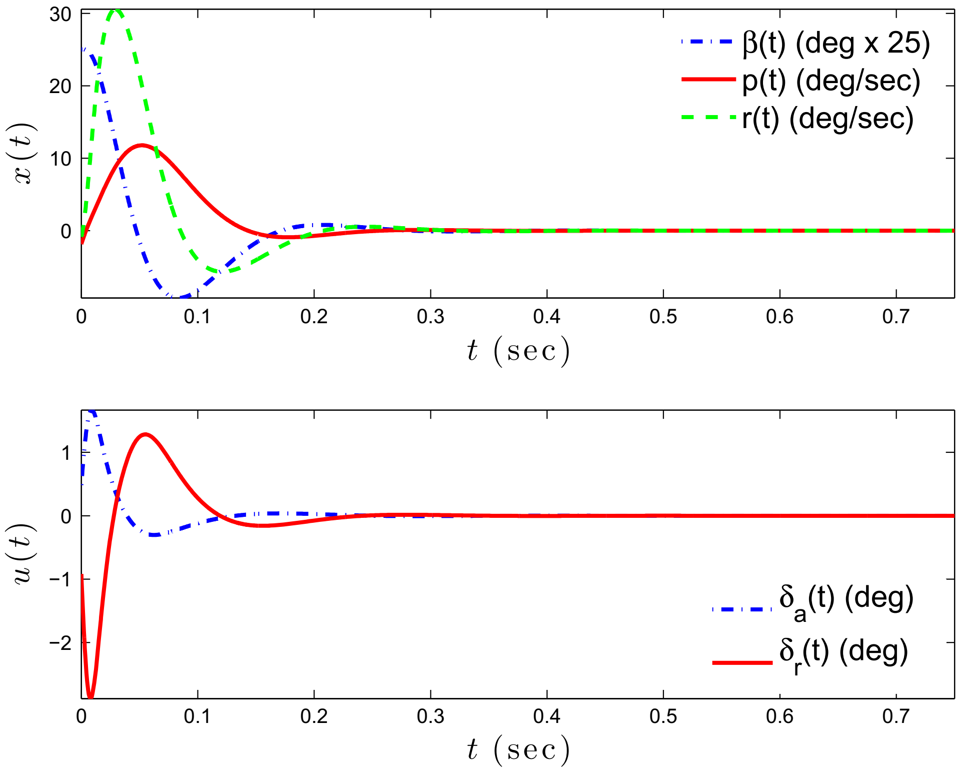

Figure 12. System performance of the lateral directional dynamics of the aircraft given by (57) in the presence of time-varying and state-dependent sensor attacks with the proposed corrective signal given by (43) and (44) with $\gamma = 10$ and $R = I_3$.

$$K = \begin{bmatrix} 2.053 & 0.079 & -0.045 \\ -3.823 & -0.128 & 0.102 \end{bmatrix}, \tag{58}$$

where the state vector $x(t) = \left[\beta(t),\ p(t),\ r(t)\right]^{\mathrm{T}}$, $t \geq 0$, contains the sideslip angle in deg, the roll rate in deg/sec, and the yaw rate in deg/sec, respectively, and the control input $u(t) = \left[\delta_{\mathrm{a}}(t),\ \delta_{\mathrm{r}}(t)\right]^{\mathrm{T}}$, $t \geq 0$, contains the aileron command in deg and the rudder command in deg, respectively. The nominal performance of this dynamical system is given in Figure 8.

To illustrate the results of Theorem 3 consider a time-invariant and state-dependent sensor attack given by (10) with $w = -0.75$. The system performance of the controller $\mathcal{G}_{\mathrm{c}}$ given by (5) without any corrective action (i.e. $v(t) \equiv 0$) results in an unstable closed-loop system and is shown in Figure 9. To design the proposed corrective signal given by (36) and (37), we set $\gamma = 10$ and $R = I_3$. The system performance of the controller $\mathcal{G}_{\mathrm{c}}$ given by (5) with the proposed corrective signal is depicted in Figure 10. As expected from Theorem 3, the proposed control architecture asymptotically stabilises the lateral directional dynamics of the aircraft given by (57) for this sensor attack.

Next, to illustrate the results of Theorem 4 consider a time-varying and state-dependent sensor attack given by (10) with $w(t) = -\big(0.75 + 0.15\sin(2.5t)\big)$, $t \geq 0$. For this case, the system performance of the controller $\mathcal{G}_c$ given by (5) without any corrective action is depicted in Figure 11. To design the proposed corrective signal given by (43) and (44), we set $\gamma = 10$ and $R = I_3$. The system performance of the controller $\mathcal{G}_c$ given by (5) with the proposed corrective signal is depicted in Figure 12. This shows that the proposed adaptive control architecture recovers the nominal system performance in the face of sensor attacks.

6. Conclusion

Sensor uncertainties can significantly deteriorate achievable closed-loop system performance, especially if such uncertainties are a result of an adversarial attack on measurement devices that actively engages to maximally degrade system information. In this paper, we presented several control architectures for system stabilisation in the presence of state-independent and state-dependent sensor attacks. Specifically, using realistic assumptions for the attack models we showed that the proposed adaptive controller architectures guarantee asymptotic stability of the closed-loop dynamical system in the face of time-invariant sensor uncertainties and uniform ultimate boundedness when the uncertainties are time-varying. Future extensions of this framework will focus on adaptive control strategies that can suppress the effect of sensor attacks in the presence of unknown system dynamics. Furthermore, generalisations to nonlinear dynamical systems with partial state measurements will also be developed, as well as extending the present framework to address simultaneous actuator and sensor attacks.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This research was supported in part by the University of Missouri Research Board and the Air Force Office of Scientific Research [grant number FA9550-12-1-0192].

References

[1] Antsaklis P. Goals and challenges in cyber-physical systems research. IEEE Trans Autom Control. 2014;59:3117–3119.

[2] Massoumnia M-A, Verghese GC, Willsky AS. Failure detection and identification. IEEE Trans Autom Control. 1989;34:316–321.

[3] Blanke M, Schröder J. Diagnosis and fault-tolerant control. Vol. 691. Berlin: Springer; 2006.

[4] Schenato L, Sinopoli B, Franceschetti M, et al. Foundations of control and estimation over lossy networks. Proc IEEE. 2007;95:163–187.

[5] Gupta A, Langbort C, Basar T. Optimal control in the presence of an intelligent jammer with limited actions. In: IEEE Conference on Decision and Control. Atlanta, GA. 2010; p. 1096–1101.

[6] Pasqualetti F, Dörfler F, Bullo F. Attack detection and identification in cyber-physical systems – part I: models and fundamental limitations. 2012. arXiv:1202.6144.

[7] Pasqualetti F, Dörfler F, Bullo F. Attack detection and identification in cyber-physical systems – part II: centralized and distributed monitor design. 2012. arXiv:1202.6049.

[8] Pasqualetti F, Dorfler F, Bullo F. Attack detection and identification in cyber-physical systems. IEEE Trans Autom Control. 2013;58:2715–2729.

[9] Fawzi H, Tabuada P, Diggavi S. Secure estimation and control for cyber-physical systems under adversarial attacks. IEEE Trans Autom Control. 2012;59:1454–1467.

[10] Weimer J, Bezzo N, Pajic M, Pappas GJ, Sokolsky O, Lee I. Resilient parameter-invariant control with application to vehicle cruise control. In: Control of cyber-physical systems. New York (NY): Springer; 2013. p. 197–216.

[11] Sou KC, Sandberg H, Johansson KH. On the exact solution to a smart grid cyber-security analysis problem. IEEE Trans Smart Grid. 2013;4:856–865.

[12] Kosut O, Jia L, Thomas RJ, et al. Malicious data attacks on the smart grid. IEEE Trans Smart Grid. 2011;2:645–658.

[13] Kim TT, Poor HV. Strategic protection against data injection attacks on power grids. IEEE Trans Smart Grid. 2011;2:326–333.

[14] Narendra KS, Annaswamy AM. Stable adaptive systems. New York (NY): Courier Dover Publications; 2012.

[15] Ioannou PA, Sun J. Robust adaptive control. New York (NY): Courier Dover Publications; 2012.

[16] Lavretsky E, Wise K. Robust and adaptive control with aerospace applications. London: Springer; 2012.

[17] Yucelen T, Haddad WM, Calise AJ. Output feedback adaptive command following and disturbance rejection for nonminimum phase uncertain dynamical systems. Int J Adapt Control Signal Process. 2011;25:352–373.

[18] Yucelen T, Haddad WM. A robust adaptive control architecture for disturbance rejection and uncertainty suppression with $\mathcal{L}_\infty$ transient and steady-state performance guarantees. Int J Adapt Control Signal Process. 2012;26:1024–1055.

[19] Yucelen T, Haddad WM. Low-frequency learning and fast adaptation in model reference adaptive control. IEEE Trans Autom Control. 2013;58:1080–1085.

[20] Haddad WM, Chellaboina V. Nonlinear dynamical systems and control: a lyapunov-based approach. Princeton (NJ): Princeton University Press; 2008.

[21] Lewis FL, Yesildirek A, Liu K. Multilayer neural-net robot controller with guaranteed tracking performance. IEEE Trans Neural Netw. 1996;7:388–399.

[22] Rohrs CE, Schultz D, Melsa J. Linear control systems. New York (NY): McGraw-Hill Higher Education; 1992.

[23] Aström KJ, Murray RM. Feedback systems: an introduction for scientists and engineers. Princeton (NJ): Princeton University Press; 2010.

[24] Pomet J-B, Praly L. Adaptive nonlinear regulation: estimation from the Lyapunov equation. IEEE Trans Autom Control. 1992;37:729–740.

[25] Khalil HK. Nonlinear systems. Upper Saddle River (NJ): Prentice Hall; 2002.