International Journal of Automation and Computing

15(3), June 2018, 345-354
DOI: 10.1007/s11633-017-1059-x

Resilient Control for Networked Control Systems Subject to Cyber/Physical Attacks

Taouba Rhouma Karim Chabir Mohamed Naceur Abdelkrim

Modeling, Analysis and Control of Systems (MACS) Laboratory, National Engineering School of Gabes (ENIG), University of Gabes, Gabes, Tunisia

Abstract: In this paper, we investigate a resilient control strategy for networked control systems (NCSs) subject to zero dynamic attacks which are stealthy false-data injection attacks that are designed so that they cannot be detected based on control input and measurement data. Cyber resilience represents the ability of systems or network architectures to continue providing their intended behavior during attack and recovery. When a cyber attack on the control signal of a networked control system is computed to remain undetectable from passive model-based fault detection and isolation schemes, we show that the consequence of a zero dynamic attack on the state variable of the plant is undetectable during attack but it becomes apparent after the end of the attack. A resilient linear quadratic Gaussian controller, having the ability to quickly recover the nominal behavior of the closed-loop system after the attack end, is designed by updating online the Kalman filter from information given by an active version of the generalized likelihood ratio detector.

Keywords: Networked control systems (NCSs), cyber physical attacks, Kalman filtering, resilient control, anomaly detector.

1 Introduction

With the rapid advancements of technology and novel control strategies, networked control systems (NCSs) have been at the core of infrastructure systems and industrial plants[1]. NCSs are spatially distributed systems consisting of actuators, sensors, and controllers, the operations of which are coordinated by the exchange of information passed over a communication network as illustrated in Fig. 1.

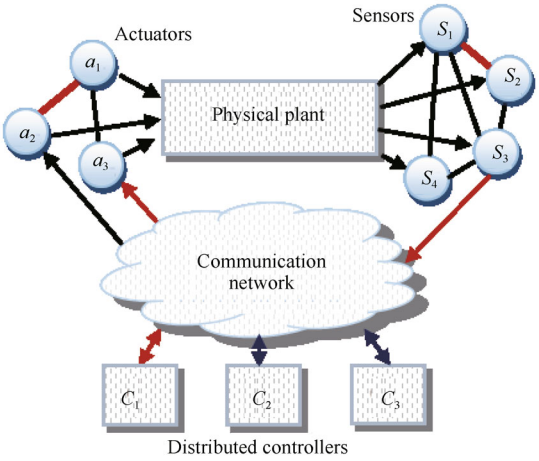

Fig. 1 Block diagram of cyber-physical systems

Research Article
Manuscript received February 24, 2016; accepted July 8, 2016; published online May 4, 2017
This work was supported by the Ministry of the Higher Education and Scientific Research in Tunisia.
Recommended by Associate Editor Shuang-Hua Yang

Several results on estimation, analysis and controller synthesis for NCSs have been discussed in [2]. Transport systems, electrical power systems, chemical processes, water and gas distribution networks, manufacturing and transportation networks can be considered as examples of application areas of cyber-physical systems (CPSs). CPS is an integration of communication capabilities, computational resources and physical processes. Such systems are often considered as large scale distributed physical processes but not necessarily always large and can be monitored and controlled by using a supervisory control and data acquisition (SCADA) software which can be critical to system operation[3] in various infrastructures.

The design of control systems taking into account the effects of packet losses and packet delays for NCS have been presented in [4]. Besides several network-induced effects such as time-delays and packet losses, NCSs become vulnerable to cyber physical attacks incorporating cyber and physical activities into a malicious attack. Recently, a sharp rise in the number of cyber attacks has been reported. Consequently, many researchers have shown a great concern for the analysis of vulnerabilities of NCS integrating physical processes, computational resources, and communication capabilities to external attacks[5, 6]. For instance, in [7] denial of service (DoS) attacks against a networked control system are defined when the adversary prevents the controller from receiving sensor measurement or the plant from receiving control law. In [8–10], deception attacks (also called false data injection attacks) are introduced when the adversary sends false information on sensors or actuators. Replay attacks are discussed in [11]

when the adversary generates artificial measurement delays. The effects of covert attacks against control systems are investigated in [12] when the adversary takes the control of the plant. Direct physical attacks on the plant (including sensors and actuators) close to traditional faults are taken into account by fault detection and isolation (FDI) techniques.

After having represented, a NCS under attack as a linear time-invariant system subject to target and nuisance faults[13, 14], the detection problem of coordinated attacks in CPS seems to be closely related to the detection problem of multiple component, sensor or actuators faults from traditional model-based FDI schemes[15−18], but there exists a significant difference: multiple faults are considered as a phenomenon which occurs randomly on actuators, sensors or communication channels while a coordinated attack is an intentional action designed by adversaries to remain undetectable. In this new context, it is necessary to design an active FDI scheme as explained in [19] having the ability to detect the presence of coordinated attacks. This paper considers a special covert attack called zero dynamic attack[20] designed by using the output-nulling controlled invariant subspace in geometric control theory. In other words, zero dynamic attacks are stealthy false-data injection attacks that are constructed so that they cannot be detected based on control input and measurement data. Keller et al.[21, 22] presented a detection scheme to destroy the stealthy attack strategy of the adversary by modifying the system′s structure or by triggering data losses on the control signals due to unreliable communication networks. When the attacker and the defender both consider the same model of the plant, the only chance to detect the attack is to assume the existence of defensive actions forcing the adversary to perform the malicious activity in a limited period of time[23]. After having represented a cyber-physical system under zero dynamic attack of finite duration as a linear time-invariant system subject to two sequential pulses, this paper shows that the attack end cannot remain stealthy and proposes to detect this event from an active version of the generalized likelihood ratio (GLR) test developed in [24].

Conventional active fault-tolerant control systems (FTCS) have the ability to accommodate component failures automatically from a controller reconfiguration mechanism driven by the FDI results, see [25] and references therein. Consequences of undetected coordinated attacks on active FTCS are potentially catastrophic in safety-critical systems. Nuclear power plants and chemical plants can be considered as examples of these safety-critical systems. Consequently, it is also necessary to design active FTCS capable of tolerating potential coordinated attacks to enforce the overall system stability and survivability at the occurrence of such attacks. A zero dynamic attack is designed to be stealthy to any anomaly detectors with respect to any observer-based controllers. This paper presents an active FTCS having the ability to quickly recover the behavior of the nominal linear quadratic gaussian (LQG) controller after the end of the attack. The obtained controller, including the nominal LQG controller, the active GLR test and the Kalman filter working in closed-loop with the FDI results will be called resilient LQG controller in reference with various definitions of resilience used in different areas of the science. Resilience in computing science represents the ability of a system or network architecture to recover normal operation after a brutal crash. Recently, the concept of resilient control of NCS against denial-of-service attacks has been proposed in [26–28], but only few work has tackled cyber resilience for NCSs under zero dynamic attacks.

The paper is organized as follows: Section 2 presents a stealthy attack scheme close to covert attack that a malicious agent can use to successfully realize the attack without being detected. Section 3 investigates a resilient defense strategy that a defender can use to quickly recover the nominal behavior of the NCS. Obtained results are proved through an illustrative example presented in Section 4. Conclusion follows in Section 5.

2 Problem statement

In this Section, we formulate the cyber/physical attack detection problem in networked control systems described by a physical plant and communication network, an LQG controller and an anomaly detector as illustrated in Fig. 2.

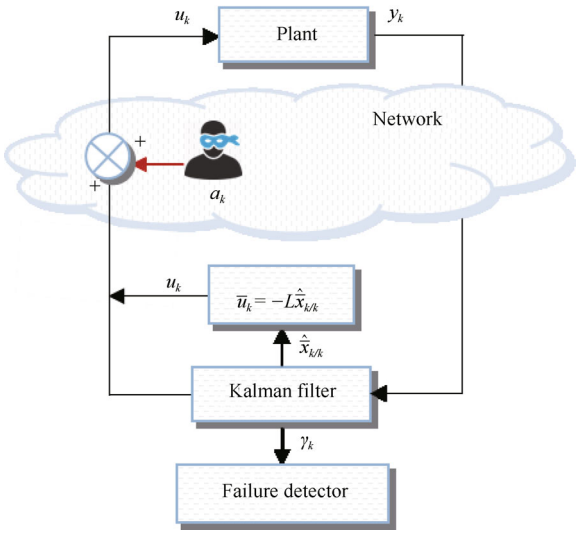

Fig. 2 NCS under attack with LQG controller

The plant is represented by the following linear discrete-time stochastic system

$$x_{k+1} = Ax_k + Bu_k + w_k \tag{1a}$$

$$y_k = Cx_k + \varepsilon_k \tag{1b}$$

where $x_k \in \mathbf{R}^n$, $u_k \in \mathbf{R}^q$ and $y_k \in \mathbf{R}^m$ are the state, input and measurement vectors, $w_k \in \mathbf{R}^n$ and $\varepsilon_k \in \mathbf{R}^m$ are zero mean uncorrelated Gaussian random sequences with

$$\mathrm{E}\left\{\begin{bmatrix} w_k \\ \varepsilon_k \end{bmatrix}\begin{bmatrix} w_j \\ \varepsilon_j \end{bmatrix}^{\mathrm{T}}\right\} = \begin{bmatrix} W & 0 \\ 0 & V \end{bmatrix}\delta_{k,j}$$
$$W \succeq 0, \quad V > 0. \tag{2}$$

The initial state x_0, assumed to be uncorrelated with w_k and ε_k, is a Gaussian random variable with $\mathrm{E}\{x_0\} = \bar{x}_0$ and $P_0 = \mathrm{E}\left\{(x_0 - \bar{x}_0)(x_0 - \bar{x}_0)^{\mathrm{T}}\right\} \succeq 0$. The pair (A, C) is detectable, (A, B) is stabilizable and $\mathrm{rank}(\begin{bmatrix} Iz - A & -B \\ C & 0 \end{bmatrix}) = n + q$ for almost all z.

Under no attack ($u_k = \bar{u}_k$), the model of the plant viewed by the controller is described by

$$\bar{x}_{k+1} = A\bar{x}_k + B\bar{u}_k + w_k \tag{3a}$$
$$y_k = C\bar{x}_k + \varepsilon_k \tag{3b}$$

and the nominal control law of the infinite horizon LQG controller solution to

$$J = \min \lim_{T\to\infty} \mathrm{E}\left\{\frac{1}{T}\left[\sum_{k=0}^{T-1} \bar{x}_k^{\mathrm{T}} Q \bar{x}_{k_k} + \bar{u}_k^{\mathrm{T}} R \bar{u}_k\right]\right\} \tag{4a}$$

where the controller design parameters $Q \succeq 0$ and $R > 0$, is given by

$$\bar{u}_k = -L\widehat{\bar{x}}_{k/k} \tag{4b}$$

with

$$L = (B^{\mathrm{T}}SB + R)^{-1}B^{\mathrm{T}}SA \tag{4c}$$
$$S = A^{\mathrm{T}}SA + Q - A^{\mathrm{T}}SB(B^{\mathrm{T}}SB + R)^{-1}B^{\mathrm{T}}SA \tag{4d}$$

where $\widehat{\bar{x}}_{k/k}$ is the minimum variance unbiased state estimate of the plant under no attack generated by the Kalman filter

$$\widehat{\bar{x}}_{k/k} = \widehat{\bar{x}}_{k/k-1} + K_k(y_k - C\widehat{\bar{x}}_{k/k-1}) \tag{5a}$$
$$\bar{P}_{k/k} = (I - K_kC)\bar{P}_{k/k-1}(I - K_kC)^{\mathrm{T}} + K_kVK_k^{\mathrm{T}} \tag{5b}$$
$$K_k = \bar{P}_{k/k-1}C^{\mathrm{T}}(C\bar{P}_{k/k-1}C^{\mathrm{T}} + V)^{-1} \tag{5c}$$
$$\widehat{\bar{x}}_{k+1/k} = A\widehat{\bar{x}}_{k/k} + B\overline{u}_k \tag{5d}$$
$$\bar{P}_{k+1/k} = A\bar{P}_{k/k}A^{\mathrm{T}} + W \tag{5e}$$

with $\widehat{\bar{x}}_{0/-1} = \bar{x}_0$ and $\bar{P}_{0/-1} = P_0$.

Assume for simplicity that the plant has one real unstable invariant zero λ so that

$$\mathrm{rank}\left(\begin{bmatrix} I\lambda - A & -B \\ C & 0 \end{bmatrix}\right) = n + q - 1 \ \text{ with } \ |\lambda| > 1 \tag{6}$$

and $\lambda \notin sp(A)$ where $sp(A)$ represents the eigenvalues of A. The false data injection a_k can cause catastrophic damage the plant while remaining undetectable from standard FDI scheme applied on the Kalman filter′s innovation sequence $\gamma_k = y_k - C\hat{\bar{x}}_{k/k-1}$.

The attacker may prefer to perform the malicious activities within a short period of time due to the resource limit. Assume that the attack window of the adversary can be limited to a false data injection during τ periods of time. Let us assume that the adversary launches the attack during the period $\tau = [k_0, k_f]$, where k_0 is the attack begin instant and k_f is the attack end instant. By representing the begin and the end of a stealthy zero dynamic attack as two sequential pulses acting on the attack-free system (3), we show that the begin of the attack is undetectable but its end can be detected. To quickly recover the nominal behavior of the LQG controller after the end time of the attack, Section 3.2 proposes an autonomous resilient LQG control strategy obtained by updating online the Kalman filter (5) from information given by a GLR detector designed on the Kalman filter′s innovation sequence.

2.1 Modeling zero dynamic attacks

Let us assume that the malicious agent can realise a particular deception attack a_k, called zero dynamic attack[20] on the control signals, at the intrusion time k_0. We suppose that to compute the appropriate attack policy, the attacker has access to the detailed model of the system.

Definition 1. In deception attacks, the adversary attempts to prevent the actuator or the sensor from receiving a data integrity. The goal is to modify the control signals or the sensor measurements from their real values by sending false information from controllers or sensors. The false information can be a wrong sender identity, an incorrect sensor measurement, a false control input or an untrue time when a measurement is observed.

When the false data sequences $a_k \neq 0$, $\forall k \succeq k_0$, are added by the attacker on the control signal transmitted by the controller to the plant, the control signal received by the plant is $u_k = \bar{u}_k + a_k$, and the model of the plant viewed by the controller becomes

$$x_{k+1} = Ax_k + B\bar{u}_k + Ba_k + w_k \tag{7a}$$
$$y_k = Cx_k + \varepsilon_k. \tag{7b}$$

The model of the plant under no attack is expressed as $x_k = \bar{x}_k + \Delta x_k^a$ and $y_k = C\bar{x}_k + \Delta y_k^a$, where the additive consequence of the attack Δx_k^a and Δy_k^a, $\forall k \succeq k_0$, are described by

$$\Delta x_{k+1}^a = A\Delta x_k^a + Ba_k \tag{8a}$$
$$\Delta y_k^a = C\Delta x_k^a \tag{8b}$$

with $\Delta x_{k_0}^a = 0$.

When the adversary knows the state model of the plant, a particular deception attack $a_k = -\Sigma\Delta\tilde{x}_k^a$, called zero dynamic attack, can be designed from the following autonomous system:

$$\Delta\tilde{x}_{k+1}^a = (A - B\Sigma)\Delta\tilde{x}_k^a \tag{9a}$$
$$\Delta\tilde{y}_k^a = C\Delta\tilde{x}_k^a \tag{9b}$$

initialised with $\Delta\tilde{x}_{k_0}^a$ close to $\Delta x_{k_0}^a$. Otherwise, if it is equal to zero than $a_k = 0$, $\forall k \succeq k_0$.

The stealthy strategy of the adversary consists of determining Σ so that

$$\Delta\tilde{y}_k^a = 0, \quad \forall k \succeq k_0 \tag{10a}$$

$$\lim_{k\to\infty} |\Delta\tilde{x}_k^a| \to \infty \tag{10b}$$

with $\Delta\tilde{x}_{k_0}^a$ close to zero.

Under (6), there exist ξ and g solution to

$$\begin{bmatrix} I\lambda - A & -B \\ C & 0 \end{bmatrix} \begin{bmatrix} \xi \\ g \end{bmatrix} = 0 \tag{11a}$$

$$\text{or equivalently} \begin{bmatrix} I\lambda - (A - B\Sigma) & -B \\ C & 0 \end{bmatrix} \begin{bmatrix} \xi \\ g - \Sigma\xi \end{bmatrix} = 0. \tag{11b}$$

Under $g = \Sigma\xi$, (11b) gives $(A - B\Sigma)\xi = \lambda\xi$ and $C\xi = 0$ showing that the invariant zero λ becomes an unobservable mode of the pair $(A - B\Sigma, C)$. With $\Sigma = h(\xi)^+$, $\Delta\tilde{x}_{k_0}^a = d\xi$ and d close to zero, the solution $\Delta\tilde{x}_k^a = d\xi\lambda^{k-k_0}$ to (9a) shows that the zero dynamic attack reaches the destabilizing and stealthy goals with $a_k = dg\lambda^{k-k_0}$, $\forall k \succeq k_0$, the goal (10) of the adversary is then reached. An illustrative example will be given in Section 4 to show the appearance effects of the proposed stealthy attack strategy on the nominal control signals, the outputs and the system states.

2.2 Modeling passive attack detection scheme

We propose to design a passive attack detection scheme that the defender can be useed by using anomaly detectors designed on the innovation sequence of the Kalman filter. By defining $d\delta_{k,k_0-1}$ as a pulse of size d triggered at time $k_0 - 1$ with $\delta_{k,k_0-1} = 0$, $\forall k \neq k_0 - 1$ and $\delta_{k,k_0-1} = 1$, when $k = k_0 - 1$, the attack model of (9) can be rewritten as

$$\Delta\tilde{x}_{k+1}^a = (A - B\Sigma)\Delta\tilde{x}_k^a + \xi d\delta_{k,k_0-1} \tag{12a}$$

$$\Delta\tilde{y}_k^a = C\Delta\tilde{x}_k^a \tag{12b}$$

with $\Delta\tilde{x}_{k_0-1}^a = 0$. The augmented state model of the plant under attack, given from (12) and $a_k = -\Sigma\Delta\tilde{x}_k^a$ in (7), can be described as

$$\begin{bmatrix} x_{k+1} \\ \Delta\tilde{x}_{k+1}^a \end{bmatrix} = \begin{bmatrix} A & -B\Sigma \\ 0 & A - B\Sigma \end{bmatrix} \begin{bmatrix} x_k \\ \Delta\tilde{x}_k^a \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} \bar{u}_k + \begin{bmatrix} 0 \\ \xi \end{bmatrix} d\delta_{k,k_0-1} + \begin{bmatrix} I \\ 0 \end{bmatrix} w_k \tag{13a}$$

$$y_k = \begin{bmatrix} C & 0 \end{bmatrix} \begin{bmatrix} x_k \\ \Delta\tilde{x}_k^a \end{bmatrix} + \varepsilon_k. \tag{13b}$$

By letting $\begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}_k^a \end{bmatrix} = T \begin{bmatrix} x_k \\ \Delta\tilde{x}_k^a \end{bmatrix}$ with $T = \begin{bmatrix} I & -I \\ 0 & I \end{bmatrix}$, (13) can be equivalently rewritten as

$$\begin{bmatrix} \tilde{x}_{k+1} \\ \Delta\tilde{x}_{k+1}^a \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & A - B\Sigma \end{bmatrix} \begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}_k^a \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} \bar{u}_k + \begin{bmatrix} -\xi \\ \xi \end{bmatrix} d\delta_{k,k_0-1} + \begin{bmatrix} I \\ 0 \end{bmatrix} w_k \tag{14a}$$

$$y_k = \begin{bmatrix} C & C \end{bmatrix} \begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}_k^a \end{bmatrix} + \varepsilon_k. \tag{14b}$$

From $C\Delta\tilde{x}_k^a = 0$ with $\forall k \succeq k_0$, $\Delta\tilde{x}_k^a = d\xi\lambda^{k-k_0}$ and $C\xi = 0$, the augmented state model (14) shows that $\Delta\tilde{x}_k^a$ is unobservable and that $\tilde{x}_k$ evolves in accordance to

$$\tilde{x}_{k+1} = A\tilde{x}_k + B\bar{u}_k - \xi d\delta_{k,k_0-1} + w_k \tag{15a}$$

$$y_k = C\tilde{x}_k + \varepsilon_k. \tag{15b}$$

If the attacker chooses d close to zero and ξ orthogonal to the eigenvectors of A associated with unstable eigenvalues, the pulse $d\delta_{k,k_0-1}$ cannot be detected from the anomaly detector designed on the innovation sequence $\gamma_k = y_k - C\widehat{\tilde{x}}_{k/k-1}$ of the Kalman filter. The proof that the attacker can perform the malicious act while forcing the system out of its safe operating region without any consequences on the nominal control law (4b) are established via a simulation example given in Section 4.1.

3 Resilient defensive strategy

Resilient defensive strategy injection on the control signal generated by a LQG controller can be designed to act on the state variables of the NCS while remaining undetectable to any passive detector applied on the innovation sequence of the Kalman filter. In this section, we give an active attack detection scheme to reveal the presence of a zero dynamic attack and investigate a resilient control strategy that a defender can use to quickly recover the normal behavior of the NCS, see Fig. 3.

3.1 Detection of zero dynamic attack

When the attack is stopped at the intrusion time k_f, the consequences of a_k, $\forall k \succeq k_f$ can be described as

$$\Delta\tilde{x}_{k+1}^a = A\Delta\tilde{x}_k^a \tag{16a}$$

$$\Delta\tilde{y}_k^a = C\Delta\tilde{x}_k^a \tag{16b}$$

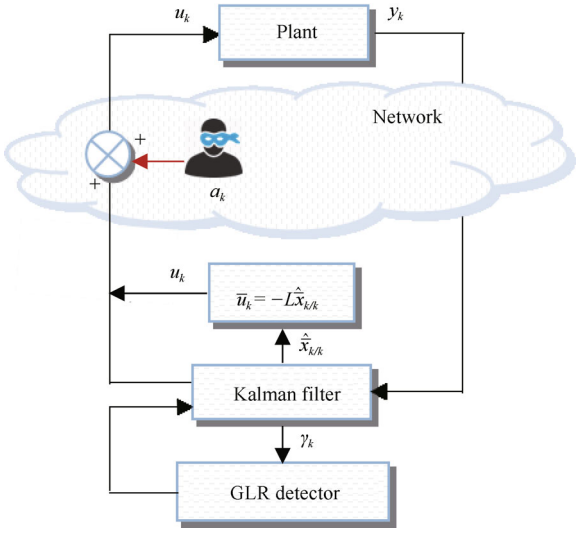

Fig. 3 NCS under attack with resilient LQG controller

with $\Delta\tilde{x}^a_{k_f} = d\xi\lambda^{k_f-k_0-1}$ and $\Delta\tilde{x}^a_{k_f-1} = 0$. From $\nu\delta_{k,k_f-1}$, a pulse of size $\nu = d\lambda^{k_f-k_0-1}$, (16) can be equivalently rewritten as

$$\Delta\tilde{x}^a_{k+1} = A\Delta\tilde{x}^a_k + \xi\nu\delta_{k,k_f-1} \tag{17a}$$
$$\Delta\tilde{y}^a_k = C\Delta\tilde{x}^a_k. \tag{17b}$$

When d is assumed to be close to zero, substituting (14) for (17), the model of the plant view by the controller $\forall k \succeq k_f$ becomes

$$\begin{bmatrix} \tilde{x}_{k+1} \\ \Delta\tilde{x}^a_{k+1} \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} \begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}^a_k \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} \bar{u}_k + \begin{bmatrix} 0 \\ \xi \end{bmatrix} \nu\delta_{k,k_f-1} + \begin{bmatrix} I \\ 0 \end{bmatrix} w_k \tag{18a}$$

$$y_k = \begin{bmatrix} C & C \end{bmatrix} \begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}^a_k \end{bmatrix} + \varepsilon_k. \tag{18b}$$

From $\begin{bmatrix} x_k \\ \Delta\tilde{x}^a_k \end{bmatrix} = T^{-1} \begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}^a_k \end{bmatrix}$ with $T^{-1} = \begin{bmatrix} I & I \\ 0 & I \end{bmatrix}$, the augmented state model of the plant refers to (18) is rewritten as

$$\begin{bmatrix} x_{k+1} \\ \Delta\tilde{x}^a_{k+1} \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} \begin{bmatrix} x_k \\ \Delta\tilde{x}^a_k \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} \bar{u}_k + \begin{bmatrix} \xi \\ \xi \end{bmatrix} \nu\delta_{k,k_f-1} + \begin{bmatrix} I \\ 0 \end{bmatrix} w_k \tag{19a}$$

$$y_k = \begin{bmatrix} C & 0 \end{bmatrix} \begin{bmatrix} x_k \\ \Delta\tilde{x}^a_k \end{bmatrix} + \varepsilon_k \tag{19b}$$

and can be reduced to

$$x_{k+1} = Ax_k + B\bar{u}_k + \xi\nu\delta_{k,k_f-1} + w_k \tag{20a}$$
$$y_k = Cx_k + \varepsilon_k. \tag{20b}$$

The size $\nu = d\lambda^{k_f-k_0-1}$ of $\nu\delta_{k,k_f-1}$ in (20) (upper bounded by $d\lambda^{\mathrm{T}}$) is greater than the size d of $d\delta_{k,k_0-1}$ in (15) via $|\lambda| > 1$, and the pulse $\nu\delta_{k,k_f-1}$ has now a chance to be detected from anomaly detectors. When the model of the plant switches from (15) to (20), the active model-based FDI scheme consists of detecting the hypothesized pulse $\nu\delta_{k,k_f-1}$ of unknown size ν and occurrence time k_f from the GLR test as

$$x_{k+1} = Ax_k - B\bar{u}_k + \xi\nu\delta_{k,k_f-1} + w_k \tag{21a}$$
$$y_k = Cx_k + \varepsilon_k. \tag{21b}$$

The state prediction error $e_{k/k-1} = x_k - \hat{x}_{k/k-1}$ and the innovation $\gamma_k = y_k - C\hat{x}_{k/k-1}$ of the Kalman filter propagate as

$$e_{k+1/k} = (A - K_kC)e_{k/k-1} - K_k\varepsilon_k + \xi\nu\delta_{k,k_f-1} + w_k \tag{22a}$$
$$\gamma_k = Ce_{k/k-1} + \varepsilon_k \tag{22b}$$

where $\nu\delta_{k,k_f-1}$ is a pulse of unknown size $\nu = d\lambda^l$ greater than d when $1 < l \leq \tau$ via $\lambda > 1$. The pulse $d\delta_{k,k_f-1}$ chosen undetectable with d close to zero, the following section proposes to detect $\nu\delta_{k,k_f-1}$ from a GLR detector applied on the innovation sequence of the Kalman filter. To avoid the detection of $\nu\delta_{k,k_f-1}$ several times, the Kalman filter will be updated online according to the detected event. The updating strategy of the Kalman filter associated to the infinite horizon LQG controller of Section 2 will lead to an autonomous resilient LQG controller. The additive effect of $\nu\delta_{k,k_f-1}$ on the state prediction error $\bar{e}_{k/k-1} = \bar{x}_k - \widehat{\bar{x}}_{k/k-1}$ and the innovation sequence $\bar{\gamma}_k = y_k - C\widehat{\bar{x}}_{k/k-1}$ of the Kalman filter can be expressed as

$$e_{k+1/k} = \bar{e}_{k+1/k} + f(k, k_f - 1)\nu \tag{23a}$$
$$\gamma_k = \bar{\gamma}_k + h(k, k_f - 1)\nu \tag{23b}$$

where $f(k, k_f-1)$ and $h(k, k_f-1)$ are recursively computed as

$$f(k, k_f - 1) = (A - K_kC)f(k-1, k_f - 1) - \xi\delta_{k,k_f-1} \tag{24a}$$
$$h(k, k_f - 1) = Cf(k, k_f - 1) \tag{24b}$$

with $f(k_f - 1, k_f - 1) = 0$.

Let H_0 denotes the null hypothesis under which no attack exists and H_1 denotes the attack end hypothesis at time k_f. The hypothesis H_1 can be confronted to the null hypothesis H_0 as

$$H_0 : \mathrm{E}\{\gamma_j\} = 0, \quad k \succeq j \succeq 0 \tag{25a}$$
$$H_1 : \mathrm{E}\{\gamma_j\} = h(j, \quad k_f - 1)\nu, k \succeq j \succeq k_f - 1 \tag{25b}$$

and

$$\mathrm{E}\{\gamma_j\} = 0, \quad k_f - 1 > j \succeq 0. \tag{25c}$$

Let $P(\frac{\gamma_j}{H_1})$, $P(\frac{\gamma_j}{H_0})$ be the Gaussian probability density functions of γ_j conditioned on H_1, H_0, and define the like-

lihood ratio as

$$\lambda(k,k_f-1)=\frac{P\left(\frac{\gamma_{k_f-1}}{H_1}\right)P\left(\frac{\gamma_{k_f}}{H_1}\right)\cdots P\left(\frac{\gamma_k}{H_1}\right)}{P\left(\frac{\gamma_{k_f-1}}{H_0}\right)P\left(\frac{\gamma_{k_f}}{H_0}\right)\cdots P\left(\frac{\gamma_k}{H_0}\right)}. \quad (26)$$

From $h(k_f-1,k_f-1)=0$ and $h(k_f,k_f-1)=0$ via $C\xi=0$, we have $P(\frac{\gamma_{k_f-1}}{H_1})=P(\frac{\gamma_{k_f-1}}{H_0})$, $P(\frac{\gamma_{k_f}}{H_1})=P(\frac{\gamma_{k_f}}{H_0})$, and the likelihood ratio (26) becomes

$$\lambda(k,k_f-1)=\frac{\exp\Big(-\frac{1}{2}\sum\limits_{j=k_f+1}^{k}\|\gamma_j-h(j,k_f-1)\nu\|^2_{\bar{Q}_j^{-1}}\Big)}{\exp\Big(-\frac{1}{2}\sum\limits_{j=k_f+1}^{k}\|\gamma_j\|^2_{\bar{Q}_j^{-1}}\Big)} \quad (27)$$

where $\bar{Q}_j=C\bar{P}_{j/j-1}C^{\mathrm{T}}+V$ is the covariance of γ_j. The maximum likelihood estimate of the pulse magnitude ν conditioned on k_f is given by

$$\hat{\nu}(k,k_f-1)=\frac{b(k,k_f-1)}{a(k,k_f-1)} \quad (28a)$$

where

$$a(k,k_f-1)=\sum_{j=k_f+1}^{k}[h^{\mathrm{T}}_{j,k_f-1}(\bar{Q}_j)^{-1}h_{j,k_f-1}] \quad (28b)$$

$$b(k,k_f-1)=\sum_{j=k_f+1}^{k}[h^{\mathrm{T}}_{j,k_f-1}(\bar{Q}_j)^{-1}\gamma_j]. \quad (28c)$$

After having replaced ν by $\hat{\nu}(k,k_f-1)$ in (27), the log-likelihood ratio $T(k,k_f-1)=2\log(\lambda(k,k_f-1))$ can be expressed from the normalized estimate $\widehat{\overline{\nu}}(k,k_f-1)=a(k,k_f-1)^{-\frac{1}{2}}b(k,k_f-1)$ of the pulse conditioned on H_1 as $T(k,k_f-1)=\widehat{\overline{\nu}}(k,k_f-1)^2$ and the decision rules of the GLR detector becomes

$$T(k)=\max_{k_f\in\begin{bmatrix}0 & k-1\end{bmatrix}}\left\{\widehat{\overline{\nu}}(k,k_f-1)^2\right\}\begin{cases}\leqslant\varepsilon \text{ decision for } \mathrm{H}_0\\ >\varepsilon \text{ decision for } \mathrm{H}_1\end{cases} \quad (29)$$

where ε is the threshold level. For a real time implementation of (29), the maximization can be realized on a sliding window of limited size. False alarms, missed detections and good decisions rate depend on the choice of the decision level and on the size of the sliding window.

3.2 Resilient LQG controller

When $T(k)>\varepsilon$, the detection of the same pulse $\nu\delta_{k,k_f-1}$ several times can be avoided by using a Kalman filter updating strategy described as

$$\widehat{\overline{x}}'_{k/k}=\widehat{\overline{x}}_{k/k}+f(k,\hat{k}_f-1)\hat{\nu}(k,\hat{k}_f-1) \quad (30a)$$

$$\bar{P}'_{k/k}=\bar{P}_{k/k}+f(k,\hat{k}_f-1)a(k,\hat{k}_f-1)^{-1}f(k,\hat{k}_f-1)^{\mathrm{T}} \quad (30b)$$

where $a(k,\hat{k}_f-1)^{-1}$ presents the covariance of $\hat{\nu}(k,\hat{k}_f-1)$. $\widehat{\overline{x}}'_{k/k}$ and $\widehat{\overline{x}}_{k/k}$ denote the new and the old minimum variance unbiased estimate, respectively. The same notation is used for the new state covariance $\bar{P}'_{k/k}$ and the old one $\bar{P}_{k/k}$.

The attack end time estimate $\widehat{k}_f$ is given by

$$\widehat{k}_f=\arg\left(\max_{k_f\in\begin{bmatrix}k-1-M & k-1\end{bmatrix}}\left\{\widehat{\overline{\nu}}(k,k_f-1)^2\right\}\right). \quad (31)$$

The autonomous resilient LQG controller is then derived from the updating strategy (30) applied on the Kalman filter (5) and associated to the infinite horizon LQG controller designed in Section 2. To evaluate the overall characteristic of the obtained resilient LQG controller, a performance criterion needs to be studied in relation with the maximum duration τ of the attack signal. An illustrative example will be given in Section 4 to prove that the proposed resilient controller works very well when a zero dynamic attack significantly impacts the state variables of the plant before being stopped.

4 Results and discussion

After the completion of the modelling of attack detection schemes and the resilient control strategy, a simulation example is given in this section to demonstrate the effectiveness of the obtained results. First, we illustrate how the attacker can successfully realise the malicious act while remaining undetectable from passive detectors. We then apply the proposed detection scheme of Section 3 and evaluate the performance of the proposed resilient LQG controller via a comparative study with the standard LQG controller.

For illustration, we consider the following linear discrete time stochastic system:

$$A=\begin{bmatrix}0.9 & 0 & 0.34 & 0.35\\ 0 & 1.8 & 0 & 0.37\\ 0 & 0 & 0.5 & 0\\ 0 & 0 & 0 & 0.9\end{bmatrix}$$

$$B=\begin{bmatrix}1 & 0 & 0\\ 1 & 0 & 1\\ 0 & 0 & 2\\ 0 & 1 & 1\end{bmatrix}$$

$$C=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix} \quad (32)$$

where $z_0=1.18$ is the invariant unstable zero of the plant.

4.1 Zero dynamic attack's consequences

We first illustrate the consequences of the stealthy attack strategy on the NCS of Fig. 2, where the zero dynamic attack has been simulated during the time instants $\tau=[80\,\mathrm{s},120\,\mathrm{s}]$, see Fig. 4. Note that d is chosen very close to zero to remain stealthy to any passive detector applied on the innovation sequence of the Kalman filter.

As we can see in Figs. 5 and 6, the attack happens in a

stealthy way having no consequences on the control signal u_k and no consequences on measurements y_k, respectively. Whereas it has a harmful effect on the third state which increases to infinity as shown in Fig. 7. Fig. 8 shows that the detection variable T_k cannot detect the presence of the attack.

This demonstrates that an attacker located inside the network of a NCS can provide malicious consequences on the system′s state using a stealthy strategy without being detected from traditional model based fault detection and isolation schemes.

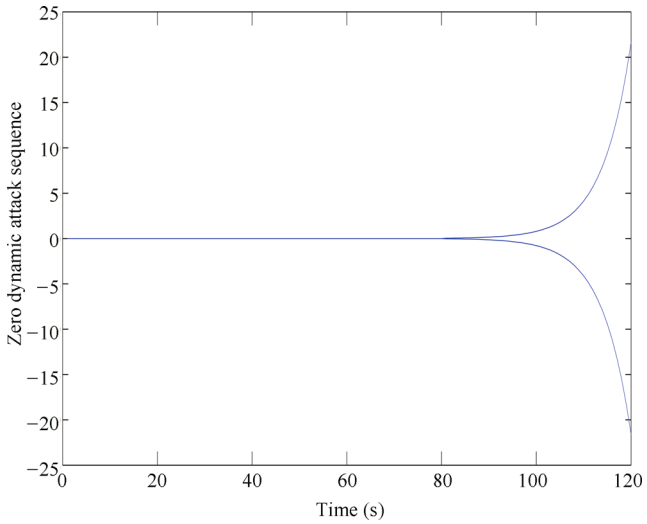

Fig. 4 Zero dynamic attack sequence/time (s)

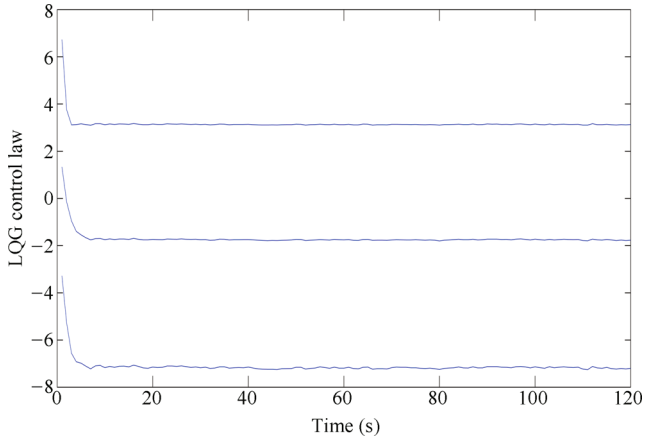

Fig. 5 LQG control law/time (s)

4.2 A comparative study between standard and resilient control

To prove the usefulness of the proposed detection scheme and the resilient control strategy, a comparative study between the standard LQG control and the resilient LQG control is presented.

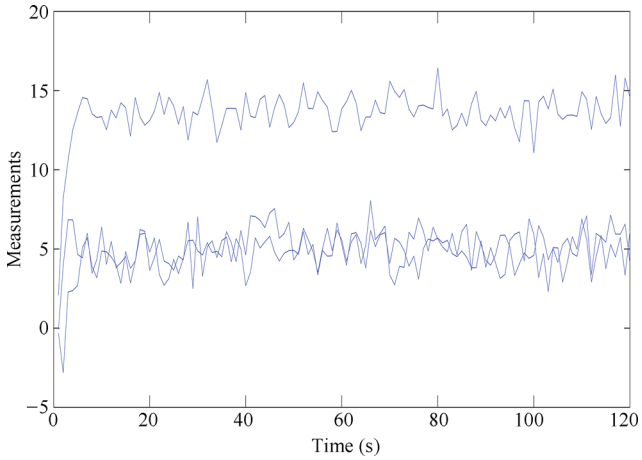

Fig. 6 Measurements y_k/time (s)

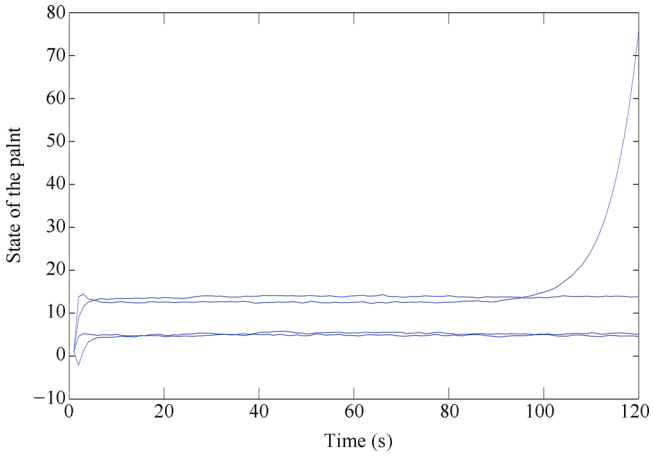

Fig. 7 States of the plant/time (s)

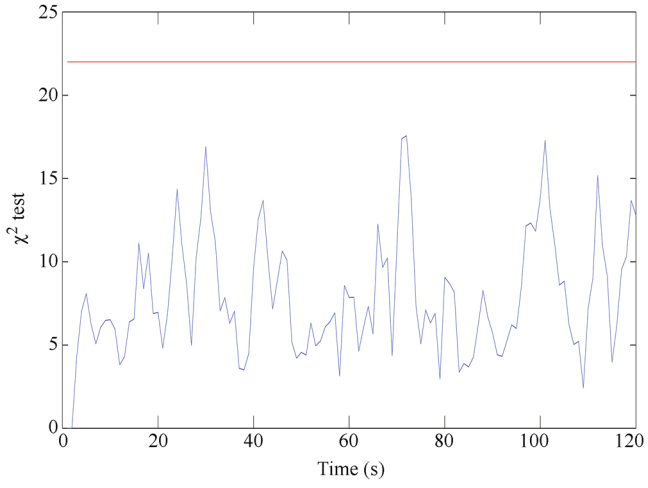

Fig. 8 Detection variable T_k of the GLR detector and the decision level ε

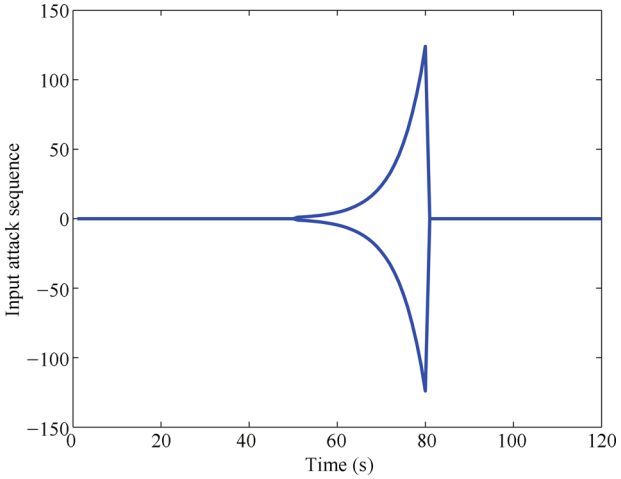

Fig. 9 Zero dynamic attack sequence/time (s)

Consider now that the NCS of Fig. 3 is attacked by a zero dynamic attack during the time instants $\tau = [50\,\text{s}, 80\,\text{s}]$ as illustrated in Fig. 9. As we can see in Fig. 10, this strategy allows to detect the presence of the stealthy attack when the detection variable T_k exceeds the threshold levels of significance values.

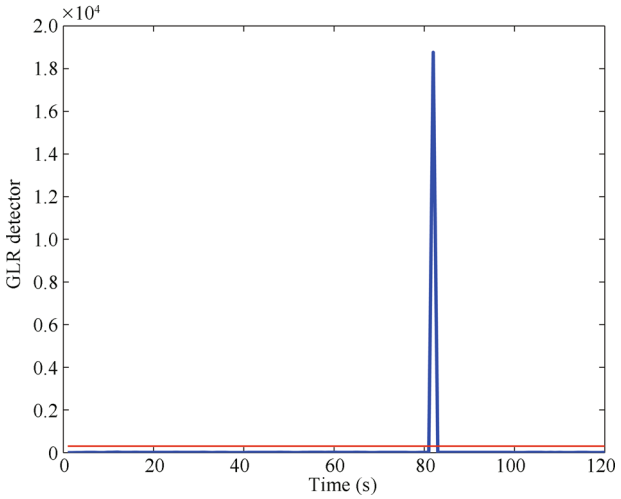

Fig. 10 Detection variable T_k of the GLR detector

By using the standard control strategy (4) and (5) with $V = R = I_3$, $W = 0.01I_4$ and $Q = I_4$, Figs. 11–13 show the consequences of the zero dynamic attack on state variables, control signal and regulated outputs, respectively.

By using the resilient control strategy (30) and (5), the consequences of the zero dynamic attack on the state variables, control signal and regulated outputs of the plant by using the resilient LQG controller are plotted in Figs. 14–16, respectively.

Compared to the regulated outputs of Fig. 13 obtained with the standard LQG controller, Fig. 16 shows that the updating strategy (30) allows to recover more quickly the nominal behavior of the networked control system.

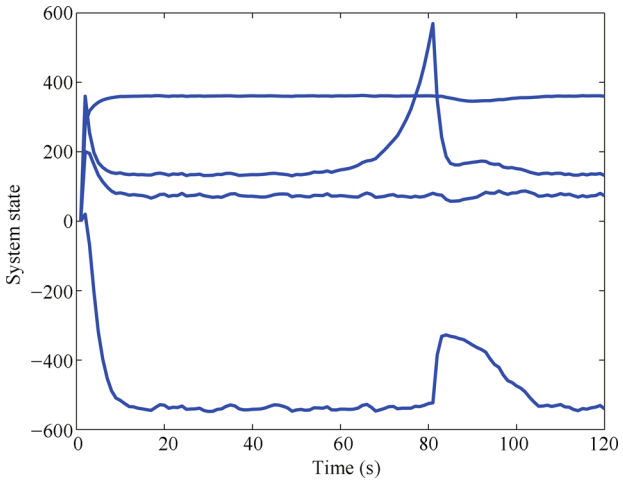

Fig. 11 States of the plant/time (s)

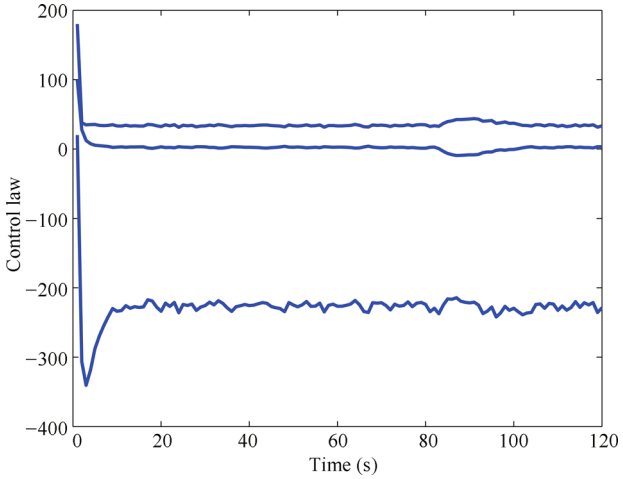

Fig. 12 Standard LQG control law/time (s)

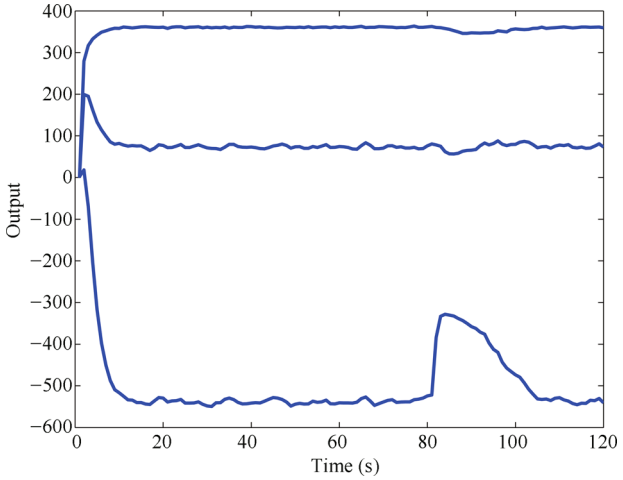

Fig. 13 Regulated outputs/time (s)

By representing the plant subject to multiple zero dynamic attacks as a linear time-invariant system subject to simultaneous or sequential pulses, the design of resilient controllers for plants having multiple invariant zeros is currently under consideration by the authors. Future works

will concern the design of distributed resilient controllers for large scale NCS decomposed into subsystems.

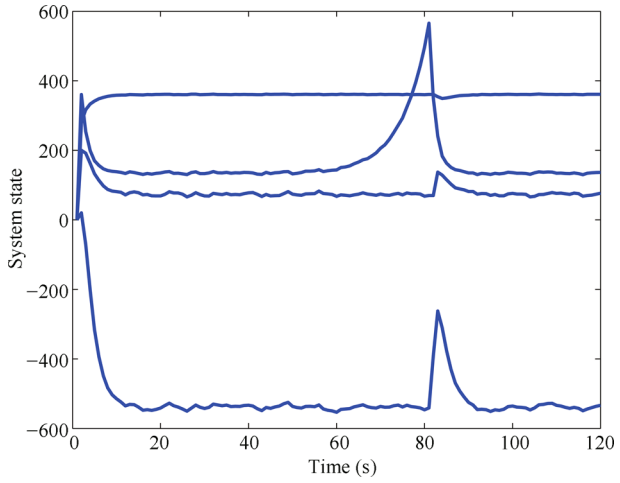

Fig. 14 States of the plant/time (s)

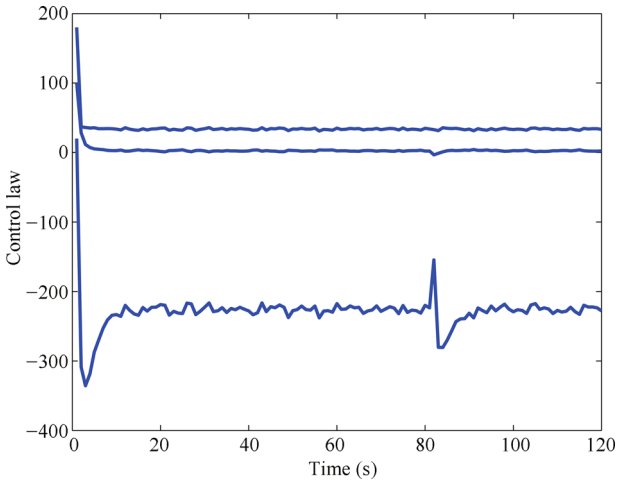

Fig. 15 LQG control law/time (s)

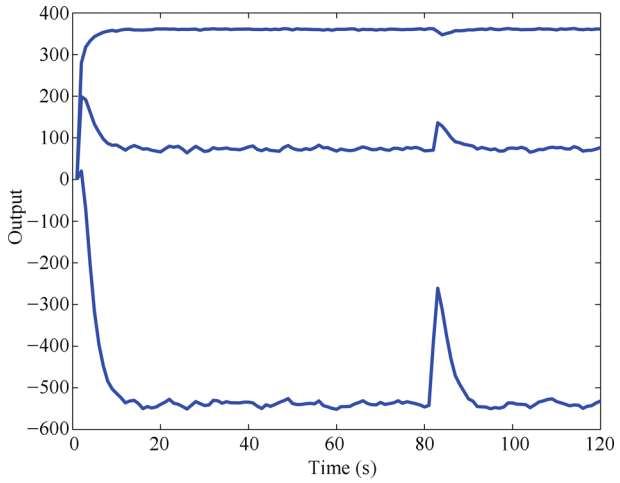

Fig. 16 Regulated outputs/time (s)

5 Conclusions

This paper has studied a resilient control strategy for linear discrete-time stochastic systems subject to zero dynamic attack. When the attack window of the adversary is limited by the defender mechanism of the cyber-physical system, we have shown in the first part of the paper that the zero dynamic attack is undetectable from traditional model based fault detection and isolation schemes. In the second part, we have designed a resilient linear quadratic Gaussian controller having the ability to quickly recover the nominal behavior of the closed-loop system. The resilient linear quadratic Gaussian controller is obtained by updating online the Kalman filter from information given by the generalized likelihood ratio detector.

References

[1] P. Antsaklis, J. Baillieul. Special issue on technology of networked control systems. *Proceedings of the IEEE*, vol. 95, no. 1, pp. 5–8, 2007.

[2] J. P. Hespanha, P. Naghshtabrizi, Y. G. Xu. A survey of recent results in networked control systems. *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, 2007.

[3] K. Stouffer, J. Falco, K. Scarfone. Guide to industrial control systems (ICS) security. *NIST Special Publication*, 2007.

[4] Z. D. Tian, X. W. Gao, B. L. Gong, T. Shi. Time-delay compensation method for networked control system based on time-delay prediction and implicit PIGPC. *International Journal of Automation and Computing*, vol. 12, no. 6, pp. 648–656, 2015.

[5] A. Teixeira, D. Pérez, H. Sandberg, K. H. Johansson. Attack models and scenarios for networked control systems. In *Proceedings of the 1st International Conference on High Confidence Networked Systems*, ACM, New York, USA, pp. 55–64, 2012.

[6] Y. Chen, S. Kar, J. M. F. Moura. *Dynamic Attack Detection in Cyber-Physical Systems with Side Initial State Information*, 2015.

[7] S. Amin, A. A. Cárdenas, S. S. Sastry, Safe and secure networked control systems under denial-of-service attacks. In *Proceedings of the 12th International Conference on Hybrid Systems: Computation and Control*, Springer, San Francisco, USA, pp. 31–45, 2009.

[8] Y. Liu, P. Ning, M. K. Reiter. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ACM, Chicago, USA, pp. 21–32, 2009.

[9] A. Teixeira, H. Sandberg, K. H. Johansson. Networked control systems under cyber attacks with applications to power networks. In *Proceedings of American Control Conference*, IEEE, Baltimore, USA, pp. 3690–3696, 2010.

[10] F. Pasqualetti, F. Dórfler, F. Bullo. Cyber-physical security via geometric control: Distributed monitoring and malicious attacks. In *Proceedings of the 51th Annual Conference on Decision and Control*, IEEE, Maui, USA, pp. 3418–3425, 2012.

[11] Y. L. Mo, B. Sinopoli. Secure control against replay attacks. In *Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing*, IEEE, Monticello, USA, pp. 911–918, 2009.

[12] R. S. Smith. A decoupled feedback structure for covertly appropriating networked control systems. In *Proceedings of the 18th IFAC World Congress*, IFAC, Milan, Italy, pp. 90–95, 2011.

[13] A. A. Cardenas, S. Amin, S. Sastry. Secure control: Towards survivable cyber-physical systems. In *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops*, IEEE, Beijing, China, pp. 495–500, 2008.

[14] F. Pasqualetti. Secure Control Systems: A Control-Theoretic Approach to Cyber-Physical Security, Ph. D. dissertation, University of California, USA, 2012.

[15] P. M. Frank. Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results. *Automatica*, vol. 26, no. 3, pp. 459–474, 1990.

[16] J. Chen and R. J. Patton. *Robust Model-Based Fault Diagnosis for Dynamic Systems*, Boston, USA: Kluwer Academic Publishers, 1999.

[17] S. X. Ding. *Model-Based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools*, Berlin Heidelberg, Germany: Springer, 2008.

[18] K. Chabir, D. Sauter, I. M. Al-Salami, C. Aubrun. On fault detection and isolation (FDI) design for networked control systems with bounded delay constraints. In *Proceedings of the 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Mexico City, Mexico, pp. 1107–1112, 2012.

[19] M. Brunner, H. Hofinger, C. Krauss, C. Roblee, P. Schoo, S. Todt. Infiltrating critical infrastructures with next-generation attacks. *Fraunhofer Institute for Secure Information Technology*, [Online], Available: http://publica.fraunhofer.de/documents/N-151330.html, 2010.

[20] A. Teixeira, I. Shames, H. Sandberg, K. H. Johansson. Revealing stealthy attacks in control systems. In *Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing*, IEEE, Monticello, USA, pp. 1806–1813, 2012.

[21] J. Y. Keller, D. Sauter. Monitoring of stealthy attack in networked control systems. In *Proceedings of Conference on Control and Fault-Tolerant Systems*, IEEE, Nice, France, pp. 462–467, 2013.

[22] J. Y. Keller, K. Chabir, D. Sauter. Input reconstruction for networked control systems subject to deception attacks and data losses on control signals. *International Journal of Systems Science*, vol. 47, no. 4, pp. 814–820, 2016.

[23] V. L. Do, L. Fillatre, I. Nikiforov. A statistical method for detecting cyber/physical attacks on SCADA systems. In *Proceedings of IEEE Conference on Control Applications*, IEEE, Antibes, France, pp. 364–369, 2014.

[24] A. Willsky, H. Jones. A generalized likelihood ratio approach to the detection and estimation of jumps in linear systems. *IEEE Transactions on Automatic Control*, vol. 21, no. 1, pp. 108–112, 1976.

[25] Y. M. Zhang, J. Jiang. Bibliographical review on reconfigurable fault-tolerant control systems. *Annual Reviews in Control*, vol. 32, no. 2, pp. 229–252, 2008.

[26] Y. Yuan, Q. Y. Zhu, F. C. Sun, Q. Y. Wang, T. Başar. Resilient control of cyber-physical systems against denial-of-service attacks. In *Proceedings of the 6th International Symposium on Resilient Control Systems*, IEEE, San Francisco, USA, pp. 54–59, 2013.

[27] C. De Persis, P. Tesi. Resilient control under denial-of-service. *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 134–139, 2014.

[28] X. Zhu. Resilient Control and Intrusion Detection for SCADA Systems, Ph. D. dissertation, University of California, USA, 2011.

Taouba Rhouma received B. Eng. degree in electrical-automatic engineering from the National Engineering School of Gabes (ENIG), Tunisia in 2013. Since that, she is a Ph. D. candidate in electrical engineering at Modeling, Analysis and Control of Systems Laboratory (MACS), Tunisia.

Her research interests include fault detection and diagnosis of networked control systems.

E-mail: taouba.rhouma@gmail.com (Corresponding author)
ORCID iD: 0000-0002-3763-212X

Karim Chabir received the B. Eng. degree in electrical engineering and automatic engineering from The Higher School of Sciences and Technology of Tunis (ESSTT), Tunisia in 2003, the M. Sc. degree in automatic and intelligent techniques from the National Engineering School of Gabes, Tunisia in 2006, and the Ph. D. degree in automatic control from Henri Poincare University, France in 2011. The research works were carried out at the Research Centre for Automatic Control of Nancy (CRAN) and at the Research Unit of Modelling, Analysis and Control Systems of the National Engineering School of Gabes. He was a member of the dependability and system diagnosis group (SURFDIAG). He was a secondary school teacher of Gabes from 2003 to 2007, where he was also an assistant professor in the Faculty of Science of Gabes from 2007 to 2011. He is now assistant professor at the National Engineering School of Gabes (ENIG), Tunisia.

His research interests include model-based fault diagnosis and fault-tolerant control with emphasis on networked control systems.

E-mail: karim.chabir@yahoo.fr
ORCID iD: 0000-0002-2377-7205

Mohamed Naceur Abdelkrim received the B. Sc. degree in electrical construction in 1980, and the M. Sc. degree in electrical construction in 1981 from the High Normal School of Technical Education of Tunis, Tunisia. He also received the Ph. D. degree in automatic control from the National School of Engineers of Tunis, Tunisia in 2003. He began teaching in 1981 at the National School of Engineers of Tunis and since 2003, he has been a professor of automatic control at the National School of Engineers of Gabes, Tunisia. He is currently the head of the research unit on Modeling, Analysis and Control of Systems (MACS), Tunisia.

His research interests include diagnosis, optimal control, robust control and robotics.

E-mail: naceur.abdelkrim@enig.rnu.tn