Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 48-21 (2015) 754–759

Active GLR detector for resilient LQG controller in networked control systems

T. Rhouma * **J.Y. Keller** ** **D. Sauter** ** **K. Chabir** * **M.N. Abdelkrim** *

* *National Engineering School of Gabès, Gabès University, MACS 06-UR-11-12, 6029 Gabès, Tunisia, (e-mail: taouba.rhouma@gmail.com)*

** *Faculty of Sciences and Technologies, BP 70239, 54506 Nancy, France, (e-mail: jean-yves.keller@univ-lorraine.fr)*

Abstract: In computing science, resilience is the ability of system or network architecture to recover normal operation after a brutal crash. When malicious cyber act on control signals of a Networked Control System (NCS) is designed to remain undetectable from passive model-based Fault Detection and Isolation (FDI) schemes, we show that the unobservable consequence on the state variable of the plant becomes brutally observable after the disappearance of the damaging action. In order to quickly recover the nominal behavior of the Linear Quadratic Gaussian (LQG) controller, a resilient LQG controller is obtained from an active version of the Generalized Likelihood Ratio (GLR) test designed to detect the disappearance of the malicious act and to increase the tracking ability of the Kalman filter at detection time.

Keywords: Networked control systems, Network security, Kalman filters, Resilient Linear Quadratic Gaussian control, Anomaly detector.

1. INTRODUCTION

Recent technological advances are revolutionizing our ability to build distributed Networked Control Systems (NCS) where the communication network plays an extremely important role in geographically dispersed NCS, stressed in Hespanha et al. (2007). Central, decentralized or distributed NCS are critical to system operation (Stouffer et al., 2007) in various infrastructures such as electric power grids, transportation systems, communication networks, oil and gas pipelines, waste-water treatment systems, water distribution and irrigation networks.

Besides failures of components, NCS are vulnerable to Cyber Physical Attacks (CPA) incorporating cyber and physical activities into a malicious attack. Specific analysis tools as well as monitoring mechanisms need then to be developed to enforce system security and reliability (see Fovino et al. (2010) and Krutz (2005)). As pointed out in Cardenas et al. (2008), the security of Cyber-Physical Systems (CPS) integrating computation, communication and physical capabilities must be improved from both information technology and control theory.

CPA in CPS summarized in Cardenas et al. (2008) and Pasqualetti (2012) can be divided into three categories as follows: Denial of Service (DoS) attacks in Amin et al. (2009) when adversaries prevent controllers from received sensors measurement or the plant from received control laws, deception attacks in Liu et al. (2009), Teixeira et al. (2010), Pasqualetti et al. (2012), Smith (2011) and Teixeira et al. (2012a) when adversaries inject false data on control signals or on information transmitted by sensors to the plant via communication channels, and finally physical attacks on sensors and actuators close to faults considered in traditional model-based Fault Detection and Isolation (FDI) schemes studied by Frank (1990), Ding (2008), Patton and Chen (1999), Basseville and Nikiforov (1993), Willsky and Jones (1976) and Keller and Sauter (2011). The last generation of malwares of type Stuxnet in Brunner et al. (2010) infecting Programmable Logic Controllers (PLC) or Replay attack in Mo and Sinopoli (2009) can be viewed as deception attack on control signals coordinated with the generation of artificial delays on measurements.

The detection problem of coordinated attacks in CPS seems closely related to the detection problem of multiple component, sensor or actuators faults, 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 from traditional model-based FDI schemes. In this new context, it is necessary to design a new generation of FDI schemes having the ability to detect the presence of coordinated attacks.

In conventional active FDI methods, some input signals are activated to reveal the presence of stealthy attacks (see Mo and Sinopoli (2009) and references therein). In Teixeira et al. (2012b), Keller and Sauter (2013) and Keller et al. (2014), the authors consider a special deception attack called a zero dynamic attack (designed in Teixeira et al. (2012b) by using the output-nulling controlled invariant subspace in geometric control theory) and show that the stealthy strategy of the adversary is destroyed by modifying the systems structure or by data losses on the

2405-8963 © 2015, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2015.09.617

control signals due to unreliable communication networks. This paper assumes that the Intrusion Detection System (IDS) (see Giani et al. (2009) for more information) is able to take the right countermeasures against an attacker having obtained the cryptographic keys and able to access the control signal transmitted by the controller to the plant, in other words that the IDS can stop the false data injection (a dual solution to conventional active FDI methods) by forcing the adversary to perform his malicious activity on a limited period of time. 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 disappearance cannot remains stealthy and proposes to detect this event from an active version of the GLR test developed in Willsky and Jones (1976).

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, presented in Zhang and Jiang (2008) and references therein. Undetectable attacks from passive FDI methods, driven the system out of its safe operating region without to trigger the controller reconfiguration mechanism, are potentially catastrophic in safety-critical systems such as aircrafts, nuclear power plants and chemical plants. Consequently, it is also necessary to design active FTCS with the help of active FDI methods. This paper presents a particular active FTCS having the ability to quickly recover the safe operating region in response to the disappearance of attack signal caused by the IDS. 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.

The paper is organized as follows: Section 2 shows that the occurrence of a zero dynamic attack is undetectable. Section 3 describes the proposed resilient LQG controller. A simulation example is presented at section 4 before to conclude at section 5.

2. PROBLEM STATEMENT

Consider the NCS of Fig. 1 where the plant is represented by a linear discrete-time stochastic system

$$x_{k+1} = Ax_k + Bu_k + w_k \quad (1)$$
$$y_k = Cx_k + \nu_k \quad (2)$$

where $x_k \in \Re^n$,$u_k \in \Re^q$ and $y_k \in \Re^m$ are the state, input and measurement vectors and where $w_k \in \Re^n$ and $\nu_k \in \Re^m$ are zero mean uncorrelated Gaussian random sequences with

$$E\left\{\begin{bmatrix} w_k \\ v_k \end{bmatrix}\begin{bmatrix} w_j \\ v_j \end{bmatrix}^T\right\} = \begin{bmatrix} W & 0 \\ 0 & V \end{bmatrix}\delta_{k,j},\ W \succeq 0,\ V > 0 \quad (3)$$

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

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

$$\bar{x}_{k+1} = A\bar{x}_k + B\bar{u}_k + w_k \quad (4)$$
$$y_k = C\bar{x}_k + v_k \quad (5)$$

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

$$J = \min \lim_{T\to\infty} E\left\{\frac{1}{T}\left[\sum_{k=0}^{T-1} \bar{x}_k^T Q \bar{x}_{k_k} + \bar{u}_k^T R \bar{u}_k\right]\right\} \quad (6)$$

is given by

$$\bar{u}_k = -L\widehat{\bar{x}}_{k/k} \quad (7)$$

with

$$L = (B^T S B + R)^{-1} B^T S A \quad (8)$$
$$S = A^T S A + Q - A^T S B (B^T S B + R)^{-1} B^T S A \quad (9)$$

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

$$\widehat{\bar{x}}_{k/k} = \widehat{\bar{x}}_{k/k-1} + K_k(y_k - C\widehat{\bar{x}}_{k/k-1}) \quad (10)$$
$$\bar{P}_{k/k} = (I - K_k C)\bar{P}_{k/k-1}(I - K_k C)^T + K_k V K_k^T \quad (11)$$
$$K_k = \bar{P}_{k/k-1} C^T (C\bar{P}_{k/k-1} C^T + V)^{-1} \quad (12)$$
$$\widehat{\bar{x}}_{k+1/k} = A\widehat{\bar{x}}_{k/k} + B\overline{u}_k \quad (13)$$
$$\bar{P}_{k+1/k} = A\bar{P}_{k/k} A^T + W \quad (14)$$

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

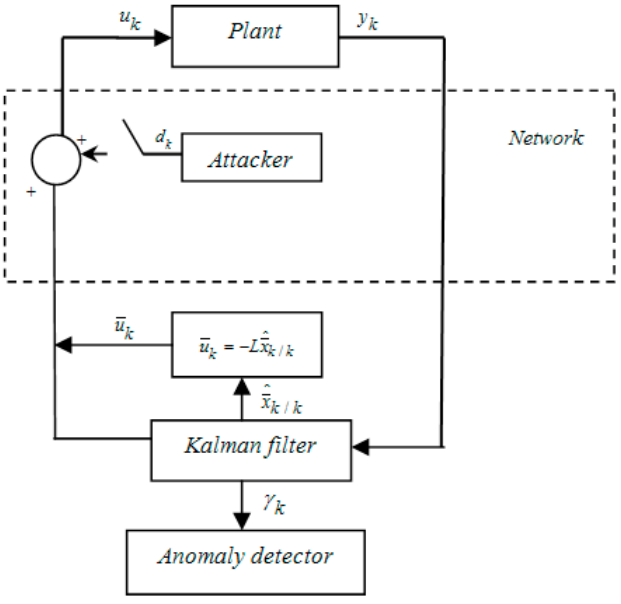

Fig. 1. NCS under attack with LQG controller.

When the false data sequence $d_k \neq 0\ \forall k \succeq t$ are added by the attacker on the control signal transmitted by the controller to the plant at the intrusion time t, the control

signal received by the plant is expressed $u_k = \bar{u}_k + d_k$ and the model of the plant viewed by the controller becomes

$$x_{k+1} = Ax_k + B\bar{u}_k + Bd_k + w_k \quad (15)$$

$$y_k = Cx_k + v_k \quad (16)$$

The additive consequence Δx_k^a and Δy_k^a $\forall k \succeq t$ of $d_k \neq 0$ $\forall k \succeq t$ expressed from the model of the plant under no attack as $x_k = \bar{x}_k + \Delta x_k^a$ and $y_k = C\bar{x}_k + \Delta y_k^a$ are described by

$$\Delta x_{k+1}^a = A\Delta x_k^a + Bd_k \quad (17)$$

$$\Delta y_k^a = C\Delta x_k^a \quad (18)$$

with $\Delta x_t^a = 0$.

2.1 Attacker's view point

When the adversary knows the state model of the plant, a particular deception attack $d_k = -G\Delta\tilde{x}_k^a$, called zero dynamic attack described in Teixeira et al. (2012b), can be designed from the following autonomous system

$$\Delta\tilde{x}_{k+1}^a = (A - BG)\Delta\tilde{x}_k^a \quad (19)$$

$$\Delta\tilde{y}_k^a = C\Delta\tilde{x}_k^a \quad (20)$$

with $\tilde{\Delta}x_t^a$ close to Δx_t^a, but not zero otherwise $d_k = 0$ $\forall k \succeq t$.

The stealthy strategy of the adversary consists then in determining G so that

$$\Delta\tilde{y}_k^a = 0 \ \forall k \succeq t \quad (21)$$

$$\lim_{k\to\infty} |\Delta\tilde{x}_k^a| \to \infty \ with \ \ \Delta\tilde{x}_t^a \ \ close \ to \ zero \quad (22)$$

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

$$rank(\begin{bmatrix} I\lambda - A & -B \\ C & 0 \end{bmatrix}) = n + q - 1 \quad with \ \ |\lambda| > 1 \quad (23)$$

and $\lambda \notin sp(A)$ where $sp(A)$ represents the eigenvalues of A. Under (23), there exists ξ and g solution to

$$\begin{bmatrix} I\lambda - A & -B \\ C & 0 \end{bmatrix} \begin{bmatrix} \xi \\ g \end{bmatrix} = 0 \quad (24)$$

or equivalently

$$\begin{bmatrix} I\lambda - (A - BG) & -B \\ C & 0 \end{bmatrix} \begin{bmatrix} \xi \\ g - G\xi \end{bmatrix} = 0 \quad (25)$$

Under $g = G\xi$, (25) gives $(A - BG)\xi = \lambda\xi$ and $C\xi = 0$ showing that the invariant zero λ becomes an unobservable mode of the pair $(A - BG, C)$. With $G = g(\xi)^+$, $\Delta\tilde{x}_t^a = \alpha\xi$ and α close to zero, the solution $\Delta\tilde{x}_k^a = \alpha\xi\lambda^{k-t}$ to (19) shows that the goal (21) and (22) of the adversary is reached.

2.2 Passive model-based defender's view point

The attack model (19) and (20) can be rewritten

$$\Delta\tilde{x}_{k+1}^a = (A - BG)\Delta\tilde{x}_k^a + \xi\alpha\delta_{k,t-1} \quad (26)$$

$$\Delta\tilde{y}_k^a = C\Delta\tilde{x}_k^a \quad (27)$$

and $\Delta\tilde{x}_{t-1}^a = 0$ where $\alpha\delta_{k,t-1}$ is a pulse ($\delta_{k,t-1} = 0$ $\forall k \neq t-1$ and $\delta_{k,t-1} = 1$ when $k = t-1$) of size α triggered at time $t-1$. From (26), (27) and $d_k = -G\Delta\tilde{x}_k^a$ in (15) and (16), the augmented state model of the plant under attack is then described by

$$\begin{bmatrix} x_{k+1} \\ \Delta\tilde{x}_{k+1}^a \end{bmatrix} = \begin{bmatrix} A & -BG \\ 0 & A - BG \end{bmatrix} \begin{bmatrix} x_k \\ \Delta\tilde{x}_k^a \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} \bar{u}_k + \begin{bmatrix} 0 \\ \xi \end{bmatrix} \alpha\delta_{k,t-1} + \begin{bmatrix} I \\ 0 \end{bmatrix} w_k \quad (28)$$

$$y_k = [\, C \ 0 \,] \begin{bmatrix} x_k \\ \Delta\tilde{x}_k^a \end{bmatrix} + v_k \quad (29)$$

Let $\begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}_k^a \end{bmatrix} = T \begin{bmatrix} x_k \\ \Delta\tilde{x}_k^a \end{bmatrix}$ with $T = \begin{bmatrix} I & -I \\ 0 & I \end{bmatrix}$ so that (28) and (29) is equivalently rewritten

$$\begin{bmatrix} \tilde{x}_{k+1} \\ \Delta\tilde{x}_{k+1}^a \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & A - BG \end{bmatrix} \begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}_k^a \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} \bar{u}_k + \begin{bmatrix} -\xi \\ \xi \end{bmatrix} \alpha\delta_{k,t-1} + \begin{bmatrix} I \\ 0 \end{bmatrix} w_k \quad (30)$$

$$y_k = [\, C \ C \,] \begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}_k^a \end{bmatrix} + v_k \quad (31)$$

From $C\Delta\tilde{x}_k^a = 0$ $\forall k \succeq t$ in (31), the augmented state model (30) and (31) shows that $\Delta\tilde{x}_k^a$ is unobservable and that $\tilde{x}_k$ evolves in accordance with

$$\tilde{x}_{k+1} = A\tilde{x}_k + B\bar{u}_k - \xi\alpha\delta_{k,t-1} + w_k \quad (32)$$

$$y_k = C\tilde{x}_k + v_k \quad (33)$$

When α is chosen close to zero by the adversary (and ξ orthogonal to the eigenvectors of A associated with unstable eigenvalues, see Teixeira et al. (2012b)), the pulse $\alpha\delta_{k,t-1}$ in (32) and (33) has no any chance to be detected from anomaly detectors designed on the innovation sequence $\gamma_k = y_k - C\widehat{\tilde{x}}_{k/k-1}$ of the Kalman filter.

The proof that such attack can force the system out of its safe operating region and that the nominal control law (7) cannot interact with this result is not established in this paper.

3. ACTIVE DETECTOR FOR RESILIENT LQG CONTROLLER

This section considers that the IDS can disable the attack signal with a time delay. In our worst case scenario, we assume that the disabled delay is not always sufficiently small for the nominal LQG controller to maintain the system in its safe operating region and that the IDS cannot inform in real time the model-based anomaly detector (see Fig. 2).

When the IDS stop the false data injection at time $r > t$ so that $r - t \leq T$ where T is the maximum duration of the attack characterizing the performance of the IDS, $G = 0$ $\forall k \succeq r$ in (19) and (20) leads to

$$\Delta\tilde{x}_{k+1}^a = A\Delta\tilde{x}_k^a \quad (34)$$

$$\Delta\tilde{y}_k^a = C\Delta\tilde{x}_k^a \quad (35)$$

with $\Delta\tilde{x}^a_r = \alpha\xi\lambda^{r-t-1}$ or equivalently

$$\Delta\tilde{x}^a_{k+1} = A\Delta\tilde{x}^a_k + \xi\nu\delta_{k,r-1} \quad (36)$$
$$\Delta\tilde{y}^a_k = C\Delta\tilde{x}^a_k \quad (37)$$

with $\Delta\tilde{x}^a_{r-1} = 0$ where $\nu\delta_{k,r-1}$ is a pulse of size $\nu = \alpha\lambda^{r-t-1}$.

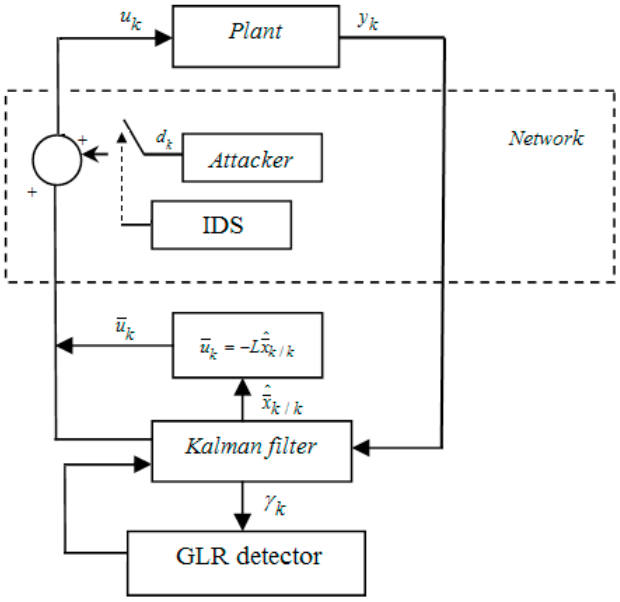

Fig. 2. NCS under attack with resilient LQG controller.

From (36), (37) in (30), (31) and α assumed close to zero, the model of the plant view by the controller $\forall k \succeq r$ becomes

$$\begin{bmatrix} \tilde{x}_{k+1} \\ \Delta\tilde{x}^a_{k+1} \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} \begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}^a_k \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} \bar{u}_k + \begin{bmatrix} 0 \\ \xi \end{bmatrix} \nu\delta_{k,r-1} + \begin{bmatrix} I \\ 0 \end{bmatrix} w_k \quad (38)$$

$$y_k = [\, C \;\; C \,] \begin{bmatrix} \tilde{x}_k \\ \Delta\tilde{x}^a_k \end{bmatrix} + v_k \quad (39)$$

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 refer to (38) and (39) is rewritten

$$\begin{bmatrix} x_{k+1} \\ \Delta\tilde{x}^a_{k+1} \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} \begin{bmatrix} x_k \\ \Delta\tilde{x}^a_k \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} \bar{u}_k + \begin{bmatrix} \xi \\ \xi \end{bmatrix} \nu\delta_{k,r-1} + \begin{bmatrix} I \\ 0 \end{bmatrix} w_k \quad (40)$$

$$y_k = [\, C \;\; 0 \,] \begin{bmatrix} x_k \\ \Delta\tilde{x}^a_k \end{bmatrix} + v_k \quad (41)$$

and can be reduced to

$$x_{k+1} = Ax_k + B\bar{u}_k + \xi\nu\delta_{k,r-1} + w_k \quad (42)$$
$$y_k = Cx_k + v_k \quad (43)$$

The size $\nu = \alpha\lambda^{r-t-1}$ of $\nu\delta_{k,r-1}$ in (42) and (43) (upper bounded by $\alpha\lambda^T$) is greater than the size α of $\alpha\delta_{k,t-1}$ in (32) and (33) via $|\lambda| > 1$ and the pulse $\nu\delta_{k,r-1}$ has now a chance to be detected from anomaly detectors. When the model of the plant switches from (32) and (33) to (42) and (43), the active model-based FDI scheme consists in detecting the hypothesized pulse $\nu\delta_{k,r-1}$ of unknown size ν and occurrence time r from the GLR test designed in Willsky and Jones (1976) as follows:

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 on (42) and (43) propagate as

$$e_{k+1/k} = (A - K_kC)e_{k/k-1} - K_kv_k + \xi\nu\delta_{k,r-1} + w_k \quad (44)$$
$$\gamma_k = Ce_{k/k-1} + v_k \quad (45)$$

The additive effect of $\nu\delta_{k,r-1}$ 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 by using (10), (11), (12), (13), and (14) on (4) and (5) can be expressed

$$e_{k+1/k} = \bar{e}_{k+1/k} + f(k, r-1)\nu \quad (46)$$
$$\gamma_k = \bar{\gamma}_k + g(k, r-1)\nu \quad (47)$$

where $f(k, r-1)$ and $g(k, r-1)$ are recursively computed as

$$f(k, r-1) = (A - K_kC)f(k-1, r-1) - \xi\delta_{k,r-1} \quad (48)$$
$$g(k, r-1) = Cf(k, r-1) \quad (49)$$

with $f(r-1, r-1) = 0$. Let H_0 the null hypothesis (no attack or presence of a stealthy attack) and H_1 the attack disappearance hypothesis at time r. The hypothesis H_1 can be confronted to the null hypothesis H_0 as follows

$$H_0 : E\{\gamma_j\} = 0,\ k \succeq j \succeq 0 \quad (50)$$
$$H_1 : E\{\gamma_j\} = g(j, r-1)\nu,\ k \succeq j \succeq r-1 \quad (51)$$

and

$$E\{\gamma_j\} = 0,\ r-1 > j \succeq 0 \quad (52)$$

Let $P(\gamma_j/H_1)$, $P(\gamma_j/H_0)$ the Gaussian probability density functions of γ_j conditioned on H_1, H_0 and define the likelihood ratio

$$\lambda(k, r-1) = \frac{P(\gamma_{r-1}/H_1)P(\gamma_r/H_1)...P(\gamma_k/H_1)}{P(\gamma_{r-1}/H_0)P(\gamma_r/H_0)...P(\gamma_k/H_0)} \quad (53)$$

From $g(r-1, r-1) = 0$ and $g(r, r-1) = 0$ via $C\xi = 0$, we have $P(\gamma_{r-1}/H_1) = P(\gamma_{r-1}/H_0)$, $P(\gamma_r/H_1) = P(\gamma_r/H_0)$ and the likelihood ratio (53) becomes

$$\lambda(k, r-1) = \frac{exp(-0.5 \sum_{j=r+1}^{k} \|\gamma_j - g(j, r-1)\nu\|^2_{\bar{Q}_j^{-1}})}{exp(-0.5 \sum_{j=r+1}^{k} \|\gamma_j\|^2_{\bar{Q}_j^{-1}})} \quad (54)$$

where $\bar{Q}_j = C\bar{P}_{j/j-1}C^T + V$ is the covariance of γ_j.

The maximum likelihood estimate of the pulse magnitude ν conditioned on r is given by

$$\hat{\nu}(k, r-1) = a(k, r-1)^{-1}b(k, r-1) \quad (55)$$

where

$$a(k,r-1) = \sum_{j=r+1}^{k} [g_{j,r-1}^T (\bar{Q}_j)^{-1} g_{j,r-1}] \quad (56)$$

$$b(k,r-1) = \sum_{j=r+1}^{k} [g_{j,r-1}^T (\bar{Q}_j)^{-1} \gamma_j] \quad (57)$$

After having replaced ν by $\hat{\nu}(k,r-1)$ in (54), the log-likelihood ratio $T(k,r-1) = 2\log(\lambda(k,r-1))$ can be expressed from the normalized estimate $\widehat{\overline{\nu}}(k,r-1) = a(k,r-1)^{-1/2} b(k,r-1)$ of the pulse conditioned on H_1 as $T(k,r-1) = \widehat{\overline{\nu}}(k,r-1)^2$ and the decision rules of the GLR detector becomes

$$T(k) = \max_{r \in [\,0\ k-1\,]} \left\{ \widehat{\overline{\nu}}(k,r-1)^2 \right\} \underset{H_0}{\overset{H_1}{\gtrless}} \mu \quad (58)$$

where μ is the decision level. For a real time implementation of (58), the maximization can be realized on a sliding window of limited size. False alarms, missed detections and good decisions rates depend on the choice of the decision level and on the size of the sliding window. We refer the reader to Basseville and Nikiforov (1993) for optimal solutions to the sequential change detection under performance criteria or to Do et al. (2014) for optimal solution to the quickest change detection problem dedicated to covert attacks. When $T(k) > \mu$, the ability of the Kalman filter to track the suddenly observable consequence of the attack is increased from the following updating strategy

$$\widehat{\overline{x}}_{k/k}^{new} = \widehat{\overline{x}}_{k/k}^{old} + f(k,\hat{r}-1)\hat{\nu}(k,\hat{r}-1) \quad (59)$$

$$\bar{P}_{k/k}^{new} = \bar{P}_{k/k}^{old} + f(k,\hat{r}-1)a(k,\hat{r}-1)^{-1} f(k,\hat{r}-1)^T \quad (60)$$

where

$$\widehat{r} = \arg\Big(\max_{r \in [\,k-1-M\ \ k-1\,]} \left\{ \widehat{\overline{\nu}}(k,r-1)^2 \right\} \Big) \quad (61)$$

is the attack disappearance time estimate and $a(k,\hat{r}-1)^{-1}$ in (60) the covariance of $\hat{\nu}(k,\hat{r}-1)$. The resilient LQG controller is then obtained with (59), (60) and (61) applied on the Kalman filter associated to the infinite horizon LQG controller of section 2. To evaluate the overall characteristic of the obtained resilient LQG controller, a performance criterion need to be studied in relation with the maximum duration T of the attack signal. As shown in the illustrative example given in section 4, the resilient LQG controller works very well when a zero dynamic attack significantly impacts the state variables of the plant before to be stopped by the IDS.

4. NUMERICAL EXAMPLE

The following linear discrete-time stochastic system

$$A = \begin{bmatrix} 0.6 & 0 & 0.34 & 0.35 \\ 0 & 0.8 & 0 & 0.37 \\ 0 & 0 & 0.5 & 0 \\ 0 & 0 & 0 & 0.9 \end{bmatrix}, \; B = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 2 \\ 0 & 1 & 1 \end{bmatrix},$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (62)$$

of real instable invariant zero $z_0 = 1.18$ is attacked on its vulnerability by a zero dynamic attack occurring at time $t = 40$ and stopped by the IDS at time $r = 70$ (see Fig. 3).

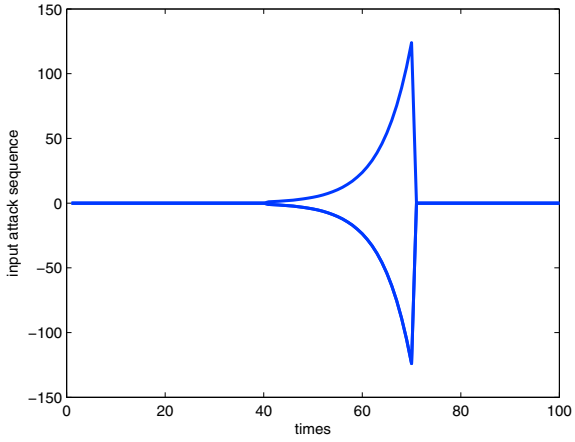

Fig. 3. Zero dynamic attack sequence.

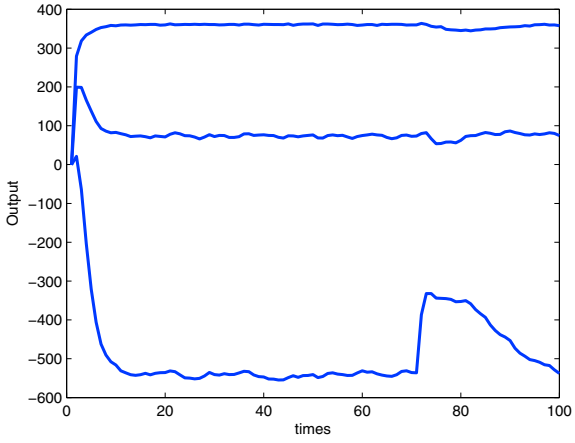

Fig. 4. Regulated outputs (LQG controller).

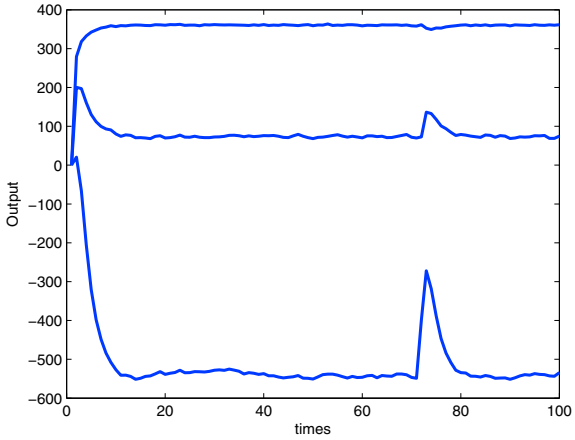

Fig. 5. Regulated outputs (Resilient LQG controller).

Standard LQG controller: The consequences of the zero dynamic attack on regulated outputs designed with $V = R = I_3$, $W = 0.01 I_4$ and $Q = I_4$ are plotted on Fig. 4.

Resilient LQG controller: The consequences of the zero dynamic attack on regulated outputs are plotted on Fig. 5. Compared to the regulated outputs of Fig. 4 obtained with the standard LQG controller, Fig. 5 shows that the updating strategy (59), (60) and (61) allows to recover more quickly the nominal behavior of the networked control system.

By representing the plant subject to multiple zero dynamic attack 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 as explained in Sauter et al. (2006) or Pasqualetti (2012).

5. CONCLUSION

After having represented a plant under zero dynamic attack of finite duration as a linear time-invariant system subject to two sequential pulses, the first at the occurrence time of the attack and the second at the disappearance time of the attack, this paper has presented a resilient LQG controller obtained by increasing the tracking ability of the Kalman filter at the attack disappearance time estimate.

REFERENCES

Amin, S., Cárdenas, A.A., and Sastry, S.S. (2009). Safe and secure networked control systems under denial-of-service attacks. In *Hybrid Systems: Computation and Control*, 31–45. Springer.

Basseville, M. and Nikiforov, I.V. (1993). *Detection of Abrupt Changes: Theory and Application*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA.

Brunner, M., Hofinger, H., Krauß, C., Roblee, C., Schoo, P., and Todt, S. (2010). Infiltrating critical infrastructures with next-generation attacks. *Fraunhofer Institute for Secure Information Technology (SIT), Munich*.

Cardenas, A.A., Amin, S., and Sastry, S. (2008). Secure control: Towards survivable cyber-physical systems. *System*, 1.

Ding, S.X. (2008). *Model-based fault diagnosis techniques*, volume 2013. Springer.

Do, V.L., Fillatre, L., and Nikiforov, I.V. (2014). A statistical method for detecting cyber/physical attacks on scada systems. *IEEE Multi-conference on Systems and Control (MSC), Antibe*.

Fovino, I.N., Coletta, A., and Masera, M. (2010). Taxonomy of security solutions for scada sector. *JRC-Joint Research Centre of the European Commission*.

Frank, P.M. (1990). Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results. *Automatica*, 26(3), 459–474.

Giani, A., Sastry, S., Johansson, K.H., and Sandberg, H. (2009). The viking project: an initiative on resilient control of power networks.

Hespanha, J.P., Naghshtabrizi, P., and Xu, Y. (2007). A survey of recent results in networked control systems. *Proceedings of the IEEE*, 95(1), 138.

Keller, J.Y. and Sauter, D. (2011). Restricted diagonal detection filter and updating strategy for multiple fault detection and isolation. *International Journal of Adaptive Control and Signal Processing*, 25(1), 68–87.

Keller, J.Y. and Sauter, D. (2013). Monitoring of stealthy attack in networked control systems. In *2nd International Conference on Control and Fault-Tolerant Systems, SysTol'13*, CID, CDROM. Nice, France.

Keller, J., Chabir, K., and Sauter, D. (2014). Input reconstruction for networked control systems subject to deception attacks and data losses on control signals. *International Journal of Systems Science*, (ahead-of-print), 1–7.

Krutz, R.L. (2005). *Securing SCADA systems*. John Wiley & Sons.

Liu, Y., Ning, P., and Reiter, M.K. (2009). False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, 21–32. ACM, New York, NY, USA.

Mo, Y. and Sinopoli, B. (2009). Secure control against replay attacks. In *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, 911–918. IEEE.

Pasqualetti, F. (2012). *Secure control systems: A control-theoretic approach to cyber-physical security*. Ph.D. thesis, Citeseer.

Pasqualetti, F., Dörfler, F., and Bullo, F. (2012). Cyber-physical security via geometric control: Distributed monitoring and malicious attacks. In *CDC*, 3418–3425.

Patton, R.J. and Chen, J. (1999). Robust model-based fault diagnosis for dynamic systems.

Sauter, D., Boukhobza, T., and Hamelin, F. (2006). Decentralized and autonomous design for fdi/ftc of networked control systems.

Smith, R.S. (2011). A decoupled feedback structure for covertly appropriating networked control systems. *Proc. IFAC World Congress*, 90–95.

Stouffer, K., Falco, J., and Scarfone, K. (2007). Guide to industrial control systems (ics) security. *NIST Special Publication*, 800(82), 16–16.

Teixeira, A., Pérez, D., Sandberg, H., and Johansson, K.H. (2012a). Attack models and scenarios for networked control systems. In *Proceedings of the 1st international conference on High Confidence Networked Systems*, 55–64. ACM.

Teixeira, A., Sandberg, H., and Johansson, K.H. (2010). Networked control systems under cyber attacks with applications to power networks. In *American Control Conference (ACC), 2010*, 3690–3696. IEEE.

Teixeira, A., Shames, I., Sandberg, H., and Johansson, K.H. (2012b). Revealing stealthy attacks in control systems. In *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, 1806–1813. IEEE.

Willsky, A.S. and Jones, H.L. (1976). A generalized likelihood ratio approach to the detection and estimation of jumps in linear systems. *Automatic Control, IEEE Transactions on*, 21(1), 108–112.

Zhang, Y. and Jiang, J. (2008). Bibliographical review on reconfigurable fault-tolerant control systems. *Annual reviews in control*, 32(2), 229–252.