HAL
open science

Input reconstruction for networked control systems subject to deception attacks and data losses on control signals

Jean-Yves Keller, Karim Chabir, Dominique Sauter

To cite this version:

Jean-Yves Keller, Karim Chabir, Dominique Sauter. Input reconstruction for networked control systems subject to deception attacks and data losses on control signals. International Journal of Systems Science, 2016, 47 (4), pp.814-820. 10.1080/00207721.2014.906683 . hal-01094322

HAL Id: hal-01094322

https://hal.science/hal-01094322

Submitted on 16 Dec 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Input reconstruction for networked control systems subject to deception attacks and data losses on control signals

J.Y. Keller, K. Chabir, D. Sauter

University of Lorraine, CRAN-CNRS UMR 7039,
BP 239, 54506 Vandoeuvre les Nancy, France.

Corresponding author:
J.Y. Keller; phone: +33(0)3 83 82 90 49; e-mail: jean-yves.keller@univ-lorraine.fr.

***Abstract*- State estimation of stochastic discrete-time linear systems subject to unknown inputs or constant biases has been widely studied but no work has been dedicated to the case where a disturbance switches between unknown input and constant bias. We show that such disturbance can affect a networked control system subject to deception attacks and data losses on the control signals transmitted by the controller to the plant. This paper proposes to estimate the switching disturbance from an augmented state version of the intermittent unknown input Kalman filter recently developed by the authors. Sufficient stochastic stability conditions are established when the arrival binary sequence of data losses follows a Bernoulli random process.**

***Keywords*-Kalman filter, intermittent unknown inputs, cyber-attacks.**

1. Introduction

Recent technological advances are revolutionizing our ability to build massively distributed Networked Control Systems (NCS) exchanging information from communication networks. Critical infrastructures such that power grids, water distribution networks and transport systems are examples of Cyber-Physical Systems (CPS). These systems consist in large-scale physical processes monitored and controlled by SCADA (supervisory control and data acquisition) systems running over a heterogeneous set of communication networks and computers. The design of control systems taking into account random data losses and/or packet delays due to communication networks have been widely studied (see Hespanha *et al.* 2007 or Hu *et al.* 2012 and references therein). Used for the NCS monitoring or in state feedback control laws based observers, the Kalman filtering with random lost of observations represented by Markovian or Bernoulli processes has been also widely studied (Sinopoli *et al.* 2004, Liu and Goldsmith 2004, Schenato *et al.* 2007, Shi *et al.* 2010, Yang *et al.* 2011). More recently, the vulnerabilities analysis of CPS to attacks triggered through unreliable communication networks has received increasing attention (Cardenas *et al.* 2008). Attacks to NCS are summarized as follows: Denial of Service (DoS) attacks (Amin *et al.* 2009) when the adversary prevents the controller from received sensor measurement or the plant from received control law, deception attacks (Liu *et al.* 2009, Teixeira *et al.* 2010, Pasqualetti *et al.* 2012) when the adversary sends false information on sensors or actuators, replay attacks (Mo and Sinopoli 2010), when the adversary generates artificial measurement delays, covert attacks (Smith 2011) when the adversary takes the control of the plant, and finally direct physical attacks on the plant (including sensors and actuators) closes to traditional faults taken into account by Fault Detection and Isolation (FDI) techniques (Chen and Patton 1996 and references therein).

This paper assumes that an attacker located inside the network of the NCS can add false data on the control signal transmitted by the controller to the plant. Our goal is to solve the state filtering problem of NCS subject to mixed deception attack and random packet dropouts. When the corrupted control signal is received by the plant, the Unknown Inputs Kalman Filter (UIKF) (Kitanidis 1987, Chen and Patton 1996, Darouach and Zasadzinski 1997, Hou and Patton 1998) should be used to jointly estimate the state of the system and the exogenous unknown input (attacks are modeled as unknown inputs in a great number of papers, see Pasqualetti *et al.* 2012 and references therein). When the corrupted control signal is blocked to its previous value at the occurrence times of data losses, the unknown input is transformed to a constant bias at the input of the plant. Even if the Augmented State Kalman Filter (ASKF) (Alouani *et al*. 1992, Kim *et al.* 2006, Ignagni 2000) should be used to estimate the constant bias, no work has been dedicated to estimate a disturbance that switches between unknown input and constant bias at the occurrence times of packet dropouts, probably because such

disturbance leads to a variable dimensional state in the state model of the plant viewed by the controller.

This paper avoids the use of a variable dimensional state model by forcing the intermittent unknown input to be the complementary state of the intermittent bias. The resulting fixed dimensional augmented state model of the plant is used to estimate the switching disturbance from an augmented state version of the Intermittent Unknown Input Kalman Filter (IIKF) (Keller and Sauter 2013). Necessary and sufficient stochastic stability conditions are established when the arrival sequence of data losses follows a Bernoulli random process.

The paper is organized as follows: Section 2 presents the augmented state model of the plant. Section 3 designs the Augmented State IIKF (ASIIKF) and studies its stochastic stability conditions. Section 4 gives a numerical example before to conclude at section 5.

2. Problem statement

Considers a plant represented by the following discrete-time stochastic linear system

$$x_{k+1}=Ax_k+Bu_k+w_k \tag{2.1}$$

$$y_k^*=Cx_k+\varepsilon_k \tag{2.2}$$

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 $\varepsilon_k\in\Re^m$ are zero mean uncorrelated Gaussian random sequences with

$$E\left\{\begin{bmatrix} w_k \\ \varepsilon_k \end{bmatrix}\begin{bmatrix} w_j \\ \varepsilon_j \end{bmatrix}^T\right\}=\begin{bmatrix} W & 0 \\ 0 & I \end{bmatrix}\delta_{k,j} \text{ with } W\geq 0 \tag{2.3}$$

The initial state x_0, uncorrelated with w_k and v_k, is a Gaussian random variable with $E\{x_0\}=\bar{x}_0$ and $P_0=E\{(x_0-\bar{x}_0)(x_0-\bar{x}_0)^T\}\geq 0$. We assume $rank(C)=m$, $rank(B)=q$, (A,C) detectable and $rank(CB)=q\leq m$.

The plant is controlled in the following NCS:

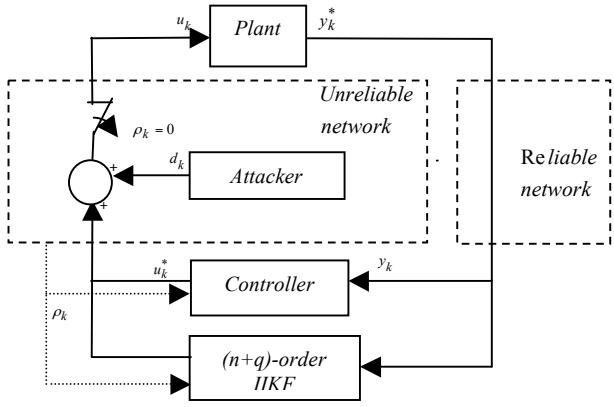

Fig.1: NCS subject to deception attacks and random data losses.

The binary variable $\rho_k\in\{0,1\}$ represents the acknowledgement signal indicating the status of reception/delivery (TCP for example) with $\rho_k=1$ when the control signal u_k^* transmitted by the controller is received by the plant or $\rho_k=0$ when u_k^* is lost on the unreliable network.

From the following blocking logic

$$u_k=(1-\rho_k)u_{k-1}+\rho_k u_k^* \tag{2.4}$$

we consider that actuators use the past value of the control signal when u_k^* is lost. The study of u_k^* is not the purpose of this paper.

We assume that the attacker can corrupt the control signal received by the plant as $u_k=u_k^*+d_k$ when $\rho_k=1$ where d_k represents the attack signal. The output of the plant y_k^* is transmitted to the controller via a reliable network ensuring $y_k=y_k^*$ at any time.

Under attack, (2.4) can be rewritten

$$u_k = \bar{u}_k + \nu_k \tag{2.5}$$

$$\bar{u}_k = (1-\rho_k)\bar{u}_{k-1} + \rho_k u_k^* \tag{2.6}$$

$$\nu_k = (1-\rho_k)\nu_{k-1} + \rho_k d_k \tag{2.7}$$

where $\bar{u}_k$ in (2.6) is known to the controller having access to the binary sequence $\{\rho_j\}_0^k$ and where the hybrid disturbance ν_k in (2.7) switches between unknown input $\nu_k = d_k$ when $\rho_k = 1$ and constant bias $\nu_k = \nu_{k-1}$ when $\rho_k = 0$.

By rewriting the hybrid disturbance (2.7) as a constant bias

$$\nu_k = \nu_{k-1} + d_k^\rho \tag{2.8}$$

driven by a bias dependent intermittent unknown input

$$d_k^\rho = \rho_k (d_k - \nu_{k-1}) \tag{2.9}$$

we can derive the following $(n+q)$-order linear (time-invariant) state model of the plant

$$X_{k+1} = \bar{A}X_k + \bar{B}\bar{u}_k + \bar{F}d_k^\rho + \bar{w}_k \tag{2.10}$$

$$y_k = \bar{C}X_k + \varepsilon_k \tag{2.11}$$

with $X_k = \begin{bmatrix} x_k \\ \nu_{k-1} \end{bmatrix} \in \Re^{n+q}$, $\bar{A} = \begin{bmatrix} A & B \\ 0 & I \end{bmatrix}$, $\bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}$, $\bar{F} = \begin{bmatrix} B \\ I \end{bmatrix}$, $\bar{C} = [C \;\; 0]$, $\bar{w}_k = \begin{bmatrix} w_k^T & 0 \end{bmatrix}^T$ and $E\{\bar{w}_k \bar{w}_j^T\} = \bar{W}\delta_{k,j}$ where $\bar{W} = \begin{bmatrix} W & 0 \\ 0 & 0 \end{bmatrix}$.

This paper shows how to derive the unbiased minimum variance estimates $\hat{\nu}_{k-1/k}$ of the switching disturbance ν_k from the ASIIKF designed on (2.10) and (2.11) and how to establish the sufficient stochastic stability conditions when ρ_k follows a random Bernoulli process with $\lambda = Pr[\rho_k = 1]$.

3. Switching disturbance reconstruction

The implementation of the $(n+q)$-order ASIIKF is explained in the following theorem.

Theorem 3.1: The ASIIKF is described by a standard Kalman filter

$$\hat{X}_{k/k} = \begin{bmatrix} \hat{x}_{k/k} \\ \hat{\nu}_{k-1/k} \end{bmatrix} = (I - \bar{K}_k\bar{C})(\hat{X}_{k/k-1} + \bar{F}\hat{d}_k^\rho) + \bar{K}_k y_k \tag{3.1}$$

$$P_{k/k} = (I - \bar{K}_k\bar{C})(P_{k/k-1} + \bar{F}Q_k^\rho\bar{F}^T)(I - \bar{K}_k\bar{C})^T + \bar{K}_k\bar{K}_k^T \tag{3.2}$$

$$\hat{X}_{k+1/k} = \bar{A}\hat{X}_{k/k} + \bar{B}\bar{u}_k \tag{3.3}$$

$$P_{k+1/k} = \bar{A}P_{k/k}\bar{A}^T + \bar{W} \tag{3.4}$$

with $\bar{K}_k = P_{k/k-1}\bar{C}^T H_k^{-1}$ and $H_k = \bar{C}P_{k/k-1}\bar{C}^T + I$ updated online from the intermittent unknown input estimate $\hat{d}_k^\rho$ of covariance $Q_k^\rho = E\{(\hat{d}_k^\rho - E\{\hat{d}_k^\rho\})(\hat{d}_k^\rho - E\{\hat{d}_k^\rho\})^T\}$ with $E\{\hat{d}_k^\rho\} = d_{k-1}^\rho$ given by

$$\hat{d}_k^\rho = \rho_{k-1}[(CB)^T H_k^{-1} CB]^{-1}(CB)^T H_k^{-1}(y_k - \bar{C}\hat{X}_{k/k-1}) \tag{3.5}$$

$$Q_k^\rho = \rho_{k-1}[(CB)^T H_k^{-1} CB]^{-1} \tag{3.6}$$

The ASIIKF is initialized with $\hat{X}_{0/-1} = \begin{bmatrix} \bar{x}_0 \\ 0 \end{bmatrix}$, $P_{0/-1} = \begin{bmatrix} P_0 & 0 \\ 0 & 0 \end{bmatrix}$ and $\rho_{-1} = 0$.

Proof. Consider the following linear state filter

$$\hat{X}_{k/k} = \hat{X}_{k/k-1} + K_k(y_k - \bar{C}\hat{X}_{k/k-1}) \tag{3.7}$$

$$P_{k/k} = (I - K_k\bar{C})P_{k/k-1}(I - K_k\bar{C})^T + K_k K_k^T \tag{3.8}$$

$$\hat{X}_{k+1/k} = \bar{A}\hat{X}_{k/k} + \bar{B}\bar{u}_k \tag{3.9}$$

$$P_{k+1/k} = \bar{A}P_{k/k}\bar{A}^T + \bar{W} \tag{3.10}$$

where $\hat{X}_{k/k-1}$ is the state prediction of covariance $P_{k/k-1} = E\{(X_k - \hat{X}_{k/k-1})(X_k - \hat{X}_{k/k-1})^T\}$ based on measurements available until time $k-1$ and $\{\rho_j\}_0^{k-1}$,

$\hat{X}_{k/k}$ the estimate of X_k of covariance matrix $P_{k/k}=E\{(X_k-\hat{X}_{k/k})(X_k-\hat{X}_{k/k})^T\}$ based on measurements available until time k and $\{\rho_j\}_0^{k-1}$. The attack signal d_k and the binary variable ρ_k are both considered as deterministic in the design of the filter:

From (2.10), (3.1) and (3.3), the state prediction error $e_{k/k-1}=X_k-\hat{X}_{k/k-1}$ and the state estimation error $e_{k/k}=X_k-\hat{X}_{k/k}$ propagate as

$$e_{k/k-1}=\bar{A}e_{k-1/k-1}+\bar{F}d_{k-1}^{\rho}+\bar{w}_{k-1} \tag{3.11}$$

$$e_{k/k}=(I-K_k\bar{C})e_{k/k-1}-K_k\varepsilon_k \tag{3.12}$$

At initial time, $E\{e_{0/0}\}=0$. Assume $E\{e_{k-1/k-1}\}=0$ at time $k-1$. From (3.11) and (3.12), we have $E\{e_{k/k}\}=(I-K_k\bar{C})\bar{F}\bar{d}_{k-1}^{\rho}$ and thus $E\{e_{k/k}\}=0$ if and only if K_k satisfies the algebraic constraint $(I-K_k\bar{C})\bar{F}\bar{d}_{k-1}^{\rho}=0$ rewritten via (2.9) as

$$(I-K_k\bar{C})\bar{F}=0 \quad \text{when} \quad \rho_{k-1}=1 \tag{3.13}$$

The hybrid gain K_k minimizing $tr(P_{k/k})$ subject to (3.13) is given by

$$K_k=\bar{K}_k+\rho_{k-1}(I-\bar{K}_k\bar{C})\bar{F}[(CB)^T H_k^{-1}CB]^{-1}(CB)^T H_k^{-1} \tag{3.14}$$

leading to the ASIIKF of theorem 3.1 after some manipulations (Keller and Sauter 2012).

End of proof

Note that data losses have a benefic filtering effect on the estimate $\hat{v}_{k-1/k}$, the algebraic constraint (3.13) disappearing when $\rho_{k-1}=0$.

The Riccati Difference Equation (RDE) of the ASIIKF is described by

$$P_{k+1/k}=(\bar{A}-\bar{A}K_k\bar{C})P_{k/k-1}(\bar{A}-\bar{A}K_k\bar{C})^T+\bar{A}K_kK_k^T\bar{A}^T+\bar{W} \tag{3.15}$$

with K_k given by (3.14). Define the following Riccati operators

$$f_0(X)=\bar{A}X\bar{A}^T+\bar{W}-\bar{A}X\bar{C}^T(\bar{C}X\bar{C}^T+I)^{-1}\bar{C}X\bar{A}^T \tag{3.16}$$

$$f_1(X)=\tilde{\bar{A}}X\tilde{\bar{A}}^T+\tilde{\bar{W}}-\tilde{\bar{A}}X\tilde{\bar{C}}^T(\tilde{\bar{C}}X\tilde{\bar{C}}^T+\Sigma\Sigma^T)^{-1}\tilde{\bar{C}}X\tilde{\bar{A}}^T \tag{3.17}$$

with $\tilde{\bar{A}}=\bar{A}-\bar{A}\bar{F}(CB)^+\bar{C}$, $\tilde{\bar{W}}=\bar{W}+\bar{A}\bar{F}(CB)^+(CB)^{+T}\bar{F}^T\bar{A}^T$, $\tilde{\bar{C}}=\Sigma\bar{C}$, $\Sigma=\beta(I-CB(CB)^+)$ and $\beta\in\Re^{m-q,m}$ so that $rank(\Sigma)=m-q$. As shown by Keller and Sauter (2013), the ASIIKF's RDE (3.15) can take the form of a switching standard RDE

$$P_{k+1/k}=(1-\rho_{k-1})f_0(P_{k/k-1})+\rho_{k-1}f_1(P_{k/k-1}) \tag{3.18}$$

Let $E\{P_{k+1/k}\}$ the mathematical expectation of $P_{k+1/k}$ taken with respect to the random sequence $\{\rho_j\}_0^k$ and λ_c the critical data arrival rate (Sinopoli *et al.* 2004) so that $\lim_{k\to\infty}E\{P_{k/k-1}\}<\infty$ when $\lambda\le\lambda_c$ or $\lim_{k\to\infty}E\{P_{k/k-1}\}\to\infty$ when $\lambda>\lambda_c$.

Theorem 3.2: We have

$$\lim_{k\to\infty}E\{P_{k+1/k}\}<\infty \quad \forall\lambda\in[0\ \breve{\lambda}] \tag{3.19}$$

if there exists $\bar{K}\in\Re^{n+q,m}$, $\tilde{\bar{K}}\in\Re^{n+q,m-q}$ and $0<Y<I$ so that $\Psi_{\lambda}(Y)>0$ with

$$\Psi_{\lambda}(Y)=\begin{bmatrix} Y & \sqrt{(1-\lambda)}(Y\bar{A}+\bar{K}\bar{C}) & \sqrt{\lambda}(Y\tilde{\bar{A}}+\tilde{\bar{K}}\tilde{\bar{C}}) \\ \sqrt{(1-\lambda)}(Y\bar{A}+\bar{K}\bar{C})^T & Y & 0 \\ \sqrt{\lambda}(Y\tilde{\bar{A}}+\tilde{\bar{K}}\tilde{\bar{C}})^T & 0 & Y \end{bmatrix} \tag{3.20}$$

The lower bound $\breve{\lambda}$ of λ_c is solution to the LMI (Linear Matrix Inequality) feasibility problem $\breve{\lambda}=arg\left\{\max_{\lambda}\Psi_{\lambda}(Y)>0\right\}$. Under

$$rank\begin{bmatrix} -Iz+\bar{A} & \bar{F} \\ \bar{C} & 0 \end{bmatrix}=n+2q, \forall|z|\ge 1 \tag{3.21}$$

we have also

$$\lim_{k\to\infty}P_{k+1/k}<\infty \quad \forall\lambda\in[0\ 1] \tag{3.22}$$

Proof. From (3.18), the mean covariance $E\{P_{k+1/k}\}$ gives

$$E\{P_{k+1/k}\}=(1-\lambda)E\{f_0(P_{k/k-1})\}+\lambda E\{f_1(P_{k/k-1})\} \tag{3.23}$$

The Riccati operators (3.16) and (3.17) are concave, increase with X and the Jensen's inequality gives

$$E\{P_{k+1/k}\}\leq(1-\lambda)f_0(E\{P_{k/k-1}\})+\lambda f_1(E\{P_{k/k-1}\}) \tag{3.24}$$

A deterministic upper bound S_{k+1} of $E\{P_{k+1/k}\}$ so that $E\{P_{k+1/k}\}\leq S_{k+1}$ is then solution to the modified RDE

$$S_{k+1}=(1-\lambda)f_0(S_k)+\lambda f_1(S_k) \tag{3.25}$$

with $S_0=P_{0/-1}\geq 0$. Let

$$S=(1-\lambda)f_0(S)+\lambda f_1(S) \tag{3.26}$$

the modified ARDE associated to (3.25). Sinopoli *et al.* (2004) have shown that there exists a stabilizing solution $S\geq 0$ to (3.26) if there exists $\bar{K}$, $\tilde{\bar{K}}$ and $X>0$ so that

$$\begin{aligned} X>&(1-\lambda)[(\bar{A}-\bar{K}\bar{C})X(\bar{A}-\bar{K}\bar{C})^T+\bar{K}\bar{K}^T+\bar{W}] \\ &+\lambda[(\tilde{\bar{A}}-\tilde{\bar{K}}\tilde{\bar{C}})X(\tilde{\bar{A}}-\tilde{\bar{K}}\tilde{\bar{C}})^T+\tilde{\bar{K}}\Sigma\Sigma^T\tilde{\bar{K}}+\tilde{\bar{W}}] \end{aligned} \tag{3.27}$$

or equivalently if there exists $\bar{K}$, $\tilde{\bar{K}}$ and $0<\bar{Y}\leq 1$ so that $\Psi_\lambda(Y)>0$ with $\Psi_\lambda(Y)$ given by (3.20). We have also $P_{k+1/k}\leq\hat{P}_{k+1/k}$ where $\hat{P}_{k+1/k}$ is generated by the ASIIKF's RDE (3.18) under $\rho_k=1\ \forall k\geq 0$ described by $\hat{P}_{k+1/k}=f_1(\hat{P}_{k/k-1})$ with $\hat{P}_{0/-1}=P_{0/-1}\geq 0$. Darouach and Zasadzinski (1997) have shown that $\lim_{k\to\infty}\hat{P}_{k+1/k}<\infty$ under the necessary and sufficient rank condition (3.21).

End of proof

When $m=q$, we have $\tilde{\bar{K}}=0$ in (3.20) and the stochastic stability conditions of the ASIIKF become dual to those obtained by Sinopoli *et al.* (2004) for the Kalman filter with intermittent observations.

4. Numerical example

Considers the NCS of figure 1 and the following minimum phase plant $A=\begin{bmatrix}0.6 & 0.5 & 0.1 & 0\\ 0 & 0.3 & -0.6 & -0.1\\ 0 & 0 & 0.4 & 0.3\\ 0 & 0 & 0 & 0.7\end{bmatrix}$, $B=\begin{bmatrix}0 & 0\\ 1 & 0\\ 0 & 0\\ 0 & 1\end{bmatrix}$, $C=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$, $W=0.01I$. Under (3.21), there exists no instable invariant zeros and the attacker cannot generate zero dynamic attacks (Teixeira *et al.* 2012). This explain why the attack signal $d_k=[d_k^1\ d_k^2]^T$ is here chosen randomly and why our numerical simulation is restricted to a comparative study between the proposed ASIIKF and the standard unknown input Kalman filter (the standard unknown input Kalman filter, called here the ASUIKF, is derived from the ASIIKF with $\rho_k=1\ \forall k\geq 0$ in theorem 3.1), both used for the reconstruction of $v_k=[v_k^1\ v_k^2]$. The binary variable ρ_k is plotted on figure 2 with $\lambda=0.3$ chosen very low to accentuate the benefic effect of data losses on $\hat{v}_{k-1/k}=[\hat{v}_{k-1/k}^1\ \hat{v}_{k-1/k}^2]^T$. Figure 3 shows $tr(P_{k/k-1})$, its upper bound $tr(\hat{P}_{k/k-1})$ and the upper bound $tr(S_k)$ of $tr(E\{P_{k/k-1}\})$. The switching disturbance v_k^1 and its one period time delayed estimate $\hat{v}_{k-1/k}^1$ given by the ASIIKF are plotted on figure 4. Figure 5 shows the estimate $\hat{v}_{k-1/k}^1$ generated by the ASUIKF. The switching disturbance v_k^2 and its one period time delayed estimate $\hat{v}_{k-1/k}^2$ given by the ASIIKF are plotted on figure 6. Figure 7 shows the estimate $\hat{v}_{k-1/k}^2$ generated by the ASUIKF. The state estimation errors $e_{k/k}^1=x_k^1-\hat{x}_{k/k}^1$, $e_{k/k}^2=x_k^2-\hat{x}_{k/k}^2$, $e_{k/k}^3=x_k^3-\hat{x}_{k/k}^3$ and

$e^4_{k/k}=x^4_k-\hat{x}^4_{k/k}$ obtained from the ASIIKF and the ASUIKF are plotted on figures 8, 9, 10 and 11. We can see that the ASIIKF gives better filtering results, especially under successive data losses. Figure 12 also shows the accumulative state estimation error $\sum_{j=0}^{k}\sum_{i=1}^{4}\left|e^i_{j/j}\right|$.

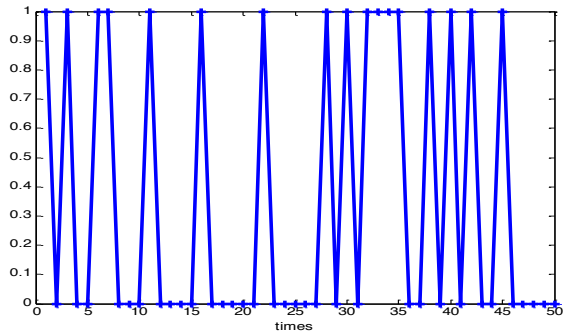

Fig. 2: Binary sequence ρ_k .

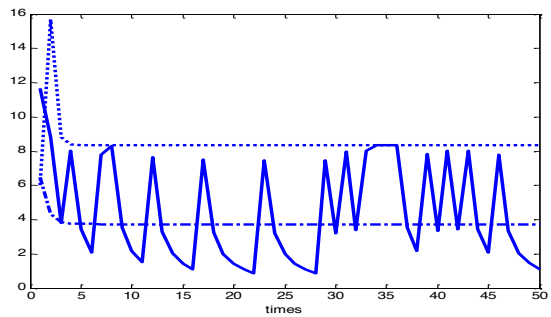

Fig. 3: $tr(P_{k/k-1})$(solid line), $tr(\hat{P}_{k/k-1})$(dotted line) $tr(S_k)$(dashdot line).

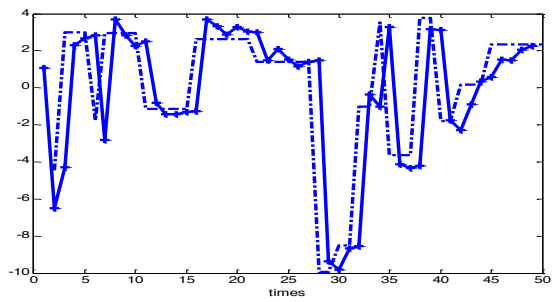

Fig. 4: v^1_k (dashdot line) and its estimate $\hat{v}^1_{k-1/k}$(solid line).

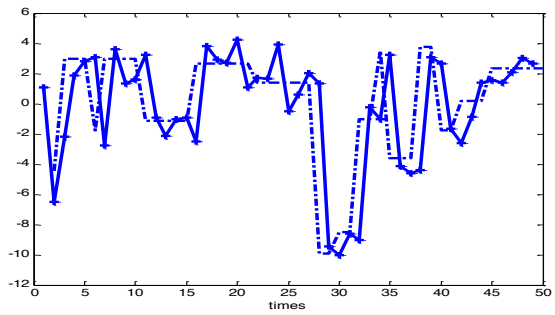

Fig. 5: $\hat{v}^1_{k-1/k}$ given by the ASUIKF.

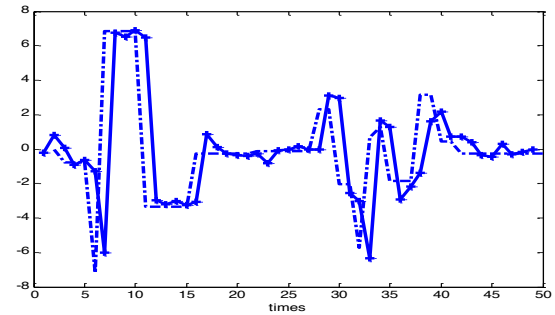

Fig. 6: v^2_k (dashdot line) and its estimate $\hat{v}^2_{k-1/k}$(solid line).

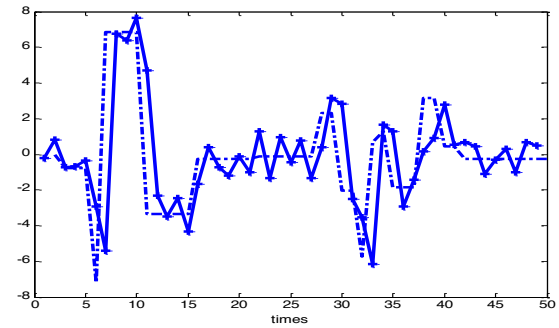

Fig. 7: $\hat{v}^2_{k-1/k}$ given by the ASUIKF.

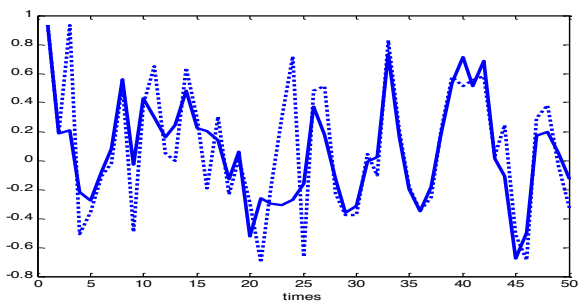

Fig. 8: First state estimation error: ASIIKF (solid line), ASUIKF (dotted line).

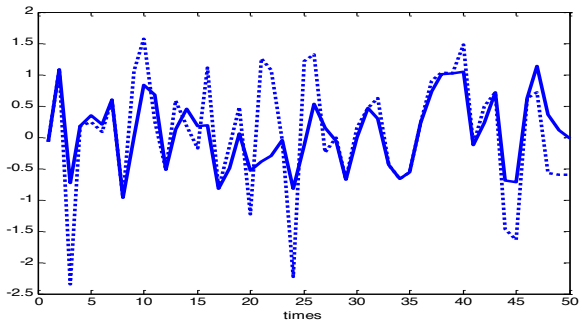

Fig. 9: Second state estimation error: ASIIKF (solid line), ASUIKF (dotted line).

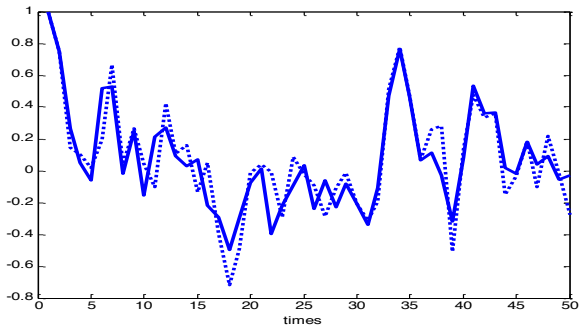

Fig. 10: Third state estimation error: ASIIKF (solid line), ASUIKF (dotted line).

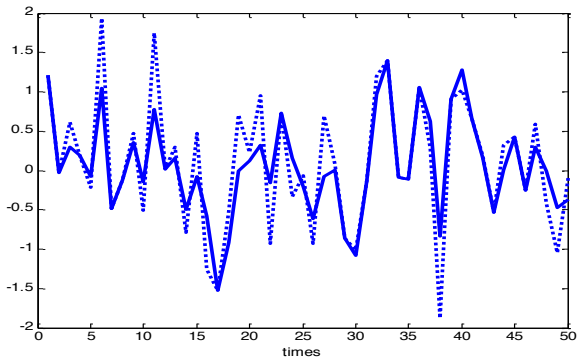

Fig. 11: Fourth state estimation error: ASIIKF (solid line), ASUIKF (dotted line).

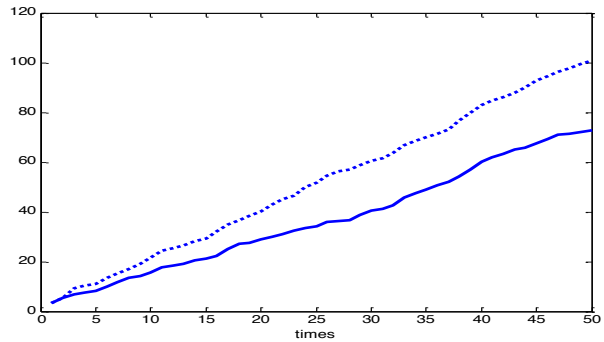

Fig. 12: Accumulative state estimation errors: ASIIKF (solid line), ASUIKF (dotted line).

The ASIIKF should be used to derive a model-based attack detection method from statistical decision tests designed on $\hat{v}_{k-1/k}$. Further researches must be also realized in the worst case situation when the attacker can compute zero dynamic attacks on non minimum phase systems (data losses improving the switching disturbance estimate should also destroy the stealthy strategy of the attacker).

5. Conclusion

This paper has presented a state filtering for linear stochastic discrete-time systems subject to deception attacks and data losses on the control signals transmitted by the controller to the plant. A bias state dependent intermittent unknown input disabled at the occurrence time of data losses has been used to derive a fixed dimensional augmented state model of the plant allowing a direct application of the intermittent unknown input Kalman filter. An extension of the augmented state intermittent unknown input Kalman filter with incomplete information is currently under consideration by the authors.

References

Alouani, A.T., Rice, T.R., and Blair, W.D., 1992, A two-stage filter for state estimation in the presence of dynamic stochastic bias. *Proceedings of the American Control Conference*, 1784-1788.

Amin, S., Cardenas, A., and Sastry, S., 2009, Safe and secure networked control systems under denial-of-service attacks. *Proceedings of the conference on Hybrid Systems: Computation and Control*, 31-45.

Cardenas, A., Amin, S., and Sastry, S., 2008, Secure control: Towards survivable cyber-physical systems. In *First International Workshop on Cyber-Physical System*, Beijing, China, 495-500.

Chen, J., and Patton, R.J., 1996, Optimal filtering and robust fault diagnosis of stochastic systems with unknown disturbances. *Control Theory and Applications*, **143**, 31-36.

Darouach, M., and Zasadzinski, M., 1997, Unbiased minimum variance estimation for systems with unknown exogenous inputs. *Automatica*, **33**, 717-719.

Friedland, B., 1969, Treatment of bias in recursive filtering. *IEEE Trans. Autom. Control*, **14**, 359-367.

Hou, M., and Patton, R.J., 1998, Optimal filtering for systems with unknown inputs. *IEEE Trans. Autom. Control*, **43**, 445-449.

Hespanha, J.P., Naghshtabrizi, P., and Xu, Y., 2007, Survey of recent results in networked control systems. *Proceeding of IEEE*, **95**, 138–162.

Hsieh, C.S., and Chen, F.C., 1999, Optimal solution of the two stage Kalman estimator. *IEEE Trans. Autom. Control*, **44**, 194-199.

Hu, S., Yue, D., liu, J. and Du Z., 2012, Robust H_∞ control for networked systems with parameter uncertainties and multiple stochastic sensors and actuators faults. *International Journal of Innovative Computing, Information and Control*, **8**, 2693-2704.

Ignagni, M., 2000, Optimal and suboptimal separate-bias Kalman filter estimators of a stochastic bias. *IEEE Trans. Autom. Control*, **45**, 547-551.

Keller, J.Y., and Sauter, D., 2013, Kalman filter for discrete-time stochastic linear systems subject to intermittent unknown inputs. *IEEE transactions on Automatic Control*, **58**, 1882-1887.

Kim, K.H., Lee, J.G., and Park, C.G., 2006, Adaptive two-stage Kalman filter in the presence of unknown random bias. *Adaptive Control and Signal Processing*, **20**, 305–319.

Kitanidis, P.K., 1987, Unbiased minimum-variance linear state estimation. *Automatica*, **23**, 775-778.

Liu, X., and Goldsmith, A.J., 2004, Kalman filtering with partial observation losses. *Proceedings of the IEEE conference on decision and control*, Bahamas: Paradise Island, 4180-4186.

Liu, Y., Reiter, M.K., and Ning, P., 2009, False data injection attacks against state estimation in electric power grids. *Proceeding of the ACM Conference on Computer and Communications Security*, Chicago, 21–32.

Mo, Y., and Sinopoli, B., 2010, Secure control against replay attacks. *Proceeding of the conference on Communications, Control and Computing*, Monticello, USA, 911-918.

Pasqualetti, F., Dorfler, F., and Bullo, F., 2012, Cyber-physical security via geometric control: Distributed monitoring and malicious attacks.

Proceeding of the IEEE Conf. on Decision and Control, USA, 3418-3425.

Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., and Sastry, S., 2007, Foundations of control and estimation over lossy networks. *Proceedings of IEEE*, **95**, 163–187.

Shi, L., Epstein, M., and Murray, R.M., 2010, Kalman filtering over a packed-dropping network: A probabilistic perspective. *IEEE Trans. Autom. Control*, **55**, 594-604.

Sinopoli, B., Schenato, L., Franceschetti, M., Poolla, K., Jordan, M., and Sastry, S., 2004, Kalman filtering with intermittent observations. *IEEE Trans. Autom. Control*, **49**, 1453-1464.

Smith, R., 2011, A decoupled feedback structure for covertly appropriating network control systems. *Proceeding of the IFAC World Congress*, Milan, 90–95.

Teixeira, A., Sandberg, H., and Johansson, K.H., 2010, Networked control system under cyber attacks with applications to power networks. *Proceedings of the American Control Conference*, Baltimore, 3690-3696.

Teixeira, A., Shames, I., Sandberg, H., and Johansson, K.H., 2012, Revealing stealthy attacks in control systems. *Proceeding of the international Conference on Communication, Control, and Computing*.

Yang, R., Shi, P., and Liu, G.P., 2011, Filtering for discrete-time networked nonlinear systems with mixed random delays and packet dropouts. *IEEE Trans. Autom. Control*, **11**, 2655-2660.

J.Y. Keller received his Ph.D. degree in Automatic Control from the University of Nancy I, France, in 1991. Since 1993, he teaches as "Maître de Conférences HC" at the University Institute of Technology Henri Poincaré (IUT de Longwy). He works with Research Center In Automatic Control of Nancy (CRAN) associated to the French National Center For Scientific Research (CNRS). He obtained his "Habilitation à diriger des recherches" from University Henri Poincaré, Nancy, in 2003. His main interests include state filtering, fault diagnosis and fault tolerant control for network controlled systems.

K. Karim received his Ph.D. in Automatic Control from University Henri Poincar (France) and University of Gabes in 2011. His 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, Tunisia. His current research interests are focused on model-based fault diagnosis and fault tolerant with emphasis on networked control systems. He was a secondary school teacher of Gabes, Tunisia, from 10/2003 to 09/2007. He was also an Assistant professor in Faculty of Science of Gabes, Tunisia, from 10/2007 to 08/2011 and Temporary Teaching and Research (ATER) since 2011 at Faculty of Science and Technology of Nancy, France.

D. Sauter received the Doctorat ès Sciences Degree (1991) from the University Henri Poincaré, Nancy1, France. Since 1993 he is a full Professor at University of Lorraine. He has been the head of the Electrical Engineering Department during 4 years and Vice-Dean of the Faculty of Sciences and Technology. He also works with Research Center In Automatic Control of Nancy (CRAN) associated to the French National Center For Scientific Research (CNRS). His current research interests are focused on model-based fault diagnosis and fault tolerant with emphasis on networked control systems. The results of his research works are published in over 50 articles in journals and book contributions and 150 conference papers. Pr Sauter is currently serving as an associate editor for the journal of Applied Mathematics and Computer Science and senior editor for the Journal of Intelligent & Robotic Systems.