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, Taylor & Francis, 2016, 47 (4), pp.814-820. <10.1080/00207721.2014.906683>. <hal-01094322>

HAL Id: hal-01094322
https://hal.archives-ouvertes.fr/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.
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 as 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

\[ x_{k+1} = Ax_k + Bu_k + w_k \]  
\[ y_k^* = Cx_k + e_k \]

where \( x_k \in \mathbb{R}^n \), \( u_k \in \mathbb{R}^q \) and \( y_k^* \in \mathbb{R}^m \) are the state, input and measurement vectors and where \( w_k \in \mathbb{R}^n \) and \( e_k \in \mathbb{R}^m \) are zero mean uncorrelated Gaussian random sequences with

\[ E\left[ \begin{bmatrix} w_k & w_j \\ e_k & e_j \end{bmatrix} \right] = \begin{bmatrix} W & 0 \\ 0 & I \end{bmatrix} \delta_{kj} \text{ with } W>0 \]

The initial state \( x_0 \), uncorrelated with \( w_k \) and \( e_k \), is a Gaussian random variable with \( E[x_0] = \overline{x}_0 \) and \( P_0 = E[(x_0 - \overline{x}_0)(x_0 - \overline{x}_0)^T] = \Theta \). We assume \( \text{rank}(C)=m \), \( \text{rank}(B)=q \), \((A,C)\) detectable and \( \text{rank}(CB)=q+m \).

The plant is controlled in the following NCS:

![Fig.1: NCS subject to deception attacks and random data losses.](image)

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

\[ u_k = (1-\rho_k)u_{k-1} + \rho_k u_k^* \]  
\[ y_k = y_k^* \]

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
\[ u_k = \overline{u}_k + v_k \]  \hspace{1cm} (2.5)
\[ \tilde{u}_k = (1 - \rho_k) \tilde{u}_{k-1} + \rho_k \tilde{d}_k^* \]  \hspace{1cm} (2.6)
\[ v_k = (1 - \rho_k) v_{k-1} + \rho_k \tilde{d}_k \]  \hspace{1cm} (2.7)
where \( \tilde{u}_k \) in (2.6) is known to the controller having access to the binary sequence \( \{ \rho_j \}_j \) and where the hybrid disturbance \( v_k \) in (2.7) switches between unknown input \( v_k = d_k \) when \( \rho_k = 1 \) and constant bias \( v_k = v_{k-1} \) when \( \rho_k = 0 \).

By rewriting the hybrid disturbance (2.7) as a constant bias
\[ v_k = v_{k-1} + \tilde{d}_k \rho_k \]  \hspace{1cm} (2.8)
driven by a bias dependent intermittent unknown input
\[ \tilde{d}_k^* = \rho_k(d_k - v_{k-1}) \]  \hspace{1cm} (2.9)
we can derive the following \((n+q)\)-order (time-invariant) state model of the plant
\[ X_{k+1} = \bar{A}_k X_k + \bar{E} \tilde{d}_k^* + \bar{w}_k \] \hspace{1cm} (2.10)
\[ y_k = \bar{C}_k X_k + \bar{v}_k \] \hspace{1cm} (2.11)
with \( \bar{A}_k = \begin{bmatrix} A & B \\ 0 & I \end{bmatrix} \), \( \bar{E} = \begin{bmatrix} B \\ 0 \end{bmatrix} \), \( \bar{F} = \begin{bmatrix} B \\ I \end{bmatrix} \), \( \bar{C}_k = \begin{bmatrix} C \\ 0 \end{bmatrix} \), \( \bar{v}_k = \begin{bmatrix} v_k^T \\ 0 \end{bmatrix} \) and \( \bar{W} = \begin{bmatrix} W & 0 \\ 0 & 0 \end{bmatrix} \).

This paper shows how to derive the unbiased minimum variance estimates \( \hat{v}_{k-1/k} \) of the switching disturbance \( v_k \) from the ASIIKF designed on (2.10) and (2.11) and how to establish the sufficient stochastic stability conditions when \( \rho_k \) 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
\[
\begin{align*}
\dot{\hat{x}}_{k/l} &= \bar{A} \hat{x}_{k/l} + \bar{E} \hat{d}_k^* + \bar{w}_k
\end{align*}
\]  \hspace{1cm} (3.1)
\[
\begin{align*}
\dot{P}_{k/l} &= (1 - \bar{K}_k \bar{C}) \hat{P}_{k/l} \bar{C}^T + \bar{K}_k \bar{C} \hat{P}_{k/l} \bar{C}^T \hat{x}_{k/l} + \bar{Q}_k
\end{align*}
\]  \hspace{1cm} (3.2)
\[
\begin{align*}
\hat{x}_{k+1/l} &= \bar{A} \hat{x}_{k/l} + \bar{E} \hat{d}_k^* + \bar{w}_k
\end{align*}
\]  \hspace{1cm} (3.3)
\[
\begin{align*}
\dot{P}_{k+1/l} &= \bar{AP}_{k/l} + \bar{P}^T \bar{A}^T + \bar{W}
\end{align*}
\]  \hspace{1cm} (3.4)
with \( \bar{K}_k = \bar{P}_{k/l} \bar{C}^T \bar{R}_k^{-1} \) and \( \bar{H}_k = \bar{C} \bar{P}_{k/l} \bar{C}^T + \bar{Q}_k \) updated online from the intermittent unknown input estimate \( \hat{d}_k^* \) of covariance \( Q_k = Pr(\hat{d}_k^* = \hat{d}_k^* | \hat{d}_k^* |) \) with \( \bar{E} \hat{d}_k^* \).

\[
\begin{align*}
\hat{d}_k^* &= \rho_k \bar{C} (B) \bar{P}_{k/l} \bar{C}^T + \rho_k \bar{Q}_k
\end{align*}
\]  \hspace{1cm} (3.5)
\[
\begin{align*}
\bar{Q}_k^* &= \rho_k \bar{C} (B) \bar{P}_{k/l} \bar{C}^T + \rho_k \bar{Q}_k
\end{align*}
\]  \hspace{1cm} (3.6)

The ASIIKF is initialized with \( \hat{x}_{0/l} = \begin{bmatrix} \bar{x}_0 \\ \bar{0} \end{bmatrix} \), \( \bar{P}_{0/l} = \begin{bmatrix} \bar{P}_0 & 0 \\ 0 & 0 \end{bmatrix} \) and \( \rho_{-l} = 0 \).

**Proof.** Consider the following linear state filter
\[
\begin{align*}
\dot{\hat{x}}_{k/l} &= \bar{A} \hat{x}_{k/l} + \bar{E} \hat{d}_k^* + \bar{w}_k
\end{align*}
\]  \hspace{1cm} (3.7)
\[
\begin{align*}
\dot{P}_{k/l} &= (1 - \bar{K}_k \bar{C}) \hat{P}_{k/l} \bar{C}^T + \bar{K}_k \bar{C} \hat{P}_{k/l} \bar{C}^T \hat{x}_{k/l} + \bar{Q}_k
\end{align*}
\]  \hspace{1cm} (3.8)
\[
\begin{align*}
\hat{x}_{k+1/l} &= \bar{A} \hat{x}_{k/l} + \bar{E} \hat{d}_k^* + \bar{w}_k
\end{align*}
\]  \hspace{1cm} (3.9)
\[
\begin{align*}
\dot{P}_{k+1/l} &= \bar{AP}_{k/l} + \bar{P}^T \bar{A}^T + \bar{W}
\end{align*}
\]  \hspace{1cm} (3.10)
where \( \hat{x}_{k/l} \) is the state prediction of covariance \( Pr(\hat{x}_{k/l} = \hat{x}_{k/l} | \hat{x}_{k/l} \) based on measurements available until time \( k-l \) and \( \{ \rho_j \}_{j} \).
\[ \dot{X}_{k/k} \text{ the estimate of } X_k \text{ of covariance matrix} \]
\[ P_{k/k} = E[(X_k - \dot{X}_{k/k})(X_k - \dot{X}_{k/k})^T] \]

based on measurements available until time \( k \) and \( \theta^k_{k^l} \). The attack signal \( d_k \) and the binary variable \( \rho_k \) are both considered as deterministic in the design of the filter:

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

\[ e_{k/k} = X_k - \dot{X}_{k/k} = e_{k/l} + \hat{F}d_{k/l} + \bar{w}_{k/l} \]  
(3.11)

\[ e_{k/k} = e_{k/l} + K_k e_{k/k} \]  
(3.12)

At initial time, \( E[E_{\theta^0_{k^0}}] = 0 \). Assume \( E[E_{\theta^0_{k^0}}] = 0 \) at time \( k-1 \). From (3.11) and (3.12), we have

\[ E[E_{\theta^k_{k^0}}] = 0 \]  
if only if \( K_k \) satisfies the algebraic constraint \( (I - K_k C) - \bar{F} \) rewritten via (2.9) as

\[ (I - K_k C) = 0 \]  
(3.13)

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

\[ K_k = K_k + \rho_k \theta^k C \bar{F} \]  
(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 beneficial filtering effect on the estimate \( \dot{X}_{k-k} \), the algebraic constraint (3.13) disappearing when \( \rho_{k-1} = 0 \).

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

\[ P_{k+1/k} = (A - AK_k C)P_{k/k}^{(l)} (A - AK_k C)^T + AK_k K_k T + I \]  
(3.15)

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

\[ f_d(X) = \bar{F} \bar{C} + \bar{F} \bar{C} + h^T \bar{C} X \bar{F} \]  
(3.16)

\[ f_p(X) = \bar{F} \bar{C} + \bar{F} \bar{C} + \bar{C} \Sigma \bar{F} + I \bar{C} X \bar{F} \]  
(3.17)

with

\[ \bar{F} = \bar{F}(CB)^T \bar{C}, \bar{W} = \bar{W} \]  
\( \bar{F} = \bar{F}(GB)^T \bar{C} \)

and \( \beta \in 0^{m - q} \) so that the rank of \( \Sigma = m - q \). As shown by Keller and Sauter (2013), the ASIIKF's RDE (3.15) can take the form of a switching standard RDE

\[ P_{k+1/k} = \theta (P_{k-1/k}) \]  
(3.18)

Let \( E[E_{\theta^k_{k^0}}] \) the mathematical expectation of \( P_{k+1/k} \) taken with respect to the random sequence \( \{\theta^k_{k^0}\} \) and \( \lambda_c \) the critical data arrival rate (Sinopoli et al. 2004) so that

\[ \lim_{k \to \infty} E[E_{\theta^k_{k^0}}] \]  
(3.19)

when \( \lambda = \lambda_c \) or \( \lim_{k \to \infty} E[E_{\theta^k_{k^0}}] \) otherwise.

**Theorem 3.2:** We have

\[ \lim_{k \to \infty} E[E_{\theta^k_{k^0}}] \]  
(3.20)

if there exists \( K \in \mathbb{R}^{m \times m} \), \( \bar{K} \in \mathbb{R}^{n \times m} \) and \( \theta < \lambda < \lambda_c \) so that \( \Psi(\lambda) > 0 \) with

\[ \Psi(\lambda) = \begin{bmatrix} Y & Y & Y \\ Y & 0 & 0 \\ Y & 0 & 0 \end{bmatrix} \]  
(3.21)

The lower bound \( \lambda_c \) of \( \lambda_c \) is solution to the LMI (Linear Matrix Inequality) feasibility problem

\[ \lambda = \arg\max_{\lambda} \Psi(\lambda) > 0 \]  
(3.22)

where \( \Psi(\lambda) \) is the LMI.
\textbf{Proof.} From (3.18), the mean covariance $E[P_{k+1/k}]$ gives
\begin{equation}
E[P_{k+1/k}] = (I-\lambda_k P_{k-1/k}) \{ P_{k-1/k} \} (I-\lambda_k P_{k-1/k})^T + \lambda_k Q_k \big[ f_j P_{k-1/k} \big]^Tf_j \big[ f_j P_{k-1/k} \big] + \lambda_k Q_k \big[ f_j P_{k-1/k} \big] \big[ f_j P_{k-1/k} \big] ^T + \lambda_k Q_k \big[ f_j P_{k-1/k} \big] \big[ f_j P_{k-1/k} \big] ^T \lambda_k Q_k \big[ f_j P_{k-1/k} \big] + \lambda_k Q_k \big[ f_j P_{k-1/k} \big] \big[ f_j P_{k-1/k} \big] ^T \lambda_k Q_k \big[ f_j P_{k-1/k} \big] + \lambda_k Q_k \big[ f_j P_{k-1/k} \big] \big[ f_j P_{k-1/k} \big] ^T
\end{equation}

The Riccati operators (3.16) and (3.17) are concave, increase with $\lambda$ and the Jensen’s inequality gives

\begin{equation}
E[P_{k+1/k}] = (I-\lambda_k P_{k-1/k}) \{ P_{k-1/k} \} (I-\lambda_k P_{k-1/k})^T + \lambda_k Q_k \big[ f_j P_{k-1/k} \big]^Tf_j \big[ f_j P_{k-1/k} \big] \big[ f_j P_{k-1/k} \big] ^T + \lambda_k Q_k \big[ f_j P_{k-1/k} \big] \big[ f_j P_{k-1/k} \big] ^T \lambda_k Q_k \big[ f_j P_{k-1/k} \big] + \lambda_k Q_k \big[ f_j P_{k-1/k} \big] \big[ f_j P_{k-1/k} \big] ^T \lambda_k Q_k \big[ f_j P_{k-1/k} \big] + \lambda_k Q_k \big[ f_j P_{k-1/k} \big] \big[ f_j P_{k-1/k} \big] ^T
\end{equation}

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

\begin{equation}
S_{k+1} = (I-\lambda_k f_j S_k) + \lambda_k f_j S_k
\end{equation}

with $S_0 = P_{0,0} I$. Let

\begin{equation}
S = (I-\lambda_k f_j S) + \lambda_k f_j S
\end{equation}

the modified ARDE associated to (3.25). Sinopoli et al. (2004) have shown that there exists a stabilizing solution $S_{k+1}$ to (3.26) if there exists $K$, $\hat{K}$ and $\lambda > 0$ so that

\begin{equation}
X^T (I-\lambda_k f_j S) X + \lambda_k f_j S \big[ f_j X \big] X^T + \lambda_k f_j S \big[ f_j X \big] X^T \lambda_k f_j S \big[ f_j X \big] + \lambda_k f_j S \big[ f_j X \big] X^T \lambda_k f_j S \big[ f_j X \big]
\end{equation}

or equivalently if there exists $K$, $\hat{K}$ and $\omega$, $\gamma > 0$ so that $\gamma f_j (\omega)$ with $\gamma f_j (\omega)$ given by (3.20). We have also

\begin{equation}
P_{k+1/k} = \hat{P}_{k+1/k} \big[ f_j X \big]
\end{equation}

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

\begin{equation}
\hat{P}_{k+1/k} = f_j \hat{P}_{k+1/k} \big[ f_j X \big]
\end{equation}

with $\hat{P}_{0,0} = P_{0,0} I$. 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).

\textbf{End of proof}

When $m=q$, we have $\hat{K} = 0$ 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

\begin{equation}
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}, \quad B = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},
\end{equation}

\begin{equation}
C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad W = 0.01 I.
\end{equation}

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 $d_k = \begin{bmatrix} d^T_1 \\ d^T_2 \end{bmatrix}$ 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 ASUKF, is derived from the ASIIKF with $\rho_k = 1 \forall k \geq 0$ in theorem 3.1), both used for the reconstruction of $v_k = \begin{bmatrix} v^T_1 \\ v^T_2 \end{bmatrix}$. The binary variable $\rho_k$ is plotted on figure 2 with $\lambda = 0.3$ chosen very low to accentuate the benefic effect of data losses on $\hat{v}_{k-1/k} = \begin{bmatrix} v^T_{1,1/k} \\ v^T_{2,1/k} \end{bmatrix}$. Figure 3 shows $tr(P_{k-1/k})$, its upper bound $tr(\hat{P}_{k-1/k})$ and the upper bound $tr(S_k)$ of $tr(\hat{P}_{k-1/k})$. The switching disturbance $v^1_k$ and its one period time delayed estimate $\hat{v}_k$ given by the ASIIKF are plotted on figure 4. Figure 5 shows the estimate $\hat{v}_{k-1/k}$ generated by the ASIIKF. The switching disturbance $v^2_k$ and its one period time delayed estimate $\hat{v}_k$ given by the ASIIKF are plotted on figure 6. Figure 7 shows the estimate $\hat{v}_{k-1/k}$ generated by the ASIIKF. The state estimation errors $e^1_k = x^1_k - \hat{x}^1_k$, $e^2_k = x^2_k - \hat{x}^2_k$, $e^3_k = x^3_k - \hat{x}^3_k$ and $e^4_k = x^4_k - \hat{x}^4_k$.\[\text{Figure 1 and the following}\]
\( e_{k/k}^4 = x_k^4 - \hat{x}_{k/k}^4 \) 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

\[
\sum_{j=0}^{k} \sum_{i=j}^{k} |y_{i,j}|
\]
The ASIIKF should be used to derive a model-based attack detection method from statistical decision tests designed on $\nu_{k-\ell/k}$. 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
Proceeding of the IEEE Conf. on Decision and Control, USA, 3418-3425.


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.