Preprints of the 2012 20th Mediterranean Conference on Control & Automation (MED), Barcelona, Spain, July 3-6, 2012

State filtering for discrete-time stochastic linear systems subject to random cyber attacks and losses of measurements

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

Université de Lorraine, CRAN CNRS UMR 7039, BP 239, 54506 Vandoeuvre les Nancy, France

***Abstract*- This paper presents a state filtering strategy for network controlled systems subject to cyber attacks assumed to occur when the control signal sent by the controller to the plant is lost. After having represented the hypothesized cyber attacks as intermittent unknown inputs, the state filtering scheme is obtained by designing a modified version of the unknown input Kalman filter restricted, in its original version, to the treatment of permanent unknown inputs. The existence condition of the unknown input Kalman filter is ensured by a secure network for the transmission of measurements directly affected by cyber attacks. The stochastic stability of the state filter is studied when independent Bernoulli processes govern the random arrival of cyber attacks and measurements. A numerical example illustrates the obtained results.**

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

I. INTRODUCTION

Recent technological advances are revolutionizing our ability to build massively distributed Networked Control Systems (NCS). They present challenging problems arising from the fact that sensors, actuators and controllers exchange information via a digital communication network. The state of the art on design control systems that take into account the effects of packet loss and packet delay in networked control systems have been surveyed in [1]. In particular, Kalman filtering with random lost of observations represented by Markovian or Bernoulli processes has been studied in [2], [3], extended later to include both packet loss and random delay in [4], [5] and more recently in [6] when the arrival of observations is driven by a semi-Markov chain.

The communication network shared by sensors, actuators and controllers is also vulnerable to cyber attacks from malicious outsiders (see [7] and references therein). This paper presents a state filtering strategy for network controlled stochastic linear discrete-time systems subject to cyber attacks acting on the system through the unreliable network. We assume that cyber attacks, represented by exogenous unknown inputs, can only appear when the control signal sent by the controller to the plant is lost. For the state filtering of such systems, we extend the use of the standard Unknown Input Kalman Filter UIKF ([8], [9], [10]) to the treatment of intermittent unknown inputs. The existence condition of the modified UIKF, linked to the analytical redundancy of the system, is ensured by a secure network for the transmission of measurements directly affected by the unknown inputs. The other part of measurements is transmitted by the plant to the controller on the unreliable channel with a protocol of type TCP. When the random arrival of cyber attacks and measurements follow independent random Bernoulli processes, the stochastic stability of the proposed filter is studied on the upper bound of the mean prediction error covariance matrix by transposing the results obtained in [3] and [11].

The paper is organised as follows: Section 2 presents the structure of the modified UIKF. Section 3 designs the filter and studies its stochastic stability conditions. An illustrative example is given in Section 4 before conclusions in Section 5.

978-1-4673-2529-5/12/$31.00 ©2012 IEEE

II. PROBLEM STATEMENT

Let us consider the following linear discrete-time stochastic systems

$$x_{k+1} = Ax_k + Bu_k + Fd_k^\theta + w_k \quad (1.a)$$

$$y_k^* = Cx_k + v_k \quad (1.b)$$

where $x_k \in \Re^n$, $u_k \in \Re^d$, $y_k^* \in \Re^m$ and $d_k^\theta \in \Re^q$ are the state, control, measurement and unknown input vectors. Matrices A, B, C and F are of appropriate dimensions, with (A, C) detectable, (A, $W^{1/2}$) stabilizable and $rank(CF) = rank(F) = q \le m$. The process and sensor noises are zero mean uncorrelated random sequences with

$$E\left\{\begin{bmatrix} w_k \\ v_k \end{bmatrix}\begin{bmatrix} w_j \\ v_j \end{bmatrix}^T\right\} = \begin{bmatrix} W & 0 \\ 0 & I \end{bmatrix}\delta_{k,j}\ ,\ W \ge 0 \quad (2)$$

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 $P_0 = E\{(x_0 - \bar{x}_0)(x_0 - \bar{x}_0)^T\} \ge 0$. We assume that x_0, w_k and v_k are mutually independent. Let u_k^* the control signal transmitted by the controller to the plant via the unreliable network and $\rho_k \in \{0,1\}$ the acknowledgement signal indicating the status of reception/delivery (TCP protocol) with $\rho_k = 0$ when $u_k = u_k^*$ and $\rho_k = 1$ when $u_k = 0$. With $F = B$, the unknown inputs vector

$$d_k^\theta = \rho_k d_k \quad (3)$$

in (1.a) represents cyber attacks assumed to occur randomly when the control signal sent by the controller to the plant is lost i.e. when $\rho_k = 1$. We also assume that the random binary sequence ρ_k follows a stochastic Bernoulli process with $\lambda = \Pr[\rho_k = 1]$ where λ is the rate of hypothesized cyber attacks, coinciding with the rate of packet dropout. In order to allow a minimum variance unbiased state filtering for the system (1), (2) and (3), the measurement vector y_k^* is assumed transmitted to the controller via a particular communication strategy using two communication channels: when $\rho_{k-1} = 0$, the whole measurement vector y_k^* is transmitted to the controller via the unreliable network. When $\rho_{k-1} = 1$, the reduced part of measurements $y_k^1 = Hy_k^* \in \Re^q$ directly affected by d_{k-1} (with $H = (CF)^+$) is transmitted to the controller via a secure communication channel while the other part $y_k^2 = \Sigma y_k^* \in \Re^{m-q}$ (with $\Sigma = \beta(I - CF(CF)^+)$ and $\beta \in \Re^{m-q,m}$ so that $rank(\Sigma) = m - q$) is transmitted to the controller via the unreliable network. The random lost of measurements on the unreliable channel is described by a binary variables $\gamma_k \in \{0,1\}$ with $\gamma_k = 1$ when the measurements are received by the local controller and $\gamma_k = 0$ otherwise. The random binary sequence $\gamma_k \in \{0,1\}$ is known to the controller (TCP protocol) and follows a stochastic Bernoulli process with $\mu = \Pr[\gamma_k = 1]$. We also assume that the stochastic binary random variables ρ_k and γ_k are independent. The measurements vector $y_k = \begin{bmatrix} y_k^{1T} & y_k^{2T} \end{bmatrix}^T$ received by the controller can be expressed

$$y_k = Q_k y_k^* \quad (4.a)$$

with

$$Q_k = (1 - \rho_{k-1})\gamma_k I_m + \rho_{k-1}\begin{bmatrix} I_q & 0 \\ 0 & \gamma_k I_{m-q} \end{bmatrix}\begin{bmatrix} H \\ \Sigma \end{bmatrix} \quad (4.b)$$

Under cyber attacks occurring randomly when $\rho_k = 1$, the model of the plant viewed by the controller becomes

$$x_k = Ax_{k-1} + Bu_{k-1} + Fd_{k-1}^\theta + w_{k-1} \quad (5.a)$$

$$y_k = C_k x_k + Q_k v_k \quad (5.b)$$

with

$$C_k = Q_k C = (1 - \rho_{k-1})\gamma_k C + \rho_{k-1}\begin{bmatrix} \widetilde{C} \\ \gamma_k \overline{C} \end{bmatrix} \quad (5.c)$$

where $\widetilde{C} = HC$ and $\overline{C} = \Sigma C$. Considers the following filter

$$\begin{aligned} \hat{x}_{k/k} &= (1 - \rho_{k-1})[\hat{x}_{k/k-1} + K_k(y_k - C_k\hat{x}_{k/k-1})] \\ &\quad + \rho_{k-1}[\hat{x}_{k/k-1} + K_k^1(y_k - C_k\hat{x}_{k/k-1})] \end{aligned} \quad (6.a)$$

$$\begin{aligned} P_{k/k} &= (1 - \rho_{k-1})[(I - K_k C_k)P_{k/k-1}(I - K_k C_k)^T + K_k K_k^T] \\ &\quad + \rho_{k-1}[(I - K_k^1 C_k)P_{k/k-1}(I - K_k^1 C_k)^T + K_k^1 K_k^{1T}] \end{aligned} \quad (6.b)$$

and

$$\hat{x}_{k+1/k} = A\hat{x}_{k/k} + Bu_k \quad (6.c)$$

$$P_{k+1/k} = AP_{k/k}A^T + W \quad (6.d)$$

where $\hat{x}_{k/k}$ and $\hat{x}_{k+1/k}$ are the state estimation and prediction of covariance $P_{k/k} = E\{(x_k - \hat{x}_{k/k})(x_k - \hat{x}_{k/k})^T\}$ and $P_{k+1/k} = E\{(x_{k+1} - \hat{x}_{k+1/k})(x_{k+1} - \hat{x}_{k+1/k})^T\}$ depending on the known binary sequences $\{\rho_j\}_0^{k-1}$ and $\{\gamma_j\}_0^k$. The trace of

the state estimation error covariance $P_{k/k}$ will be minimized with respect to $K_k \in \Re^{n,m}$ and $K_k^1 \in \Re^{n,m}$ so that the minimum variance unbiased property remains valid for any sequences $\{\rho_j\}_0^{k-1}$ and $\{\gamma_j\}_0^k$.

III. INTERMITTENT UNKNOWN INPUT KALMAN FILTER WITH PARTIAL MEASUREMENT LOSSES

In the first part of this section, the known binary sequences $\{\rho_j\}_0^{k-1}$ and $\{\gamma_j\}_0^k$ are assumed deterministic.

Theorem 3.1: For any sequences $\{\rho_j\}_0^{k-1}$ and $\{\gamma_j\}_0^k$, the minimum variance unbiased property of the state filter (6) is obtained with

$$K_k = \gamma_k P_{k/k-1} C^T (C P_{k/k-1} C^T + I)^{-1} \quad (7.a)$$

$$K_k^1 = \begin{bmatrix} F & \gamma_k \overline{K}_k \end{bmatrix} \quad (7.b)$$

$$\overline{K}_k = \gamma_k N P_{k/k-1} \overline{C}^T (\overline{C} P_{k/k-1} \overline{C}^T + \Sigma\Sigma^T)^{-1} \quad (7.c)$$

where $N = I - F\widetilde{C}$.

Proof. The state estimation error $e_{k/k} = x_k - \hat{x}_{k/k}$ and state prediction error $e_{k+1/k} = x_{k+1} - \hat{x}_{k+1/k}$ propagate as

$$\begin{aligned} e_{k/k} = {} & (1-\rho_{k-1})[(I - K_k C_k) e_{k/k-1} - K_k Q_k v_k + w_k] \\ & + \rho_{k-1}[(I - K_k^1 C_k) e_{k/k-1} - K_k^1 Q_k v_k + w_k] \end{aligned} \quad (8.a)$$

$$e_{k+1/k} = A e_{k/k} + F d_k^\theta + w_k \quad (8.b)$$

For an inductive reasoning, assume that $E\{e_{k-1/k-1}\} = 0$. Under $\rho_{k-1} = 0$, we have $d_{k-1}^\theta = 0$ and thus $E\{e_{k/k-1}\} = 0$. So, $E\{e_{k/k}\} = 0 \ \forall \gamma_k \in \{0,1\}$ without constraint on K_k . Under $\rho_{k-1} = 1$, we have $d_{k-1}^\theta = d_{k-1}$ and thus $E\{e_{k/k-1}\} = F d_{k-1}$. So, $E\{e_{k/k}\} = 0 \ \ \forall \gamma_k \in \{0,1\}$ if and only if $K_k^1 \in \Re^{n,m}$ is solution to the following structure-varying algebraic constraint

$$(I - K_k^1 \begin{bmatrix} \widetilde{C} \\ \gamma_k \overline{C} \end{bmatrix}) F = 0 \quad (9)$$

We can verify from $\widetilde{C}F = I$ and $\overline{C}F = 0$ that the structure-varying gain (7.b) is solution to (9) $\forall \overline{K}_k \in \Re^{n,m-q}$. Substituting (7.b) in (6.b), we obtain

$$P_{k/k} = (1-\rho_{k-1}) P_{k/k}^1 + \rho_{k-1} P_{k/k}^2 \quad (10.a)$$

$$P_{k/k}^1 = (I - K_k \gamma_k C) P_{k/k-1} (I - K_k \gamma_k C_k)^T + \gamma_k K_k K_k^T \quad (10.b)$$

$$\begin{aligned} P_{k/k}^2 = {} & (N - \gamma_k \overline{K}_k \overline{C}) P_{k/k-1} (N - \gamma_k \overline{K}_k \overline{C})^T \\ & + FHH^T F^T + \gamma_k \overline{K}_k \Sigma\Sigma^T \overline{K}_k^T \end{aligned} \quad (10.c)$$

Under $\rho_{k-1} = 0$ and $\gamma_k = 1$, the minimization of $tr(P_{k/k}^1)$ with respect to K_k gives (7.a). Under $\rho_{k-1} = 1$ and $\gamma_k = 1$, the minimization of $tr(P_{k/k}^2)$ with respect to $\overline{K}_k$ gives (7.c), closing the proof.

After having substituted (7.a) and (7.c) in (10.a) and the resulting expression of $P_{k/k}$ in (6.d), we derive the following modified Riccati Difference Equation (RDE)

$$P_{k+1/k} = (1-\rho_{k-1}) P_{k+1/k}^1 + \rho_{k-1} P_{k+1/k}^2 \quad (11.a)$$

$$\begin{aligned} P_{k+1/K}^1 = {} & A P_{k/k-1} A^T + W \\ & - \gamma_k A P_{k/k-1} C^T (C P_{k/k-1} C^T + I)^{-1} C P_{k/k-1} A^T \end{aligned} \quad (11.b)$$

$$\begin{aligned} P_{k+1/k}^2 = {} & \overline{A} P_{k/k-1} \overline{A}^T + \overline{W} \\ & - \gamma_k \overline{A} P_{k/k-1} \overline{C}^T (\overline{C} P_{k/k-1} \overline{C}^T + \Sigma\Sigma^T)^{-1} \overline{C} P_{k/k-1} \overline{A}^T \end{aligned} \quad (11.b)$$

where $\overline{A} = A - AF\widetilde{C}$, $\overline{W} = W + AFHH^T F^T A^T$ and $P_{0/-1} = P_0 \geq 0$.

When the known binary sequences $\{\rho_j\}_0^\infty$ and $\{\gamma_j\}_0^\infty$ are random, the modified RDE (11) generates random covariance sequences. Assume that $\{\rho_j\}_0^\infty$ and $\{\gamma_j\}_0^\infty$ follow independent Bernoulli processes with $\lambda = \Pr[\rho_k = 1]$ and $\mu = \Pr[\gamma_k = 1]$. Let λ_c the critical arrival rate of cyber attacks and μ_c the critical arrival rate of measurements so that $\lim_{k\to\infty} E\{P_{k+1/k}\} \to \infty$ when $\lambda > \lambda_c$ and $\mu < \mu_c$ and $\lim_{k\to\infty} E\{P_{k+1/k}\} < \infty$ otherwise, where $E\{P_{k+1/k}\}$ is the mathematical expectation of the random covariance $P_{k+1/k}$ taken with respect to the sequences $\{\rho_j\}_{j=1}^{k-1}$ and $\{\gamma_j\}_{j=0}^k$.

Following [3], the deterministic upper bound S_{k+1} of $E\{P_{k+1/k}\}$ satisfying $E\{P_{k+1/k}\} \leq S_{k+1}$ is solution to the modified RDE

$$S_{k+1} = S_k^{00} + S_k^{10} + S_k^{01} + S_k^{11} \quad (12.a)$$

where

$$S_k^{00} = p_{00}^2[AS_kA^T + W - AS_kC^T(CS_kC^T + I)^{-1}CS_kA^T] \quad (12.b)$$

$$S_k^{10} = p_{10}^2[\overline{A}S_k\overline{A}^T + \overline{W} - \overline{A}S_k\overline{C}^T(\overline{C}S_k\overline{C}^T + \Sigma\Sigma^T)^{-1}\overline{C}S_k\overline{A}^T] \quad (12.c)$$

$$S_k^{01} = p_{01}^2(AS_kA^T + W) \quad (12.d)$$

$$S_k^{11} = p_{11}^2(\overline{A}S_k\overline{A}^T + \overline{W}) \quad (12.e)$$

$$p_{00} = \sqrt{(1-\lambda)\mu} \quad (12.f)$$

$$p_{10} = \sqrt{\lambda\mu} \quad (12.g)$$

$$p_{01} = \sqrt{(1-\lambda)(1-\mu)} \quad (12.h)$$

$$p_{11} = \sqrt{\lambda(1-\mu)} \quad (12.i)$$

and $S_0 = P_0 \geq 0$.

Theorem 3.2: If there exists $K \in \Re^{n,m}$, $\overline{K} \in \Re^{n,m-q}$ and $0 < Y < I$ such that $\Psi_{\lambda,\mu}(Y) > 0$ with

$$\Psi_{\lambda,\mu}(Y) = \begin{bmatrix} Y & p_{00}X_{00} & p_{10}X_{10} & p_{01}X_{01} & p_{11}X_{11} \\ p_{00}X_{00}^T & Y & 0 & 0 & 0 \\ p_{10}X_{10}^T & 0 & Y & 0 & 0 \\ p_{01}X_{01}^T & 0 & 0 & Y & 0 \\ p_{11}X_{11}^T & 0 & 0 & 0 & Y \end{bmatrix} \quad (13.a)$$

where $X_{00} = YA + KC$, $X_{10} = Y\overline{A} + \overline{K}\overline{C}$, $X_{01} = YA$, $X_{11} = Y\overline{A}$ the

$$\lim_{k\to\infty} E\left\{P_{k+1/k}\right\} \leq S < \infty \quad (13.b)$$

where S is solution to the modified ARDE

$$S = g_{\lambda\mu}(S) = S^{00} + S^{01} + S^{10} + S^{11} \quad (13.c)$$

with

$$S^{00} = p_{00}^2[ASA^T + W - ASC^T(CSC^T + I)^{-1}CSA^T] \quad (13.d)$$

$$S^{10} = p_{10}^2[\overline{A}S\overline{A}^T + \overline{W} - \overline{A}S\overline{C}^T(\overline{C}S\overline{C}^T + \Sigma\Sigma^T)^{-1}\overline{C}S\overline{A}^T] \quad (13.e)$$

$$S^{01} = p_{01}^2(ASA^T + W) \quad (13.f)$$

$$S^{11} = p_{11}^2(\overline{A}S\overline{A}^T + \overline{W}) \quad (13.g)$$

For a fixed arrival rate λ of cyber attacks, the lower bound $\breve{\mu}$ of μ_c is solution to the LMI (Linear Matrix Inequality) feasibility problem

$$\breve{\mu} = \arg\left\{\min_{\mu} \Psi_{\lambda,\mu}(Y) > 0\right\} \quad (14.a)$$

For a fixed arrival rate μ of measurements, the upper bound $\hat{\lambda}$ of λ_c is solution of

$$\hat{\lambda} = \arg\left\{\max_{\lambda} \Psi_{\lambda,\mu}(Y) > 0\right\} \quad (14.b)$$

Proof. Let us define the auxiliary function

$$\Phi_{\lambda,\mu}(X) = p_{00}^2[(A-KC)X(A-KC)^T + KK^T + W] + p_{10}^2[(\overline{A}-\overline{K}\overline{C})X(\overline{A}-\overline{K}\overline{C})^T + \overline{K}\Sigma\Sigma^T\overline{K}^T + \overline{W}] + p_{01}^2(AXA^T + W) + p_{11}^2(\overline{A}X\overline{A}^T + \overline{W}) \quad (15.a)$$

satisfying

$$g_{\lambda\mu}(X) \leq \Phi_{\lambda,\mu}(X) \ \ \forall(K,\overline{K}) \quad (15.b)$$

If there exists $K \in \Re^{n,m}$, $\overline{K} \in \Re^{n,m-q}$ and $Z > 0$ such that $Z > \Phi_{\lambda,\mu}(Z)$ then there exists an unique stabilizing solution $S \geq 0$ to the modified ARDE (13.c). In [3], the following statements are equivalent :

(a) $\exists(K,\overline{K})$ and $Z > 0$ such that $Z > \Phi_{\lambda,\mu}(Z)$ (16.a)

(b) $\exists(K,\overline{K})$ and $0 < Y < I$ such that $\Psi_{\lambda,\mu}(Y) > 0$ (16.b)

For a fixed arrival rate of cyber attacks, we conclude from the works in [11] that $\lim_{k\to\infty} E\left\{P_{k+1/k}\right\} \leq S < \infty \ \ \forall\mu \in [\breve{\mu} \ 1]$ with $\breve{\mu}$ solution to (14.a). For a fixed arrival rate of measurements, we also conclude that $\lim_{k\to\infty} E\left\{P_{k+1/k}\right\} \leq S < \infty$ $\forall\lambda \in [0 \ \hat{\lambda}]$ with $\hat{\lambda}$ solution to (14.b).

Theorem 3.3: Under persistent cyber attacks i.e. when $\lambda = 1$, the optimized filter (6) becomes

$$\hat{x}_{k/k} = \hat{x}_{k/k-1} + K_k^1(y_k - C_k\hat{x}_{k/k-1}) \quad (17.a)$$

$$P_{k/k} = (I - K_k^1C_k)P_{k/k-1}(I - K_k^1C_k)^T + K_k^1K_k^{1T} \quad (17.b)$$

$$\hat{x}_{k+1/k} = A\hat{x}_{k/k} + Bu_k \quad (17.c)$$

$$P_{k+1/k} = AP_{k/k}A^T + W \quad (17.d)$$

with

$$K_k^1 = \begin{bmatrix} F & \gamma_k\overline{K}_k \end{bmatrix} \quad (17.e)$$

$$\overline{K}_k = \gamma_k NP_{k/k-1}\overline{C}^T(\overline{C}P_{k/k-1}\overline{C}^T + \Sigma\Sigma^T)^{-1} \quad (17.f)$$

leading to a modified version of the standard UIKF with partial intermittent observations. Let $\tilde{\mu}_c$ the critical arrival rate of measurements. If there exists $\overline{K} \in \Re^{n,m-q}$ and $0 < Y < I$ such that $\overline{\Psi}_{\mu}(Y) > 0$ with

$$\overline{\Psi}_{\mu}(Y) = \begin{bmatrix} Y & \sqrt{(1-\mu)}Y\overline{A} & \sqrt{\mu}(Y\overline{A} + \overline{K}\overline{C}) \\ \sqrt{(1-\mu)}(Y\overline{A})^T & Y & 0 \\ \sqrt{\mu}(Y\overline{A} + \overline{K}\overline{C})^T & 0 & Y \end{bmatrix} \quad (18.a)$$

then

$$\lim_{k\to\infty} E\{P_{k+1/k}\} \le \bar{V} < \infty \quad \forall \mu \in [\breve{\mu}\ 1] \tag{18.b}$$

where $\bar{V} \ge 0$ is solution to the modified ARDE

$$\begin{aligned} \bar{V} &= (1-\mu)(\bar{A}\bar{V}\bar{A}^T + \bar{W}) \\ &+ \mu[\bar{A}\bar{V}\bar{A}^T + \bar{W} - \bar{A}\bar{V}\bar{C}^T(\bar{C}\bar{V}\bar{C}^T + \Sigma\Sigma^T)^{-1}\bar{C}\bar{V}\bar{A}^T] \end{aligned} \tag{18.c}$$

The lower bound $\breve{\mu}$ of $\bar{\mu}_c$ is solution to the LMI feasibility problem $\breve{\mu} = \arg\left\{\min_{\mu} \bar{\Psi}_\mu(Y) > 0\right\}$.

Proof. The proof of theorem 3.3 is obtained by considering $\rho_k = 1 \ \ \forall k$ in theorem 3.1 and by letting $\lambda = 1$ in theorem 3.2.

Theorem 3.4: Without cyber attacks i.e. when $\lambda = 0$, the optimised filter (6) becomes

$$\hat{x}_{k/k} = \hat{x}_{k/k-1} + K_k(y_k - C_k\hat{x}_{k/k-1}) \tag{19.a}$$

$$P_{k/k} = (I - K_kC_k)P_{k/k-1}(I - K_kC_k)^T + K_kK_k^T \tag{19.b}$$

$$\hat{x}_{k+1/k} = A\hat{x}_{k/k} + Bu_k \tag{19.c}$$

$$P_{k+1/k} = AP_{k/k}A^T + W \tag{19.d}$$

with

$$K_k = \gamma_k P_{k/k-1}C^T(CP_{k/k-1}C^T + I)^{-1} \tag{19.e}$$

and recovers the Kalman filter with intermittent observation given in [3]. Let $\bar{\mu}_c$ the critical arrival rates of measurements under $\lambda = 0$. If there exists $K \in \Re^{n,m}$ and $0 < Y < I$ such that $\Psi_\mu(Y) > 0$ with

$$\Psi_\mu(Y) = \begin{bmatrix} Y & \sqrt{(1-\mu)}YA & \sqrt{\mu}(YA + KC) \\ \sqrt{(1-\mu)}(YA)^T & Y & 0 \\ \sqrt{\mu}(YA + KC)^T & 0 & Y \end{bmatrix} \tag{20.a}$$

then

$$\lim_{k\to\infty} E\{P_{k+1/k}\} \le V < \infty \quad \forall \mu \in [\breve{\mu}\ 1] \tag{20.b}$$

where $V \ge 0$ is solution to the modified ARDE

$$\begin{aligned} V &= (1-\mu)(\bar{A}V\bar{A}^T + \bar{W}) \\ &+ \mu[\bar{A}V\bar{A}^T + \bar{W} - \bar{A}V\bar{C}^T(\bar{C}V\bar{C}^T + \Sigma\Sigma^T)^{-1}\bar{C}V\bar{A}^T] \end{aligned} \tag{20.c}$$

The lower bound $\breve{\mu}$ of $\bar{\mu}_c$ is solution to the LMI feasibility problem $\breve{\mu} = \arg\left\{\min_{\mu} \Psi_\mu(Y) > 0\right\}$.

Proof. The proof of theorem 3.4, given in [3], can be recovered by considering $\rho_k = 0 \ \ \forall k$ in theorem 3.1 and by letting $\lambda = 0$ in theorem 3.2.

IV. ILLUSTRATIVE EXAMPLE

Consider the following linear discrete-time stochastic system

$$A = \begin{bmatrix} 1.3 & 1 & 0 & 0 \\ 0 & 0.8 & 1 & 0 \\ 0 & 0 & 1.5 & 1 \\ 0 & 0 & 0 & 0.3 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \ F = B$$

$W = 0.01I_4$, $V = I_3$ where $rank(CF) = rank(F) = 2 \le 3$. The pairs (A , C) and (A , $W^{1/2}$) are detectable and stabilizable, respectively. The condition under which the standard UIKF is stable do not hold i.e. the pair ($\bar{A}$, $\bar{C}$) is not detectable .

The arrival rate of hypothesized cyber attacks (or the arrival rate of packet dropout with $\rho_k = 1$ when $u_k = 0$) is fixed at $\lambda = \Pr[\rho_k = 1] = 0.05$. The lower bound for the critical arrival rate of measurements, solution to the LMI feasibility problem (14.a), is given by $\breve{\mu} = 0.76$. When the arrival rate of measurements $\mu = 0{,}8$ is so that $\mu > \breve{\mu}$, figure 1 shows the random evolution of $tr(P_{k+1/k})$ and the upper bound $tr(S_{k+1})$ of $tr(E\{P_{k+1/k}\})$ with S_{k+1} generated by (12.a). The figure 2 shows the random evolution of $tr(P_{k+1/k})$ when $\mu = 0{,}5$ is so that $\mu \ll \breve{\mu}$ (the sequence S_{k+1} diverges and $tr(S_{k+1})$ is not plotted).

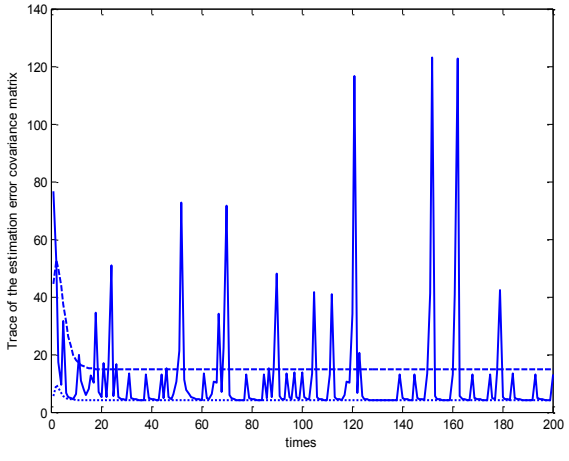

Fig. 1. $tr(P_{k+1/k})$ (solid line), $tr(S_{k+1})$ (dashed line).

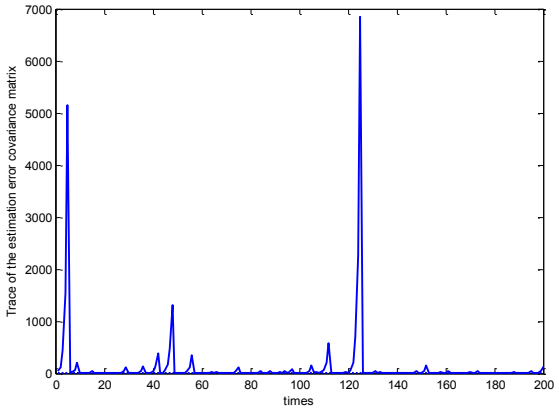

Fig. 2. $tr(P_{k+1/k})$.

For the transmission of measurements directly affected by cyber attacks, the use of the secure communication channel should be avoided by using the joint state and intermittent unknown inputs estimator developed in [12] and by blocking the unknown inputs estimate when the whole measurements vector is lost. Note that the additive term Fd_k^θ with $d_k^\theta = \rho_k d_k$ may also describe intermittent interconnection signals between a particular subsystem and its neighbour in the area of large scale NCS (see [13]). So, the filter proposed in this paper, relaxing the deterministic stability of the standard UIKF, should be apply on each subsystem in order to simplify the discrimination between cyber attacks acting within one subsystem and cyber attacks acting in other areas of the network.

V. Conclusion

This paper has presented a modified unknown input Kalman filter for the state filtering of network controlled systems subject to cyber attacks occurring randomly. Sufficient stochastic stability conditions have been established from an upper bound of the mean prediction error covariance matrix depending on the arrival rate of cyber attacks. A lower bound for the critical arrival rate of measurements has also been derived. Further researches must be made to avoid the use of a secure communication network for the transmission of measurements directly affected by cyber attacks.

References

[1] J.P. Hespanha, P. Naghshtabrizi, and Y. Xu, "Survey of recent results in networked control systems", Proceedings of the IEEE, 95 (1), 2007, pp. 138–162.

[2] A. Fletcher, S. Rangan and V. Goyal, "Estimation from lossy sensor data: jump linear modeling and Kalman filtering", Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, California, 2004, pp.251–258.

[3] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. Jordan and S. Sastry, "Kalman filtering with intermittent observations", IEEE transactions on Automatic Control, 49, 2004, pp. 1453-1464.

[4] L. Schenato, B. Sinopoli,, M. Franceschetti, K. Poolla and S. Sastry, "Foundations of control and estimation over lossy networks", Proceedings of IEEE, 95(1), 2007, pp. 163–187.

[5] L. Shi, L. Xie and R.M. Murray, "Kalman filtering over a packed-delayed network: A probabilistic approach". Automatica, 45, 2009, pp. 2134-2140.

[6] A. Censi, "Kalman Filtering with intermittent observations: Convergence for semi-Markov chains and an intrinsic performance measure", *IEEE transactions on Automatic Control*, 56, 2011, pp. 376-381.

[7] A. Teixeira, H. Sandberg and K. Johansson, "Networked control system under cyber attacks with applications to power networks", American Control Conference, Baltimore, 2010, pp. 3690-3696.

[8] P.K. Kitanidis, "Unbiased minimum-variance linear state estimation", Automatica, 23, 1987, pp.775-778.

[9] J. Chen and R.J. Patton, "Optimal filtering and robust fault diagnosis of stochastic systems with unknown disturbances", IEE Proceedings -Control Theory and Applications, 143 (1), 1996, pp. 31-36.

[10] M. Darouach and M. Zasadzinski, "Unbiased minimum variance estimation for systems with unknown exogenous inputs", Automatica, 33 (4), 1997, pp. 717-719.

[11] X. Liu and A.J. Goldsmith, "Kalman filtering with partial observation losses", Proceedings of the 43 *IEEE conference on decision and control*. Bahamas: Paradise Island, 2004.

[12] J.Y. Keller and D. Sauter, "Kalman filter for discrete-time stochastic linear systems subject to intermittent unknown inputs", *Submitted to IEEE TAC*.

[13] S. Klinkhieo, R.J. Patton and C. Kambhampati, "Robust FDI for FTC Coordination in a distributed Network System", Proceedings of the 17th World Congress, Korea, 2008, pp. 13551-13556.