Proceedings of the 33rd Chinese Control Conference
July 28-30, 2014, Nanjing, China

Robust H_∞ cyber-attacks estimation for control systems

LI Yumei[1], VOOS Holger[1], DAROUACH Mohamed[2]

1. Interdisciplinary Centre for Security Reliability and Trust (SnT), University of Luxembourg, L-2721, Luxembourg
E-mail: yumei.li@uni.lu; Holger.Voos@uni.lu;

2. Centre de la Recherche en Automatique de Nancy (CRAN), Universite de Lorraine, France.
E-mail: mohamed.darouach@univ-lorraine.fr.

Abstract: This paper deals with the robust H_∞ cyber-attacks estimation problem for control systems under stochastic cyber-attacks and disturbances. The focus is on designing a H_∞ filter which maximize the attack sensitivity and minimize the effect of disturbances. The design requires not only the disturbance attenuation, but also the residual to remain the attack sensitivity as much as possible while the effect of disturbance is minimized. A stochastic model of control system with stochastic cyber-attacks which satisfy the Markovian stochastic process is constructed. And we also present the stochastic attack models that a control system is possibly exposed to. Furthermore, applying H_∞ filtering technique-based on linear matrix inequalities (LMIs), the paper obtains sufficient conditions that ensure the filtering error dynamic is asymptotically stable and satisfies a prescribed ratio between cyber-attack sensitivity and disturbance sensitivity. Finally, the results are applied to the control of a Quadruple-tank process (QTP) under a stochastic cyber-attack and a stochastic disturbance. The simulation results underline that the designed filters is effective and feasible in practical application.

Key Words: Cyber attacks; control systems ; stochastic data DoS attack; stochastic data deception attack

1 Introduction

In recent years, the problem of cyber-attacks on controlled systems has attracted considerable attention [1]-[9]. Unlike traditional information technology (IT) system where cyber-security mainly involves the protection of data, cyber-attacks on control systems may influence the physical processes through the communication infrastructure. It will no doubt increase the challenging of networked control systems security and the detection and isolation of these threats. These challenging requirements increase the interest of researchers in the development of cyber-attack fault detection and isolation (FDI) techniques [3]-[4] and fault estimation methods. In the recent literatures, [5]-[6] proposed the centralized FDI schemes; [7]-[8] proposed the distributed FDI schemes. Moreover, it is well know that the fault estimation about complex cyber-attacks can significantly affect the safe and reliable operation of infrastructures. The main state estimators have Kalman filter and H_∞ filter. In contrast to the traditional Kalman filter, the advantage of the H_∞ filter is insensitive to the exact knowledge of systems state model, the stochastic properties of cyber-attacks and the disturbances. In addition, the H_∞ filtering technique can give a quantization upper bound based on the disturbance attenuation performance, which can maximize the fault sensitivity on the estimated signals and then identify the vulnerabilities of control systems as far as possible. However, as we know in our area of expertise, not so much research applying H_∞ filter technique to the security and safety of control systems, which motivates our research in this area.

The paper presents the robust H_∞ cyber-attacks estimation problem for control systems under stochastic cyber-attacks and disturbances. The basic idea is to design an observer to generate residual information with regard to cyber-attacks. Moreover the residual is required to remain the sensitive of the attack signals as much as possible while increasing robustness against disturbances. A stochastic model of control system with stochastic cyber-attacks which satisfy the Markovian stochastic process is constructed. And we also present the stochastic attack models that a control system is possibly exposed to. Furthermore, applying H_∞ filtering technique, the paper respectively designs filters for the control system with disturbance attenuation and without disturbance attenuation. Based on LMIs algorithm, the sufficient conditions are derived, which guarantee the asymptotical stability of the filtering error dynamic and the prescribed H_∞ performance level. Finally, the results are applied to the control of the QTP [11] that is subject to a stochastic data DoS attack and a stochastic disturbance. The simulation results underline that the designed filter efficiently solve the robust cyber-attacks estimation problem in practical application.

For convenience, we adopt the following notations: I identity matrix. $L_{F}^{2}([0,\infty);R^{n})$ space of nonanticipative stochastic processes $\phi(t)$ with respect to filtration F_t satisfying

$$\|\phi(t)\|_{L_F^2}^2 = E\int_0^\infty \|\phi(t)\|^2\, dt < \infty.$$

$E\{\cdot\}$ mathematical expectation operator with respect to the given probability measure P.

2 Problem Formulation

Consider the general framework to model a continuous-time linear system under stochastic cyber-attacks and disturbances

$$\begin{array}{rcl} \dot{x}(t) & = & Ax(t)+Bu(t)+\alpha(t)F_1a_k^a(t)+E_1w(t) \\ x(0) & = & x_0 \\ y(t) & = & Cx(t)+\beta(t)F_2a_k^s(t)+E_2\nu(t) \end{array} \qquad (1)$$

where $x(t)\in R^n$ is the state vector, x_0 is the initial state, $y(t)\in R^m$ is the measurement output, $u(t)\in R^r$ is the known input vector. $a_k^a(t)\in R^r$ denotes the actuator cyber-attack or the physical attack and $a_k^s(t)\in R^m$ denotes the sensor cyber-attack. Systems noise $w(t)$ and process noise

This work was supported by the Fonds National de la Recherche, Luxembourg, under the project CO11/IS/1206050 (SeSaNet).

$v(t)$ are Gaussian white noises with mean 0 and covariance Q and R, respectively. A, B, F_1, E_1,and C, F_2, E_2 are known constant matrices with appropriate dimensions. $\alpha(t)$ and $\beta(t)$ are Markovian stochastic processes taking the values of 0 and 1 and satisfy the following probability

$$\begin{aligned} E\{\alpha(t)\} = \Pr ob\{\alpha(t) = 1\} = \rho \\ E\{\beta(t)\} = \Pr ob\{\beta(t) = 1\} = \sigma \end{aligned} \tag{2}$$

where event $\alpha(t) = 1$ shows that the actuator of the system is subject to a cyber-attack, so an actuator cyber-attack $a_k^a(t)$ occurs; event $\alpha(t) = 0$ implies no a cyber-attack on the actuator. $\rho \in [0, 1]$ reflects the occurrence probability of the event that the actuator of the system is subject to a cyber-attack. Event $\beta(t) = 1$ shows that the sensor of the systems is subject to a cyber-attack, so systems have a sensor cyber-attack $a_k^s(t)$; while event $\beta(t) = 0$ implies no a cyber-attack on the sensor. $\sigma \in [0, 1]$ reflects the occurrence probability of the event that the sensor is subject to a cyber-attack. Assuming $\alpha(t)$ and $\beta(t)$ are independent stochastic variables and satisfy

$$E\{\alpha(t)\beta(t)\} = E\{\alpha(t)\}E\{\beta(t)\}. \tag{3}$$

Further, assuming $\alpha(t)$ and $\beta(t)$ are independent of measurement noises $w(t), v(t)$ and the initial state x_0. The general framework can be used to model a control system that is subject to different kinds of cyber-attacks. Generally, attacks targeting control systems can be mainly classified as physical attack and cyber-attacks including denial-of-service (DoS) attacks and deception attacks. In the sequel of the paper, we introduce these attack models that can be modelled by the stochastic systems model (1).

2.1 Modelling Stochastic Physical Attack

A control system may suffer from stochastic physical attacks from an internal operator or a disgruntled employee or an adversary, which often in conjunction with cyber-attacks. The adversary can steal or damage the field devices or the communication devices in order to remain a cyber-attack stealthy. For example, in [9] the adversary may damage the water level measurements when he was attempting to pump the water out of an irrigation system so that the cyber-attack remains stealthy. A stochastic physical attack can be modelled as

$$\begin{aligned} \alpha(t) &= \{0, 1\}, t \geq t_0 \\ \beta(t) &= 0 \\ a_k^a(t) &= f_k(t) \end{aligned} \tag{4}$$

where we consider $f_k(t)$ to be the physical attack.

2.2 Modelling Stochastic Data Denial-of-Service Attack

In stochastic data DoS attacks, the objective of the adversary is to prevent the actuator from receiving control commands or the controller from receiving sensor measurements. Therefore, by jamming the communication channels, compromising devices and preventing them from sending data, attacking the routing protocols, flooding the communication network with random data and so on, the adversary can launch a stochastic data DoS attack. Using the general framework (1), we can model a stochastic DoS attack on the actuator as

$$\begin{aligned} \alpha(t) &= \{0, 1\}, t \geq t_0 \\ F_1 &= B \\ a_k^a(t) &= -u(t) \end{aligned} \tag{5}$$

and model a stochastic data DoS attack on the sensors as

$$\begin{aligned} \beta(t) &= \{0, 1\}, t \geq t_0 \\ F_2 &= C \\ a_k^s(t) &= -x(t). \end{aligned} \tag{6}$$

2.3 Modelling Stochastic Data Deception Attack

In stochastic data deception attack, the adversary attempts to prevent the actuator or the sensor from receiving a integrity data, therefore, he sends false information $\widetilde{u}(t) \neq u(t)$ or $\widetilde{y}(t) \neq y$ from controllers or sensors. The false information can include: a wrong sender identity, an incorrect sensor measurement or an incorrect control input; an incorrect time when a measurement was observed, or inject a bias data that can't be detected in the system. The adversary can launch these stochastic attacks by obtaining the secret keys or by compromising some controllers or sensors. A stochastic data deception attack on the actuator can be modelled as

$$\begin{aligned} \alpha(t) &= \{0, 1\}, t \geq t_0 \\ F_1 &= B \\ a_k^a(t) &= -u(t) + b_k^a(t) \end{aligned} \tag{7}$$

and a stochastic data deception attack on the sensor can be modelled as

$$\begin{aligned} \beta(t) &= \{0, 1\}, t \geq t_0 \\ F_2 &= C \\ a_k^s(t) &= -x(t) + b_k^s(t) \end{aligned} \tag{8}$$

where $b_k^a(t)$ and $b_k^s(t)$ are deceptive data that the adversary attempts to launch on the actuator and the sensor, respectively.

3 Robust Cyber-Attacks Estimation Based on H_∞ filtering technique

In this section, our objective is to estimate the stochastic cyber-attack signal $a_k(t) = [\ a_k^a(t) \quad a_k^s(t)\ ]^T$ and maximize its sensitivity based on H_∞ filter technique [10]. We assume the following conditions are satisfied:(1) the pair $\{C, A\}$ is observable; (2) $\{C, E_2\}$ has full row rank; (3) $\{A, F_1, C, F_2\}$ has no transmission zeros.

These assumptions guarantee the detectability of the attacks in system (1). By making the residual as close to the attack signal as possible, then it can provide all information about the stochastic attack signal. i.e.

$$\begin{cases} a_k(t) = 0, \text{ if } r(t) = 0 \\ a_k(t) \neq 0, \text{ if } r(t) \neq 0. \end{cases}$$

Here, we ignore the control input because it does not affect to the residual when there are no modelling errors in the system transfer matrix. Therefore, the system (1) can be rewritten into

$$\begin{array}{rcl} \dot{x}(t) & = & Ax(t)+\alpha(t)F_1a_k^a(t)+E_1w(t) \\ x(0) & = & x_0 \\ y(t) & = & Cx(t)+\beta(t)F_2a_k^s(t)+E_2v(t). \end{array} \quad (9)$$

We set up the following filter

$$\begin{array}{rcl} \dot{\widehat{x}}(t) & = & A\widehat{x}(t)+Kr(t) \\ \widehat{x}(0) & = & 0 \\ r(t) & = & y(t)-C\widehat{x}(t) \end{array} \quad (10)$$

where $r(t)$ is the residual signal that is used as an estimation of the cyber-attack.

We consider system (1) and filter (10). Let $e(t)=x(t)-\widehat{x}(t)$, then we obtain the following error dynamic:

$$\begin{array}{rcl} \dot{e}(t) & = & \overline{A}e(t)+\overline{F}_1a_k(t)+\overline{E}_1d(t) \\ e(0) & = & e_0 \\ r(t) & = & Ce(t)+\overline{F}_2a_k(t)+\overline{E}_2d(t) \end{array} \quad (11)$$

with the matrices

$$\begin{array}{rcl} \overline{A} & = & (A-KC),\ \overline{F}_1=\left[\begin{array}{cc} F_1\alpha(t) & -\beta(t)KF_2 \end{array}\right] \\ \overline{F}_2 & = & \left[\begin{array}{cc} 0 & F_2\beta(t) \end{array}\right],\ \overline{E}_1=\left[\begin{array}{cc} E_1 & -KE_2 \end{array}\right] \\ \overline{E}_2 & = & \left[\begin{array}{cc} 0 & E_2 \end{array}\right] \end{array} \quad (12)$$

and the vectors

$$a_k(t)=\left[\begin{array}{c} a_k^a(t) \\ a_k^s(t) \end{array}\right],\ d(t)=\left[\begin{array}{c} w(t) \\ v(t) \end{array}\right]. \quad (13)$$

3.1 Robust H_∞ Estimation of Stochastic Cyber-Attacks

Our task here is to find an optimal estimator of the stochastic cyber-attack signal. The objective of the problem is to minimize the following performance index based on H_∞ filter technique.

$$J:=E\left\|G_{\tilde{z}a_k}\right\|_\infty=E\sup_{0<\|d_1\|^2<\infty}\frac{\|r-a_k\|^2}{\|d_1\|^2} \quad (14)$$

where

$$d_1(t)=\left[\begin{array}{c} a_k(t) \\ d(t) \end{array}\right].$$

This can be formulated according to the scheme given in Fig.1.

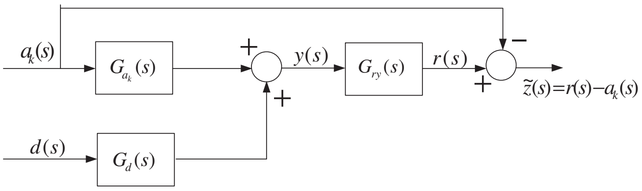

Fig. 1: Formulation of filtered cyber-attack estimation with disturbance attenuation

Remark: *Here $E\left\|G_{\tilde{z}a_k}\right\|_\infty$ is a new performance index. Because the cyber-attack presented in this paper satisfies a Markovian stochastic process, we introduce the mathematical expectation of $\left\|G_{\tilde{z}a_k}\right\|_\infty$ that is different from that of ref.[10].*

Based on the above discussion, the problem to be addressed in this paper is stated as follows. Given a prescribed disturbance attenuation level $\gamma>0$, design a H_∞ filter of the form (10) such that the filtering error dynamic satisfies the following performance indexes: 1) the error dynamic (11) with $d_1(t)=0$ is asymptotically stable; 2) the error dynamic (11) with $d_1(t)\neq 0$ ($d_1(t)\in L_{\mathcal{F}}^2([0,\infty);R^n)$) satisfies the following performance index

$$J_1=E\int_0^\infty[\|r(t)-a_k(t)\|^2-\gamma^2\|d_1(t)\|^2]dt\leq 0. \quad (15)$$

Before presenting the main results, we first give the following lemmas.

lemma: The error dynamic (11) with $d_1(t)=0$ is asymptotically stable, if there exists symmetric positive definite matrix $P>0$ and matrix X such that the following inequation holds

$$\Lambda=A^TP+PA-C^TX^T-XC<0. \quad (16)$$

Proof. Choose a Lyapunov functional for system (11) to be

$$V(t)=e^T(t)Pe(t)$$

where P is a symmetric positive definite matrix with appropriate dimension. Then we have

$$\dot{V}(t)=\eta^T(t)\Gamma\eta(t)$$

where

$$\begin{array}{rcl} \Gamma & = & \left[\begin{array}{ccc} \overline{A}^TP+P\overline{A} & P\overline{F}_1 & P\overline{E}_1 \\ * & 0 & 0 \\ * & * & 0 \end{array}\right] \\ \eta^T(t) & = & \left[\begin{array}{ccccc} e^T(t) & a_k^{Ta}(t) & a_k^{Ts}(t) & w^T(t) & v^T(t) \end{array}\right] \end{array}$$

an ellipsis * denotes a block symmetry matrix. When the $d_1(t)=0$, it has

$$\dot{V}(t)_{d_1(t)=0}=e^T(t)(\overline{A}^TP+P\overline{A})e(t). \quad (17)$$

Substituting (12) into (17) and let $X=PK$, by inequation (16) we get

$$\begin{array}{rcl} \dot{V}(t)_{d_1(t)=0} & = & e^T(t)(A^TP+PA-C^TX^T-XC)e(t) \\ & = & e^T(t)\Lambda e(t)<0 \end{array}$$

therefore, the error dynamic (11) with $d_1(t)=0$ is asymptotically stable. The proof of Lemma 1 is completed.

3.2 H_∞ Cyber-Attacks Estimation without Disturbances Attenuation

To detect attack faults reliably, the residual should be designed to have maximum sensitivity against attack signals. Therefore, to concentrate on the attack sensitivity, we first ignore the disturbance on the system (9), i.e. $d(t)=0$. For this case, the performance index (14) can be written as

$$J:=E\left\|G_{\tilde{z}a_k}\right\|_\infty=E\sup_{0<\|a_k\|^2<\infty}\frac{\|r-a_k\|^2}{\|a_k\|^2}. \quad (18)$$

For the objective of H_∞ estimation, the error dynamic (11) with cyber-attack $a_k(t) \neq 0$ must satisfy the following performance index

$$J_2 = E\int_0^\infty [\|r(t) - a_k(t)\|^2 - \gamma^2 \|a_k(t)\|^2]dt \leq 0. \quad (19)$$

We obtain the following theorem.

Theorem 1: *Consider the system (9) without disturbance, i.e. $d(t) = 0$. Given a scalar $\gamma > 0$, there exists a H_∞ filter of the form (10) if there exists symmetric positive definite matrix $P > 0$ and matrix X solving the following LMI*

$$E(\Pi_1) = \begin{bmatrix} \Phi_0 & \Phi_1 & \Phi_3 \\ * & \Phi_2 & \Phi_4 \\ * & * & \Phi_5 \end{bmatrix} < 0 \quad (20)$$

*where an ellipsis * denotes a block symmetry matrix and*

$$\begin{aligned} \Phi_0 &= A^TP + PA - C^TX^T - XC + C^TC \\ \Phi_1 &= \rho PF_1 - C^T \\ \Phi_2 &= I - \gamma^2 I \\ \Phi_3 &= -\sigma XF_2 + C^T(\sigma F_2 - I) \\ \Phi_4 &= -(\sigma F_2 - I) \\ \Phi_5 &= (\sigma F_2 - I)^T(\sigma F_2 - I) - \gamma^2 I. \end{aligned}$$

When the LMI is solvable, the filter H_∞ gain matrix is given by $K = P^{-1}X$.

Proof. By the proof of the Lemma 1, we can deduce that the error dynamic (11) with the cyber-attack $a_k(t) = 0$ is asymptotically stable. Next, we prove $J_2 < 0$ for $0 \neq a_k(t) \in L^2_{\mathcal{F}}([0,\infty); R^n)$. Note that for any $T > 0$

$$\begin{aligned} J_2(T) &= E\int_0^T [\|r(t) - a_k(t)\|^2 - \gamma_2^2 \|a_k(t)\|^2]dt \\ &\leq E\int_0^T [\|r(t) - a_k(t)\|^2 - \gamma_2^2 \|a_k(t)\|^2 + \dot{V}(t)]dt \\ &= \int_0^T \eta^T(t)E(\Pi_1)\eta(t)dt. \end{aligned}$$

Since $E(\Pi_1) < 0$,

$$\begin{aligned} J_2(T) &\leq -\lambda_{\min}(-E(\Pi_1))E\int_0^T (\|e(t)\|^2 + \|a_k(t)\|^2)dt \\ &\leq -\lambda_{\min}(-E(\Pi_1))\int_0^T \|a_k(t)\|^2 dt < 0 \end{aligned}$$

for any $0 \neq a_k(t) \in L^2_{\mathcal{F}}([0,\infty); R^n)$, which yield $J_2(t) \leq -\lambda_{\min}(-E(\Pi_1))\int_0^t(\|a_k(t)\|^2)dt < 0$, then an H_∞ filter of form (10) is constructed and the filter gain $K = P^{-1}X$. The proof of Theorem is completed.

3.3 Robust H_∞ Cyber-Attacks Estimation with Disturbances Attenuation

In practice, cyber-attacks estimation and disturbances attenuation problem have to be considered together. In this section, we further estimate the result for control systems with disturbances. A control system under stochastic cyber-attacks and disturbances can be modelled as the system (9). Extending the theorem 1, we obtain the following theorem.

Theorem 2: *Consider the system (9). Given a scalar $\gamma > 0$, there exists a H_∞ filter of the form (10) if there exists symmetric positive definite matrix $P > 0$ and matrix X solving the following LMI*

$$\begin{bmatrix} \Phi_0 & \Phi_1 & \Phi_3 & PE_1 & -XE_2 + C^TE_2 \\ * & \Phi_2 & \Phi_4 & 0 & -E_2 \\ * & * & \Phi_5 & 0 & (\sigma F_2 - I)^TE_2 \\ * & * & * & -\gamma^2 I & 0 \\ * & * & * & * & E_2^TE_2 - \gamma^2 I \end{bmatrix} < 0 \quad (21)$$

*where an ellipsis * denotes a block symmetry matrix and $\Phi_i(i = 0, \cdots, 5)$ is defined in (20). When the LMI is solvable, the filter H_∞ gain matrix is given by $K = P^{-1}X$.*

Proof. The proof is similar to that of the Theorem 1, therefore, the proof of the Theorem 2 is omitted.

In the case, we assume that the system (9) has no cyber-attacks, that is to say, the stochastic processes $\alpha(t)$ and $\beta(t)$ are assumed to be zero. The following corollary can be obtained from Theorem 2.

Corollary: *Consider the system (9) without stochastic cyber-attacks. Given a scalar $\gamma > 0$, there exists a H_∞ filter of the form (10) if there exists symmetric positive definite matrix $P > 0$ and matrix X solving the following LMI*

$$\begin{bmatrix} \Phi_0 & PE_1 & -XE_2 + C^TE_2 \\ * & -\gamma^2 I & 0 \\ * & * & E_2^TE_2 - \gamma^2 I \end{bmatrix} < 0 \quad (22)$$

where

$$\Phi_0 = A^TP + PA - C^TX^T - XC + C^TC.$$

The filter H_∞ gain matrix is given by $K = P^{-1}X$.

4 Application on the Quadruple-Tank Process Networks

In [11] a laboratory process that consists of four interconnected water tanks is presented, which will also be used here as a suitable simulation example. In this section, based on robust H_∞ filtering technique, we will estimate the cyber-attack on the QTP controlled through a wireless communication network, which is depicted in Fig.2. The model of the QTP is a nonlinear model and applying a linear transformation it can be described as (see [11]):

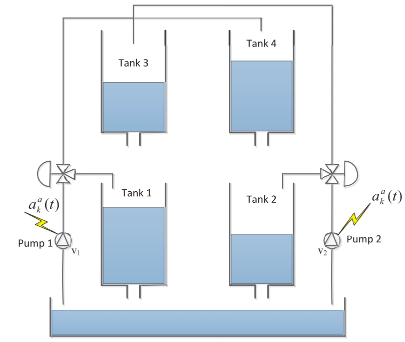

Fig. 2: QTP with wireless communication network

$$\begin{aligned} \dot{x} &= Ax + Bu \quad (23) \\ y &= Cx \end{aligned}$$

For operating point P_{-}[11], the system (23) has the following parameters:

$$\begin{aligned} A &= \left[\begin{array}{cccc} -0.0159 & 0 & 0.0419 & 0 \\ 0 & -0.0111 & 0 & 0.0333 \\ 0 & 0 & -0.0419 & 0 \\ 0 & 0 & 0 & -0.0333 \end{array}\right] \\ B &= \left[\begin{array}{cc} 0.0833 & 0 \\ 0 & 0.0628 \\ 0 & 0.0479 \\ 0.0312 & 0 \end{array}\right], C = \left[\begin{array}{cccc} 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0 \end{array}\right]. \end{aligned}$$

First assume that the system (23) is subject to a stochastic data DoS attack $a_k^a(t)$ on the actuator, but it has not been affected by the disturbance $w(t)$, i.e.

$$\begin{aligned} \alpha(t) &\in \{0,1\}, t \geq t_0 \\ F_1 &= B \\ a_k^a(t) &= -u(t) \\ w(t) &= 0. \end{aligned}$$

Then the system (23) can be described as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \alpha(t)Ba_k^a(t) \\ y(t) &= Cx(t). \end{aligned} \qquad (24)$$

As we mentioned before, because the control input does not affect to the residual, we ignored it in the sequel of the discussion.

Applying the Theorem 1, when the attacked probability $\rho = 0.5$, we obtain the $\gamma_{\min} = 1.0000000000047$. When we take $\gamma = 1.05$, the corresponding filter matrix obtained is

$$K = \left[\begin{array}{cc} 0.0933 & 0.1426 \\ -0.0343 & 0.1026 \\ 0.0657 & 0.2048 \\ 0.1040 & 0.1489 \end{array}\right].$$

Set the initial conditions as $x(0) = [0.8, -0.2, 1, -1]^T$and $\widehat{x}(0) = [0, 0, 0, 0]^T$. Fig.3. displays the time responses of the corresponding error dynamic and the QTP state with $a_k^a(t) = 0$ and $w(t) = 0$. It shows that the error dynamic is asymptotically stable and the QTP works well under this case. Fig.4. shows the cyber-attack signal and the time responses of the residual $r(t)$ under the attack $a_k^a(t)$. Obviously, the responses of the residual indicates that a cyber-attack occurs. Fig.5. shows that the time responses of the corresponding error dynamic and the QTP state under the cyber-attack. Further, Fig.5. demonstrates the QTP on the operating point P_- can not work normally under the attack $a_k^a(t)$.

Next we consider the robust filter for the system (23) under the attack $a_k^a(t)$ and the disturbance noise $w(t)$, then the system (23) can be described as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \alpha(t)Ba_k^a(t) + E_1w(t) \\ y(t) &= Cx(t) \end{aligned} \qquad (25)$$

where

$$E_1 = \left[\begin{array}{c} -0.4545 \\ -0.9090 \\ -0.1195 \\ -0.1562 \end{array}\right].$$

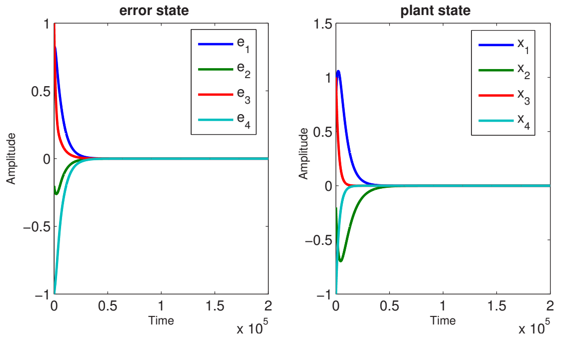

Fig. 3: The time responses of the corresponding error dynamic and the QTP state with $a_k^a(t) = 0$ and $w(t) = 0$

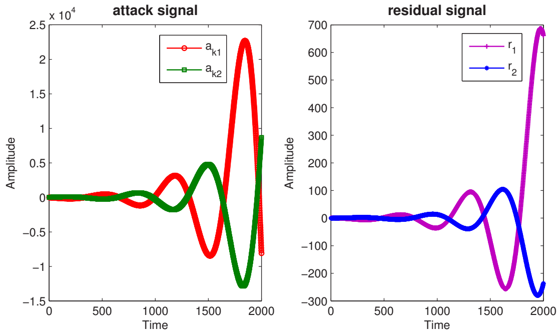

Fig. 4: The attack signal $a_k^a(t)$ and The time responses of residual under the attack $a_k^a(t)$

We take the attacked probability $\rho = 0.5$ and the H_∞ performance level $\gamma = 1.05$. Fig.6. displays the noise signal and the responses of the residual. The corresponding filter matrix obtained by Theorem 2 is

$$K = \left[\begin{array}{cc} 17.9795 & 37.7416 \\ 34.3542 & 76.2783 \\ 4.8394 & 10.3646 \\ 6.1680 & 12.9542 \end{array}\right]$$

Fig.7. gives the time responses of the corresponding error dynamic and the QTP state under the attack $a_k^a(t)$ and the disturbance noise $w(t)$, which shows the QTP can not work normally.

Finally, we simulate the case that the system (23) is only affected by the disturbance noise w(t), that is to say $a_k^a(t) = 0$. Applying the Corollary 1, we get the minimum

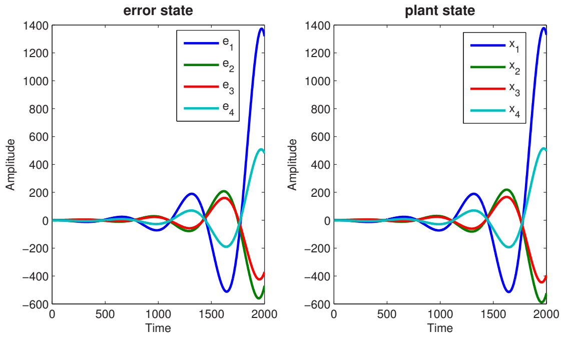

Fig. 5: The time responses of the corresponding error dynamic and the QTP state under the attack $a_k^a(t)$

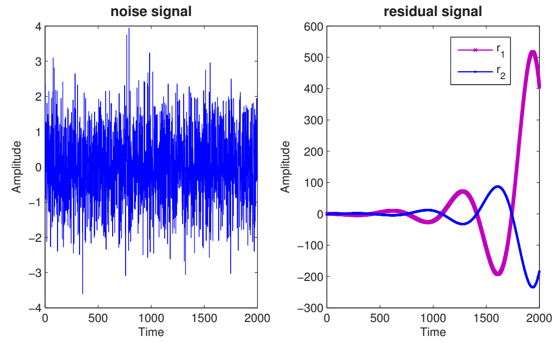

Fig. 6: The noise signal $w(t)$ and the time responses of residual under the attack $a_k^a(t)$ and the noise $w(t)$

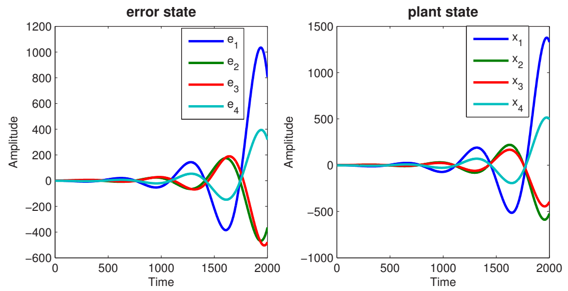

Fig. 7: The time responses of corresponding error dynamic and the QTP state under the DoS attack $a_k^a(t)$ and the noise $w(t)$

H_∞ performance level $\gamma = 0.00000099$. Comparing to the minimum H_∞ performance level of the system under cyber-attack, $0.00000099 \ll 1.0000000000047$, which indicates the designed filter can effectively attenuate the disturbance. Letting $\gamma = 0.3$, the corresponding filter matrix is

$$K = 10^{16}\begin{bmatrix} -2.5090 & 1.0290 \\ -5.0180 & 2.0581 \\ -0.6597 & 0.2706 \\ -0.8623 & 0.3537 \end{bmatrix}$$

Fig.8. displays the time responses of the residual and the QTP state under the disturbance. It is evident that no cyber-attack occurs. Moreover, Fig.8. underline the designed filter attenuate the disturbance very well so that the plant is still able to work normally under the disturbance. The simulation results clearly manifest that the cyber-attack has a larger impact than a disturbance noise on the control system.

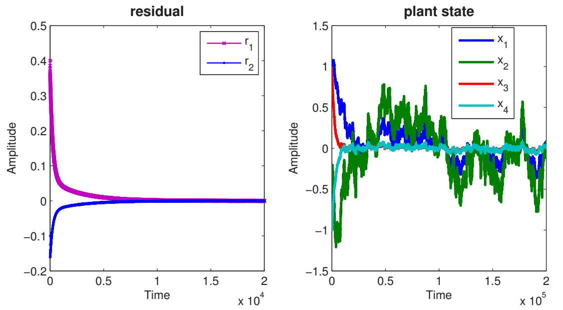

Fig. 8: The time responses of residual and the QTP state under the noise $w(t)$

5 Conclusion

This paper presents the cyber-attacks estimation for control systems under stochastic cyber-attacks and disturbances. Based on H_∞ filtering technique, filters that the residual can provide the maximum attack sensitivity are designed. The main work focus on attack signal estimation on control systems and we propose the models of the stochastic attacks that a control system is possibly exposed to. We applied the proposed scheme to the QTC under a stochastic data DoS attack and a stochastic noise. The simulation results demonstrate that designed filters efficiently solve the robust estimation problem of the cyber-attacks in practical application.

References

[1] K.C. Nguyen, T. Alpcan, T. Basar, A decentralized Bayesian attack detection algorithm for network security, *Proc. of 23rd Intl. Information Security Conf.Milan*,pp. 413-428, 2008.

[2] S. Sridhar, A. Hahn, and M. Govindarasu, Cyber–physical system security for the electric power grid, *Proceedings of the IEEE*, vol. 99, no. 1, pp. 1-15, 2012.

[3] A. H. Mohsenian-Rad and A. Leon-Garcia, “Distributed internet-based load altering attacks against smart power grids, *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667-674, 2011.

[4] F. Pasqualetti, F. D¨orfler, and F. Bullo, Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design,in *IEEE Conf. on Decision and Control and European Control Conference*, Orlando, FL, USA, Dec. 2011, pp. 2195–2201.

[5] E. Scholtz and B. Lesieutre, Graphical observer design suitable for large-scale DAE power system,in *Proceedings of the IEEE Conf. on Decision and Control*, Cancun, Dec. 2008, pp. 2955-2960.

[6] M. Aldeen and F. Crusca, Oberver-based fault detection and identification scheme for power systems, *IEE Proceedings-Generation, Transmission and Distribution*, vol.153, no.1, Jan. 2006, pp. 71-79.

[7] I. Shames, A. M. H. Teixeira, H. Sandberg, and K. H. Johansson, Distributed fault detection for interconnected seconde-order systems with applications to power networks,in *FIRST WORKSHOP ON SECURE CONTROL SYSTEMS*, 2010.

[8] J. Weimer, S. Kar and K. H. Johansson, Distributed detection and Isolation of Topology Attacks in Power Networks, *1st ACM International Conference on High Confidence Networked Systems (HiCoNS ’12)*. Beijing, China. April 2012.

[9] S. Amin, X. Litrico, S. S. Sastry and A. M. Bayen, Stealthy deception attacks on water scada systems,in *Proc. of the 13th ACM Int. Conf. on Hybrid systems: computation and control*, HSCC’10, New York, USA, 2010.

[10] J. Chen, R. J. Patton, *Robust Model-Based Fault Diagnosis for Dynamic Systems*. Springer Science+Business Media,LLC, 1999 chapter 8.

[11] K. H. Johansson, The Quadruple-Tank Process: A Multivariable Laboratory Process with an Adjustable Zero, *IEEE Transactions on Control Systems Technology*, VOL. 8, NO. 3, 2000.