Stochastic Cyber-Attacks Estimation for Nonlinear Control Systems Based on Robust H_∞ Filtering Technique

Yumei LI[1], Holger VOOS[1], Lin PAN[1], Mohamed DAROUACH[2], Changchun HUA[3]

1. Interdisciplinary Centre for Security Reliability and Trust (SnT), University of Luxembourg, L-1359, Luxembourg
E-mail: yumei.li@uni.lu, Holger.Voos@uni.lu, lin.pan@uni.lu

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

3. Institute of Electrical Engineering Yanshan, University, Qinhuangdao, 066004, China
E-mail: cch@ysu.edu.cn

Abstract: Based on robust H_∞ filtering technique, this paper presents the cyber-attacks estimation problem for nonlinear control systems under stochastic cyber-attacks and disturbances. A nonlinear H_∞ filter that maximize the sensitivity of the cyber-attacks and minimize the effect of the disturbances is designed. The nonlinear filter is required to be robust to the disturbances and the residual need to remain the sensitivity of the attacks as much as possible. Applying linear matrix inequality (LMI), the sufficient conditions guaranteeing the H_∞ filtering performance are obtained. Simulation results demonstrate that the designed nonlinear filter efficiently solve the robust estimation problem of the stochastic cyber-attacks.

Key Words: H_∞ filter, stochastic nonlinear system, stochastic cyber-attacks

1 INTRODUCTION

As control systems are connected using different, even open public networks, they are increasingly exposed to cyber-attacks. Therefore, security and safety of control systems become increasingly critical. Recently, the cyber-attacks on control systems has attracted considerable attentions [1]-[12]. Cyber-attacks on control systems may influence the physical processes through the communication infrastructure, it will no doubt increase the challenging of security, the detection and isolation of these threats in control systems, which increase the interest of researchers in the development of cyber-attack fault estimation, fault detection and isolation (FDI)techniques [3]-[7]. [8]-[9] proposed the centralized FDI schemes; [10]-[11] proposed the distributed FDI schemes. As we know, H_∞ filter is an important state estimator in control area and it is insensitive to the exact knowledge of systems state model, the stochastic properties of cyber-attacks and the disturbances. Moreover, the H_∞ filter can not only maximize the fault sensitivity on the estimated signals but also identify the vulnerabilities of control systems as far as possible. However, in our area of expertise, not so much research applying H_∞ filtering technique to the cyber-attacks estimation of control systems, especially nonlinear control systems, which motivates our research in this area.

Based on H_∞ filtering technique, the paper presents the stochastic cyber-attacks estimation problem for nonlinear control systems under stochastic cyber-attacks and disturbances. A robust nonlinear H_∞ filter is designed, which maximize the sensitivity of the cyber-attacks and minimize the effect of the disturbances. We also construct a stochastic nonlinear model under stochastic cyber-attacks which satisfy the Markovian stochastic process. Generally speaking, in practice, most of nonlinear models including attack information can be transformed into the proposed nonlinear form by using the Taylor's expansion. Therefore, it is no doubt that the new model is more representative and widespread adaptability in practical application. Moreover, we use a simply way to deal with the nonlinear term. During the process of proving main results, we regard the nonlinear term as a state vector, which reduces the constraint on the nonlinear term largely and makes the proof of main results be easier. In contrast to the existing literatures, we also use norm-bounded condition of the nonlinear term, however, no extra constraints are increased on the nonlinear term. Therefore, the obtained results have less conservativeness than existing results. Applying the H_∞ filtering technique-based on LMI, some sufficient conditions are derived, which guarantee the filtering augmented dynamic satisfies a given disturbance attenuation level as well as a prescribed ratio between cyber-attacks sensitivity and disturbance sensitivity. Simulation results underline that the designed nonlinear H_∞ filter is effective and feasible. For convenience, we adopt the following notations: I is corresponding identity matrix; $\mathbf{0}$ is corresponding zero matrix; $E\{\cdot\}$ denotes mathematical expectation operator with respect to the given probability measure P.

This work was supported by the Fonds National de la Recherche, Luxembourg, under the project CO11/IS/1206050 (SeSaNet) and the National Natural Science Foundation of China under Grant 61273222.

978-1-4799-7016-2/15/$31.00

2 PROBLEM FORMULATION

Consider the following nonlinear system under stochastic cyber-attacks and disturbances

$$\begin{aligned} \dot{x}(t) &= Ax(t)+cf(x(t))+B(u(t)+\alpha(t)a_k^a(t))+E_1w(t) \\ x(0) &= x_0 \\ y(t) &= C(x(t)+\beta(t)a_k^s(t))+E_2v(t) \end{aligned} \tag{1}$$

where $x(t) \in R^n$ is the state vector, $f(x)$ is the nonlinear term, c is a constant that denotes the nonlinear coupling strength. x_0 is the initial state, $y(t) \in R^m$ is the measurement output, $u(t) \in R^r$ is the control input. $a_k^a(t) \in R^r$ denotes the actuator cyber-attack and $a_k^s(t) \in R^n$ denotes the sensor cyber-attack. $w(t)$ and $v(t)$ are stochastic noises. A, B, E_1 and C, E_2 are known constant matrices with appropriate dimensions. $\alpha(t)$ and $\beta(t)$ are Markovian stochastic processes taking the values 0 and 1 and satisfy the following probability

$$\begin{aligned} E\{\alpha(t)\} &= Prob\{\alpha(t)=1\}=\rho \\ E\{\beta(t)\} &= Prob\{\beta(t)=1\}=\sigma. \end{aligned} \tag{2}$$

Herein, the event $\alpha(t)=1$(or $\beta(t)=1$) shows the actuator (or the sensor) of the system is subject to a cyber-attack, so an actuator cyber-attack $a_k^a(t)$ (or a sensor cyber-attack $a_k^s(t)$) occurs; event $\alpha(t)=0$ (or $\beta(t)=0$) implies no a cyber-attack on the actuator (or on the sensor). $\rho \in [0,1]$ (or $\sigma \in [0,1]$) reflects the occurrence probability of the event that the actuator (or the sensor) of the system is subject to a cyber-attack. While $\alpha(t)$ and $\beta(t)$ are independent from each other, they are also independent from stochastic noises $w(t)$, $v(t)$ and the initial state x_0.

In order to deal with the nonlinear term effectively, we also give the following assumption that will be used in the sequel of our study.

Assumption 1: $\exists \lambda > 0$ such that the unknown nonlinear term $f(x(t))$ satisfies the following norm-bounded condition

$$\|f(x(t))\| \le \lambda \|x(t)\|, \forall x \in R^n.$$

Generally, cyber-attacks targeting control systems can be mainly classified as the stochastic DoS attacks and the stochastic deception attacks. In [12], we introduce these stochastic cyber-attacks in detail. They can be respectively modelled as follows:

1) A stochastic DoS attack on the actuator and on the sensor are modelled as

$$\begin{cases} \alpha(t) \in \{0,1\}, t \ge t_0 \\ a_k^a(t) = -u(t) \end{cases} \text{ and } \begin{cases} \beta(t) \in \{0,1\}, t \ge t_0 \\ a_k^s(t) = -x(t) \end{cases}$$

2) A stochastic data deception attack on the actuator and on the sensor are modelled as

$$\begin{cases} \alpha(t) \in \{0,1\}, t \ge t_0 \\ a_k^a(t) = -u(t)+b_k^a(t) \end{cases} \text{ and } \begin{cases} \beta(t) \in \{0,1\}, t \ge t_0 \\ a_k^s(t) = -x(t)+b_k^s(t) \end{cases}$$

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.

3 MAIN RESULTS

In this section, our objective is to estimate the stochastic cyber-attack and maximize its fault sensitivity based on H_∞ filtering technique. In order to guarantee the detectability of the attacks in system (1), we assume that the following conditions are satisfied: 1) the pair $\{C,A\}$ is observable; 2) $\{C,E_2\}$ has full row rank; 3) $\{A,B,C\}$ has no transmission zeros. These assumptions guarantee the detectability of the attacks in system (1).

For simplification, we ignore the control input and only consider the following system

$$\begin{aligned} \dot{x}(t) &= Ax(t)+cf(x(t))+\alpha(t)Ba_k^a(t)+E_1w(t) \\ x(0) &= x_0 \\ y(t) &= Cx(t)+\beta(t)Ca_k^s(t)+E_2v(t). \end{aligned} \tag{3}$$

The nonlinear filter is constructed as follows

$$\begin{aligned} \dot{\widetilde{x}}(t) &= \widetilde{A}\widetilde{x}(t)+\widetilde{c}f(\widetilde{x}(t))+Kr(t) \\ \widetilde{x}(0) &= \widetilde{x}_0 \\ r(t) &= y(t)-C\widetilde{x}(t) \end{aligned} \tag{4}$$

where $r(t)$ is the residual signal that is used as the estimation of the stochastic attack signal. $\widetilde{c}$ represents the nonlinear coupling strength, when $\widetilde{c}=0$, (4) is a linear filter.

Remark 1: $\widetilde{c}$ is a known scalar in filter (4), it can be selected or designed according to the nonlinear coupling constant c. when $c=0$, i.e. the system (3) is a linear system, we can correspondingly design a linear filter for system (3) by selecting $\widetilde{c}=0$. Let

$$\xi(t)=\begin{bmatrix} x(t) \\ \widetilde{x}(t) \end{bmatrix}, g(\xi(t))=\begin{bmatrix} f(x(t)) \\ f(\widetilde{x}(t)) \end{bmatrix}$$

then we obtain the following augmented dynamic system:

$$\begin{aligned} \dot{\xi}(t) &= \overline{A}\xi(t)+\overline{c}g(\xi(t))+\overline{B}a_k(t)+\overline{E}_1d(t) \\ \xi(0) &= \xi_0 \\ r(t) &= \overline{C}\xi(t)+\overline{F}a_k(t)+\overline{E}_2d(t) \end{aligned} \tag{5}$$

with the following matrices

$$\begin{aligned} \overline{A} &= \begin{bmatrix} A & 0 \\ KC & \widetilde{A}-KC \end{bmatrix}, \overline{E}_1=\begin{bmatrix} E_1 & 0 \\ 0 & KE_2 \end{bmatrix} \\ \overline{B} &= \begin{bmatrix} \alpha(t)B & 0 \\ 0 & \beta(t)KC \end{bmatrix}, \overline{c}=\begin{bmatrix} cI & 0 \\ 0 & \widetilde{c}I \end{bmatrix} \\ \overline{C} &= \begin{bmatrix} C & -C \end{bmatrix}, \overline{F}=\begin{bmatrix} 0 & \beta(t)C \end{bmatrix} \\ \overline{E}_2 &= \begin{bmatrix} 0 & E_2 \end{bmatrix} \end{aligned} \tag{6}$$

and the vectors

$$a_k(t)=\begin{bmatrix} a_k^a(t) \\ a_k^s(t) \end{bmatrix}, d(t)=\begin{bmatrix} w(t) \\ v(t) \end{bmatrix}. \tag{7}$$

Our objective is to make the residual as close to the stochastic attack signal as possible, then it can provide all information about the stochastic attack events. i.e.

$$\begin{cases} \alpha(t)=0 \text{ and } \beta(t)=0, \text{ if } r(t)=0 \\ \alpha(t)=1 \text{ or } \beta(t)=1, \text{ if } r(t)\neq 0. \end{cases} \tag{8}$$

Assume that B is a $n \times r$ matrix and C is a $m \times n$ $(m \leq n)$ matrix, we construct a stochastic attack signal as follows

$$u_k(t) = \alpha(t)\mathbf{I}_{m\times r}a_k^a + \beta(t)\mathbf{I}_{m\times n}a_k^s$$

which is a linear combination of stochastic attacks on the actuator and on the sensor. Herein, we define matrices $\mathbf{I}_{m\times r}$ as follows:

$$\mathbf{I}_{m\times r} := \left[\begin{array}{cc} I_m & \mathbf{0}_{m\times(r-m)} \end{array}\right] \tag{9}$$

where the subscript $m \times r$ indicates that $\mathbf{I}$ is a matrix of m rows and r columns, I_m denotes a m order unit matrix and $\mathbf{0}_{m\times(r-m)}$ denotes a $m \times (r-m)$ zero matrix. Especially, when $m = r$, we define $\mathbf{I}_{m\times r} = I_m$ i.e. $\mathbf{I}_{m\times r}$ is a m order unit matrix. The matrix $\mathbf{I}_{m\times n}$ also has the same definition.

Next, we set up an optimal estimator that can minimize the following performance index.

$$J := E\left\|G_{\tilde{z}a_k}\right\|_\infty = E \sup_{0<\|d_1\|^2<\infty} \frac{\|r(t)-u_k(t)\|^2}{\|d_1\|^2} \tag{10}$$

where

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

Let

$$\theta(t) = \left[\begin{array}{cc} \alpha(t)\mathbf{I}_{m\times r} & \beta(t)\mathbf{I}_{m\times n} \end{array}\right] \tag{11}$$

and

$$\left\{\begin{array}{l} \theta(t) = 0 \Leftrightarrow \alpha(t) = 0 \text{ and } \beta(t) = 0 \\ \theta(t) = 1 \Leftrightarrow \alpha(t) = 1 \text{ or } \beta(t) = 1. \end{array}\right. \tag{12}$$

then H_∞ performance index (10) is equivalent to the following index

$$J := E\left\|G_{\tilde{z}a_k}\right\|_\infty = E \sup_{0<\|d_1\|^2<\infty} \frac{\|r(t)-\theta a_k(t)\|^2}{\|d_1\|^2} \tag{13}$$

and (8) is equivalent to the following implication

$$\left\{\begin{array}{l} \theta(t) = 0, \text{ if } r(t) = 0 \\ \theta(t) = 1, \text{ if } r(t) \neq 0. \end{array}\right.$$

In order to get an effective transfer function from input signal to output signal, the nonlinear term $g(\xi(t))$ is regarded as an unknow input signal in the augmented system (5).

First, we give the following definition.

Definition 1: The augmented dynamic (5) with the unknown input $g(\xi)$ is said to have a disturbance attenuation level δ $(\delta > 0)$, if it is asymptotically stable for disturbance $d(t) = 0$ and it holds that

$$\int_0^\infty \|r\|^2 dt < \int_0^\infty \delta \|d\|^2 dt \tag{14}$$

for nonzero disturbance $d(t)$ $(d(t) \in L_f^2([0,\infty); R^n))$.

Based on the above discussion, the problem to be addressed in this paper is stated as follows. Given a performance level $\gamma > 0$, design a nonlinear H_∞ filter of the form (4) such that the filtering augmented dynamic satisfies: 1) when the stochastic cyber-attack event $\theta(t) = 0$, the augmented dynamic (5) under the unknown input $g(\xi)$ has a disturbance attenuation level $\delta > 0$; 3) when the stochastic cyber-attack event $\theta(t) = 1$, the augmented dynamic (5) with the unknown input $g(\xi(t))$ satisfies the following H_∞ performance index

$$J_0 = E\int_0^\infty [\|r(t)-\theta a_k(t)\|^2 - \gamma^2\|d_1(t)\|^2]dt \leq 0. \tag{15}$$

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

Lemma 1. When the stochastic attack events $\theta(t) = 0$, there are the following conclusions:

1) the augmented dynamic (5) with the unknown input $g(\xi(t))$ is asymptotically stable for disturbances $d(t) = 0$, if there exists a scalar $\tau \geq 0$, a symmetric positive definite matrices $P_1 > 0$ and matrices X, Y such that the following LMI holds

$$\Gamma_0 = \left[\begin{array}{cccc} \Psi_{01} & C^TX^T & cP_1 & 0 \\ * & \Psi_{02} & 0 & \widetilde{c}P_1 \\ * & * & -\tau I & 0 \\ * & * & * & -\tau I \end{array}\right] < 0 \tag{16}$$

2) the augmented dynamic (5) with the unknown input $g(\xi(t))$ satisfies disturbance attenuation condition (14) for nonzero disturbances $d(t)$ $(d(t) \in L_f^2([0,\infty); R^n))$, if there exists a scalar $\tau \geq 0$, a symmetric positive definite matrices $P_1 > 0$ and matrices X, Y such that the following LMI holds

$$\Lambda = \left[\begin{array}{cccccc} \Psi_{11} & \Psi_{12} & cP_1 & 0 & P_1E_1 & C^TE_2 \\ * & \Psi_{22} & 0 & \widetilde{c}P_1 & 0 & \Psi_{26} \\ * & * & -\tau I & 0 & 0 & 0 \\ * & * & * & -\tau I & 0 & 0 \\ * & * & * & * & -\delta^2 I & 0 \\ * & * & * & * & * & \Psi_{66} \end{array}\right] < 0 \tag{17}$$

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

$$\begin{aligned} \Psi_{01} &= A^TP_1 + P_1A + \tau\lambda^2 I \\ \Psi_{02} &= Y^T + Y - C^TX^T - XC + \tau\lambda^2 I \\ \Psi_{11} &= A^TP_1 + P_1A + \tau\lambda^2 I + C^TC \\ \Psi_{12} &= C^TX^T - C^TC \\ \Psi_{22} &= Y^T + Y - C^TX^T - XC + \tau\lambda^2 I + C^TC \\ \Psi_{26} &= -C^TE_2 + XE_2 \\ \Psi_{66} &= -(\delta^2 I - E_2^TE_2). \end{aligned}$$

Proof. Choose a Lyapunov functional for system (5) to be

$$V(t) = \xi^T(t)P\xi(t)$$

where $P > 0$ is symmetric positive definite matrix with appropriate dimension. Then we have

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

where

$$\begin{aligned} \Gamma &= \left[\begin{array}{cccc} \overline{A}^TP + P\overline{A} & P\overline{c} & P\overline{B} & P\overline{E}_1 \\ * & 0 & 0 & 0 \\ * & * & 0 & 0 \\ * & * & * & 0 \end{array}\right] \\ \eta^T(t) &= \left[\begin{array}{cccc} \xi(t)^T & g^T(\xi(t)) & d^T(t) & a_k^T(t) \end{array}\right]. \end{aligned}$$

When $\theta(t)=0$ and $d(t)=0$, it has

$$\begin{aligned}\dot{V}(t)_{\theta(t)=0} &= \xi^T(t)(\overline{A}^T P+P\overline{A})\xi(t)+g^T(\xi(t))\overline{c}^T P\xi(t)\\ &\quad +\xi^T(t)P\overline{c}g(\xi(t))\\ &= \begin{bmatrix} \xi(t)^T & g^T(\xi(t)) \end{bmatrix}\begin{bmatrix} \overline{A}^T P+P\overline{A} & P\overline{c} \\ \overline{c}^T P & 0 \end{bmatrix}\begin{bmatrix} \xi(t) \\ g(\xi(t)) \end{bmatrix}.\end{aligned}$$

Let $L=\lambda^2\xi(t)^T\xi(t)-g^T(\xi(t))g(\xi(t))$, since assumption 1, $L\geq 0$, then for a scalar $\tau\geq 0$, we have

$$\begin{aligned}\dot{V}(t)_{\theta(t)=0} &\leq \dot{V}(t)_{\theta(t)=0}+\tau L \qquad (18)\\ &= \eta_0^T(t)\begin{bmatrix} \overline{A}^T P+P\overline{A}+\tau\lambda^2 I & P\overline{c} \\ \overline{c}^T P & -\tau I \end{bmatrix}\eta_0(t).\end{aligned}$$

Substituting (6) into (18) and let

$$\begin{aligned}P &= \begin{bmatrix} P_1 & 0 \\ 0 & P_1 \end{bmatrix},\ Y=P_1\widetilde{A},\ X=P_1K\\ \eta_0^T(t) &= \begin{bmatrix} \xi(t)^T & g^T(\xi(t)) \end{bmatrix}\end{aligned}$$

by LMI (16), we obtain

$$\dot{V}(t)_{\theta(t)=0}=\eta_0(t)^T\Gamma_0\eta_0(t)<0.$$

Therefore, when the stochastic cyber-attack event $\theta(t)=0$ and disturbances $d(t)=0$, the augmented dynamic (5) with the unknown input $g(\xi(t))$ is asymptotically stable. Next, we prove $\int_0^\infty \|r\|^2 dt<\int_0^\infty \delta\|d\|^2 dt$ for nonzero disturbances $d(t)$ $(d(t)\in L_f^2([0,\infty);R^n))$. Note that for any $T>0$

$$\begin{aligned}J_1(T) &= \int_0^T[\|r(t)\|^2-\delta^2\|d(t)\|^2]dt\\ &= \int_0^T[\|r(t)\|^2-\delta^2\|d(t)\|^2]dt+V(t)-V(t)\\ &\leq \int_0^T[\|r(t)\|^2-\delta^2\|d(t)\|^2+\dot{V}(t)]dt\\ &= \int_0^T \eta_1^T(t)\Lambda\eta_1(t)dt.\\ \eta_1^T(t) &= \begin{bmatrix} \xi(t)^T & g^T(\xi(t)) & d^T(t) \end{bmatrix}\end{aligned}$$

since the LMI (17) is equivalent to $\Lambda<0$,

$$J_1(T) \leq -\lambda_{\min}(-\Lambda))\int_0^T\|d(t)\|^2dt<0$$

for any $0\neq d(t)\in L_f^2([0,\infty);R^n)$, which yield $J_1(t)\leq -\lambda_{\min}(-\Lambda))\int_0^t(\|d(t)\|^2)dt<0$, therefore, the augmented dynamic (5) with the unknown input $g(\xi(t))$ satisfies disturbance attenuation condition (14). The proof of Lemma 1 is completed.

In according to Definition 1, Lemma 1 is actually equivalent to the conception that the augmented dynamic (5) has a disturbance attenuation level δ.

3.1 Stochastic Cyber-Attacks Estimation Based on Robust H_∞ Filtering Technique

In this section, based on robust H_∞ filtering technique, we estimate the stochastic cyber-attacks that the control system is possibly subjected to. First, we consider the system (3) under stochastic cyber-attacks and noise disturbances and we obtain the following theorem.

Theorem 1: Consider the system (3). Given scalars $\gamma\geq\delta>0$, there exists a H_∞ filter of the form (4) if there exists a scalar $\tau\geq 0$, symmetric positive definite matrices $P_1>0$ and matrices X, Y solving the following LMI

$$\begin{bmatrix} \Phi_{11} & \Phi_{12} & cP_1 & 0 & \Phi_{15} & \Phi_{16} & \Phi_{17} & \Phi_{18} \\ * & \Phi_{22} & 0 & \widetilde{c}P_1 & 0 & \Phi_{26} & \Phi_{27} & \Phi_{28} \\ * & * & -\tau I & 0 & 0 & 0 & 0 & 0 \\ * & * & * & -\tau I & 0 & 0 & 0 & 0 \\ * & * & * & * & \Phi_{55} & 0 & 0 & 0 \\ * & * & * & * & * & \Phi_{66} & \Phi_{67} & \Phi_{68} \\ * & * & * & * & * & 0 & \Phi_{77} & \Phi_{78} \\ * & * & * & * & * & * & * & \Phi_{88} \end{bmatrix}<0 \qquad (19)$$

herein

$$\begin{aligned}\Phi_{11} &= A^T P_1+P_1A+\tau\lambda^2 I+C^T C\\ \Phi_{12} &= C^T X^T-C^T C\\ \Phi_{15} &= P_1E_1,\ \Phi_{16}=C^T E_2\\ \Phi_{17} &= \rho P_1B-\rho C^T\mathbf{I}_{m\times r},\ \Phi_{18}=\sigma C^T(C-\mathbf{I}_{m\times n})\\ \Phi_{22} &= Y^T+Y-C^T X^T-XC+\tau\lambda^2 I+C^T C\\ \Phi_{26} &= -C^T E_2+XE_2,\ \Phi_{27}=\rho C^T\mathbf{I}_{m\times r}\\ \Phi_{28} &= -\sigma C^T(C-\mathbf{I}_{m\times n})+\sigma XC\\ \Phi_{55} &= -\delta^2 I,\ \Phi_{66}=-(\delta^2 I-E_2^T E_2)\\ \Phi_{67} &= -\rho E_2^T\mathbf{I}_{m\times r},\ \Phi_{68}=\sigma E_2^T(C-\mathbf{I}_{m\times n})\\ \Phi_{77} &= \rho^2\mathbf{I}_{m\times r}^T\mathbf{I}_{m\times r}-\gamma^2 I\\ \Phi_{78} &= -\rho\sigma\mathbf{I}_{m\times r}^T(C-\mathbf{I}_{m\times n})\\ \Phi_{88} &= \sigma^2(C^T-\mathbf{I}_{m\times n}^T)(C-\mathbf{I}_{m\times n})-\gamma^2 I.\end{aligned}$$

When the LMI is solvable, the filter matrices are given by $\widetilde{A}=P_1^{-1}Y$, $K=P_1^{-1}X$.

Proof. Since the Lemma 1, we can deduce that the augmented dynamic (5) with the unknown input $g(\xi)$ has a disturbance attenuation level $\delta>0$ when the stochastic cyber-attack event $\theta(t)=0$. Next, we prove when the stochastic cyber-attack event $\theta(t)=1$, the augmented dynamic (5) satisfies $J_0<0$. Note that for any $T>0$

$$\begin{aligned}J_0(T) &= E\int_0^T[\|r(t)-\theta a_k(t)\|^2-\gamma^2\|d_1(t)\|^2]dt\\ &= E\int_0^T[\|r(t)-\theta a_k(t)\|^2-\gamma^2\|a_k(t)\|^2\\ &\quad -\gamma^2\|g(\xi(t))\|^2-\gamma^2\|d(t)\|^2]dt\\ &\leq E\int_0^T[\|r(t)-\theta a_k(t)\|^2-\gamma^2\|a_k(t)\|^2\\ &\quad -\delta^2\|d(t)\|^2+\dot{V}(t)]dt\\ &= \int_0^T\eta^T(t)E(\Pi)\eta(t)dt.\end{aligned}$$

Since the LMI (19) is equivalent to $E(\Pi) < 0$,

$$\begin{aligned} J_1(T) &\leq -\lambda_{\min}(-E(\Pi))E\int_0^T (\|\xi(t)\|^2 + \|a_k(t)\|^2)dt \\ &\leq -\lambda_{\min}(-E(\Pi))\int_0^T \|a_k(t)\|^2 dt < 0 \end{aligned}$$

for any $0 \neq a_k(t) \in L_F^2([0,\infty);R^n)$, which yield $J_0(t) \leq -\lambda_{\min}(-E(\Pi))\int_0^t (\|a_k(t)\|^2)dt < 0$, then a H_∞ filter of form (4) is constructed and the filter matrices $\widetilde{A} = P_1^{-1}Y$, $K = P_1^{-1}X$. That completes the proof of Theorem 1.

4 SIMULATION RESULTS

In this section, we provide a simulation example to illustrate the effectiveness of our results.

Example 1. Consider the nonlinear system with the following parameters:

$$A = \begin{bmatrix} -0.9 & 0 & 0.1 & 0 \\ 0 & -0.2 & 0 & -0.1 \\ 0 & 0 & -0.4 & 0 \\ 0 & 0 & 0 & -0.3 \end{bmatrix}, E_1 = \begin{bmatrix} 0.1 \\ -0.1 \\ 0.2 \\ -0.1 \end{bmatrix}, c = 1$$

$$B = \begin{bmatrix} 0.03 & 0 \\ 0 & 0.04545 \\ 0 & 0.09090 \\ 0.09 & 0 \end{bmatrix}, C = \begin{bmatrix} 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0 \end{bmatrix}$$

$$E_2 = 0\, f(x(t)) = \begin{bmatrix} 0.5\sin(x_1(t)) - 0.5\sin(x_3(t)) \\ 0.1x_2^2(t) - 0.1x_4^2(t) \\ 0 \\ 0 \end{bmatrix}$$

Assuming that it is subjected to a stochastic data DoS attack on the actuator, i.e.

$$\begin{aligned} \alpha(t) &\in \{0,1\}, t \geq t_0 \\ a_k^a(t) &= -u(t) \end{aligned} \tag{20}$$

Set the initial conditions as $x(0) = [0.8, -0.5, -0.8, 0.5]^T$, $\widetilde{x}(0) = [-1.5, -0.2, 1.5, 0.2]^T$ and select the nonlinear coupling strength $\widetilde{c} = 1$. First, we detect the filter case that the stochastic event $\alpha(t) = 0$ and $w = 0$, according to Lemma 1, the augmented dynamic should be asymptotically stable. Fig.1. displays the time response of the residual signals and the augmented dynamic under the case, which shows the augmented dynamic is asymptotically stable. Further, we simulate the case that the system is only affected by the stochastic noise, i.e. $\alpha(t) = 0$ and $w(t) \neq 0$. Let $\gamma = 0.9$, the corresponding filter matrix is

$$\widetilde{A} = \begin{bmatrix} -1.5429 & 0.0283 & -0.0948 & 0.0273 \\ 0.0284 & -1.7690 & 0.0923 & -0.1087 \\ -0.1003 & 0.0983 & -1.5813 & 0.0844 \\ 0.0287 & -0.1171 & 0.0829 & -1.5154 \end{bmatrix}$$

$$K = \begin{bmatrix} 0.1282 & -0.0027 \\ -0.0027 & 0.1463 \\ 0.0088 & -0.0092 \\ -0.0028 & 0.0126 \end{bmatrix}.$$

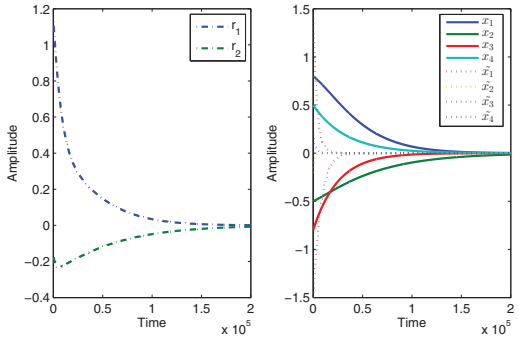

Figure 1: The time responses of the residual and the augmented dynamic with $\alpha(t) = 0$ and $w = 0$

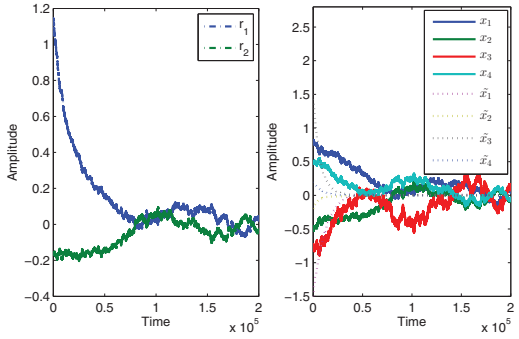

Figure 2: The state responses of the augmented dynamic under the noise $w(t)$

Fig.2. displays the time responses of the residual and the augmented dynamic under the noise $w(t)$. Fig.2. underlines the designed filter attenuate the noise disturbance very well so that the system is still able to work normally under the stochastic noise.

Next, we consider the robust filter of the system under the stochastic attack $a_k^a(t)$ and the stochastic noise $w(t)$. When $\alpha(t) = 1$ and $\rho = 0.8$, $\gamma = 0.9$ according to the Theorem 1, the corresponding filter matrices are

$$\widetilde{A} = \begin{bmatrix} -1.8443 & 0.1353 & -0.3742 & 0.0871 \\ 0.1426 & -1.9777 & 0.5018 & -0.3535 \\ -0.3706 & 0.4650 & -2.5837 & 0.4927 \\ 0.0864 & -0.3535 & 0.5327 & -2.0268 \end{bmatrix}$$

$$K = \begin{bmatrix} 0.1662 & 0.0053 \\ -0.0524 & 0.1776 \\ 0.0481 & -0.0387 \\ -0.0174 & 0.0291 \end{bmatrix}$$

Fig.3. shows the attack signal $a_k^a(t)$ and the time responses of the residual signals under the attack.Fig.4. displays the noise signal and the responses of the residual. Fig.5. gives the time response of the augmented dynamic under the case, which shows the control system can not work normally.

5 CONCLUSION

A nonlinear H_∞ filter is designed, which solve the stochastic cyber-attacks estimation problem for nonlinear control

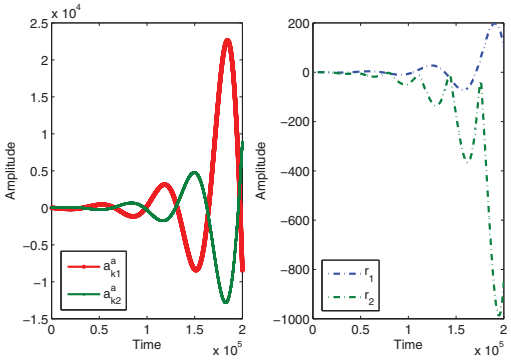

Figure 3: The stochastic attack signal and the time response of the residual under the attack $a_k^a(t)$

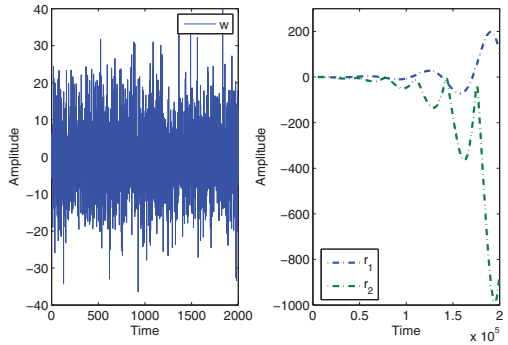

Figure 4: The stochastic noise signal and the time response of the residual under the attack $a_k^a(t)$ and the noise $w(t)$

systems under stochastic cyber-attacks and disturbances. The obtained results are applied on a nonlinear control system under a stochastic data DoS attack and disturbance. The simulation results underline that designed nonlinear H_∞ filter is effective and feasible 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, 413-428, 2008.

[2] S. Sridhar, A. Hahn, and M. Govindarasu, Cyber–physical system security for the electric power grid, Proc. of the IEEE, Vol.99, No.1, 1-15, 2012.

[3] A. Rosich, H. Voos, Y.M. Li and M. Darouach, A Model Predictive Approach for Cyber-Attack Detection and Mitigation in Control Systems, IEEE 52nd Annual Conference on Decision and Control, Florence, Italy, 6621-6626, 2013.

[4] Y.M. Li, H. Voos, A. Rosich and M. Darouach, A stochastic Cyber-Attack Detection Scheme for Stochastic Control Systems Based on Frequency-Domain Transformation Technique, the 8th International Conference on Network and System Security, Xian, China, 209-222, 2014.

[5] 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, 667-674, 2011.

[6] Y.M. Li, H. Voos, M. Darouach and C.C. Hua, An algebraic detection approach for control systems under multiple stochastic cyber-attacks, IEEE/CAA Journal of Automatica Sinica (JAS), accepted.

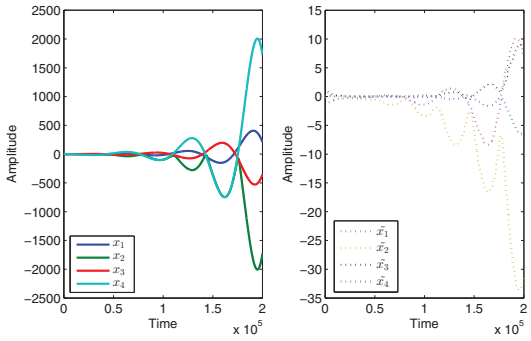

Figure 5: The time responses of the system and the filter under the attack $a_k^a(t)$ and the noise $w(t)$

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

[8] E. Scholtz and B. Lesieutre, Graphical observer design suitable for large-scale DAE power system, Proc. of the IEEE Conf. on Decision and Control, Cancun, 2955-2960, 2008.

[9] 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, 71-79, 2006.

[10] 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, FIRST WORKSHOP ON SECURE CONTROL SYSTEMS, 2010.

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

[12] Y.M. Li, H. Voos, M. Darouach, Robust H_∞ fault estimation for control systems under stochastic cyber-attacks, the 33rd China Control Conference, China, 3124-3129, 2014.