Proceedings of the 36th Chinese Control Conference
July 26-28, 2017, Dalian, China

Stabilization for networked control systems under stochastic cyber-attacks

Lili Wei[1],Jinliang Liu[1,*]

1. College of Information Engenering, Nanjing University of Finance and Economics, Nanjing, Jiangsu 210023, P. R. China
E-mail: 18262814091@163.com, liujinliang@vip.163.com

Abstract: In this paper, the problem of controller design for networked control systems with stochastic cyber-attacks is investigated. Firstly, considering the network-induced delay and cyber-attacks, a mathematical controller model for networked control systems is constructed for analysis. Secondly, based on this model, sufficient conditions for the stability of controller design and gain parameters of desired controller are achieved by using Lyapunov function approach and linear matrix inequality techniques. Finally, a simulated example is given to show the usefulness of designed controller for networked system with stochastic cyber-attacks.

Key Words: Controller design, cyber-attacks, networked control systems, network-induced delay

1 Instructions

In the past few years, networked control systems(NCSs) have attracted persistent increasing research interests due to its appealing advantages in low cost, high flexibility, reduced wiring and simple installation [1] and so on. Therefore, NCSs have a large number fruitful applications in a broad range of areas, such as industrial fields, spacecrafts, vehicles, manufacturing plants and remote surgeries [2, 3]. However, there still exists various challenging problems because of the insertion of network in the control systems like packet dropouts [4, 5], network-induced delays [6, 7] and randomly occurring nonlinearities [8, 9]. It is worth pointing out that lots of methods are proposed to reduce the bad impact of these phenomena. For example, the introduction of event-triggered scheme in the NCSs can effectively save the bandwidth of communicated channels and reduce the burden of network [10, 11], so along with the quantization in the NCSs [12, 13]. Nevertheless, the other phenomena named cyber-attacks can be more destroyable, it is hard to detect and weaken the effect of the cyber-attacks via conventional approaches [14].

Recently, networked security protection has been arisen unexpectedly for the existence of malevolent attacks, which can result in the loss of transmitted data and deterioration of the networked systems. As is well known, the cyber-attacks are consist of three types including Denial of Service (DoS) attacks [15], relay attacks [16, 17] and deception attacks [18, 19]. When under the circumstance of DoS attacks, various resources can't run effectively and deliver service normally on the internet, it poses a severe threat to the network. The limited network bandwidth and resources are depleted by a substantial amount of useless packets, it causes a permanent cessation. Replay attacks is another type of attacks, it occurs repeatedly by capturing some of the messages exchanged between two entitles. The last internet attacks named deception attacks, under this circumstance, the adversaries try to inject the incorrect data into sensor measurements on the transmission from the sensor and the controller. It is obvious that the cyber-attacks usually launch in a consecutive or random manner with a minimum number or a minimum probability [17, 14]. With the development of network, what can not be neglected is the negative influence cyber-attacks have brought. So lots of researches take the cyber-attacks into consideration under the networked systems. In [20], considering the cyber attacks, the authors investigate the observer-based event-triggering consensus control problem with lossy sensor; In [21], this paper describes how to design optimal security mechanism for the Kalman filtering of NCSs with cyber-attacks under limited resources.

Motivated by the aforementioned discussions, there are few achievements focusing on the exploring in the networked systems regarding cyber attacks [22]. In this paper, we concentrate on designing a stable controller with stochastic cyber-attacks for networked systems. In the typical networked control systems, the networked links among sensors, controllers and actuators are vulnerable to cyber-attacks which can destroy the transmitted data through the network communication and make the plant unstable. But the traditional networked control systems choose to ignore the existence of cyber-attacks. Unlike the traditional controller design, in this paper, not only the network-induced delay is introduced, but also the random cyber-attacks are taken into consideration, it can be highly possible to imitate

This work is partly supported by the National Natural Science Foundation of China (No.61403185), Six TalentPeaks Project in Jiangsu Province (No.2015-DZXX-021), and Major project supported by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (Grant No.15KJA120001), the Natural Science Foundation of Jiangsu Province of China (No.BK20161023), the Natural Science Foudation of the Jiangsu Higher Education Institutions of China (No.16KJB520015), Jiangsu Agricutural Science and Technology Independent Innovation Fund Project (No.CX(15)1051).

*Corresponding author. Tel: +02586718770
Email address : liujinliang@vip.163.com

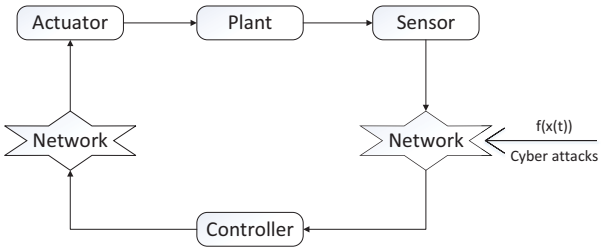

Figure 1: The structure of controller design system with cyber-attacks

the networked transmission in real life.

The rest of this paper is organized as follows. Section II describes the designing controller briefly by constructing a mathematical model for networked systems by taking the network-induced delay and cyber-attacks into consideration. In the Section III, we obtain the sufficient conditions to guarantee the augmented system being stable and present the designing algorithm for desired controller parameters. And finally Section IV gives a simulated example to illustrate the feasibility of desired controller.

Notation: R^n and $R^{n\times m}$ denote the n-dimensional Eculidean space, and the set of $n \times m$ real matrices; the superscript "T" stands for matrix transposition; I is the identity matrix of appropriate dimension; $\|\cdot\|$ stands for the Euclidean vector norm or the induced matrix 2-norm as appropriate; the notation $X > 0$(respectively, $X \geq 0$), for $X \in R^{n\times n}$ means that the matrix X is real symmetric positive definite (respectively,positive semi-definite).

2 System description

Consider the following system:

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{1}$$

where $x(t) \in R^n$ and $u(t) \in R^m$ denote the state vector and control vector, respectively; A and B are parameter matrices with appropriate dimensions.

In this paper, we concentrate on designing a controller with stochastic cyber-attacks for networked control systems, the structure of controller design system is shown as Fig.1. Assume that the sensor is time-driven, the sampler samples the data periodically in the interval time h. And the system (1) is controlled through a network. If only taking the effect of transmission delay into consideration, the controller can be described as follows.

$$u(t) = Kx(t_k h), t \in [t_k h + \tau_{t_k}, t_{k+1} h + \tau_{t_{k+1}}) \tag{2}$$

Where $t_k h$ represent the sampling instants, $k = \{0, 1, 2, 3, \ldots\}$, $t_k h + \tau_{t_k}$ represent the instants the sampling data arrive at the controller, τ_{t_k} is the corresponding network-induced delay. Then we can take the method in [23] as a reference, define $\tau(t) = t - t_k h$, (2) can be rewritten as

$$u(t) = Kx(t - \tau(t)) \tag{3}$$

where $\tau(t) \in [0, \tau_M]$, τ_M is the upper bound of the networked delay.

Remark 1: As is well known, cyber-attacks are the main threats to the stability and safety of the networked system when signals transmitted through the network. Different from the traditional controller designing for networked control systems, we suppose that the procession of transmission through network may be attacked randomly and consecutively by the malicious signals. Except the network between the sensor and the controller, there still exists network between the controller and the actuator. However, in this paper, just the network between the sampler and the controller is taken into account for simplicity.

This paper aims to design a controller with stochastic cyber-attacks, suppose that there exists an unknown nonlinear function $f(x(t))$ to describe the stochastic cyber-attacks, and it satisfies the following condition.

$$||f(x(t))||_2 \leq ||Gx(t)||_2 \tag{4}$$

where G is a constant matrix representing the upper bound of the nonlinearity.

Remark 2: Since the method in [24] make upper bounds information to be the constraint condition of nonlinear perturbation, similarly, in this paper matrix G is chosen to be the upper bounds of proposed stochastic cyber-attacks, thus its value is closely related to the actual situation of networked attacks.

Remark 3: Due to the random and untraceable cyber-attacks, we can't judge precisely what instant the hostile operation may occur to the networked control systems. Normal data transmitted from the sampler to the controller may be attacked at any time except that the cyber-attacks only launch at the very moment when normal data reach the controller. While no matter when the malicious signal launch attacks, they are always transmitted through the network, so time-varying delay of aggressive signals must be taken into consideration.

As shown in Fig.1, when the network suffers from cyber-attacks which represented by function $f(x(t))$, and variable $d(t)$ is used to represent the delay of cyber-attacks, the controller can be described as follows.

$$u(t) = Kf(x(t - d(t))) \tag{5}$$

where $d(t) \in [0, d_M]$,

Considering that the malicious signals are stochastic and irregular, similar to the methods in [20], in this paper we use variable $\theta(t)$ to describe the probability of stochastic cyber-attacks which obeys the Bernoulli distribution. Combine (3) and (5), then the real control input can be written as

$$u(t) = (1 - \theta(t))Kx(t - \tau(t))$$

$$+\theta(t)Kf(x(t - d(t))) \tag{6}$$

Remark 4: Some literatures adopt Bernoulli random variable to describe the probability of stochastic delay for networked control system [25], or to represent the random changes in complex dynamic behavior of networked isolated nodes [26]. In this paper, the Bernoulli distribution is introduced here to describe the probability of stochastic

cyer-attacks. When $\theta(t) = 0$, it means that the data is transmitted through the network without cyber-attacks, equation (6) can be described as $u(t) = Kx(t - \tau(t))$. Otherwise, when $\theta(t) = 1$, the system is under cyber-attacks totally, equation (6) can be written as $u(t) = Kf(x(t - d(t)))$. However, most of the system original states can not reach the controller due to the long duration of cyber-attacks, which cause the instability of the system. In other words, $\bar{\theta}$ has a maximum upper bound to guarantee the stability of designed controller, and the maximum probability of cyber-attacks will be given in this paper.

According to (6), then the system (1) can be described as follows

$$\dot{x}(t) = Ax(t) + (1 - \theta(t))BKx(t - \tau(t))$$

$$+\theta(t)BKf(x(t - d(t))) \tag{7}$$

Here the expectation of stochastic variable $\theta(t)$ can be shown as

$$E\{\theta(t)\} = \bar{\theta}, E\{(\theta(t) - \bar{\theta})^2\} = \bar{\theta}(1 - \bar{\theta}) = \gamma^2$$

where $0 \leq \bar{\theta} \leq 1$, $\bar{\theta}$ represent the expectation of $\theta(t)$, γ^2 is utilized to represent the mathematical variance of $\theta(t)$.

In the following, we will introduce some definitions and lemmas which can be used in the proof of the stability of system later.

Definition 1:[27] For a given function V: $C^b_{F_0}([-\tau_M, 0], R^n) \times S$, its infinitesimal operator $\mathcal{L}$ is defined as

$$\mathcal{L}(V_\eta(t)) = \lim_{\triangle \to 0^+} \frac{1}{\triangle} \left[E(V(\eta_t + \triangle) \mid \eta_t) - V(\eta_t)\right] \tag{8}$$

Lemma 1:[28] For any vectors $x, y \in R^n$, and positive definite matrix $Q \in R^{n \times n}$, the following inequality holds.

$$2x^T y \leq x^T Q x + y^T Q^{-1} y \tag{9}$$

Lemma 2:[29] Suppose $\tau(t) \in [0, \tau_M]$, $d(t) \in [0, d_M]$, $\Xi_1, \Xi_2, \Xi_3, \Xi_4$ and Ω are matrices with appropriate dimensions, then

$$\tau(t)\Xi_1 + (\tau_M - \tau(t))\Xi_2$$

$$+d(t)\Xi_3 + (d_M - d(t))\Xi_4 + \Omega < 0$$

if and only if

$$\begin{aligned}
&\tau_M\Xi_1 + d_M\Xi_3 + \Omega < 0 \\
&\tau_M\Xi_2 + d_M\Xi_3 + \Omega < 0 \\
&\tau_M\Xi_1 + d_M\Xi_4 + \Omega < 0 \\
&\tau_M\Xi_2 + d_M\Xi_4 + \Omega < 0
\end{aligned}$$

3 Main results

In this section, main results shall be established based on LMI techniques. The sufficient conditions will be given to demonstrate the stability of the controller described in (7).

Theorem 1: For given positive parameters $\bar{\theta}$, τ_M, d_M, matrix G and K, the system (7) is exponentially stable if there exist matrixes $P > 0$, $Q_i > 0$, $R_i > 0$ $(i = 1, 2)$, and M, N, T, S with appropriate dimensions satisfying

$$\Omega(s) < 0, s = 1, 2, 3, 4 \tag{10}$$

where

$$\Omega(s) = \begin{pmatrix}
\Omega_{11} + \Gamma + \Gamma^T & * & * & * & * \\
\Omega_{21}(s) & \Omega_{22} & * & * & \\
\Omega_{31} & 0 & \Omega_{33} & * & * \\
\Omega_{41} & 0 & 0 & \Omega_{44} & * \\
\Omega_{51} & 0 & 0 & 0 & -P
\end{pmatrix}$$

$$\Omega_{11} = \begin{pmatrix}
\phi_{11} & * & * & * & * & * \\
0 & 0 & * & * & * & * \\
0 & 0 & -Q_1 & * & * & * \\
\phi_{22} & 0 & 0 & 0 & * & * \\
0 & 0 & 0 & 0 & -Q_2 & * \\
\phi_{33} & 0 & 0 & 0 & 0 & -\bar{\theta}P
\end{pmatrix}$$

$\phi_{11} = PA + A^T P + Q_1 + Q_2$

$\phi_{22} = (1 - \bar{\theta})K^T B^T P, \phi_{33} = \bar{\theta}K^T B^T P$

$\Gamma = \begin{pmatrix} M + T & N - M & -N & S - T & -S \end{pmatrix}$

$\Omega_{21}(1) = \begin{pmatrix} \sqrt{d_M}M^T \\ \sqrt{\tau_M}T^T \end{pmatrix}, \Omega_{21}(2) = \begin{pmatrix} \sqrt{d_M}M^T \\ \sqrt{\tau_M}S^T \end{pmatrix}$

$\Omega_{21}(3) = \begin{pmatrix} \sqrt{d_M}N^T \\ \sqrt{\tau_M}T^T \end{pmatrix}, \Omega_{21}(4) = \begin{pmatrix} \sqrt{d_M}N^T \\ \sqrt{\tau_M}S^T \end{pmatrix}$

$\Omega_{31} = \begin{pmatrix} \psi_{11} & \psi_{12} \end{pmatrix}, \Omega_{41} = \begin{pmatrix} \psi_{21} & \psi_{22} \end{pmatrix}$

$\psi_{11} = \begin{pmatrix} \sqrt{d_M}R_1 A & 0 & 0 \\ \sqrt{\tau_M}R_2 A & 0 & 0 \end{pmatrix}, \psi_{21} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

$\psi_{12} = \begin{pmatrix} (1 - \bar{\theta})\sqrt{d_M}R_1 BK & 0 & \bar{\theta}\sqrt{d_M}R_1 BK \\ (1 - \bar{\theta})\sqrt{\tau_M}R_2 BK & 0 & \bar{\theta}\sqrt{\tau_M}R_2 BK \end{pmatrix}$

$\psi_{12} = \begin{pmatrix} -r\sqrt{d_M}R_1 BK & 0 & r\sqrt{d_M}R_1 BK \\ -r\sqrt{\tau_M}R_2 BK & 0 & r\sqrt{\tau_M}R_2 BK \end{pmatrix}$

$\Omega_{51} = \begin{pmatrix} 0 & \sqrt{\bar{\theta}}PG & 0 & 0 & 0 & 0 \end{pmatrix}$

$\Omega_{22} = \Omega_{33} = \Omega_{44} = diag\{-R_1, -R_2\}$

$M^T = \begin{pmatrix} M_1^T & M_2^T & M_3^T & M_4^T & M_5^T & M_6^T \end{pmatrix}$

$N^T = \begin{pmatrix} N_1^T & N_2^T & N_3^T & N_4^T & N_5^T & N_6^T \end{pmatrix}$

$T^T = \begin{pmatrix} T_1^T & T_2^T & T_3^T & T_4^T & T_5^T & T_6^T \end{pmatrix}$

$S^T = \begin{pmatrix} S_1^T & S_2^T & S_3^T & S_4^T & S_5^T & S_6^T \end{pmatrix}$

Proof: Choose the following Lyapunov functional candidate as

$$V(t) = V_1(t) + V_2(t) + V_3(t) \tag{11}$$

where

$$\begin{aligned}
V_1(t) &= x^T(t)Px(t) \\
V_2(t) &= \int_{t - d_M}^{t} x^T(s)Q_1 x(s)ds + \int_{t - \tau_M}^{t} x^T(s)Q_2 x(s)ds \\
V_3(t) &= \int_{t - d_M}^{t} \int_{s}^{t} \dot{x}^T(v)R_1 \dot{x}(v)dvds + \int_{t - \tau_M}^{t} \int_{s}^{t} \dot{x}^T(v)
\end{aligned}$$

$R_2\dot{x}(v)dvds, P > 0, Q_i > 0, R_i > 0 (i = 1, 2)$.

By applying the infinitesimal operator (7) for $V_k(t)(k = 1, 2, 3)$ and taking expectation on it, and combining the definition of $f(t, x(t))$, the inequality can be written as follows with

$$E\{\mathcal{L}V(t)\} \leq \xi^T(t)(\Upsilon + d(t)MR_1^{-1}M^T$$

$$+(d_M - d(t))NR_1^{-1}N^T + \tau(t)TR_2^{-1}T^T$$

$$+(\tau_M - \tau(t))SR_2^{-1}S^T)\xi(t)$$

where

$$\Upsilon = \Omega_{11} + \Gamma + \Gamma^T + \mathcal{C}^T\tilde{R}\mathcal{C} + \mathcal{D}^T\tilde{R}\mathcal{D} + \Omega_{51}^T P\Omega_{51}$$
$$\tilde{R} = (d_M R_1 + \tau_M R_2)$$
$$\mathcal{C} = \begin{pmatrix} A & 0 & 0 & (1-\bar{\theta})BK & 0 & \bar{\theta}BK \end{pmatrix}$$
$$\mathcal{D} = \begin{pmatrix} 0 & 0 & 0 & -\gamma BK & 0 & \gamma BK \end{pmatrix}$$

Similar to [2, 31], by using free-weighting matrixes method and reciprocally convex approach, along with Schur complement and lemma 2, we can obtain that (10) is sufficient condition to guarantee $E\{\mathcal{L}(V(t))\} < 0$. the proof can be completed.

Based on the Theorem 1, we have obtained the sufficient conditions to ensure the stability of controller, next we are in a position to design the feedback gain K under the cyber-attack by using linear matrix inequality techniques.

Theorem 2: For given positive parameters $\bar{\theta}$, τ_M, d_M and ϵ_i $(i = 1, 2)$, matrix G, the system (7) under the cyber-attack condition is exponentially stable if there exist positive matrixes $X > 0$, $\tilde{Q}_i > 0$, $\tilde{R}_i > 0$ $(i = 1, 2)$, and $\tilde{M}$, $\tilde{N}$, $\tilde{T}$, $\tilde{S}$, Y with appropriate dimensions satisfying

$$\tilde{\Omega}(s) < 0, s = 1, 2, 3, 4 \tag{12}$$

where

$$\tilde{\Omega}(s) = \begin{pmatrix} \tilde{\Omega}_{11} + \tilde{\Gamma} + \tilde{\Gamma}^T & * & * & * & * \\ \tilde{\Omega}_{21}(s) & \tilde{\Omega}_{22} & * & * & \\ \tilde{\Omega}_{31} & 0 & \tilde{\Omega}_{33} & * & * \\ \tilde{\Omega}_{41} & 0 & 0 & \tilde{\Omega}_{44} & * \\ \tilde{\Omega}_{51} & 0 & 0 & 0 & -X \end{pmatrix}$$

$$\tilde{\Omega}_{11} = \begin{pmatrix} \tilde{\phi}_{11} & * & * & * & * & * \\ 0 & 0 & * & * & * & * \\ 0 & 0 & -\tilde{Q}_1 & * & * & * \\ \tilde{\phi}_{22} & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & -\tilde{Q}_2 & * \\ \tilde{\phi}_{33} & 0 & 0 & 0 & 0 & -\bar{\theta}X \end{pmatrix}$$

$$\tilde{\phi}_{11} = AX + XA^T + \tilde{Q}_1 + \tilde{Q}_2$$
$$\tilde{\phi}_{22} = (1-\bar{\theta})Y^T B^T, \tilde{\phi}_{33} = \bar{\theta}Y^T B^T$$
$$\tilde{\Gamma} = \begin{pmatrix} \tilde{M} + \tilde{T} & \tilde{N} - \tilde{M} & -\tilde{N} & \tilde{S} - \tilde{T} & -\tilde{S} \end{pmatrix}$$
$$\tilde{\Omega}_{21}(1) = \begin{pmatrix} \sqrt{d_M}\tilde{M}^T \\ \sqrt{\tau_M}\tilde{T}^T \end{pmatrix}, \tilde{\Omega}_{21}(2) = \begin{pmatrix} \sqrt{d_M}\tilde{M}^T \\ \sqrt{\tau_M}\tilde{S}^T \end{pmatrix}$$
$$\tilde{\Omega}_{21}(3) = \begin{pmatrix} \sqrt{d_M}\tilde{N}^T \\ \sqrt{\tau_M}\tilde{T}^T \end{pmatrix}, \tilde{\Omega}_{21}(4) = \begin{pmatrix} \sqrt{d_M}\tilde{N}^T \\ \sqrt{\tau_M}\tilde{S}^T \end{pmatrix}$$
$$\tilde{\Omega}_{31} = \begin{pmatrix} \tilde{\psi}_{11} & \tilde{\psi}_{12} \end{pmatrix}, \tilde{\Omega}_{41} = \begin{pmatrix} \tilde{\psi}_{21} & \tilde{\psi}_{22} \end{pmatrix}$$
$$\tilde{\psi}_{11} = \begin{pmatrix} \sqrt{d_M}AX & 0 & 0 \\ \sqrt{\tau_M}AX & 0 & 0 \end{pmatrix}, \tilde{\psi}_{21} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$
$$\tilde{\psi}_{12} = \begin{pmatrix} (1-\bar{\theta})\sqrt{d_M}BY & 0 & \bar{\theta}\sqrt{d_M}BY \\ (1-\bar{\theta})\sqrt{\tau_M}BY & 0 & \bar{\theta}\sqrt{\tau_M}BY \end{pmatrix}$$
$$\tilde{\psi}_{12} = \begin{pmatrix} -r\sqrt{d_M}BY & 0 & r\sqrt{d_M}BY \\ -r\sqrt{\tau_M}BY & 0 & r\sqrt{\tau_M}BY \end{pmatrix}$$
$$\Omega_{51} = \begin{pmatrix} 0 & \sqrt{\bar{\theta}}GX & 0 & 0 & 0 & 0 \end{pmatrix}$$
$$\Omega_{22} = \Omega_{33} = \Omega_{44} = diag\{-\tilde{R}_1, -\tilde{R}_2\}$$
$$\Omega_{33} = \Omega_{44} = diag\{-2\epsilon_1 X + \epsilon_1^2\tilde{R}_1, -2\epsilon_2 X + \epsilon_2^2\tilde{R}_2\}$$
$$\tilde{M}^T = \begin{pmatrix} \tilde{M}_1^T & \tilde{M}_2^T & \tilde{M}_3^T & \tilde{M}_4^T & \tilde{M}_5^T & \tilde{M}_6^T \end{pmatrix}$$
$$\tilde{N}^T = \begin{pmatrix} \tilde{N}_1^T & \tilde{N}_2^T & \tilde{N}_3^T & \tilde{N}_4^T & \tilde{N}_5^T & \tilde{N}_6^T \end{pmatrix}$$
$$\tilde{T}^T = \begin{pmatrix} \tilde{N}_1^T & \tilde{N}_2^T & \tilde{N}_3^T & \tilde{N}_4^T & \tilde{N}_5^T & \tilde{N}_6^T \end{pmatrix}$$
$$\tilde{S}^T = \begin{pmatrix} \tilde{S}_1^T & \tilde{S}_2^T & \tilde{S}_3^T & \tilde{S}_4^T & \tilde{S}_5^T & \tilde{S}_6^T \end{pmatrix}$$

Moreover, the controller gain is given as following if the conditions above are feasible.

$$K = YX^{-1} \tag{13}$$

Proof: Due to

$$(R_i - \epsilon_i^{-1}P)R_i^{-1}(R_i - \epsilon_i^{-1}P) \geq 0, (i = 1, 2)$$

we have

$$-PR_i^{-1}P \leq -2\epsilon_i P + \epsilon_i^2 R_i$$

Substitute $-PR_i^{-1}P$ with $-2\epsilon_i P + \epsilon_i^2 R_i$. Then define $X = P^{-1}$, $\tilde{Q}_i = XQ_iX$, $\tilde{R}_i = XR_iX$, $\tilde{M} = XMX$, $\tilde{N} = XNX$, $\tilde{T} = XTX$, $\tilde{S} = XSX$, $Y = KX$ and $\mathcal{F} = diag\{X, X, X, X, X, X, X, X, X, X, X, X, X\}$. Multiply the matrix by $\mathcal{F}$ from the left side and its transpose from the right side, then we can obtain (12). According to $Y = KX$, it is easily derived that the parameter of controller gain is $K = YX^{-1}$. This completes the proof.

4 Simulation examples

In this section, an simulated example is given to demonstrate the effectiveness of designed controller. Consider the continuous controller system described by the following mathematical model.

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{14}$$

where

$$A = \begin{pmatrix} 0 & 1 \\ -1 & -2 \end{pmatrix}, B = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

In addition, in this paper, the main task is to design a stable controller with stochastic cyber-attacks, the real input of the controller is shown as follows.

$$u(t) = (1 - \theta(t))Kx(t - \tau(t)) + \theta(t)f(x(t - d(t)))$$

Suppose that function $f(x(t))$ which representing the cyber-attacks can be shown as $f(x(t)) = \begin{pmatrix} -tanh(0.1x_2(t)) \\ -tanh(0.05x_1(t)) \end{pmatrix}$, and according to the limiting condition of nonlinear stochastic cyber-attacks (4), we can calculate the upper bound $G = \begin{pmatrix} 0.05 & 0 \\ 0 & 0.1 \end{pmatrix}$.

We can easily see that the system is unstable without a controller. The initial state is given as $x_0 = \begin{pmatrix} -0.5 & 0.5 \end{pmatrix}$. Then, we will give two cases to demonstrate the feasibility of designed controller.

Case 1: Set $\bar{\theta} = 0$, the model of controller system (14) can be described as

$$\dot{x}(t) = Ax(t) + BKx(t - \tau(t))$$

In the following, we will consider three possible situations, which will illustrate the effectiveness of the proposed two channel communication schemes. It means that the data transmission is normal which avoiding the cyber-attacks. Set initial value $x_0 = \begin{pmatrix} 2 & -2 \end{pmatrix}^T$, networked delay $\tau_M = 0.1$, $d_M = 0.3$ and regulating parameters $\epsilon_1 = \epsilon_2 = 1$, we can get the controller gain parameter $K = \begin{pmatrix} 0.0116 & -0.2259 \end{pmatrix}$ based on the Theorem. 2. According to the figure of the system state shown in Fig. 2, we can see that the system is stable.

Case 2: Set $\bar{\theta} = 0.5$, the model of controller system (14) can be described as

$$\dot{x}(t) = Ax(t) + (1 - \theta(t))BKx(t - \tau(t))$$

$$+\theta(t)f(x(t - d(t)))$$

It means that probability of the cyber attacks is 50%. Set initial value $x_0 = \begin{pmatrix} 1 & -1 \end{pmatrix}^T$, networked delay $\tau_M = 0.1$, $d_M = 0.3$ and regulating parameters $\epsilon_1 = \epsilon_2 = 1$, we can get the controller gain parameter $K = \begin{pmatrix} 0.0777 & -0.0614 \end{pmatrix}$ by using Theorem. 2. Fig. 3 represents the function of cyber-attacks which is nonlinear, and according to the figure of the system state shown in Fig.4, we can see that the system is stable with stochastic cyber-attacks. According to the set value of $\bar{\theta}$, we can derive that the maximum probability of cyber-attacks is 99.6%, the designed controller can be a failure if $\bar{\theta}$ is beyond the threshold value. Set $\theta(t) = 0.996$, the initial value $x_0 = \begin{pmatrix} 2 & -2 \end{pmatrix}^T$, networked delay $\tau_M = 0.1$, $d_M = 0.3$ and regulating parameters $\epsilon_1 = \epsilon_2 = 1$, we can get the controller gain parameter $K = \begin{pmatrix} 0.0011 & -0.0007 \end{pmatrix}$. From the figure of the system state shown in Fig.5, we can see that the system is still stable.

According to the simulated examples shown above, we can summarize that the designed controller is stable even in the case of suffering stochastic cyber-attacks from the malicious signals, it also demonstrates the feasibility of proposed designing method.

5 Conclusion

In this paper, a controller design for network control systems with cyber-attacks is considered. In order to be consistent with the real life, the network-induced delay and

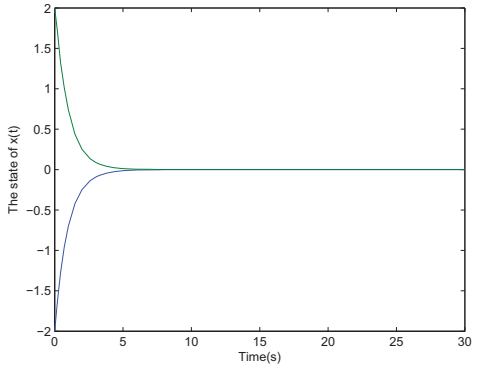

Figure 2: $\bar{\theta} = 0$, the response state of x(t)

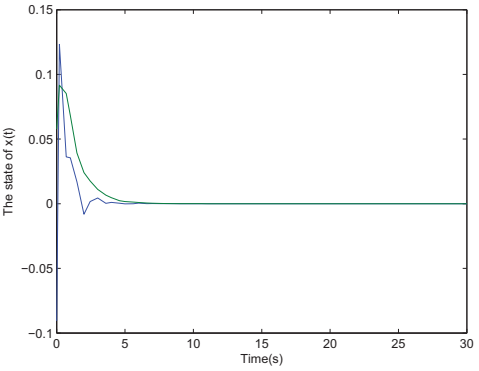

Figure 3: the function of cyber attacks $f(x(t))$

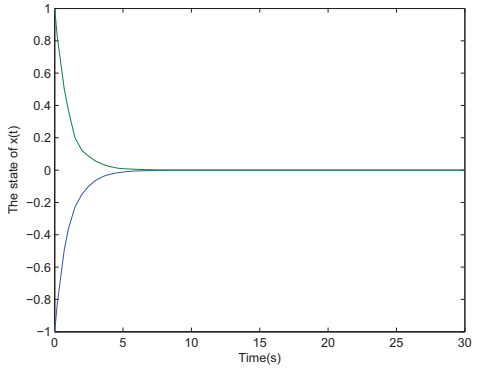

Figure 4: $\bar{\theta} = 0.5$, the response state of x(t)

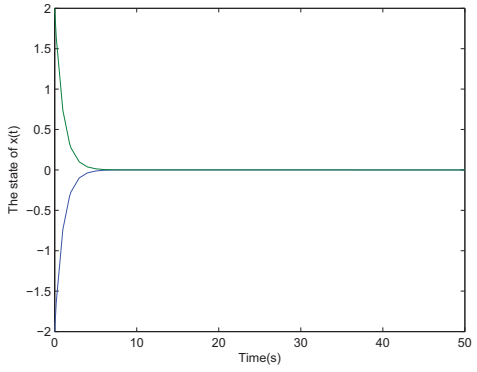

Figure 5: $\bar{\theta} = 0.996$, the response state of x(t)

cyber-attacks are both to be given to construct the mathematical model of desired controller. Based on this model, sufficient conditions are obtained to guarantee the stability of the system by using Lyapunov function approach and linear matrix inequality techniques. Also, the parameters of desired controller are acquired. Lastly a simulated example is utilized to demonstrate the feasibility of the designed controller.

REFERENCES

[1] L. Qiu, Y. Shi, J. Pan, B. Xu, and H. Li, "Robust control for a networked direct-drive linear motion control system: Design and experiments," *Information Sciences*, vol. 370, pp. 725–742, 2016.

[2] J. Liu and D. Yue, "Event-triggering in networked systems with probabilistic sensor and actuator faults," *Information Sciences*, vol. 240, no. 10, pp. 145–160, 2013.

[3] L. Zhang, H. Gao, and O. Kaynak, "Network-induced constraints in networked control systemsła survey," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 403–416, 2013.

[4] X. W. Jiang, B. Hu, Z. H. Guan, X. H. Zhang, and L. Yu, "The minimal signal-to-noise ratio required for stability of control systems over a noisy channel in the presence of packet dropouts," *Information Sciences*, vol. 372, pp. 579–590, 2016.

[5] Y. Song, J. Hu, D. Chen, D. Ji, and F. Liu, "Recursive approach to networked fault estimation with packet dropouts and randomly occurring uncertainties," *Neurocomputing*, vol. 214, pp. 340–349, 2016.

[6] Y. Niu, L. Sheng, and W. Wang, "Delay-dependent H_∞ synchronization for chaotic neural networks with network-induced delays and packet dropouts," *Neurocomputing*, vol. 214, pp. 7–15, 2016.

[7] S. Liu, P. X. Liu, and X. Wang, "Stability analysis and compensation of network-induced delays in communication-based power system control: A survey," *ISA Transactions*, vol. 66, pp. 143–153, 2016.

[8] D. Li, Z. Wang, G. Ma, and C. Ma, "Non-fragile synchronization of dynamical networks with randomly occurring nonlinearities and controller gain fluctuations," *Neurocomputing*, vol. 168, pp. 719–725, 2015.

[9] Y. Ma and H. Chen, "Reliable finite-time H_∞ filtering for discrete time-delay systems with markovian jump and randomly occurring nonlinearities," *Applied Mathematics and Computation*, vol. 268, pp. 897–915, 2015.

[10] H. Li, Z. Chen, L. Wu, and H. K. Lam, "Event-triggered control for nonlinear systems under unreliable communication links," *IEEE Transactions on Fuzzy Systems,*, DOI: 10.1109/TFUZZ.2016.2578346, 2016.

[11] S. F. Jinliang Liu, Jia Tang, "Event-triggered H_∞ filter design for delayed neural network with quantization," *Neural Networks*, vol. 82, pp. 39–48, 2016.

[12] Z. Li, X. Chang, X. Du, and L. Yu, "H_∞ control of discrete-time uncertain linear systems with quantized feedback," *Neurocomputing*, vol. 174, pp. 790–794, 2016.

[13] S. Hu and D. Yue, "Event-triggered control design of linear networked systems with quantizations." *ISA Transactions*, vol. 51, no. 1, pp. 153, 2012.

[14] D. Ding, G. Wei, S. Zhang, Y. Liu, and F. E. Alsaadi, "On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors," *Neurocomputing*, vol. 219, no. 5, pp. 99–106, 2016.

[15] S. Amin, G. A. Schwartz, and S. Shankar Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186–192, 2013.

[16] F. Miao, M. Pajic, and G. J. Pappas, "Stochastic game approach for replay attack detection," in *IEEE Conference on Decision and Control*, pp. 1854–1859, 2013.

[17] M. Zhu and S. Martłnez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 804–808, 2014.

[18] J. Hu, S. Liu, D. Ji, and S. Li, "On co-design of filter and fault estimator against randomly occurring nonlinearities and randomly occurring deception attacks," *International Journal of General Systems*, vol. 45, no. 5, pp. 1–14, 2016.

[19] Z. H. Pang and G. P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 20, no. 5, pp. 1334–1342, 2012.

[20] D. Ding, Z. Wang, D. W. C. Ho, and G. Wei, "Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks," *IEEE Transactions on Cybernetics*, pp. 1–12, 2016.

[21] S. Liu and S. Liu, "A stochastic security game for kalman filtering in networked control systems under denial of service (DoS) attacks," in *Ifac Icons*, pp. 106–111, 2013.

[22] S. Liu, G. Wei, Y. Song, and Y. Liu, "Extended kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks ," *Neurocomputing*, vol. 207, pp. 708–716, 2016.

[23] E. Tian, D. Yue, and C. Peng, "Brief paper: reliable control for networked control systems with probabilistic sensors and actuators faults," *Control Theory and Applications Iet*, vol. 4, no. 8, pp. 1478–1488, 2010.

[24] E. Tian and D. Yue, "Decentralized control of network-based interconnected systems: A state-dependent triggering method," *International Journal of Robust and Nonlinear Control*, vol. 25, no. 8, pp. 1126–1144, 2013.

[25] J. Liu, D. Yue, Z. Gu, and E. Tian, "H_∞ filtering for systems with time-varying delay satisfying a certain stochastic characteristic," *IET Signal Processing*, vol. 5, no. 8, pp. 757–766, 2011.

[26] J. L. Liu, "Research on synchronization of complex networks with random nodes," *Acta Physica Sinica*, vol. 62, no. 4, pp. 221–229, 2013.

[27] X. X. Liao and X. Mao, "Exponential stability of stochastic delay interval systems ," *Automatic Control IEEE Transactions on*, vol. 40, no. 3, pp. 171–181, 2000.

[28] Y. Wang, L. Xie, and C. E. D. Souza, "Robust control of a class of uncertain nonlinear systems ," *Systems and Control Letters*, vol. 19, no. 2, pp. 139–149, 1997.

[29] D. Yue, E. Tian, Y. Zhang, and C. Peng, "Delay-distribution-dependent stability and stabilization of T-S fuzzy systems with probabilistic interval delay," *IEEE Transactions on Systems Man and Cybernetics Part B Cybernetics*, vol. 39, no. 2, pp. 503–516, 2009.

[30] P. Chen and Dong, "Network-based robust H_∞ control of systems with state-delay and uncertainty," *Acta Automatica Sinica*, vol. 33, no. 10, pp. 1093–1096, 2007.

[31] T. Engang and Y. Dong, "Reliable H_∞ filter design for T-S fuzzy model-based networked control;systems with random sensor failure," *International Journal of Robust and Nonlinear Control*, vol. 23, no. 1, pp. 15–32, 2013.