混合攻击下时变信息物理系统的有限时域H_∞控制

刘　珊, 黎善斌, 胥布工[†]

(华南理工大学 自动化科学与工程学院, 广东 广州 510640)

摘要: 本文讨论了一类线性时变信息物理系统(CPS)在有限时域内受到混合攻击的H_∞控制问题. 上述提到的混合攻击, 包括对传感器和控制器之间通信通道发起的拒绝服务(DoS)攻击和对传感器和执行器发起的数据注入(FDI)攻击, 其目的在于破坏测量数据和控制数据, 从而危及闭环系统的功能. 本文的目的在于研究攻击注入信号和被控输出的关系, 来设计控制器增益以使闭环系统在有限时域内具有H_∞性能; 与此同时, 减少最坏情况下攻击输入信号对线性二次性能的影响. 为了解决以上问题, 本文用了随机分析方法和配方法来建立所需的控制器存在的充分条件, 并且通过求解一些设定条件下的两个耦合的倒向递推黎卡提差分方程(RDEs), 提出了一个有限时域控制器设计算法. 最后, 本文给出了数值仿真和实验结果, 来证明该方法的有效性.

关键词: 信息物理系统; 混合攻击; 时变系统; H_∞控制; 递推黎卡提差分方程

引用格式: 刘珊, 黎善斌, 胥布工. 混合攻击下时变信息物理系统的有限时域H_∞控制器设计. 控制理论与应用, 2020, 37(2): 331 – 339

DOI: 10.7641/CTA.2019.80703

Finite horizon H_∞ control for time-varying cyber-physical system under hybrid attacks

LIU Shan, LI Shan-bin, XU Bu-gong[†]

(College of Automation Science and Technology, South China University of Technology, Guangzhou Guangdong 510640, China)

Abstract: In this paper, the H_∞ control problem for a class of linear time-varying cyber-physical system (CPS) under hybrid attacks in a finite horizon is considered. The hybrid attacks, including denial of service (DoS) attacks on sensor-to-controller communication channels and false data injection (FDI) attacks on sensors and actuators, aim to destroy the measurement data and control data in order to endanger the functionality of the closed-loop system. The purpose of this paper is to study the relationship between the attack injected signals and the controlled output, and to design the controller gains so that the H_∞ performance of the closed-loop system is guaranteed over a given finite horizon, meanwhile, the impact of attack signals in the worst case on the linear quadratic performance can be reduced. In order to solve the above problems, both the methods of stochastic analysis and completing squares are utilized to establish the sufficient conditions for the existence of the desired controller, and a finite-horizon controller design algorithm is presented by solving two coupled backward recursive Riccati difference equations (RDEs) subject to some scheduled conditions. At last, the numerical simulation and experimental results are given to demonstrate the efficacy of the proposed approach.

Key words: cyber-physical system; hybrid attacks; time-varying systems; H_∞ control; recursive Riccati difference equations

Citation: LIU Shan, LI Shanbin, XU Bugong. Finite horizon H_∞ controller design for time-varying cyber-physical system under hybrid attacks. *Control Theory & Applications*, 2020, 37(2): 331 – 339

1 Introduction

In recent years, the rapid developments of calculation, control, communications and network technology, have expanded the way of the generic in interconnection between all things, greatly extended the information in time and space, and changed the organization evolutionary approach of physical systems, which have given birth to the cyber-physical system[1]. Among many advantages and benefits that cyber-physical system (CPS) can provide, one of them is the integration of the physical system and cyber system which can create value, but at the same time, there are some related challenges and risks, one of which is security[2].

Security has always been an important considera-

Received 13 September 2018; accepted 18 June 2019.

[†] Corresponding author. E-mail: aubgxu@scut.edu.cn; Tel.:+86 20-87112003.

Recommended by Associate Editor: YU Li.

Supported by the NSFC Guangdong Joint Foundation Key Project (U1401253) and the Fundamental Research Funds for the Central Universities (2015ZZ099).

tion for CPS, which can be defined as the ability to ensure the communication between different components and prevent unauthorized server access[3]. In a CPS, the protection of data and communication is difficult, so security is a complex and challenging task, this is because of the combined architecture of data, communications, process, and communication channel. The security problems of CPS in power grid systems, smart transportation systems, medical systems, water treatment system and other areas have received considerable attention in some literatures, and the security analysis and research of CPS under adversarial attacks has become a hot topic[4–6].

Among various target objects which adversary could attack, the communication channel is the most common object. This is because the communication channel which transmits measurement or control data is usually connected via hard-wired or wireless networks, and the attacker can conduct DoS attacks through the networks to make the data packet dropouts[7–8]. A lot of recent researches have focused on the DoS attacks[9–12]. With the energy constraint of the jammer and the existence of attack detection device, the jammer can not always successfully cause the packet dropouts of the communication channels[13–14]. Thus some researches have presented that the sensor data packet will be dropped randomly during the DoS attack period with a certain probability, and can be modeled by independent and identically distributed (i.i.d.) Bernoulli variables[15–18]. The research in [16] considers the optimal control feedback controller that minimizes a given objective function subject to safety and power constraints for a class of denial-of-service (DoS) attack models. In [17], the authors focus on the optimal control and scheduling problem for linear networked control systems under DoS attacks, which can jam the communication channel between the remote sensors and the controller. To solve the problem, a zero-sum static game of complete information is first utilised to investigate the optimal strategies for both the trigger and the attacker. Besides the communication channel, the sensor and actuator are also the common objects which adversary could attack. For example, false data injection (F-DI) attacks can inject false information into sensors or actuators, and cause the measurement or control data destroyed[19–23]. Mo et al. consider the case that the attacker can design his actions to inject error information into the sensor without being detected, and study the effect of false data injection attacks on state estimation[19]. The authors in [23] consider the scenario that a continuous-time, linear time-invariant (LTI) system with M inputs and P outputs are controlled and measured by vulnerable actuators and sensors, respectively. A new notion of controllability and observability for CPSs under actuator attacks and sensor attacks has been introduced to analyse safety performance. Since many commercial devices are readily available for adversary to conduct these attacks, similarly, many attack strategies have been mentioned in some papers, we can know these attacks are already serious threats for the CPS[24–25].

In practical engineering applications, for example, complex system process, intelligent robot control and the aerospace industry, the time-varying phenomenon of controlled system is common, whether the parameter of the system is time-varying or the structure is time-varying. Thus, more and more attention has been paid to it by researchers from different perspectives. Some of the previous researches have focused on the H_∞ control/filtering problem for time-varying system[26–27], and several kinds of approaches have been used for solving this problem, including the game theoretical approach[27–28], the differential/difference linear matrix inequality (DLMI) and recursive linear matrix inequality(RLMI) approach[29–32], and the backward recursive Riccati difference equation approach[26, 33–34]. On the other hand, the control objects sometimes are required to be completed in a limited time, such as missile interception, satellite orbit, etc.. In addition, if the system is under attacks, the adversary can't always successfully launch attacks with the same attack strategy due to the energy constraint of attacker or the existence of defense strategy. Therefore, considering these actual cases, the secure control problem for the time-varying system under attacks in a given finite-horizon has practical research significance, and to our best knowledge, it has not been properly researched so far, then to shorten this gap, this problem will be researched in this paper.

Based on the above discussion, we focus on the security problem of CPS under hybrid attacks, including DoS attacks on the sensor communication channel, and FDI attacks on the sensors and actuators. Assuming that the attacks period is given, the DoS attacks can be described by the Bernoulli distributed white sequences with known probability as the previous researches[15, 17], and the FDI attacks signals injected in the sensors and actuators are unknown but norm bounded[35–36]. It has the theoretical and actual meaning to research the impact from these attacks on the performance of time-varying system in a finite horizon. Therefore, we target at designing a output feedback controller by using the stochastic analysis techniques, some sufficient conditions are established to guarantee the H_∞ performance in a finite-horizon for the addressed system by using backward recursive Riccati difference equation approach. The main contribution of this paper is mainly as following three points: i) both the DoS attacks and FDI attacks are considered in the output feedback controller design for the time-varying system which has multiple sensors and multiple actuators; ii) a sufficient condition is given for the controller design which makes H$_\infty$ performance from the attacks signals to controlled output satisfied; iii) a suboptimal controller design algorithm is proposed by solving double backward recursive RDEs.

The contents of the paper are as follows. In Section 2, the mathematical models of the CPS under hybrid attacks are described, and main control objective is presented. Then the main results are given in Section 3. At last, numerical simulation and conclusion are given to demonstrate the validity and applicability of the proposed approach in Section 4 and Section 5, respectively.

Notations: We use a fairly standard notation in this paper. $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ denote, respectively, the n dimensional Euclidean space and set of all $n \times m$ real matrices. $\mathbb{N}(\mathbb{N}^+, \mathbb{N}^-)$ denotes the set of integers (positive integers, negative integers). The notation $X \geqslant Y (X > Y)$, where X and Y are real symmetric matrices, means that $X - Y$ is positive semi-definite (positive definite). $\mathrm{E}\{x\}$ and $\mathrm{E}\{x|y\}$ will, respectively, denote the expectation of the stochastic variable x and expectation of x conditional on y. $\mathbf{0}$ represents the zero matrix of compatible dimensions. The n-dimensional identity matrix is denoted as I_n or simply I, if no confusion is caused. The shorthand $\mathrm{diag}\{\cdot\}$ stands for a block-diagonal matrix. $\|A\|$ refers to the norm of a matrix A defined by $\|A\| = \sqrt{\mathrm{tr}(A^{\mathrm{T}}A)}$. M^{T} represents the transpose of M.

2 Problem formulation

Consider a discrete time-varying linear CPS model with multiple sensors and multiple actuators shown in Fig. 1. The output signal transmission is implemented between the sensors and remote controllers via network channels, which can be jammed by the DoS attacks; meanwhile, there are n_{y} sensors and n_u actuators which can be injected in unknown random attack signals by the FDI attacker.

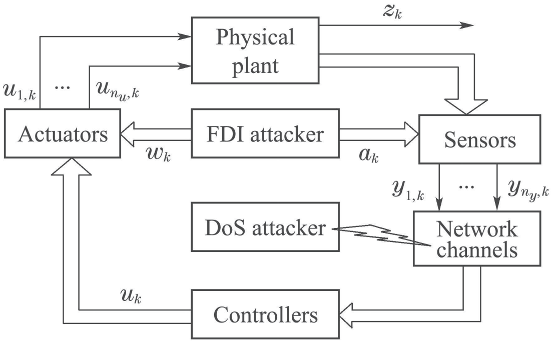


Fig. 1 The structure of CPS with hybrid attacks

The plant is a discrete time-varying system defined in the finite horizon $k \in [0, N]$ of the form

$$\begin{cases} x_{k+1} = A_k x_k + \sum\limits_{i=1}^{n_u} B_{i,k}(u_{i,k} + w_{i,k}), \\ z_k = D_k x_k, \\ y_{j,k} = C_{j,k} x_k + a_{j,k}, \end{cases} \tag{1}$$

where $i \in \{1, 2, \cdots, n_u\}$ represents the ith actuator, $j \in \{1, 2, \cdots, n_y\}$ represents the jth sensor, $x_k \in \mathbb{R}^n$ is the state vector, $u_{i,k} \in \mathbb{R}^m$ is the control signal input to the ith actuator, $w_{i,k} \in \mathbb{R}^m$ is the attack signal injected into the ith actuator which belonging to $l_2[0, N]$, $z_k \in \mathbb{R}^d$ is the controlled output, $y_{j,k} \in \mathbb{R}^p$ is the output of the jth sensor, $a_{j,k} \in \mathbb{R}^p$ is the attack signal injected into the jth sensor which belonging to $l_2[0, N]$ and $A_k \in \mathbb{R}^{n\times n}$, $B_{i,k} \in \mathbb{R}^{n\times m}$, $D_k \in \mathbb{R}^{d\times n}$ and $C_{j,k} \in \mathbb{R}^{p\times n}$ are known real-valued time-varying matrices.

Remark 1 Some previous researches have presented the model of sensor attacks and actuator attacks for linear time-invariant system, and assumed that the attack signals have bounded energy in a finite-horizon[23,35]. Inspired by these works, the time-varying CPS model subject to FDI attacks in sensors and actuators is given in (1), and the attack signals $w_{i,k}$ and $a_{j,k}$ are priori-unknown and energy bounded. If the attack signal $w_{i,k} = 0$, it means that the ith actuator is not attacked; otherwise, the ith actuator is successfully attacked by adversary, the output of the ith actuator is false. Similarly, the attack on the sensor can affect the accuracy of the measured output data[37]. The FDI attacks are unpredictable, and the attack signals can destroy the performance of the system, so that the influence of attack signals on the controlled output is worth studying.

Considering there are random DoS attacks occurring between the sensors and controllers on the S–C network channels, then the measured output model with S–C packet dropout can be expressed as

$$\hat{y}_{j,k} = \alpha_{j,k} y_{j,k}, \tag{2}$$

where $\hat{y}_{j,k} \in \mathbb{R}^p$ is the measured output, $\alpha_{j,k}$ $(j \in \{1, 2, \cdots, n_y\})$ are stochastic and mutually independent variables which indicate the DoS attacks occurrence respectively when their value is 0, and are supposed to be the Bernoulli distributed white sequences with expectations $\bar{\alpha}_j$.

Remark 2 Similar to the setup in some previous research[16,18,38], the occurrence of packet dropouts caused by the DoS attacks is stochastic and its probability is known. Then the stochastic variable α_k is Bernoulli distributed with white sequence taking the values of 0 and 1, whose expected value $\bar{\alpha}$ is known constant which means that each packet exchange attempt faces an attack with a fixed probability. If the communication channel between the jth sensor to controller is jammed by the DoS attack, then the output data packet will be dropped.

The controller can be expressed as

$$u_{i,k} = K_{i,k} \sum_{j=1}^{n_y} \hat{y}_{j,k}, \tag{3}$$

where $K_{i,k} \in \mathbb{R}^{m\times p}$ is the output feedback gain matrix.

Then the closed-loop system by substituting (2) and (3) into (1) as follows:

$$x_{k+1} =$$
$$(A_k + \mathcal{B}_k \mathcal{K}_k \bar{\Psi} \mathcal{C}_k) x_k + \mathcal{B}_k \mathcal{K}_k (\Psi_k - \bar{\Psi}) \mathcal{C}_k x_k +$$

$$(\mathcal{B}_k\mathcal{K}_k\bar{\mathcal{I}}+\bar{\mathcal{B}}_k)\xi_k+\mathcal{B}_k\mathcal{K}_k\mathcal{I}_k\xi_k, \tag{4}$$

where

$$\begin{aligned}
&\mathcal{B}_k=[B_{1,k}\ \ B_{2,k}\cdots B_{n_u,k}],\\
&\mathcal{C}_k=[C_{1,k}^{\mathrm{T}}\ \ C_{2,k}^{\mathrm{T}}\cdots C_{n_y,k}^{\mathrm{T}}]^{\mathrm{T}},\\
&\mathcal{K}_k=[K_{1,k}^{\mathrm{T}}\ \ K_{2,k}^{\mathrm{T}}\cdots K_{n_u,k}^{\mathrm{T}}]^{\mathrm{T}},\\
&\bar{\varPsi}=[\bar{\alpha}_1 I\ \ \bar{\alpha}_2 I\cdots\bar{\alpha}_{n_y} I],\\
&\varPsi_k=[\alpha_{1,k}I\ \ \alpha_{2,k}I\cdots\alpha_{n_y,k}I],\ \bar{\mathcal{I}}=[\bar{\varPsi}\ \ \mathbf{0}],\\
&\bar{\mathcal{B}}_k=[\mathbf{0}\ \ \mathcal{B}_k],\ \xi_k=[a_k^{\mathrm{T}}\ \ w_k^{\mathrm{T}}]^{\mathrm{T}},\\
&a_k=[a_{1,k}^{\mathrm{T}}\ \ a_{2,k}^{\mathrm{T}}\cdots a_{n_y,k}^{\mathrm{T}}]^{\mathrm{T}},\ \mathcal{I}_k=[\varPsi_k-\bar{\varPsi}\ \ \mathbf{0}],\\
&w_k=[w_{1,k}^{\mathrm{T}}\ \ w_{2,k}^{\mathrm{T}}\cdots w_{n_u,k}^{\mathrm{T}}]^{\mathrm{T}}.
\end{aligned}$$

The main problem addressed in this paper is described as follows.

Problem 1 For the given finite time horizon [0, N], positive scalar γ, positive definite matrix W and initial state x_0, we aim to design appropriate controller parameters $K_{i,k}$ $(i\in\{1,2,\cdots,n_u\})$ such that, the closed-loop system (4) satisfies the following H_∞ performance requirement:

$$J_1\triangleq\sum_{k=0}^{N}\mathrm{E}\{\|z_k\|^2\}-\gamma^2\sum_{k=0}^{N}\|\xi_k\|^2<\gamma^2 x_0^{\mathrm{T}}Wx_0. \tag{5}$$

Remark 3 The problem which requires H_∞ performance gain from disturbance signal to controlled output less than a given constant has been researched in previous works[16,18,39]. Based on these works, if the injected signals w and a are disturbance signals, the H_∞ performance requirement (5) can also be regard as that from disturbance signal to controlled output in a finite horizon.

3 Main results

Lemma 1 Let $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{W}$ be known nonzero matrices with appropriate dimensions. The solution $\mathcal{X}$ to $\min\limits_{\mathcal{X}}\|\mathcal{U}\mathcal{X}\mathcal{W}-\mathcal{V}\|_{\mathrm{F}}$ is $\mathcal{U}^{\dagger}\mathcal{V}\mathcal{W}^{\dagger}$[40].

Lemma 2 Given the attack attenuation level $\gamma>0$ and the positive matrix W. For any nonzero ξ_k, the closed-loop system (4) satisfies the H_∞ performance requirement (5) for any nonzero attack signal ξ_k, if there exists a family of non-negative definite matrices P_k $(0\leqslant k\leqslant N$, with the final condition $P_{N+1}=0)$ and a set of real-valued matrices $\mathcal{K}_k$ satisfying the following backward recursive RDE:

$$\varDelta_{11,k+1}-\varDelta_{12,k+1}\varDelta_{22,k+1}^{-1}\varDelta_{12,k+1}^{\mathrm{T}}=P_k, \tag{6}$$

subject to $\varDelta_{22,k+1}<0$ and $P_0<\gamma^2 W$, where

$$\begin{aligned}
&\varDelta_{11,k+1}=\\
&(A_k+\mathcal{B}_k\mathcal{K}_k\bar{\varPsi}\mathcal{C}_k)^{\mathrm{T}}P_{k+1}(A_k+\mathcal{B}_k\mathcal{K}_k\bar{\varPsi}\mathcal{C}_k)+\\
&\mathcal{C}_k^{\mathrm{T}}\varPhi_{k+1}\mathcal{C}_k+D_k^{\mathrm{T}}D_k,\\
&\varDelta_{12,k+1}=\\
&(A_k+\mathcal{B}_k\mathcal{K}_k\bar{\varPsi}\mathcal{C}_k)^{\mathrm{T}}\times P_{k+1}(\mathcal{B}_k\mathcal{K}_k\bar{\mathcal{I}}+\bar{\mathcal{B}}_k)+\\
&\mathcal{C}_k^{\mathrm{T}}\varPhi_{1,k+1},\\
&\varDelta_{22,k+1}=\\
&(\mathcal{B}_k\times\mathcal{K}_k\bar{\mathcal{I}}+\bar{\mathcal{B}}_k)^{\mathrm{T}}P_{k+1}(\mathcal{B}_k\mathcal{K}_k\bar{\mathcal{I}}+\bar{\mathcal{B}}_k)+\\
&\varPhi_{2,k+1}-\gamma^2 I,\\
&\varPhi_{k+1}=\mathrm{diag}\{\tilde{\alpha}_1^2,\tilde{\alpha}_2^2,\cdots,\tilde{\alpha}_{M_y}^2\}\otimes\\
&\qquad\{\mathcal{K}_k^{\mathrm{T}}\mathcal{B}_k^{\mathrm{T}}P_{k+1}\mathcal{B}_k\mathcal{K}_k\},\\
&\varPhi_{1,k+1}=[\varPhi_{k+1}\ \ \mathbf{0}],\ \varPhi_{2,k+1}=\mathrm{diag}\{\varPhi_{k+1},\mathbf{0}\}.
\end{aligned}$$

So far, we have conducted the H_∞ performance analysis in terms of the solvability of a backward Riccati equation in Lemma 2. In the next stage, let us propose an approach for computing the suboptimal controller parameters $K_{i,k}$ $(i\in\{1,2,\cdots,n_u\})$ in each step under the worst situation, i.e. $\xi_k=\xi_k^*=-\varDelta_{22,k+1}^{-1}\varDelta_{12,k+1}^{\mathrm{T}}x_k$. On this condition, we rewrite the closed-loop system (4) as follows:

$$\begin{aligned}
&x_{k+1}=\\
&(A_k+\bar{\varDelta}_{k+1})x_k+[\mathcal{B}_k\mathcal{K}_k(\varPsi_k-\bar{\varPsi})\mathcal{C}_k-\\
&\mathcal{B}_k\mathcal{K}_k\mathcal{I}_k(\varDelta_{22,k+1}^{-1}\varDelta_{12,k+1})]x_k+\mathcal{B}_k\bar{u}_k,
\end{aligned} \tag{7}$$

where $\bar{u}_{i,k}=K_{i,k}\sum\limits_{j=1}^{n_y}\bar{\alpha}_j C_{j,k}x_k$, then the following linear quadratic criteria for quantifying the control quality can be written as

$$\begin{aligned}
J_2\triangleq\ &\mathrm{E}\sum_{k=0}^{N}\{x_k^{\mathrm{T}}Q_k x_k+\sum_{k=0}^{n_u}\bar{u}_{i,k}^{\mathrm{T}}R_{i,k}\bar{u}_{i,k}\}+\\
&\mathrm{E}\{x_{N+1}^{\mathrm{T}}Q_{N+1}x_{N+1}\},
\end{aligned} \tag{8}$$

where $Q_k\geqslant 0$ and $R_{i,k}>0$ $(i\in\{1,2,\cdots,n_u\})$ are the known weighting matrices.

Problem 2 By employing the worst-case FDI attack, we aim to provide a design scheme of the controller parameters $\mathcal{K}_k$ to minimize the linear quadratic performance function J_2 as described below:

$$\min_{\mathcal{K}_k}J_2, \tag{9}$$

subject to Problem 1 and system dynamics (7).

Then we will solve the Problem 2 by giving the following theorem.

Theorem 1 Given the attack attenuation level $\gamma>0$ and the positive matrix W. For any nonzero ξ_k, the closed-loop system (4) satisfies the H_∞ performance requirement (5) for any nonzero attack signal ξ_k, if there exist two families of non-negative definite matrices P_k, S_k $(0\leqslant k\leqslant N)$ and a set of real-valued matrices $\mathcal{K}_k$ satisfying (6) and the following backward recursive RDE:

$$\varLambda_{11,k+1}+Q_k-\varLambda_{12,k+1}\varLambda_{22,k+1}^{-1}\varLambda_{12,k+1}^{\mathrm{T}}=S_k, \tag{10}$$

subject to

$$S_{N+1}=Q_{N+1},\ P_{N+1}=0, \tag{11}$$

$$\varDelta_{22,k+1}<0,\ P_0<\gamma^2 W,\ \varLambda_{22,k+1}>0, \tag{12}$$

$$\mathcal{K}_k=-\varLambda_{22,k+1}^{-1}\varLambda_{12,k+1}^{\mathrm{T}}(\bar{\varPsi}\mathcal{C}_k)^{\dagger}, \tag{13}$$

where

$$\varLambda_{11,k+1}=$$

$$(A_k + \bar{\varDelta}_{k+1})^{\mathrm{T}} S_{k+1}(A_k + \bar{\varDelta}_{k+1}) + \mathcal{C}_k^{\mathrm{T}}\bar{\varPhi}_{k+1}\mathcal{C}_k +$$
$$(\varDelta_{22,k+1}^{-1}\ \varDelta_{12,k+1})^{\mathrm{T}}\bar{\varPhi}_{2,k+1}(\varDelta_{22,k+1}^{-1}\ \varDelta_{12,k+1}) -$$
$$2\mathcal{C}_k^{\mathrm{T}}\bar{\varPhi}_{1,k+1} \times (\varDelta_{22,k+1}^{-1}\varDelta_{12,k+1}),$$
$$\varLambda_{12,k+1} = (A_k + \bar{\varDelta}_{k+1})^{\mathrm{T}} S_{k+1}\mathcal{B}_k,$$
$$\varLambda_{22,k+1} = \mathcal{B}_k^{\mathrm{T}} S_{k+1}\mathcal{B}_k + \bar{R}_k,$$
$$\bar{\varDelta}_{k+1} = (\mathcal{B}_k\mathcal{K}_k\bar{\mathcal{I}} + \bar{\mathcal{B}}) \times (-\varDelta_{22,k+1}^{-1}\ \varDelta_{12,k+1}),$$
$$\bar{R}_k = \mathrm{diag}\{R_{1,k}, R_{2,k}, \cdots, R_{n_n,k}\},$$
$$\bar{\varPhi}_{k+1} = \mathrm{diag}\{\tilde{\alpha}_1^2, \tilde{\alpha}_2^2, \cdots, \tilde{\alpha}_{n_y}^2\} \otimes (\mathcal{K}_k^{\mathrm{T}}\mathcal{B}_k^{\mathrm{T}} S_{k+1}\mathcal{B}_k\mathcal{K}_k),$$
$$\bar{\varPhi}_{1,k+1} = [\bar{\varPhi}_{k+1}\ 0],\ \bar{\varPhi}_{2,k+1} = \mathrm{diag}\{\bar{\varPhi}_{k+1}, 0\}.$$

Proof Firstly, it follows from Lemma 2 that, if there exist solutions P_k and $\mathcal{K}_k$ to (6), (11) and (12) so that the system (4) achieves the pre-specified H$_\infty$ performance (5). On this condition, the worst-case attack signal can be expressed as $\xi_k = \xi_k^* = -\varDelta_{22,k+1}^{-1}\varDelta_{12,k+1}^{\mathrm{T}} x_k$. By employing the worst-case attack, the closed-loop system (4) can be written as (7), then the cost function J_2 can be described by completing the square with respect to $\bar{u}_k$:

$$J_2 =$$
$$\mathrm{E}\{x_0^{\mathrm{T}} S_0 x_0 + x_{N+1}^{\mathrm{T}}(Q_{N+1} - S_{N+1})x_{N+1}\} +$$
$$\sum_{k=0}^{N} \mathrm{E}\{x_k^{\mathrm{T}}(\varLambda_{11,k+1} - S_k + Q_k - \varLambda_{12,k+1}\varLambda_{22,k+1}^{-1} \times$$
$$\varLambda_{12,k+1}^{\mathrm{T}})x_k + (\bar{u}_k - \bar{u}_k^*)^{\mathrm{T}}\varLambda_{22,k+1}(\bar{u}_k - \bar{u}_k^*)\} \leqslant$$
$$\mathrm{E}\{x_0^{\mathrm{T}} S_0 x_0 + x_{N+1}^{\mathrm{T}}(Q_{N+1} - S_{N+1})x_{N+1}\} +$$
$$\sum_{k=0}^{N} \mathrm{E}\{x_k^{\mathrm{T}}(\varLambda_{11,k+1} - S_k + Q_k - \varLambda_{12,k+1}\varLambda_{22,k+1}^{-1} \times$$
$$\varLambda_{12,k+1}^{\mathrm{T}})x_k + \|\mathcal{K}_k\bar{\varPsi}\mathcal{C}_k + \varLambda_{22,k+1}^{-1}\varLambda_{12,k+1}\mathrm{T}\|_{\mathrm{F}}^2 \times$$
$$\|\varLambda_{22,k+1}\|_{\mathrm{F}}\|x_k\|^2\}, \tag{14}$$

where $\bar{u}_k^* = -\varLambda_{22,k+1}^{-1}\varLambda_{12,k+1}^{\mathrm{T}} x_k$.

For the purpose of minimizing the cost function (8), the controller parameters $\mathcal{K}_k$ can be selected in each iteration backward as follows:

$$\mathcal{K}_k^* = \arg\min_{\mathcal{K}_k} \|\mathcal{K}_k\bar{\varPsi}\mathcal{C}_k + \varLambda_{22,k+1}^{-1}\varLambda_{12,k+1}^{\mathrm{T}}\|_{\mathrm{F}}. \tag{15}$$

It follows from Lemma 1 that (13) is the solution of the optimization problem (15). The proof is complete.

QED.

However, we can see from the above theorem that it is difficult to get the $\mathcal{K}_k$ from (13). Then in order to obtain the controller parameters $\mathcal{K}_k$ directly and simplify the calculation process, the following theorem is given.

Theorem 2 Given the attack attenuation level $\gamma > 0$ and the positive matrix W. For any nonzero ξ_k, the closed-loop system (4) satisfies the H$_\infty$ performance requirement (5) for any nonzero attack signal ξ_k, if there exist the positive scalar h_k, two families of nonnegative definite matrices P_k, S_k ($0 \leqslant k \leqslant N$) and a set of real-valued matrices $\mathcal{K}_k$ satisfying the following two backward recursive RDEs:

$$\begin{cases} \varDelta_{11,k+1} - \bar{\varDelta}_{12,k+1}\bar{\varDelta}_{22,k+1}^{-1}\bar{\varDelta}_{12,k+1}^{\mathrm{T}} = P_k, \\ \bar{\varLambda}_{11,k+1} + Q_k - \bar{\varLambda}_{12,k+1}\varLambda_{22,k+1}^{-1}\bar{\varLambda}_{12,k+1}^{\mathrm{T}} = S_k, \end{cases} \tag{16}$$

subject to

$$S_{N+1} = Q_{N+1}, P_{N+1} = 0, \tag{17}$$
$$\bar{\varDelta}_{22,k+1} < 0,\ P_0 < \gamma^2 W,\ \varLambda_{22,k+1} > 0, \tag{18}$$
$$\mathcal{K}_k = \mathcal{M}_{k+1}^{\dagger}\mathcal{N}_{k+1}(\bar{\varPsi}\mathcal{C}_k)^{\dagger}, \tag{19}$$
$$\varOmega_k < I, \tag{20}$$

where

$$\bar{\varDelta}_{12,k+1} = (A_k + \mathcal{B}_k\mathcal{K}_k\bar{\varPsi}\mathcal{C}_k)^{\mathrm{T}} P_{k+1}\mathcal{B}_{1,k},$$
$$\mathcal{B}_{1,k} = [\mathcal{B}_k\ \ h_k^{-1}\mathcal{B}_k],\ \bar{\varDelta}_{22,k+1} = \mathcal{B}_{1,k}^{\mathrm{T}} P_{k+1}\mathcal{B}_{1,k} - \gamma^2 I,$$
$$\bar{\varLambda}_{11,k+1} =$$
$$(A_k - \mathcal{B}_{1,k}\bar{\varDelta}_{22,k+1}^{-1} \times \bar{\varDelta}_{12,k+1}^{\mathrm{T}})^{\mathrm{T}} S_{k+1}$$
$$(A_k - \mathcal{B}_{1,k}\bar{\varDelta}_{22,k+1}^{-1}\bar{\varDelta}_{12,k+1}^{\mathrm{T}}) + \mathcal{C}_k^{\mathrm{T}}\bar{\varPhi}_{k+1} \times \mathcal{C}_k,$$
$$\bar{\varLambda}_{12,k+1} = (A_k - \mathcal{B}_{1,k}\bar{\varDelta}_{22,k+1}^{-1}\bar{\varDelta}_{12,k+1}^{\mathrm{T}})^{\mathrm{T}} S_{k+1}\mathcal{B}_k,$$
$$\mathcal{M}_{k+1} =$$
$$I - \varLambda_{22,k+1}^{-1}\mathcal{B}_k^{\mathrm{T}} S_{k+1}\mathcal{B}_{1,k}\bar{\varDelta}_{22,k+1}^{-1}\mathcal{B}_{1,k}^{\mathrm{T}} P_{k+1}\mathcal{B}_k,$$
$$\mathcal{N}_{k+1} =$$
$$-\varLambda_{22,k+1}^{-1}\mathcal{B}_k^{\mathrm{T}} S_{k+1}(I - \mathcal{B}_{1,k}\bar{\varDelta}_{22,k+1}^{-1}\mathcal{B}_{1,k}^{\mathrm{T}} P_{k+1})A_k,$$
$$\varOmega_k =$$
$$h_k^2[\bar{\varPsi}^{\mathrm{T}}\mathcal{K}_k^{\mathrm{T}}\mathcal{K}_k\bar{\varPsi} + \mathrm{diag}\{\tilde{\alpha}_1^2, \tilde{\alpha}_2^2, \cdots, \tilde{\alpha}_{n_y}^2\} \otimes (\mathcal{K}_k^{\mathrm{T}}\mathcal{K}_k)].$$

Proof Define $\eta_k \triangleq h_k\mathcal{K}_k\varPsi_k a_k$, where $h_k > 0$ is introduced to provide more flexibility in the controller design. Then denote $\beta_k \triangleq [w_k^{\mathrm{T}}\ \ \eta_k^{\mathrm{T}}]^{\mathrm{T}}$, the closed-loop system can be described as

$$x_{k+1} = (A_k + \mathcal{B}_k\mathcal{K}_k\bar{\varPsi}\mathcal{C}_k)x_k + \mathcal{B}_k\mathcal{K}_k(\varPsi_k - \bar{\varPsi})$$
$$\mathcal{C}_k x_k + \mathcal{B}_{1,k}\beta_k. \tag{21}$$

It follows from Theorem 1 that if there exist solutions $\{(h_k, P_k, Q_k, \mathcal{K}_k)\}_{0 \leqslant k \leqslant N}$ satisfying the backward recursive RDEs (16) with (17)–(18), then the system satisfies

$$\sum_{k=0}^{N} \mathrm{E}\{\|z_k\|^2 - \gamma^2\|\beta_k\|^2\} < \gamma^2 x_0^{\mathrm{T}} W x_0. \tag{22}$$

If the condition (20) is satisfied, we can get

$$\sum_{k=0}^{N} \mathrm{E}\{\|z_k\|^2\} < \sum_{k=0}^{N} \mathrm{E}\{\gamma^2\|\beta_k\|^2\} + \gamma^2 x_0^{\mathrm{T}} W x_0 <$$
$$\gamma^2 \sum_{k=0}^{N} \|\xi_k\|^2 + \gamma^2 x_0^{\mathrm{T}} W x_0, \tag{23}$$

which implies that the H$_\infty$ performance constraint (5) is satisfied. Then for the purpose of minimizing the cost function (9), the suboptimal controller parameters $\mathcal{K}_k$ can be selected in each iteration backward as follows:

$$\mathcal{K}_k^* = \arg\min_{\mathcal{K}_k} \|\mathcal{K}_k\bar{\varPsi}\mathcal{C}_k + \varLambda_{22,k+1}^{-1}\bar{\varLambda}_{12,k+1}^{\mathrm{T}}\|_{\mathrm{F}}, \tag{24}$$

which equal to calculate

$$\mathcal{K}_k^* = \arg\min_{\mathcal{K}_k} \|\mathcal{M}_{k+1}\mathcal{K}_k\bar{\varPsi}\mathcal{C}_k - \mathcal{N}_{k+1}\|_{\mathrm{F}}. \tag{25}$$

It follows from Lemma 1 that (19) is the solution of the optimization problem (25). The proof is complete.

QED.

Noticing that the controller parameters $\mathcal{K}_k$ are involved in the proposed double RDEs, by means of Theorem 2, the finite-horizon H_∞ controller design algorithm is proposed as follows.

Algorithm 1 finite-horizon H_∞ controller design:

```
Given: $\bar{\alpha}_j, N, Q_{N+1}, \gamma, W, Q_k, R_k$;
Output: $\mathcal{K}_k, P_k, S_k$,
    where $j \in \{1, 2, \cdots, n_y\},\ k \in \{0, 1, \cdots, N\}$.
Steps of algorithm:
    1) Initialize $k = N,\ S_{N+1} = Q_{N+1},\ P_{N+1} = 0$;
    2) Select the appropriate value $h_k$, compute $\bar{\Delta}_{22,k+1},\ \Lambda_{22,k+1}$ by (18), if $\bar{\Delta}_{22,k+1} < 0$ and $\Lambda_{22,k+1} > 0$, then the controller parameters $\mathcal{K}_k$ can be solved by (19), and go to the next step, else jump to Step 7);
    3) If the condition (20) is satisfied, go to the next step, else return to Step 2);
    4) Solve the backward RDEs (16) to get $P_k$ and $S_k$;
    5) If $k \neq 0$, set $k = k-1$, and go back to Step 2), else turn to the next step;
    6) If the condition $P_0 < \gamma^2 W$ is satisfied, this algorithm is feasible, and output the results, else go to Step 7);
    7) This algorithm is infeasible.
```

Remark 4 In this paper, the finite-horizon H_∞ controller is designed for a time-varying system with multiple actuators and multiple sensors under FDI attacks and DoS attacks by solving double backward recursive RDEs. Note that Lemma 2 and Theorem 1 are proved mainly by the completing the square method which leads to very little conservatism, and Theorem 2 is given to obtain the controller parameters $\mathcal{K}_k$ directly and simplify the calculation process, which also provides more flexibility in the controller design. We can see from Algorithm 1 that, there are several factors that can increase the complexity of controller design, including the time-varying system parameters, the prescribed attack attenuation level γ, the selected scalar h_k, and the probabilities of packet dropouts from sensors to controllers caused by DoS attacks. Therefore, the comprehensive influence of these factors will determine the control effect, and in actual implementation of the Algorithm 1, in order to obtain the better control effect, in the case that the system parameters and the probabilities of packet dropouts are known, we will adjust the scalar h_k appropriately to get a smaller prescribed attack attenuation level γ.

4 Numerical simulation

In this section, we aim to demonstrate the effectiveness of the proposed problem and algorithm.

Consider a discrete-time time-varying system with the following system parameters:

$$A_k = \begin{bmatrix} 0.42 + \sin(2k-1) & -0.4 \\ -0.4 + \mathrm{e}^{-5k} & 0.85 \end{bmatrix},$$

$$B_{1,k} = \begin{bmatrix} 0.85 \\ -0.65 \end{bmatrix},\ B_{2,k} = \begin{bmatrix} -0.2 \\ -0.1 \end{bmatrix},$$

$$B_{3,k} = \begin{bmatrix} 0.8 \\ -0.4 \end{bmatrix},\ C_{1,k} = [0.65\ \ -0.7],$$

$$C_{2,k} = [0.3\ \ -0.5],\ D_k = [0.2\ \ 0.2].$$

Let the FDI attack signals be

$$w_{1,k} = 0.05\sin k,\ w_{2,k} = 0.05\cos k,$$
$$w_{3,k} = 0.08\sin k,\ a_{1,k} = 0.08\cos(0.7k),$$
$$a_{2,k} = 0.05\sin(0.7k).$$

Case 1 Assuming that the probability parameters are given as $\bar{\alpha}_1 = 0.9$ and $\bar{\alpha}_2 = 0.9$, the H_∞ attack attenuation level $\gamma = 0.6$, the positive definite matrix $W = 0.8I$, the time horizon $N = 100$, the performance weighting matrices $Q_k = I,\ R_{1,k} = 1,\ R_{2,k} = 0.8$ and $R_{3,k} = 1$, and the selected scalar $h_k = 1$. Using Algorithm 1, we can obtain the controller gain results as shown in Table 1. The controlled outputs of closed-loop system and open-loop system are shown in Fig. 2, respectively, and the measured outputs under hybrid attacks and without attacks are shown in Fig. 3, respectively.

Table 1 The controller gain results

k	0	1	$\cdots$	99	100
$K_{1,k}$	-0.0681	-0.4656	$\cdots$	-0.4369	-0.1849
$K_{2,k}$	-0.0521	0.0300	$\cdots$	0.0078	-0.1058
$K_{3,k}$	-0.0158	-0.3666	$\cdots$	-0.3304	-0.0668

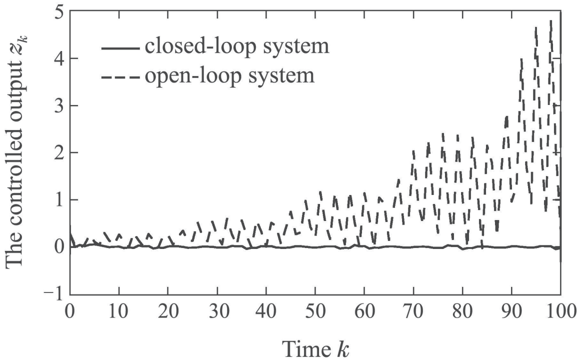
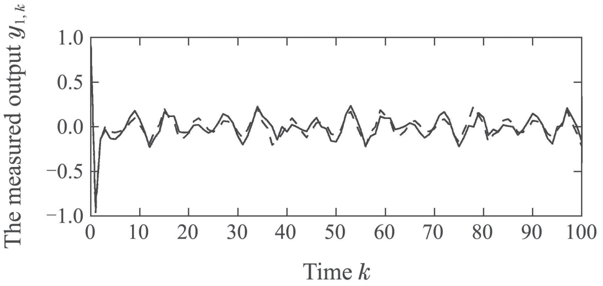


Fig. 2 The controlled outputs of system



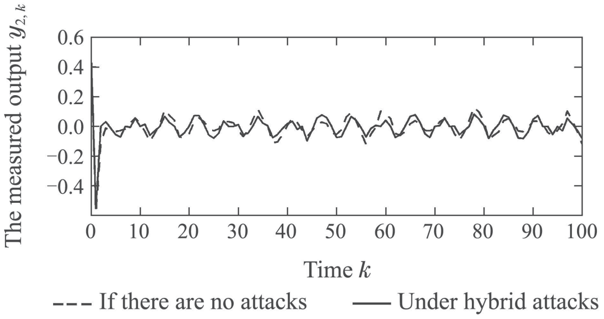


Fig. 3 The measured outputs of system

Then we consider the case that the controller parameters $\mathcal{K}_k$ are not optimal to minimize the linear quadratic performance function J_2 as we presented in Problem 2 and the other given conditions are the same as those given above, thus the controllers we obtained are common H$_\infty$ performance controllers, which can be obtained by solving Problem 1. We can compare the results of permitted minimum γ and the linear quadratic performance function J_2 in different cases, which are shown in Table 2, and the results comparison of controlled outputs are shown in Fig. 4.

Table 2 The results comparison

Using Algorithm 1	Using common H$_\infty$ algorithm
$J_2 = 5.866$	$J_2 = 6.3669$
$\gamma_{\min} = 0.589$	$\gamma_{\min} = 0.887$

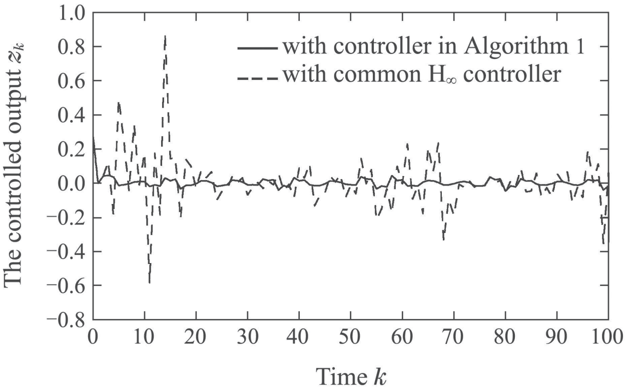


Fig. 4 The controlled outputs with different algorithms

From the above numerical results and simulated figures, we can see that the controller design by Algorithm 1 is effective.

Case 2 Assuming that the positive definite matrix W, the time horizon N, and the LQR performance weighting matrices are the same with them in Case 1. The probability parameter $\bar{\alpha}_1$ (or $\bar{\alpha}_2$) can change from 0.9 to 0.8, the scalar h_k can be selected as 1, 1.1 and 1.2. The permitted minimum γ results are shown in Table 2.

Table 3 The permitted minimum γ

Parameter	Values					
$\bar{\alpha}_1$ or $\bar{\alpha}_2$	0.9	0.9	0.9	0.8	0.8	0.8
h_k	1	1.1	1.2	1	1.1	1.2
$\gamma_{\min}$	0.589	0.563	0.588	0.594	0.568	0.928

We can see from the above table that the permitted minimum γ is related to the probability parameters and the scalar h_k, that is to say, for the same scalar h_k, if the probability parameters get smaller, it means that packet dropout probabilities get larger, then the permitted minimum γ will get larger; for the same packet dropout probabilities, if the scalar h_k get larger, the permitted minimum γ could get larger or smaller. Then for the same packet dropout probabilities, we should select proper scalar h_k, which can make the permitted minimum γ get smaller.

5 Conclusions

This paper has presented the H$_\infty$ performance control problem and given the design approach of controller for the security of time-varying CPS under hybrid attacks. The model of occurring two types of cyber attacks is presented, and the H$_\infty$ performance requirement which represents the impact of attack signals on the controlled output in a finite-horizon is proposed. Based on the attack model and control objective, the suboptimal controller is designed to reduce the performance loss which the injected attack signals caused. Through theoretical research and simulation example, the approach we proposed can solve the control problem, reduce the performance loss, and increase security of CPS under hybrid attacks.

References:

[1] LEE E A. Cyber physical systems: Design challenges. *the 11th IEEE Symposium on Object Oriented Real – Time Distributed Computing (ISORC)*. Orlando: IEEE Computer Society, 2008: 363 – 369.

[2] ALI S, BALUSGI T A, NADIR Z, et al. Cyber security for cyber physical systems. *Studies in Computational Intelligence*. Warsaw: Polish Academy of Sciences, 2018, 768: 1 – 174.

[3] PASQUALETTI F. Secure control systems: a control-theoretic approach to cyber-physical security. Santa Barbara: University of California Santa Barbara, 2012.

[4] WATTS D. Security and vulnerability in electric power systems. *The 35th North American Power Symposium*. Rolla: University of Missouri-Rolla, 2003, 2: 559 – 566.

[5] WAND E K, YE Y M, XU X F, et al. Security issues and challenges for cyber physical system. *Proceedings of the 2010 IEEE/ACM International Conference on Green Computing and Communications & International Conference on Cyber, Physical and Social Computing*. Hangzhou: IEEE Computer Society, 2010: 733 – 738.

[6] SHI L. Analysis and design of secure cyber-physical systems. *Control Theory and Technology*, 2014, 12(4): 413 – 414.

[7] SANDBERG H, AMIN S, JOHANSSON K. Cyberphysical security in networked control systems: An Introduction to the issue. *Control Systems IEEE*, 2015, 35(1): 20 – 23.

[8] LI Y Z, SHI L, CHENG P, et al. Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach. *IEEE Transactions on Automatic Control*, 2015, 60(10): 2831 – 2836.

[9] DE PERSIS C, TESI P. Input-to-state stabilizing control under denial-of-service. *IEEE Transactions on Automatic Control*, 2015, 60(11): 2930 – 2944.

[10] LIU S C, LIU P X, SADDIK A E. A stochastic game approach to the security issue of networked control systems under jamming attacks. *Journal of the Franklin Institute*, 2014, 351(9): 4570 – 4583.

[11] PELECHRINIS K, ILIOFOTOU M, KRISHNAMURTHY S V. Denial of service attacks in wireless networks: the case of jammers. *IEEE Communications Surveys & Tutorials*, 2011, 13(2): 245 – 257.

[12] DOLK V S, TESI P, PERSIS C D, et al. Event-triggered control systems under denial-of-service attacks. *IEEE Transactions on Control of Network Systems*, 2017, 4(1): 93 – 105.

[13] LAW Y W, HOESEL L V, DOUMEN J, et al. Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. *ACM Transactions on Sensor Networks (TOSN)*, 2009, 5(1): 6.

[14] ZHANG Y Y, LI X Z, LIU Y N. The detection and defence of DoS attack for wireless sensor network. *Journal of China Universities of Posts & Telecommunications*, 2012, 19(Suppl. 2): 52 – 56.

[15] ZHANG H, CHENG P, SHI L, et al. Optimal denial-of-service attack scheduling with energy constraint. *IEEE Transactions on Automatic Control*, 2015, 60(11): 3023 – 3028.

[16] AMIN S, CÁRDENAS A A, SASTRY S S. Safe and secure networked control systems under denial-of-service attacks. *International Conference on Hybrid Systems: Computation and Control*. San Francisco: Springer, 2009: 31 – 45.

[17] ZHAO Y H, HE X, ZHOU D H. Optimal joint control and triggering strategies against denial of service attacks: a zero-sum game. *IET Control Theory & Applications*, 2017, 11(14): 2352 – 2360.

[18] ZHU Q Y, BASAR T. Game-theoretic methods for robustness, security, and resilience of cyber physical control systems: games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Systems*, 2015, 35(1): 46 – 65.

[19] MO Y L, GARONE E, CASAVOLA A, et al. False data injection attacks against state estimation in wireless sensor networks. *Proceedings of the 49th IEEE Conference on Decision and Control*. Atlanta: IEEE, 2010, 58: 5967 – 5972.

[20] MOON J, BASAR T. Robust control of lti systems over unreliable communication channels with unreliable acknowledgments. *The 2016 IEEE Region 10 Conference(TENCON)*. Singapore: IEEE, 2016: 3390 – 3393.

[21] FAWZI H, TABUADA P, DIGGAVI S. Security for control systems under sensor and actuator attacks. *The 2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*. Maui: IEEE, 2012: 3412 – 3417.

[22] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 2011, 14(1): 21 – 32.

[23] LI Y N, WU J, LI S Y. Controllability and observability of cpss under networked adversarial attacks. *IET Control Theory & Applications*, 2017, 11(10): 1596 – 1602.

[24] ZHANG H, CHENG P, SHI L, et al. Optimal dos attack scheduling in wireless networked control system. *IEEE Transactions on Control Systems Technology*, 2016, 24(3): 843 – 852.

[25] CHEN Y, KAR S, MOURA J M F. Optimal attack strategies subject to detection constraints against cyber-physical systems. *IEEE Transactions on Control of Network Systems*, 2018, 5(3): 1157 – 1168.

[26] DING D R, WANG Z D, DONG H L, et al. Distributed H_∞ state estimation with stochastic parameters and nonlinearities through sensor networks: the finite-horizon case. *Automatica*, 2012, 48(8): 1575 – 1585.

[27] HUNG Y S, YANG F W. Robust H_∞ filtering for discrete time-varying uncertain systems with a known deterministic input. *International Journal of Control*, 2002, 75(15): 1159 – 1169.

[28] MA L F, WANG Z D, BO Y M, et al. A game theory approach to mixed $\mathrm{H}_2/\mathrm{H}_\infty$ control for a class of stochastic time-varying systems with randomly occurring nonlinearities. *Systems & Control Letters*, 2011, 60(12): 1009 – 1015.

[29] SHAKED U, SUPLIN V. A new bounded real lemma representation for the continuous-time case. *IEEE Transactions on Automatic Control*, 2001, 46(9): 1420 – 1426.

[30] HU J, WANG Z D, GAO H J, et al. Probability-guaranteed H_∞ finite-horizon filtering for a class of nonlinear time-varying systems with sensor saturations. *Systems & Control Letters*, 2012, 61(4): 477 – 484.

[31] LIANG J L, SUN F B, LIU X H. Finite-horizon H_∞ filtering for time-varying delay systems with randomly varying nonlinearities and sensor saturations. *Systems Science & Control Engineering: An Open Access Journal*, 2014, 2(1): 108 – 118.

[32] DING D R, WANG Z D, SHEN B, et al. H_∞ state estimation for discrete-time complex networks with randomly occurring sensor saturations and randomly varying sensor delays. *IEEE Transactions on Neural Networks and Learning Systems*, 2012, 23(5): 725 – 736.

[33] WANG Z D, DING D R, DONG H L, et al. H_∞ consensus control for multi-agent systems with missing measurements: the finite-horizon case. *Systems & Control Letters*, 2013, 62(10): 827 – 836.

[34] ZOU L, WANG Z D, GAO H J. Observer-based H_∞ control of networked systems with stochastic communication protocol: The finite-horizon case. *Automatica*, 2016, 63: 366 – 373.

[35] KWON C, HWANG I. Cyber attack mitigation for cyber-physical systems: hybrid system approach to controller design. *IET Control Theory & Applications*, 2016, 10(7): 731 – 741.

[36] DING D R, WANG Z D, WEI G L, et al. Event-based security control for discrete-time stochastic systems. *IET Control Theory & Applications*, 2016, 10(15): 1808 – 1815.

[37] FAWZI H, TABUADA P, DIGGAVI S. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, 2014, 59(6): 1454 – 1467.

[38] CETINKAYA A, ISHII H, HAYAKAWA T. Networked control under random and malicious packet losses. *IEEE Transactions on Automatic Control*, 2016, 62(5): 2434 – 2449.

[39] WANG Z D, YANG F W, HO D W C, et al. Robust H_∞ control for networked systems with random packet losses. *IEEE Transactions on Systems, Man & Cybernetics, Part B: Cybernetics*, 2007, 37(4): 916 – 924.

[40] PENROSE R. On best approximate solutions of linear matrix equations. *Mathematical Proceedings of the Cambridge Philosophical Society*, 2008, 52(1): 17 – 19.

Appendix:

Proof By defining

$$
\begin{aligned}
&V_k \triangleq \\
&\mathrm{E}\{x_{k+1}^{\mathrm{T}} P_{k+1} x_{k+1} - x_k^{\mathrm{T}} P_k x_k\} = \\
&\mathrm{E}\{x_k^{\mathrm{T}}[(A_k + \mathcal{B}_k \mathcal{K}_k \bar{\Psi} \mathcal{C}_k)^{\mathrm{T}} P_{k+1} (A_k + \mathcal{B}_k \mathcal{K}_k \bar{\Psi} \mathcal{C}_k) + \\
&\mathcal{C}_k^{\mathrm{T}} \Phi_{k+1} \mathcal{C}_k - P_k] x_k + 2 x_k^{\mathrm{T}} [(A_k + \mathcal{B}_k \mathcal{K}_k \bar{\Psi} \mathcal{C}_k)^{\mathrm{T}} \times \\
&P_{k+1} (\mathcal{B}_k \mathcal{K}_k \bar{\mathcal{I}} + \bar{\mathcal{B}}_k) + \mathcal{C}_k^{\mathrm{T}} \Phi_{1,k+1}] \xi_k + \xi_k^{\mathrm{T}} [(\mathcal{B}_k \times \\
&\mathcal{K}_k \bar{\mathcal{I}} + \bar{\mathcal{B}}_k)^{\mathrm{T}} P_{k+1} (\mathcal{B}_k \mathcal{K}_k \bar{\mathcal{I}} + \bar{\mathcal{B}}_k) + \Phi_{2,k+1}] \xi_k\},
\end{aligned}
\tag{A1}
$$

then taking the mathematical expectation (A1), and applying the completing squares method results in

$$\begin{aligned}
&J_1 = \\
&\sum_{k=0}^{N} \mathrm{E}\{x_k^{\mathrm{T}} D_k^{\mathrm{T}} D_k x_k - \gamma^2 \xi_k^{\mathrm{T}} \xi_k + x_{k+1}^{\mathrm{T}} P_{k+1} x_{k+1} - \\
&x_k^{\mathrm{T}} P_k x_k\} + \mathrm{E}\{x_0^{\mathrm{T}} P_0 x_0 - x_{N+1}^{\mathrm{T}} P_{N+1} x_{N+1}\} = \\
&\sum_{k=0}^{N} \mathrm{E}\{x_k^{\mathrm{T}} (\varDelta_{11,k+1} - P_k - \varDelta_{12,k+1} \varDelta_{22,k+1}^{-1} \times \\
&\varDelta_{12,k+1}^{\mathrm{T}}) x_k + (\xi_k - \xi_k^*)^{\mathrm{T}} \varDelta_{22,k+1} (\xi_k - \xi_k^*)\} + \\
&\mathrm{E}\{x_0^{\mathrm{T}} P_0 x_0 - x_{N+1}^{\mathrm{T}} P_{N+1} x_{N+1}\},
\end{aligned} \tag{A2}$$

where $\xi_k^* = -\varDelta_{22,k+1}^{-1} \varDelta_{12,k+1}^{\mathrm{T}} x_k$. Since $P_{N+1} = 0$, $\varDelta_{22,k+1} < 0$ and $P_0 < \gamma^2 W$, it can be obtained that

$$J_1 < \gamma^2 x_0^{\mathrm{T}} W x_0, \tag{A3}$$

which means the pre-specified H_∞ performance requirement (5) is satisfied. The proof is complete. QED.

作者简介:

刘 珊 博士研究生, 目前研究方向为鲁棒控制、信息物理系统的安全和控制器设计, E-mail: auliushan@mail.scut.edu.cn;

黎善斌 副教授, 目前研究方向为网络控制系统、随机系统、时延系统、鲁棒控制以及容错控制, E-mail: lishb@scut.edu.cn;

胥布工 教授, 目前研究方向为无线传感器网络的分析和综合、基于网络的实时控制和网络控制系统, E-mail: aubgxu@scut.edu.cn.