IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 29, 2020, accepted March 12, 2020, date of publication March 23, 2020, date of current version April 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2980978

H_∞ Control for Time-Varying Cyber-Physical System Under Randomly Occurring Hybrid Attacks: The Output Feedback Case

SHAN LIU, YONGGUI LIU, (Member, IEEE), SHANBIN LI, AND BUGONG XU, (Senior Member, IEEE)
College of Automation Science and Technology, South China University of Technology, Guangzhou 510640, China

Corresponding author: Yonggui Liu (auygliu@scut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61973128, Grant 61573153, Grant 61703167, and Grant 61104107, in part by the Special Application Project of Guangdong Province under Grant 2016B090927007, and in part by the Natural Science Foundation of Guangdong Province under Grant 2019A1515011807.

ABSTRACT In this paper, the H_∞ control problem for a class of linear time-varying cyber-physical system (CPS) under randomly occurring hybrid attacks in a finite horizon is investigated. The hybrid attacks, including denial of service (DoS) attacks on both sensor-to-controller and controller-to-actuator 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 output feedback 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 out to demonstrate the effectiveness of the proposed approach.

INDEX TERMS Cyber-physical system, hybrid attacks, time-varying systems, H_∞ control, Riccati equations.

I. INTRODUCTION

In recent years, with the development of intelligent systems, cyber physical system (CPS) has been applied into all aspects of life, including aerospace, automobile, energy, medical care, manufacturing and other fields [1]. Compared with the existing networked control system, the CPS focuses on the rational utilization and scheduling optimization of resources, can realize real-time perception and dynamic monitoring of large-scale complex systems, and provide the corresponding network information services [2]. Security and reliability are the primary indicators of large and complex systems. In a CPS, the interaction between cyber space and physical component is more convenient and frequent than the traditional network communication structure, which can also bring more security risks. Malicious attacks have been found on many CPSs, such as critical infrastructures, industrial systems and even modern vehicle systems [3]–[5]. These attacks can degrade the physical performance and even disrupt the system stability. So the security of CPS is an important issue and has been studied from different perspectives [6]–[8].

There are two main types of security problems about CPS: information security and security control theory. The former mainly deals with the data or manages the key from the aspect of computer or data communication [9]; the latter studies that how the network attacks affect the physical dynamics

The associate editor coordinating the review of this manuscript and approving it for publication was Rathinasamy Sakthivel.

of the system from the aspect of state estimation or control theory [10], [11]. We all know that it is a direct and feasible way to research the information security problem for resisting malicious attacks, but the security of CPS can't be guaranteed when the attacks penetrates into the physical system. Therefore, it is necessary to study the security control theory for CPS in combination with physical system.

Security control theory is based on the attack model to carry out research, so how to establish an appropriate attack model is very important. In previous studies, the most common malicious attacks fall into two categories. The first attack category is denial of service (DoS) attack, which can interrupt network service and is usually caused by the destruction of equipment, overloading of system resources, or exhaustion of energy. In the past decade, many researchers have focused on the security of CPS under DoS attacks [10], [12]–[14]. Amin *et al.* studied how to design an optimal feedback controller for CPS under DoS attack to minimize the performance function with the security and energy constraints. The DoS attack can jam the communication channel between the sensor and the controller or between the controller and the actuator, and is modeled as independent and identically distributed actions which can cause random packet losses [10]. In the study of literature [13], the input-to-state stabilizing control problem for CPS with multiple transmission channels under DoS attacks. Ai *et al.* [14] consider the stable state estimation and optimal attack schedule problems of the wireless CPS with two sensors under DoS attack. In order to solve these problems, researchers use a sufficient condition to ensure the stability of the state estimation based on the Kalman filter, and propose the optimal attack schedule to maximize the expected average estimation error at the remote estimator in the viewpoint of the attacker.

The second attack category is deception attack, and false data injection (FDI) attack is a typical representative of deception attack [11], [15]–[18]. It can take advantage of the vulnerability of network information transmission to inject fake data designed by attackers into sensors or actuators in order to tamper with the data packets of sensors or actuators, and destroy the physical performance and even stability of the system. Kwon *et al.* have researched a robust hybrid control scheme containing multiple sub-controllers and switched the controller accordingly to achieve the best performance [15]. Since the future attack behavior is unpredictable, the worst performance of each sub-controller is considered, and the most secure sub-controller is designed to reconstruct the past attack profile in a certain time horizon when the energy of the attack signal is limited. The work [7] also focuses on the sensor and actuator attacks which can affect the dynamic characteristics of a linear time invariant system. The system has M controlled inputs from the actuators and P measured outputs from the sensors, which can be designed controllable and observable under attacks.

In practical engineering applications, for example, complex system process, intelligent robot control and the aerospace industry, the time-varying phenomenon of controlled system occurs frequently, 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 [20]–[26], and several kinds of approaches have been used for solving this problem, including the game theoretical approach [21], [22], the differential/difference linear matrix inequality (DLMI) and recursive linear matrix inequality(RLMI) approach [23], [24], and the backward recursive Riccati difference equation approach [23], [25], [26]. On the other hand, the control objects sometimes are required to be completed in a limited time, such as missile interception, satellite orbit, etc.. Furthermore, with the energy constraint of attacker or the existence of defense strategy, the attacker can't always successfully launch attacks with the same attack strategy. Therefore, considering these actual cases, the secure control problem for the time-varying system under hybrid 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 and actuator communication channels, 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 [6], [27], and the FDI attacks signals injected in the sensors and actuators are unknown but norm bounded [15], [28]. Motivated by this, the impact from these attacks on the performance of time-varying system in a finite horizon will be researched in this paper. To be specific, the research target is to design a output feedback controller by using the stochastic analysis techniques, and 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 contributions of this paper are mainly as following points:

1) both the DoS attacks and FDI attacks on sensor-to-controller channels and controller-to-actuator channels are considered simultaneously in the output feedback controller design for the time-varying system which has multiple sensors and multiple actuators;
2) a sufficient condition is given for the controller design of above system under hybrid attacks, which makes H_∞ performance from the attacks signals to the controlled output satisfied;
3) a suboptimal controller design algorithm is proposed for reducing LQG performance loss under the worst FDI attacks by solving double backward recursive RDEs.

The contents of the paper are as follows. In Section I, 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 II. At last, numerical simulation and conclusion are given to demonstrate the validity and applicability of the proposed approach in Section III and Section IV, 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 $X \geq Y (X > Y)$, 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. $\boldsymbol{0}$ 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 $\mathrm{diag}\{\cdots\}$ stands for a block-diagonal matrix. $\|A\|$ refers to the norm of a matrix A defined by $\|A\| = \sqrt{trace(A^{\mathrm{T}}A)}$. M^{T} represents the transpose of M. $Ran(n)$ represents an n-by-n matrix containing pseudorandom values drawn from the standard uniform distribution on the open interval (0, 1).

A. PROBLEM FORMULATION

Consider a discrete time-varying linear CPS model with multiple sensors and multiple actuators shown in Figure 1. The output signal transmission and the control signal transmissions are respectively implemented via sensor-to-controller network channels and controller-to-actuator 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.

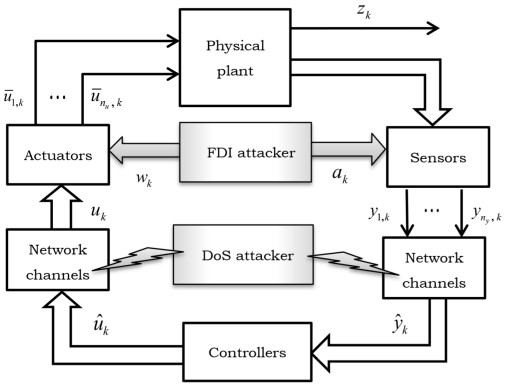


FIGURE 1. The structure of CPS with hybrid attacks.

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

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

where $i \in \{1, 2, \ldots, n_u\}$ 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 [7], [15]. 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 [11]. 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: When a DoS attacker blocks the communication channel with the same energy, the characteristics of the wireless channel itself and the bit error rate are fixed during each attack period [27], then the DoS attacks occurrences are supposed to be the Bernoulli distributed variables. Similar to the setup in some previous research [29], [30], 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. Furthermore, if the attack strategy changes, the probability of packet dropouts may change accordingly. Then the known time-varying probability case can also be taken into account in this paper. When we consider this case, we just need to replace $\bar{\alpha}_j$ with $\bar{\alpha}_{j,k}$, and use the time-varying probability parameter to design the controller at each sampling time.

The controller can be expressed as

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

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

Considering there are random DoS attacks occurring between the controllers and the actuators network channels, then the control signal model with C-A packet dropout can be expressed as

$$u_{i,k} = \beta_{i,k}\hat{u}_{i,k}, \tag{4}$$

where $\beta_{i,k}$ $(i \in \{1, 2, \cdots, n_u\})$ 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 $\bar{\beta}_i$.

Remark 3: Actually, many literatures have been devoted efforts to study the control problems subject to the occurrence of FDI or DoS attacks [7], [11]. Additionally, random occurrence of DoS attacks which obey a probabilistic law are ineluctable due to unpredictable attack techniques and unstable network circumstances has been increasingly studied [6], [27], [30]. We combine the random DoS attacks model in [6] and the FDI attacks model in [11] to build our new attacker model. As can be seen from the Figure 1, sensor attacks and DoS attacks can affect the measured output at the same time, and similarly, actuator attacks and DoS attacks can affect the control output at the same time. So it is not comprehensive to consider only one type of attack when multiple attacks can occur and affect each other. To ensure the performance of system from a comprehensive perspective, randomly occurring hybrid attacks are excogitated in this paper, which introduce different variables to characterize each attack.

Then the closed-loop system by substituting (4) and (3) into (1) as follows:

$$\begin{aligned} x_{k+1} = {} & (A_k + \bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k)x_k + \bar{B}_k\bar{\phi}\bar{K}_k(\varphi_k - \bar{\varphi})\bar{C}_k x_k \\ & + \bar{B}_k(\phi_k - \bar{\phi})\bar{K}_k\bar{\varphi}\bar{C}_k x_k + \bar{B}_k(\phi_k - \bar{\phi})\bar{K}_k(\varphi_k - \bar{\varphi})\bar{C}_k x_k \\ & + (\bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{I}_1 + \bar{B}_k\bar{I}_2)\xi_k + \bar{B}_k\bar{\phi}\bar{K}_k(\varphi_k - \bar{\varphi})\bar{I}_\Delta\xi_k \\ & + \bar{B}_k(\phi_k - \bar{\phi})\bar{K}_k\bar{\varphi}\bar{I}_1\xi_k + \bar{B}_k(\phi_k - \bar{\phi})\bar{K}_k(\varphi_k - \bar{\varphi})\bar{I}_\Delta\xi_k, \end{aligned} \tag{5}$$

where

$$\begin{aligned} &\bar{B}_k = [B_{1,k}\ B_{2,k}\cdots B_{n_u,k}], \quad \bar{C}_k = [C_{1,k}^T\ C_{2,k}^T\cdots C_{n_y,k}^T]^T, \\ &\bar{K}_k = [K_{1,k}^T\ K_{2,k}^T\ \cdots\ K_{n_u,k}^T]^T, \quad \bar{I}_1 = [I\ \ \mathbf{0}],\ \bar{I}_2 = [\mathbf{0}\ \ I], \\ &\bar{\phi} = \mathrm{diag}\{\bar{\beta}_1, \bar{\beta}_2, \cdots, \bar{\beta}_{n_u}\}, \\ &\phi_k = \mathrm{diag}\{\beta_{1,k}, \beta_{2,k}, \cdots, \beta_{n_u,k}\}, \\ &\bar{\varphi} = [\bar{\alpha}_1\ \bar{\alpha}_2\cdots\bar{\alpha}_{n_y}], \quad \varphi_k = [\alpha_{1,k}\ \alpha_{2,k}\ \cdots\ \alpha_{n_y,k}], \\ &\xi_k = [a_k^T\ \ w_k^T]^T, \quad a_k = [a_{1,k}^T\ a_{2,k}^T\ \cdots\ a_{n_y,k}^T]^T, \\ &w_k = [w_{1,k}^T\ w_{2,k}^T\ \cdots\ w_{n_u,k}^T]^T. \end{aligned}$$

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 (5) satisfies the following H_∞ performance requirement:

$$J_1 \triangleq \mathrm{E}\sum_{k=0}^{N}\{\|z_k\|^2\} - \gamma^2\mathrm{E}\sum_{k=0}^{N}\|\xi_k\|^2 < \gamma^2 x_0^{\mathrm{T}} W x_0. \tag{6}$$

Remark 4: The problem which requires H_∞ performance gain from disturbance signal to controlled output less than a given constant has been researched in previous works [12], [29], [31]–[33]. Based on these works, if the injected signals w and a are disturbance signals, the H_∞ performance requirement (6) can also be regard as that from disturbance signal to controlled output in a finite horizon.

II. MAIN RESULTS

Lemma 1: Let $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{W}$ be known nonzero matrices with appropriate dimensions. The solution $\mathcal{X}$ to $\min_{\mathcal{X}} \|\mathcal{U}\mathcal{X}\mathcal{W} - \mathcal{V}\|_F$ is $\mathcal{U}^\dagger\mathcal{V}\mathcal{W}^\dagger$ [34].

Lemma 2: Given the attack attenuation level $\gamma > 0$ and the positive matrix W. For any nonzero ξ_k, the closed-loop system (5) satisfies the H_∞ performance requirement (6) for any nonzero attack signal ξ_k, if there exists a family of nonnegative definite matrices P_k $(0 \le k \le N$, with the final condition $P_{N+1} = 0)$ and a set of real-valued matrices $\bar{K}_k$ satisfying the following backward recursive RDE:

$$\Delta_{11,k+1} - \Delta_{12,k+1}\Delta_{22,k+1}^{-1}\Delta_{12,k+1}^T = P_k, \tag{7}$$

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

$$\begin{aligned} \Delta_{11,k+1} = {} & (A_k + \bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k)^T P_{k+1}(A_k + \bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k) \\ & + \bar{C}_k^T\Upsilon_{1,k+1}\bar{C}_k + \bar{C}_k^T\bar{\varphi}^T\bar{K}_k^T\Upsilon_{2,k+1}\bar{K}_k\bar{\varphi}\bar{C}_k \\ & + \bar{C}_k^T\Upsilon_{3,k+1}\bar{C}_k + D_k^T D_k, \\ \Delta_{12,k+1} = {} & (A_k + \bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k)^T P_{k+1}(\bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{I}_1 + \bar{B}_k\bar{I}_2) \\ & + \bar{C}_k^T\Upsilon_{1,k+1}\bar{I}_1 + \bar{C}_k^T\bar{\varphi}^T\bar{K}_k^T\Upsilon_{2,k+1}\bar{K}_k\bar{\varphi}\bar{I}_1 \\ & + \bar{C}_k^T\Upsilon_{3,k+1}\bar{I}_1, \\ \Delta_{22,k+1} = {} & (\bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{I}_1 + \bar{B}_k\bar{I}_2)^T P_{k+1}(\bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{I}_1 + \bar{B}_k\bar{I}_2) \\ & + \bar{I}_1^T\Upsilon_{1,k+1}\bar{I}_1 + \bar{I}_1^T\bar{\varphi}^T\bar{K}_k^T\Upsilon_{2,k+1}\bar{K}_k\bar{\varphi}\bar{I}_1 \\ & + \bar{I}_1^T\Upsilon_{3,k+1}\bar{I}_1 - \gamma^2 I, \\ \Upsilon_{1,k+1} = {} & \tilde{\varphi} \otimes \{\bar{K}_k^T\bar{\phi}^T\bar{B}_k^T P_{k+1}\bar{B}_k\bar{\phi}\bar{K}_k\}, \\ \tilde{\varphi} = {} & \mathrm{diag}\{\tilde{\alpha}_1^2, \tilde{\alpha}_2^2, \cdots, \tilde{\alpha}_{n_y}^2\}, \quad \tilde{\alpha}_j = [(1-\bar{\alpha}_j)\bar{\alpha}_j]^{1/2}, \\ \Upsilon_{2,k+1} = {} & \tilde{\phi}^T\bar{B}_k^T P_{k+1}\bar{B}_k\tilde{\phi},\ \Upsilon_{3,k+1} = \tilde{\varphi} \otimes \{\bar{K}_k^T\Upsilon_{2,k+1}\bar{K}_k\}, \\ \tilde{\phi} = {} & \mathrm{diag}\{\tilde{\beta}_1^2, \tilde{\beta}_2^2, \cdots, \tilde{\beta}_{n_u}^2\}, \quad \tilde{\beta}_i = [(1-\bar{\beta}_i)\bar{\beta}_i]^{1/2}. \end{aligned}$$

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. $\xi_k = \xi_k^* = -\Delta_{22,k+1}^{-1}\Delta_{12,k+1}^{\mathrm{T}}x_k$. On this condition, we rewrite the closed-loop system (5) as follows:

$$\begin{aligned} x_{k+1} = {} & (A_k + \bar{\Delta}_{1,k+1})x_k + [\bar{B}_k\bar{\phi}\bar{K}_k(\varphi_k - \bar{\varphi}) + \bar{B}_k(\phi_k - \bar{\phi}) \\ & \times \bar{K}_k\bar{\varphi} + \bar{B}_k(\phi_k - \bar{\phi})\bar{K}_k(\varphi_k - \bar{\varphi})]\bar{\Delta}_{2,k+1}x_k + \bar{B}_k\bar{u}_k, \end{aligned} \tag{8}$$

where $\bar{\Delta}_{1,k+1} = -(\bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{I}_1 + \bar{B}_k\bar{I}_2)\Delta_{22,k+1}^{-1}\Delta_{12,k+1}^T$, $\bar{\Delta}_{2,k+1} = \bar{C}_k - \bar{I}_1\Delta_{22,k+1}^{-1}\Delta_{12,k+1}^T$, $\bar{u}_k = \sum_{i=1}^{n_u}\bar{u}_{i,k}$, $\bar{u}_{i,k} = \bar{\beta}_{i,k}K_{i,k}\sum_{j=1}^{n_y}\bar{\alpha}_j C_{j,k}x_k$, then the following linear quadratic criteria for quantifying the control quality can be written as:

$$J_2 \triangleq \mathrm{E}\sum_{k=0}^{N}\{x_k^{\mathrm{T}}Q_kx_k + \sum_{i=0}^{n_u}\bar{u}_{i,k}^{\mathrm{T}}R_{i,k}\bar{u}_{i,k}\} + \mathrm{E}\left\{x_{N+1}^{\mathrm{T}}Q_{N+1}x_{N+1}\right\}, \quad (9)$$

where $Q_k \geq 0$ 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 $\bar{K}_k$ to minimize the linear quadratic performance function J_2 as described below:

$$\min_{\bar{K}_k} J_2, \quad (10)$$

subject to Problem 1 and system dynamics (8).

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 (5) satisfies the H_∞ performance requirement (6) for any nonzero attack signal ξ_k, if there exist two families of non-negative definite matrices P_k, S_k ($0 \leq k \leq N$) and a set of real-valued matrices $\bar{K}_k$ satisfying (7) and the following backward recursive RDE:

$$\Lambda_{11,k+1} + Q_k - \Lambda_{12,k+1}\Lambda_{22,k+1}^{-1}\Lambda_{12,k+1}^T = S_k, \quad (11)$$

subject to

$$S_{N+1} = Q_{N+1}, \quad P_{N+1} = 0, \quad (12)$$

$$\Delta_{22,k+1} < 0, \quad P_0 < \gamma^2 W, \Lambda_{22,k+1} > 0, \quad (13)$$

$$\bar{K}_k = -\bar{\phi}^{\dagger}\Lambda_{22,k+1}^{-1}\Lambda_{12,k+1}^T(\bar{\varphi}\bar{C}_k)^{\dagger}, \quad (14)$$

where

$$\begin{aligned}
\Lambda_{11,k+1} &= (A_k+\bar{\Delta}_{1,k+1})^T S_{k+1}(A_k+\bar{\Delta}_{1,k+1})+\bar{\Delta}_{2,k+1}^T \\
&\quad\times(\bar{\Upsilon}_{1,k+1}+\bar{\varphi}^T\bar{K}_k^T\bar{\Upsilon}_{2,k+1}\bar{K}_k\bar{\varphi}+\bar{\Upsilon}_{3,k+1})\bar{\Delta}_{2,k+1}, \\
\Lambda_{12,k+1} &= (A_k+\bar{\Delta}_{1,k+1})^T S_{k+1}\bar{B}_k, \\
\Lambda_{22,k+1} &= \bar{B}_k^T S_{k+1}\bar{B}_k + \bar{R}_k, \\
\bar{R}_k &= \mathrm{diag}\{R_{1,k}, R_{2,k}, \ldots, R_{n_u,k}\}, \\
\bar{\Upsilon}_{1,k+1} &= \tilde{\varphi}\otimes\{\bar{K}_k^T\tilde{\phi}^T\bar{B}_k^T S_{k+1}\bar{B}_k\tilde{\phi}\bar{K}_k\}, \\
\bar{\Upsilon}_{2,k+1} &= \tilde{\phi}^T\bar{B}_k^T S_{k+1}\bar{B}_k\tilde{\phi}, \quad \bar{\Upsilon}_{3,k+1} = \tilde{\varphi}\otimes\{\bar{K}_k^T\bar{\Upsilon}_{2,k+1}\bar{K}_k\}.
\end{aligned}$$

Proof: Firstly, it follows from Lemma 2 that, if there exist solutions P_k and $\bar{K}_k$ to (7), (12) and (13) so that the system (5) achieves the pre-specified H_∞ performance (6). On this condition, the worst-case attack signal can be expressed as $\xi_k = \xi_k^* = -\Delta_{22,k+1}^{-1}\Delta_{12,k+1}^{\mathrm{T}}x_k$. By employing the worst-case attack, the closed-loop system (5) can be written as (8), then the cost function J_2 can be described by completing the square with respect to $\bar{u}_k$:

$$\begin{aligned}
J_2 &= \mathrm{E}\{x_0^T S_0x_0 + x_{N+1}^T(Q_{N+1}-S_{N+1})x_{N+1}\} \\
&\quad+\mathrm{E}\sum_{k=0}^{N}\{x_k^T(\Lambda_{11,k+1}-S_k+Q_k-\Lambda_{12,k+1}\Lambda_{22,k+1}^{-1} \\
&\quad\times\Lambda_{12,k+1}^{\mathrm{T}})x_k+(\bar{u}_k-\bar{u}_k^*)^T\Lambda_{22,k+1}(\bar{u}_k-\bar{u}_k^*)\} \\
&\leq \mathrm{E}\{x_0^{\mathrm{T}}S_0x_0 + x_{N+1}^T(Q_{N+1}-S_{N+1})x_{N+1}\} \\
&\quad+\mathrm{E}\sum_{k=0}^{N}\{x_k^T(\Lambda_{11,k+1}-S_k+Q_k-\Lambda_{12,k+1}\Lambda_{22,k+1}^{-1} \\
&\quad\times\Lambda_{12,k+1}^T)x_k+\|\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k+\Lambda_{22,k+1}^{-1}\Lambda_{12,k+1}^T\|_F^2 \\
&\quad\times\|\Lambda_{22,k+1}\|_F\|x_k\|^2\}, \quad (15)
\end{aligned}$$

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

For the purpose of minimizing the cost function (9), the controller parameters $\bar{K}_k$ can be selected in each iteration backward as follows:

$$\bar{K}_k^* = \arg\min_{\bar{K}_k}\|\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k + \Lambda_{22,k+1}^{-1}\Lambda_{12,k+1}^T\|_F. \quad (16)$$

It follows from Lemma 1 that (14) is the solution of the optimization problem (16). The proof is completed. □

However, we can see from the above theorem that it is difficult to get the $\bar{K}_k$ from (14). Then in order to obtain the controller parameters $\bar{K}_k$ 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 (5) satisfies the H_∞ performance requirement (6) for any nonzero attack signal ξ_k, if there exist the positive scalar h_k, two families of non-negative definite matrices P_k, S_k ($0 \leq k \leq N$) and a set of real-valued matrices $\bar{K}_k$ satisfying the following two backward recursive RDEs:

$$\begin{cases}\Delta_{11,k+1} - \bar{\Delta}_{12,k+1}\bar{\Delta}_{22,k+1}^{-1}\bar{\Delta}_{12,k+1}^T = P_k, \\ \bar{\Lambda}_{11,k+1}+Q_k-\bar{\Lambda}_{12,k+1}\Lambda_{22,k+1}^{-1}\bar{\Lambda}_{12,k+1}^T=S_k,\end{cases} \quad (17)$$

subject to

$$S_{N+1} = Q_{N+1}, \quad P_{N+1} = 0, \quad (18)$$

$$\bar{\Delta}_{22,k+1} < 0, \quad P_0 < \gamma^2 W, \Lambda_{22,k+1} > 0, \quad (19)$$

$$\bar{K}_k = \mathcal{M}_{k+1}^{\dagger}\mathcal{N}_{k+1}(\bar{\varphi}\bar{C}_k)^{\dagger}, \quad (20)$$

$$\Omega_k < I, \quad (21)$$

where

$$\begin{aligned}
\bar{\Delta}_{12,k+1} &= (A_k+\bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k)^T P_{k+1}\bar{B}_{1,k}, \\
\bar{B}_{1,k} &= [\bar{B}_k\ h_k^{-1}\bar{B}_k], \\
\bar{\Delta}_{22,k+1} &= \bar{B}_{1,k}^T P_{k+1}\bar{B}_{1,k} - \gamma^2 I, \\
\bar{\Lambda}_{11,k+1} &= (A_k-\bar{B}_{1,k}\bar{\Delta}_{22,k+1}^{-1}\bar{\Delta}_{12,k+1}^T)^T S_{k+1}(A_k-\bar{B}_{1,k} \\
&\quad\times\bar{\Delta}_{22,k+1}^{-1}\bar{\Delta}_{12,k+1}^T)+\bar{C}_k^T(\bar{\Upsilon}_{1,k+1}+\bar{\varphi}^T\bar{K}_k^T\bar{\Upsilon}_{2,k+1} \\
&\quad\times\bar{K}_k\bar{\varphi}+\bar{\Upsilon}_{3,k+1})\bar{C}_k, \\
\bar{\Lambda}_{12,k+1} &= (A_k-\bar{B}_{1,k}\bar{\Delta}_{22,k+1}^{-1}\bar{\Delta}_{12,k+1}^T)^T S_{k+1}\bar{B}_k,
\end{aligned}$$

$$\mathcal{M}_{k+1} = (I - \Lambda_{22,k+1}^{-1}\bar{B}_k^T S_{k+1}\bar{B}_{1,k}\bar{\Delta}_{22,k+1}^{-1}\bar{B}_{1,k}^T P_{k+1}\bar{B}_k)\bar{\phi},$$
$$\mathcal{N}_{k+1} = -\Lambda_{22,k+1}^{-1}\bar{B}_k^T S_{k+1}(I - \bar{B}_{1,k}\bar{\Delta}_{22,k+1}^{-1}\bar{B}_{1,k}^T P_{k+1})A_k,$$
$$\Omega_k = h_k^2[\bar{\varphi}^T\bar{K}_k^T\bar{\phi}^T\bar{\phi}\bar{K}_k\bar{\varphi} + \tilde{\varphi}\otimes\bar{K}_k^T\bar{\phi}^T\bar{\phi}\bar{K}_k + \bar{\varphi}^T\bar{K}_k^T\tilde{\phi}\bar{K}_k\bar{\varphi} + \tilde{\varphi}\otimes\bar{K}_k^T\tilde{\phi}\bar{K}_k].$$

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

$$\begin{aligned} x_{k+1} = &(A_k + \bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k)x_k + \bar{B}_k\bar{\phi}\bar{K}_k(\varphi_k - \bar{\varphi})\bar{C}_k x_k \\ &+ \bar{B}_k(\phi_k - \bar{\phi})\bar{K}_k\bar{\varphi}\bar{C}_k x_k + \bar{B}_k(\phi_k - \bar{\phi})\bar{K}_k(\varphi_k - \bar{\varphi})\bar{C}_k x_k \\ &+ \bar{B}_{1,k}\rho_k, \end{aligned} \tag{22}$$

It follows from Theorem 1 that if there exist solutions $\{(h_k, P_k, S_k, \bar{K}_k)\}_{0\le k\le N}$ satisfying the backward recursive RDEs (17) with (18)-(19), then the system satisfies

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

If the condition (21) is satisfied, we can get

$$\begin{aligned} \mathrm{E}\sum_{k=0}^{N}\{\|z_k\|^2\} &< \mathrm{E}\sum_{k=0}^{N}\{\gamma^2\|\rho_k\|^2\} + \gamma^2 x_0^{\mathrm{T}} W x_0 \\ &< \gamma^2\mathrm{E}\sum_{k=0}^{N}\|\xi_k\|^2 + \gamma^2 x_0^{\mathrm{T}} W x_0, \end{aligned} \tag{24}$$

which implies that the H_∞ performance constraint (6) is satisfied. Then for the purpose of minimizing the cost function (10), the suboptimal controller parameters $\bar{K}_k$ can be selected in each iteration backward as follows:

$$\bar{K}_k^* = \arg\min_{\bar{K}_k}\|\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k + \Lambda_{22,k+1}^{-1}\bar{\Lambda}_{12,k+1}^T\|_F, \tag{25}$$

which equal to calculate

$$\bar{K}_k^* = \arg\min_{\bar{K}_k}\|\mathcal{M}_{k+1}\bar{K}_k\bar{\varphi}\bar{C}_k - \mathcal{N}_{k+1}\|_F. \tag{26}$$

It follows from Lemma 1 that (20) is the solution of the optimization problem (26). The proof is completed. ■

Noticing that the controller parameters $\bar{K}_k$ 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: $\bar{\alpha}_j$, $\bar{\beta}_i$, N, Q_{N+1}, γ, W, Q_k, R_k;
Output: $\bar{K}_k$, P_k, S_k,
where $i \in \{1, 2, \ldots, n_u\}$, $j \in \{1, 2, \cdots, n_y\}$, $k \in \{0, 1, \cdots, N\}$.
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 (19), if $\bar{\Delta}_{22,k+1} < 0$ and $\Lambda_{22,k+1} > 0$,then the controller parameters $\bar{K}_k$ can be solved by (20), and go to the next step, else jump to Step 7);
3) If the condition (21) is satisfied, go to the next step, else return to Step 2);
4) Solve the backward RDEs (17) 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 5: 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 a 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 by introducing positive scalar h_k for the controller design, leads to a little conservatism by the incomplete equivalence of deriving equation (24). So we will also try to consider how to reduce conservatism in those two places. In addition, the LMI methods have been used to solve the H_∞ problem, and can reduce conservatism, but it is difficult to consider the performance problem under the worst attack at the same time. Therefore, the problem of reducing conservatism should be considered in combination with the above problems.

Remark 6: 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 or from controllers to actuators 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 a 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.

Remark 7: It is well known that nonlinearity is universal in engineering practice, so this paper which based on the model of linear system has its limitations. In fact, some nonlinear systems in previous studies, such as systems with random sequences whose powers depend on sector-bound nonlinear function of the state, or systems with a random sequence whose power depends on the sign of a nonlinear function of the state, can be transformed into linear systems with certain constraints for the convenience of derivation and calculation. If these nonlinear phenomenon exist, we can try to add the appropriate constraints on the designed targets or adjust variable parameter in order to obtain a feasible solution. But at the same time, the complexity and conservatism of the system will increase accordingly. Therefore, it is one of

our possible research directions to extend the control problem studied in this paper from linear system to nonlinear system. In addition, the time delay problem is also a common phenomenon and will also become one of our research directions in the future.

III. NUMERICAL SIMULATION

In this section, two examples are given to demonstrate the effectiveness of the algorithm proposed in this paper.

Example 1: The parameters of a discrete time-varying open-loop unstable system are as follows:

$$A_k = \begin{bmatrix} 0.2 - 0.8\sin 2k & 0.8 \\ 0.2 + 0.2\cos(2k-3) & -0.9 \end{bmatrix}, \quad B_{1,k} = \begin{bmatrix} 0.15 \\ 0.3 \end{bmatrix},$$
$$B_{2,k} = \begin{bmatrix} -0.1 \\ 0.4 \end{bmatrix}, \quad B_{3,k} = \begin{bmatrix} -0.2 \\ 0.3 \end{bmatrix}, \quad D_k = [\,0.1 \;\; 0.1\,],$$
$$C_{1,k} = [\,0.12\sin(6k) \;\; 0.1\,], \quad C_{2,k} = [\,0.25\cos(k) \;\; 0.3\,].$$

Let the FDI attack signals be

$$w_{1,k} = 0.05\cos 0.5k, \quad w_{2,k} = 0.07\cos 0.5k,$$
$$w_{3,k} = 0.07\cos 0.5k, \quad a_{1,k} = 0.1\sin k, \; a_{2,k} = 0.08\sin k.$$

Case 1: Assuming that the probability parameters are given as $\bar{\alpha}_1 = 0.95$, $\bar{\alpha}_2 = 0.95$, $\bar{\beta}_1 = 0.92$, $\bar{\beta}_2 = 0.92$ and $\bar{\beta}_3 = 0.92$, the H_∞ attack attenuation level $\gamma = 0.6$, the positive definite matrix $W = 0.8I$, the time horizon $N = 200$, the performance weighting matrices $Q_k = 0.8I$, $R_{1,k} = 0.7$, $R_{2,k} = 0.9$ and $R_{3,k} = 0.8$, and the selected scalar $h_k = 0.2$. 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 Figure 2, respectively, and the measured outputs under hybrid attacks and without attacks are shown in Figure 3, respectively.

TABLE 1. The controller gain results.

k	0	1	$\cdots$	99	100
$K_{1,k}$	0.7292	0.2728	$\cdots$	0.4078	0.0088
$K_{2,k}$	1.6956	1.4813	$\cdots$	1.0806	0.6997
$K_{3,k}$	1.8710	1.8116	$\cdots$	1.2200	0.9141

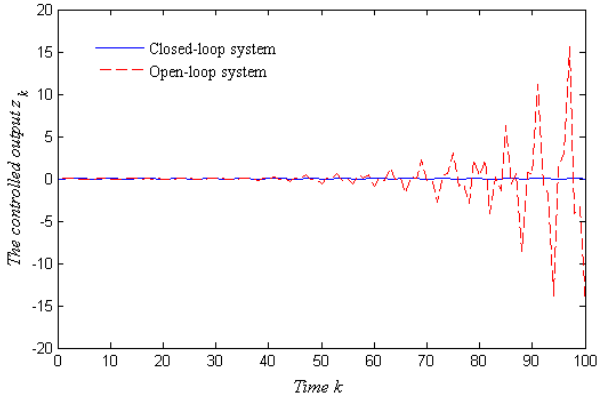


FIGURE 2. The controlled outputs of system.

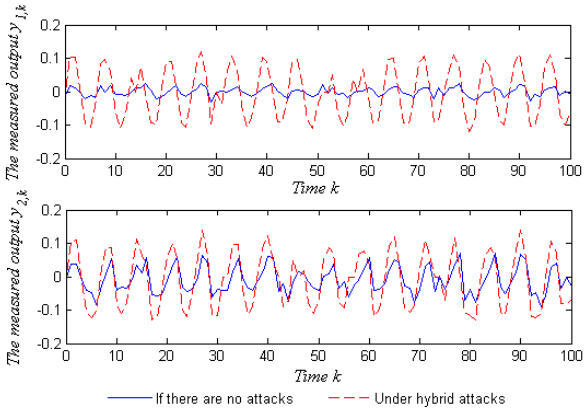


FIGURE 3. The measured outputs of system.

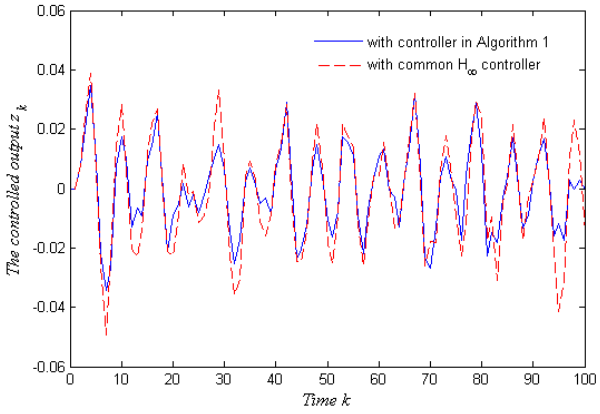


FIGURE 4. The controlled outputs with different algorithms.

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 robust H_∞ 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 Figure 4. From the above numerical results and simulated figures, we can see that the controller design by the 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 0.95 to 0.9, and the probability parameter $\bar{\beta}_1$ ($\bar{\beta}_2$ or $\bar{\beta}_3$) can change from 0.92 to 0.9, the scalar h_k can be selected as 0.21, 0.19 and 0.17. The permitted minimum γ results are shown in Table 3.

TABLE 2. The results comparison.

Using Algorithm 1	Using common H_∞ algorithm
$J_2 = 2.797$	$J_2 = 4.242$
$\gamma_{\min} = 0.73$	$\gamma_{\min} = 1.05$

TABLE 3. The permitted minimum γ.

Parameter	Values								
$\bar{\alpha}_j$	0.95	0.95	0.95	0.9	0.9	0.9	0.95	0.95	0.95
$\bar{\beta}_i$	0.92	0.92	0.92	0.92	0.92	0.92	0.90	0.90	0.90
h_k	0.21	0.19	0.17	0.21	0.19	0.17	0.21	0.19	0.17
$\gamma_{\min}$	0.76	0.72	0.74	0.85	0.73	0.77	0.80	0.74	0.75

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.

Example 2: To further demonstrate the effectiveness of the algorithm proposed above, another example is given. consider a classical angular positioning system with the transfer function $P(s) = \kappa/s(s+\alpha)$ in [35] where $\kappa = 0.787$, $0 < \alpha < 10$. The control problem is to use the input voltage to the motor to rotate the antenna so that it always points in the direction of a moving object in the plane. The transfer function can be described by the following linear time varying model when the sampling time is chosen 0.1 s:

$$A_k = \begin{bmatrix} 1 & 0.1 \\ 0 & 0.99\sin^2 k \end{bmatrix}, \quad B_{1,k} = \begin{bmatrix} 0 \\ 0.787 \end{bmatrix},$$
$$D_k = [\,0.1 \;\; -0.2\,], \quad C_{1,k} = [\,0.6 \;\; 0.1\,],$$
$$C_{2,k} = [\,0.4 \;\; -0.1\,].$$

When considering the effect of the FDI attack on the system, we assume that the attack signals can be described as $w_{1,k} = 0.02Ran(1)$, $a_{1,k} = a_{2,k} = 0.01Ran(1)$, the probability parameters are given as $\bar{\alpha}_1 = 0.8$, $\bar{\alpha}_2 = 0.9$ and $\bar{\beta}_1 = 0.9$, the H_∞ attack attenuation level $\gamma = 0.8$, the positive definite matrix $W = I$, the time horizon $N = 100$, the performance weighting matrices $Q_k = I$, $R_{1,k} = 1$, and the selected scalar $h_k = 0.5$. Using Algorithm 1, we can obtain the controlled outputs of closed-loop system and open-loop system, which are shown in Figure 5, respectively. From the results we can see that the open-loop controlled output gradually diverges after being attacked, while the closed-loop controlled output gradually converges. So the controller design algorithm is effective for the practical system.

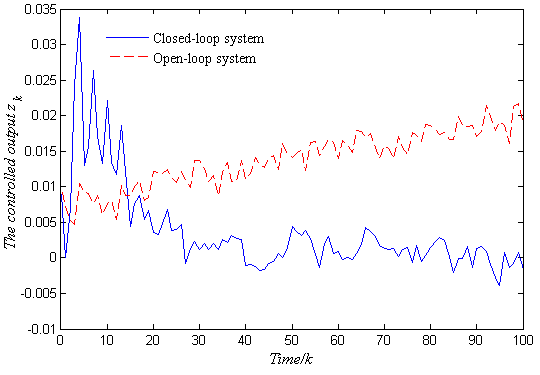


FIGURE 5. The controlled outputs of system.

IV. CONCLUSION

This paper has presented the H_∞ 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_∞ 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.

APPENDIX
PROOF OF LEMMA 2

Proof: By defining

$$\begin{aligned} V_k &\triangleq \mathrm{E}\{x_{k+1}^T P_{k+1} x_{k+1} - x_k^T P_k x_k\} \\ &= \mathrm{E}\{x_k^T[(A_k + \bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k)^T P_{k+1}(A_k + \bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k) \\ &\quad + \bar{C}_k^T\Upsilon_{1,k+1}\bar{C}_k + \bar{C}_k^T\bar{\Psi}^T\bar{K}_k^T\Upsilon_{2,k+1}\bar{K}_k\bar{\varphi}\bar{C}_k \\ &\quad + \bar{C}_k^T\Upsilon_{3,k+1}\bar{C}_k \\ &\quad - P_k]x_k + 2x_k^T[(A_k + \bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{C}_k)^T P_{k+1}(\bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{I}_1 \\ &\quad + \bar{B}_k\bar{I}_2) + \bar{C}_k^T\Upsilon_{1,k+1}\bar{I}_1 + \bar{C}_k^T\bar{\varphi}^T\bar{K}_k^T\Upsilon_{2,k+1}\bar{K}_k\bar{\varphi}\bar{I}_1 \\ &\quad + \bar{C}_k^T\Upsilon_{3,k+1}\bar{I}_1]\xi_k + \xi_k^T[(\bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{I}_1 + \bar{B}_k\bar{I}_2)^T P_{k+1} \\ &\quad \times (\bar{B}_k\bar{\phi}\bar{K}_k\bar{\varphi}\bar{I}_1 + \bar{B}_k\bar{I}_2) + \bar{I}_1^T\Upsilon_{1,k+1}\bar{I}_1 + \bar{I}_1^T\bar{\varphi}^T\bar{K}_k^T \\ &\quad \times \Upsilon_{2,k+1}\bar{K}_k\bar{\varphi}\bar{I}_1 + \bar{I}_1^T\Upsilon_{3,k+1}\bar{I}_1]\xi_k\}, \end{aligned} \tag{27}$$

then taking the mathematical expectation (27), and applying the completing squares method results in

$$\begin{aligned} J_1 &= \mathrm{E}\sum_{k=0}^{N}\{x_k^T D_k^T D_k x_k - \gamma^2\xi_k^T\xi_k + x_{k+1}^T P_{k+1}x_{k+1} \\ &\quad - x_k^T P_k x_k\} + \mathrm{E}\{x_0^T P_0 x_0 - x_{N+1}^T P_{N+1}x_{N+1}\} \\ &= \mathrm{E}\sum_{k=0}^{N}\{x_k^T(\Delta_{11,k+1} - P_k - \Delta_{12,k+1}\Delta_{22,k+1}^{-1} \\ &\quad \times \Delta_{12,k+1}^T)x_k + (\xi_k - \xi_k^*)^T\Delta_{22,k+1}(\xi_k - \xi_k^*)\} \\ &\quad + \mathrm{E}\{x_0^T P_0 x_0 - x_{N+1}^T P_{N+1}x_{N+1}\}, \end{aligned} \tag{28}$$

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

$$J_1 < \gamma^2 x_0^T W x_0, \tag{29}$$

which means the pre-specified H_∞ performance requirement (6) is satisfied. The proof is completed. □

REFERENCES

[1] E. Bou-Harb, W. Lucia, N. Forti, S. Weerakkody, N. Ghani, and B. Sinopoli, "Cyber meets control: A novel federated approach for resilient CPS leveraging real cyber threat intelligence," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 198–204, May 2017.

[2] K.-D. Kang and S. H. Son, "Real-time data services for cyber physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Beijing, China, Jun. 2008, pp. 483–488.

[3] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy Mag.*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[4] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, May 2016.

[5] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, Berkeley/Oakland, CA, USA, May 2010, pp. 447–462.

[6] Y. Zhao, X. He, and D. Zhou, "Optimal joint control and triggering strategies against denial of service attacks: A zero-sum game," *IET Control Theory Appl.*, vol. 11, no. 14, pp. 2352–2360, Sep. 2017.

[7] Y. Li, J. Wu, and S. Li, "Controllability and observability of CPSs under networked adversarial attacks," *IET Control Theory Appl.*, vol. 11, no. 10, pp. 1596–1602, Jun. 2017.

[8] S. Liu, P. X. Liu, and A. El Saddik, "A stochastic game approach to the security issue of networked control systems under jamming attacks," *J. Franklin Inst.*, vol. 351, no. 9, pp. 4570–4583, Sep. 2014.

[9] A. Burg, A. Chattopadhyay, and K.-Y. Lam, "Wireless communication and security issues for cyber–physical systems and the Internet-of-Things," *Proc. IEEE*, vol. 106, no. 1, pp. 38–60, Jan. 2018.

[10] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Beijing, China, Jun. 2008, pp. 495–500.

[11] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[12] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proc. 12th Int. Conf. Hyb. Syst. Compu. Control*, San Francisco, CA, USA, Apr. 2009, pp. 31–45.

[13] A. Y. Lu and G. H. Yang, "Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial-of-service," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1813–1820, Sep. 2017.

[14] Z. Ai, L. Peng, and M. Cao, "Optimal attack schedule for two sensors state estimation under jamming attack," *IEEE Access*, vol. 7, pp. 75741–75748, 2019.

[15] C. Kwon and I. Hwang, "Cyber attack mitigation for cyber–physical systems: Hybrid system approach to controller design," *IET Control Theory Appl.*, vol. 10, no. 7, pp. 731–741, Apr. 2016.

[16] H. Fawzi, P. Tabuada, and S. Diggavi, "Security for control systems under sensor and actuator attacks," in *Proc. IEEE 51st IEEE Conf. Decis. Control (CDC)*, Maui, HI, USA, Dec. 2012, pp. 3412–3417.

[17] Z. Wang, Y. Chen, F. Liu, Y. Xia, and X. Zhang, "Power system security under false data injection attacks with exploitation and exploration based on reinforcement learning," *IEEE Access*, vol. 6, pp. 48785–48796, 2018.

[18] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 6058–6064, Nov. 2017.

[19] D. Ding, Z. Wang, J. Lam, and B. Shen, "Finite-horizon $\mathcal{H}_\infty$ control for discrete time-varying systems with randomly occurring nonlinearities and fading measurements," *IEEE Trans. Autom. Control*, vol. 60, no. 9, pp. 2488–2493, Sep. 2015.

[20] C. E. de Souza, K. A. Barbosa, and A. T. Neto, "Robust H_∞ filtering for discrete-time linear systems with uncertain time-varying parameters," *IEEE Trans. Signal Process.*, vol. 54, no. 6, pp. 2110–2118, Jun. 2006.

[21] L. Ma, Z. Wang, Y. Bo, and Z. Guo, "A game theory approach to mixed control for a class of stochastic time-varying systems with randomly occurring nonlinearities," *Syst. Control Lett.*, vol. 60, no. 12, pp. 1009–1015, Dec. 2011.

[22] A. I. Maalouf and I. R. Petersen, "Time-varying H_∞ control for a class of linear quantum systems: A dynamic game approach," *Automatica*, vol. 48, no. 11, pp. 2908–2916, Nov. 2012.

[23] D. Ding, Z. Wang, B. Shen, and H. Dong, "Envelope-constrained $\mathcal{H}_\infty$ filtering with fading measurements and randomly occurring nonlinearities: The finite horizon case," *Automatica*, vol. 55, pp. 37–45, May 2015.

[24] L. Zou, Z. Wang, J. Hu, and H. Gao, "On $\mathcal{H}_\infty$ finite-horizon filtering under stochastic protocol: Dealing with high-rate communication networks," *IEEE Trans. Autom. Control*, vol. 62, no. 9, pp. 4884–4890, Sep. 2017.

[25] W. Xu, Z. Wang, and D. W. C. Ho, "Finite-horizon H_∞ consensus for multiagent systems with redundant channels via an observer-type event-triggered scheme," *IEEE Trans. Cybern.*, vol. 48, no. 5, pp. 1567–1576, May 2018.

[26] L. Zou, Z. Wang, and H. Gao, "Observer-based $\mathcal{H}_\infty$ control of networked systems with stochastic communication protocol: The finite-horizon case," *Automatica*, vol. 63, pp. 366–373, Jan. 2016.

[27] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.

[28] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 5, pp. 1334–1342, Sep. 2012.

[29] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 46–65, Feb. 2015.

[30] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Networked control under random and malicious packet losses," *IEEE Trans. Autom. Control*, vol. 62, no. 5, pp. 2434–2449, May 2017.

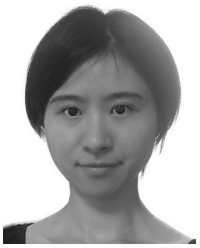
[31] A. W. A. Saif, "Control for uncertain nonlinear networked control systems with random packet losses," *IEEE Access*, vol. 7, pp. 26179–26191, 2019.

[32] R. Sakthivel, S. Santra, and B. Kaviarasan, "Resilient sampled-data control design for singular networked systems with random missing data," *J. Franklin Inst.*, vol. 355, no. 3, pp. 1040–1072, Feb. 2018.

[33] H. Shen, Y. Men, Z.-G. Wu, and J. H. Park, "Nonfragile $\mathcal{H}_\infty$ control for fuzzy Markovian jump systems under fast sampling singular perturbation," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 12, pp. 2058–2069, Dec. 2018.

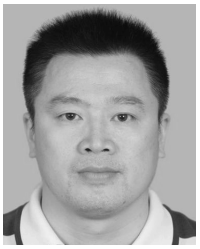
[34] R. Penrose, "On best approximate solutions of linear matrix equations," *Math. Proc. Cambridge Phil. Soc.*, vol. 52, no. 1, pp. 17–19, Jan. 1956.

[35] J. Wu, L. Zhang, and T. Chen, "Model predictive control for networked control systems," *Int. J. Robust Nonlinear*, vol. 19, no. 9, pp. 1016–1035, Jan. 2009.



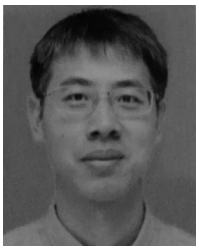
SHAN LIU was born in Dalian, Liaoning, China, in 1986. She received the B.S. and M.S. degrees from the Northeastern University, Shenyang, in 2009 and 2015, respectively. She is currently pursuing the Ph.D. degree in control theory and control engineering from the South China University of Technology, Guangzhou, China.

Her main research interests include robust control theory, security of cyber-physical systems, and networked control systems.



YONGGUI LIU (Member, IEEE) received the B.S. degree in electronic information engineering from the Hunan University of Technology, in 2001, the M.S. degree from the School of Electronic and Information Engineering, South China University of Technology(SCUT), China, in 2008, and the Ph.D. degree from the College of Automation Science and Engineering, SCUT, in 2011.

He was a Postdoctoral Fellow with the Shenzhen Research Institute, The Chinese University of Hong Kong, from September 2012 to August 2014. He is currently an Associate Professor with the Key Laboratory of Autonomous Systems and Network Control, Ministry of Education, College of Automatic Science and Engineering, SCUT. His main research interests include autonomous vehicle control, network secure, and networked control systems.



SHANBIN LI was born in Jiangxi, China, in 1978. He received the B.S. degree from Nanchang University, in 2000, and the Ph.D. degree from Zhejiang University, in 2005.

From 2005 to 2006, he was a Postdoctoral Scholar with the Research Center for Automatic Control of Nancy, Nancy University, France. From 2013 to 2014, he was a Visiting Scholar with the Research Center for Automatic Control of Nancy, University of Lorraine, France. He is currently an Associate Professor with the College of Automation Science and Engineering, South China University of Technology, China. His research interests include networked control systems, stochastic systems, time-delay systems, robust control, fault detection isolation, fault-tolerant control, and so on.

BUGONG XU (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees from SCUT, in 1982, 1989, and 1993, respectively.

From 1993 to 1995, he was a Visiting Scholar with the Power Systems Group, Department of Electronic and Electrical Engineering, University of Strathclyde, Scotland. From 2001 to 2002, he was a Research Professor with the Department of Electrical and Computer Engineering, The University of New Mexico, USA. After 2001, he was a Project Review Expert in automation with the National Natural Science Foundation of China. Since 2001, he has been an Expert with the Special Subsidy by the State Department of China. He was the Dean of the College of Automation Science and Engineering, SCUT, from 2003 to 2013. He is currently a Professor with the College of Automation Science and Engineering (CASE), SCUT. He is also the Head of the Team with the Laboratory of the Real-Time Control Through Internet and Fieldbuses, CASE. His current research interests include analysis and synthesis, wireless sensor networks, real-time control based on the internet, and networked control systems.