Observer-based $H_\infty$ PID control for discrete-time systems under hybrid cyber attacks

Pengyu Wen\textsuperscript{a,b}, Nan Hou\textsuperscript{a,b}, Yuxuan Shen\textsuperscript{a,b}, Jiahui Li\textsuperscript{a,b} and Yi Zhang\textsuperscript{c}

\textsuperscript{a}Artificial Intelligence Energy Research Institute, Northeast Petroleum University, Daqing, People’s Republic of China; \textsuperscript{b}Heilongjiang Provincial Key Laboratory of Networking and Intelligent Control, Northeast Petroleum University, Daqing, People’s Republic of China; \textsuperscript{c}Department of Natural Gas Control, Oil & Gas Administration Center of National Petroleum and Natural Gas Pipeline Network Group Co., Ltd, Beijing, People’s Republic of China

ABSTRACT
In this paper, the observer-based $H_\infty$ PID control problem is studied for linear discrete-time systems subject to hybrid cyber attacks. Two sets of Bernoulli distributed stochastic variables are utilized to characterize the random nature of the false data injection attack and the replay attack. A sector-like bounded condition is exploited to constrain the malicious signal in the false data injection attack which reflects the certain tolerable bound on the difference between the attack signal and the true signal. Sufficient conditions for the existence of the expected observer-based $H_\infty$ PID controller are given to ensure the exponential mean-square stability and the $H_\infty$ performance. Then, the controller parameters are calculated by solving a matrix inequality. Finally, a simulation example is employed to demonstrate the effectiveness of the proposed control algorithm.

ARTICLE HISTORY
Received 5 January 2021
Accepted 22 February 2021

KEYWORDS
PID control; observer-based control; hybrid cyber attacks; false data injection attack; replay attack

1. Introduction
In the past decades, the proportional-integral-derivative (PID) control has played a ruling role in practical engineering due to the advantages like ease of hardware implementation (Ang et al., 2005; Åström et al., 1993; Zhao et al., 2018; Zhuang & Atherton, 1993). In the PID control, there are three parameters which need to be adjusted, that is, the proportional parameter, the integral parameter and the derivative parameter. The parameter tuning of the PID control affects the system performance such as robustness and stability. Therefore, the issue of parameter tuning has been an active discussion topic and plenty of research results have been obtained, see e.g. Rosinová and Veselý (2007), Silva et al. (2002), Takahashi et al. (1997), Ying (2000) and the references therein.

In most of the studies concerning the PID control problem, there is an implicit assumption that the state of the controlled system is directly available. Nevertheless, such an assumption is not always true in reality. In the circumstances, it is inevitable to construct the state once again by using the available measurement output. Recently, various kinds of algorithms for state observers have been put forward and applied in system observation (Basin, Ramírez, et al., 2018), closed-loop feedback controller design (Basin, Yu, et al., 2018; Lien, 2004), robust adaptive unknown input observer (Soleymani et al., 2020), observer-based consensus control (Ding et al., 2017) and so on. On the other hand, in the traditional PID control algorithm, the impact of the external disturbance has always been ignored, which results in poor robustness to the external disturbance. To improve the robustness of the PID control scheme, considerable research results have been obtained (Zhao et al., 2018; Zhao, Wang, Ding, et al., 2020; Zhao, Wang, Wei, et al., 2020).

In another research frontier, the networked control system (NCS), with the improvement of the wireless communication technology, has been comprehensively studied in the past decades (Cetinkaya et al., 2017; Chen et al., 2018; Huang et al., 2012; Y. Li et al., 2015; Mousavinejad et al., 2018; Peng et al., 2018; Zhu & Martínez, 2014). In the NCS, when the communication network is not protected by the security protections, the signals transmitted through the communication network are vulnerable to the network threats. Among various network threats to the NCS, the cyber attacks aim to spitefully destroy the normal operation of the system by intercepting, falsifying or deleting some crucial data. In recent years, there is an increase of interest on the research of control problem subject to cyber attacks, see Zhao, Wang, Wei, et al. (2020), Ding et al. (2017), An and Yang (2018), Bai et al. (2017), and M. Zhang and Lin (2020).

In this paper, we mainly focus on two types of cyber attacks, namely, the false data-injection (FDI) attack and...
the replay attack. The FDI attack is known as one of the most dangerous attacks, where the attacker replaces the transmitted information in order to tamper the completeness of data (Yuan & Xia, 2018). Recently, the control problem for networked systems under FDI attack has received interest from researchers. For example, in Jin et al. (2017) and Zhao and Yang (2020), adaptive secure control schemes under the FDI attack have been designed. In Bai et al. (2017) and Ding et al. (2018), the control problems under the randomly occurring FDI attack have been studied. As for the replay attack, the attacker records the past transmitted information and injects the recorded information into the system, which leads to extra difficulty in detecting the attack. Up to now, the control problem for systems under the replay attack has also received attention from researchers. For example, a recording-horizon control scheme has been designed to tackle the replay attack in Zhu and Martinez (2014). In Mo et al. (2014), in order to detect whether the system is under replay attack, additional Gaussian signals have been injected into the system. It is worth mentioning that, in most of the existing literature concerning control problems under cyber attacks, only one type of cyber attack has been considered. Nevertheless, in real world, the system may be subject to more than one type of cyber attacks. As such, it is of practical significance to investigate control problem for systems under hybrid cyber attacks.

Motivated by the above discussion, the purpose of this paper is to study the observer-based \( H_\infty \) PID control problem for linear discrete-time systems under hybrid cyber attacks. Three important problems that need to be answered are listed as follows: (1) how to set up an appropriate mathematical model to characterize the FDI attack and the replay attack simultaneously? (2) how to reduce the influence of the hybrid attacks on the performance for the discrete-time system? (3) how to select a suitable and engineering-oriented constraint to characterize the malicious signal considered in this paper? Thus, effort is made to conduct the specific research and solve these problems in this paper.

The main contributions of this paper are underlined as follows: (1) both the FDI attack and the replay attack are considered which caters for the real practice; (2) a novel mathematic model is designed to characterize the FDI attack and the replay attack; and (3) by using the Lyapunov stability theory, an observer-based \( H_\infty \) PID controller is designed which guarantees the desired performance.

The remainder of this paper is outlined as follows. In Section 2, the linear discrete-time system under the hybrid cyber attacks is formulated. In Section 3, the observer-based \( H_\infty \) PID control scheme is carried out. As a simulation example is conducted in Section 4 and the conclusion is given in Section 5.

**Notation:** The notation utilized in this paper is fairly normative except where otherwise declared. For a matrix \( W \), \( W^T \) and \( W^\perp \) denote the transpose and the orthogonal basis of the null space, respectively. The space of square summable sequences is depicted by \( l_2(0, +\infty) \). The symbol \( \otimes \) represents the Kronecker product. In a symmetric matrix, an asterisk * describes a term induced by symmetry. \( I \) and \( 0 \) show, respectively, the identity matrix and zero matrix with appropriate dimensions. \( E\{x\} \) stands for the expectation of stochastic variable \( x \). For symmetric matrices \( X \) and \( Y \), \( X \succeq Y \) means that \( X-Y \) is non-negative definite, and \( X > Y \) means that \( X-Y \) is positive definite.

### 2. Problem formulation

Consider a discrete-time linear system described by:

\[
\begin{align*}
x_{k+1} &= Ax_k + Bu_k + D\omega_k \\
y_k &= Cx_k + E\omega_k \\
z_k &= Fx_k
\end{align*}
\]

where \( x_k \in \mathbb{R}^{nx} \) is the system state, \( u_k \in \mathbb{R}^{nu} \) is the control input, \( \omega_k \in (l_2[0, \infty), \mathbb{R}^{nw}) \) is the external disturbance, \( y_k \in \mathbb{R}^{ny} \) is the measurement output, \( z_k \in \mathbb{R}^{nz} \) is the control output, and \( A, B, C, D, E, F \) are known real constant matrices with appropriate dimensions.

#### 2.1. Observer-based PID controller

In this paper, an observer-based PID controller is designed as follows:

\[
\begin{align*}
\hat{x}_{k+1} &= A\hat{x}_k + L(y_k - C\hat{x}_k) + Bu_k \\
\zeta_k &= K_p\hat{x}_k + K_i\sum_{i=k-1}^{k-1} \hat{x}_i + K_D(\hat{x}_k - \hat{x}_{k-1})
\end{align*}
\]

where \( \hat{x}_k \in \mathbb{R}^{nx} \) is the estimate of \( x_k \) and \( \zeta_k \) is the output of the controller. \( K_p, K_i, K_D \) are the controller gains to be designed and \( L \) is the observer gain to be designed. \( q \) is a known positive constant which is determined according to practical engineering.

**Remark 2.1:** In this paper, an observer-based PID controller is constructed whose input is the state estimate and the output is the sum of three parts, among which are the \( P \) (proportional term), the \( I \) (integral term) and the \( D \) (differential term). To be precise, the main procedure of designing the desired PID controller is first to estimate the immeasurable system state, and then utilize the state estimate signal to perform the state-feedback control. Moreover, a time-window with limited length is applied in the integral term for the sake of reducing computation burden.
2.2. The cyber attack model

During the transmission from the controller to the actuator, the control signal is subject to random hybrid cyber attacks. The real control input is modelled as

\[ u_k = \zeta_k + a_{1k} \xi_k \]  

(3)

where \( u_k \) is the control input received by the actuator, \( \varphi_k \) is the hybrid attack signal which is defined later, and \( a_{1k} \) is a Bernoulli distributed random variable that satisfies

\[ \text{Prob}(a_{1k} = 1) = \bar{a}_1, \quad \text{Prob}(a_{1k} = 0) = 1 - \bar{a}_1. \]

The hybrid attack \( \varphi_k \) contains the FDI attack and the replay attack and is modelled as follows:

\[ \varphi_k = -\zeta_k + a_{2k} v_k + (1 - a_{2k}) \zeta_k - \xi_k \]  

(4)

where \( v_k \) is the FDI attack signal satisfying the following condition:

\[ (v_k - G\hat{x}_k)^T(v_k - G\hat{x}_k) \leq \delta^2 \hat{x}_k^T \hat{x}_k \]  

(5)

with \( G \) being a known real matrix and \( \delta \geq 0 \) being a known real constant. \( \zeta_k - \xi_k \) stands for the replay attack signal with \( \zeta_k \in [\underline{\zeta}, \overline{\zeta}] \) where \( \underline{\zeta} \) and \( \overline{\zeta} \) are non-negative integers. \( a_{2k} \) is a Bernoulli distributed random variable that satisfies

\[ \text{Prob}(a_{2k} = 1) = \bar{a}_2, \quad \text{Prob}(a_{2k} = 0) = 1 - \bar{a}_2. \]

Remark 2.2: In this paper, hybrid cyber attacks are injected into the transmission from the controller to the actuator by the adversary. The hybrid attack \( \varphi_k \) contains the FDI attack and the replay attack. From the defenders’ perspective, the attacks could occur in an intermittent or random manner. To reflect such a practical situation, we utilize two Bernoulli sequences with known statistical information to characterize the random occurrence of the FDI attack and the replay attack. On the other hand, in practice, the adversary generally does not have infinite energy and launch unbounded attack arbitrarily. Then, as for the adversary, it makes practical sense to assume simultaneously that the injected false signal \( v_k \) is sector-like bounded and the time of the recorded past signal \( \zeta_k - \xi_k \) is within a certain range.

Denoting \( \tilde{x}_k \triangleq x_k - \hat{x}_k \) as the estimation error, we have

\[ \tilde{x}_{k+1} = (A - LC)\tilde{x}_k + (D - LE)\omega_k. \]  

(6)

Under the controller (2), the augmented system is shown as follows:

\[
\begin{align*}
\dot{\tilde{x}}_{k+1} &= (A + \bar{a}_{1k}\tilde{A})\tilde{x}_k + (B + \bar{a}_{1k}\tilde{B})\xi_k + (a_{1k}\tilde{G} + a_{1k}\tilde{\bar{A}}) \\
\tilde{x}_{k-\zeta} + (a_{1k}\tilde{H} + a_{1k}\tilde{\bar{A}})\xi_{k-\zeta} + a_{1k}\tilde{D}v_k + D\omega_k \\
z_k &= F\tilde{x}_k
\end{align*}
\]  

(7)

where

\[ \tilde{x}_k \triangleq [x_k^T \cdots \tilde{x}_{k-q}^T]^T, \quad \xi_k \triangleq [\tilde{x}_{k-1}^T \cdots \tilde{x}_{k-q}^T]^T, \]

\[ K_0 \triangleq I \otimes K_0, \quad \tilde{K}_I \triangleq I \otimes K_I, \]

\[ \tilde{K}_0 \triangleq I \otimes \tilde{K}_0, \quad \tilde{W} \triangleq \begin{bmatrix} \tilde{K}_I & \tilde{K}_I & \cdots & \tilde{K}_I \end{bmatrix}_{q-1} \]

\[ \tilde{G} \triangleq [G - G], \]

\[ A_0 \triangleq [A \quad 0], \quad A_L \triangleq [0 \quad A - LC], \]

\[ J \triangleq \begin{bmatrix} (1 - \bar{a}_1)B\tilde{K}_0 \\ \bar{A} & -BK_0 \end{bmatrix}, \quad \bar{B} \triangleq \begin{bmatrix} -BK_0 \\ 0 \end{bmatrix}, \quad D \triangleq \begin{bmatrix} D \\ D - LE \end{bmatrix}, \]

\[ D \triangleq \begin{bmatrix} B \\ 0 \end{bmatrix}, \quad G \triangleq \begin{bmatrix} (1 - \bar{a}_2)B\tilde{K}_0 \\ 0 \end{bmatrix}, \quad \mathcal{H} \triangleq \begin{bmatrix} (1 - \bar{a}_2)B\tilde{K}_0 \\ 0 \end{bmatrix}, \]

\[ \mathcal{F} \triangleq [F \quad 0]. \]

The aim of this paper is to design an \( H_\infty \) PID controller for the linear discrete-time systems under hybrid cyber attacks such that:

1. the zero-solution of the closed-loop system (7) with \( \omega_k = 0 \) is exponentially mean-square stable;
2. under zero initial condition, for all nonzero \( \omega_k \), the control output \( z_k \) satisfies the \( H_\infty \) performance constraint:

\[ \sum_{k=0}^{\infty} \mathbb{E}\{z_k^Tz_k\} \leq \gamma^2 \sum_{k=0}^{\infty} \mathbb{E}\{\omega_k^T\omega_k\} \]  

(8)

where \( \gamma > 0 \) is a given scalar standing for the disturbance attenuation level.

3. Main results

3.1. Stability and \( H_\infty \) performance analysis

In this section, an observer-based \( H_\infty \) PID controller (2) is designed for the system (1) under the hybrid cyber attacks (3). Sufficient conditions are given in Theorems 3.1–3.2 to guarantee the exponential mean-square stability and the \( H_\infty \) performance, respectively. Then, the desired PID controller parameters are derived in Theorem 3.3.
\textbf{Theorem 3.1:} Let $K_p, K_v, K_D$ and $L$ be given. The zero-solution of the system (7) is exponentially mean-square stable with $\omega_k = 0$ if there exist positive definite matrices $P, Q_j$ ($j = 1, 2, \ldots, q$), $R$ and $U$ such that

$$\Xi_1 = \begin{bmatrix} \Xi_{11} & \ast \\ \Xi_{11} & \Xi_{22} \end{bmatrix} < 0 \quad (9)$$

where

$$\Theta_1 \triangleq -P + \sum_{j=1}^{q} Q_j + (\zeta - \zeta + 1)R - \mu \hat{G}^T \hat{G} + \mu \Delta^2 I^T \Delta,$$

$$\Xi_{11} \triangleq \begin{bmatrix} \Theta_1 & \ast & \ast & \ast \\ 0 & -Q + (\zeta - \zeta + 1)U & \ast & \ast \\ 0 & 0 & -R & \ast \\ 0 & 0 & 0 & -U \end{bmatrix},$$

$$\Xi_{22} \triangleq -L_S \otimes P^{-1},$$

$Q \triangleq \text{diag}(Q_1, Q_2, \ldots, Q_q), \quad a_1^* \triangleq \bar{a}_1(1 - \bar{a}_1), \quad a_2^* \triangleq \bar{a}_2(1 - \bar{a}_2).$

\textbf{Proof:} Choosing the following Lyapunov functional:

$$V_k = \sum_{i=1}^{4} V_{ik} \quad (10)$$

where

$$V_{1k} \triangleq \hat{x}_k^T P \hat{x}_k, \quad V_{2k} \triangleq \sum_{j=1}^{q} \sum_{i=k-j}^{k-1} \hat{x}_j^T Q_j \hat{x}_i,$$

$$V_{3k} \triangleq \sum_{m=k-h}^{k-1} \hat{x}_m^T R \hat{x}_m + \sum_{h=1}^{k} \sum_{m=k}^{k-1} \hat{x}_m^T R \hat{x}_m,$$

$$V_{4k} \triangleq \sum_{n=k-h}^{k-1} \xi_n^T U \xi_n + \sum_{h=1}^{k} \sum_{n=k}^{k-1} \xi_n^T U \xi_n.$$

Calculating the difference of $V_{ik}$ ($i = 1, 2, \ldots, 4$) with $\omega_k = 0$, one has

$$\mathbb{E}\{DV_{1k}\} = \mathbb{E}\{V_{k+1} - V_{1k}\}$$

$$= \mathbb{E}\{\hat{x}_{k+1}^T P \hat{x}_{k+1} - \hat{x}_k^T P \hat{x}_k\}$$

$$= \mathbb{E}\{((A + \bar{a}_1 \bar{A}) \hat{x}_k + (B + \bar{a}_1 \bar{B}) \xi_k + (a_1 \bar{G} + a_1 \bar{a}_2 \bar{B}) \hat{x}_k - \xi_k^T \xi_k)^T P((A + \bar{a}_1 \bar{A}) \hat{x}_k + (B + \bar{a}_1 \bar{B}) \xi_k + (a_1 \bar{G} + a_1 \bar{a}_2 \bar{B}) \hat{x}_k - \xi_k^T \xi_k)\}$$

$$+ \mathbb{E}\{a_1 \bar{a}_2 \bar{B} \hat{x}_k \hat{x}_k^T \xi_k^T \xi_k \}$$

$$= \mathbb{E}\{V_{k+1} - V_{1k}\}.$$
$$\mathbb{E}\{\Delta V_{2k}\} = \mathbb{E}\{V_{2k+1} - V_{2k}\}$$

$$= \mathbb{E}\left\{ \sum_{j=1}^{q} \left( \sum_{i=k-j+1}^{k} \bar{x}_j^T Q \bar{x}_i - \sum_{i=k-j}^{k-1} \bar{x}_j^T Q \bar{x}_i \right) \right\}$$

$$= \mathbb{E}\left\{ \sum_{j=1}^{q} (\bar{x}_j^T Q \bar{x}_j - \bar{x}_{k-j}^T Q \bar{x}_{k-j}) \right\}$$

$$\leq \mathbb{E}\left\{ \bar{x}_k^T \left( A^T P A + a_1^* A_1^T \bar{P} \bar{A} \right) \right\} + 2a_1 a_2 \bar{x}_k^T \left( B^T P \bar{A} \right)$$

From the constraint (5), we know that there exists a real number $\mu > 0$ such that

$$-\mu (\bar{v}_k - \bar{G} \bar{x}_k)^T (\bar{v}_k - \bar{G} \bar{x}_k) - \delta^2 \bar{x}_k^T \bar{I} \bar{x}_k \geq 0.$$  

In terms of (16), we further obtain

$$\mathbb{E}\{\Delta V_k\} \leq \mathbb{E}\left\{ \bar{x}_k^T \left( A^T P A + a_1^* A_1^T \bar{P} \bar{A} \right) \right\} + \sum_{j=1}^{q} \left( (\bar{v}_j^T - \bar{G} \bar{x}_j) (\bar{v}_k - \bar{G} \bar{x}_k) - 2a_1 \bar{x}_k^T \bar{I} \bar{x}_k \right) \geq 0.$$ 

According to (11)–(14), we have

$$\mathbb{E}\{\Delta V_k\} \leq \mathbb{E}\{\Delta V_{1k} + \Delta V_{2k} + \Delta V_{3k} + \Delta V_{4k}\}$$

$$\leq \mathbb{E}\left\{ \bar{x}_k^T \left( A^T P A + a_1^* A_1^T \bar{P} \bar{A} \right) \right\}$$

$$+ \sum_{j=1}^{q} \left( (\bar{v}_k^T - \bar{G} \bar{x}_k) (\bar{v}_j^T - \bar{G} \bar{x}_j) - 2a_1 \bar{x}_k^T \bar{I} \bar{x}_k \right) \geq 0.$$ 

where

$$\eta_{1k} \triangleq \begin{bmatrix} \bar{x}_k^T & \bar{v}_j^T & \bar{x}_{k-\bar{k}}^T & \bar{x}_{k-\bar{k}}^T \end{bmatrix}^T$$

$$\Delta_{11} \triangleq A^T P A + a_1^* A_1^T \bar{P} \bar{A} + \sum_{j=1}^{q} \left( (\bar{v}_j^T - \bar{G} \bar{x}_j) (\bar{v}_k^T - \bar{G} \bar{x}_k) - 2a_1 \bar{x}_k^T \bar{I} \bar{x}_k \right)$$

$$\Delta_{21} \triangleq A^T P A + a_1^* A_1^T \bar{P} \bar{A},$$

$$\Delta_{22} \triangleq B^T P \bar{A} + a_1^* B_1^T \bar{P} \bar{A},$$

$$\Delta_{23} \triangleq A^T P A + a_1^* A_1^T \bar{P} \bar{A}.$$
\[ \Delta_{31} \triangleq \bar{a}_1 G^T P_A, \quad \Delta_{32} \triangleq \bar{a}_1 G^T P_B, \]
\[ \Delta_{33} \triangleq \bar{a}_1 G^T P_{\mathcal{Q}} + \bar{a}_1 \sigma_2^2 \bar{a}_2^T P_{\bar{A}} - R, \]
\[ \Delta_{41} \triangleq \bar{a}_1 H^T P_A, \quad \Delta_{42} \triangleq \bar{a}_1 H^T P_B, \]
\[ \Delta_{43} \triangleq \bar{a}_1 H^T P_{\mathcal{Q}} + \bar{a}_1 \sigma_2^2 \bar{a}_2^T P_{\bar{A}}, \]
\[ \Delta_{44} \triangleq \bar{a}_1 H^T P_H + \bar{a}_1 \sigma_2^2 \bar{a}_2^T P_B - U, \]
\[ \Delta_{51} \triangleq \bar{a}_1 \bar{a}_2 D^T P_A + \mu \bar{G}, \quad \Delta_{52} \triangleq \bar{a}_1 \bar{a}_2 D^T P_B, \]
\[ \Delta_{53} \triangleq \bar{a}_1 \bar{a}_2 D^T P_{\mathcal{Q}}, \quad \Delta_{54} \triangleq \bar{a}_1 \bar{a}_2 D^T P_H, \]
\[ \Delta_{55} \triangleq \bar{a}_1 \bar{a}_2 D^T P_D - \mu l. \]

With the help of the Schur Complement Lemma, it is known that \( \Pi_1 < 0 \) can be ensured by (9). Then, there exists a positive scalar \( \phi > 0 \) such that
\[ \mathbb{E}\{\Delta V_k\} \leq -\phi \| h_{1k} \|^2. \] (18)

By following the similar analysis in Wang et al. (2017), the system (7) is exponentially mean-square stable. The proof is complete. \[ \square \]

In Theorem 3.1, the exponential mean-square stability of the system (7) is analyzed. In the following theorem, the \( H_\infty \) performance of the system (7) will be considered.

**Theorem 3.2:** Let the disturbance attenuation level \( \gamma > 0 \) and the controller gain matrices be given. The system (7) is exponentially mean-square stable and satisfies the \( H_\infty \) constraint (8) if there exist positive definite matrices \( P, Q_j \) \((j = 1, 2, \ldots, q), R \) and \( U \) such that
\[ \Xi_2 = \left[ \begin{array}{cc} \Xi_{21} & * \\ \Xi_{21}^T & \Xi_{22} \end{array} \right] < 0 \] (19)

where
\[ \Xi_{21} \triangleq -P + \sum_{j=1}^{l} Q_j + (\sigma - \xi + 1)R - \mu G^T \tilde{G} + \mu \delta^2 T^T T + F^T F, \]
\[ \Xi_{22} \triangleq -P + \sum_{j=1}^{l} Q_j + (\sigma - \xi + 1)R - \mu G^T \tilde{G} + \mu \delta^2 T^T T + F^T F, \]
\[ \Xi_{21} \triangleq \begin{bmatrix} \Theta_2 & * & * & * & * \\ -Q + (\sigma - \xi + 1)R & * & * & * & * \\ 0 & 0 & -R & * & * \\ 0 & 0 & 0 & -U & * \\ 0 & 0 & 0 & 0 & -\mu l \end{bmatrix}, \]
\[ \Xi_{22} \triangleq \begin{bmatrix} A & B & \bar{a}_1 G^T & \bar{a}_1 H^T & \bar{a}_1 \bar{a}_2 D^T \\ 0 & 0 & 0 & 0 & 0 \\ \sqrt{\sigma_1} \bar{A} & \sqrt{\sigma_1} \bar{A} & \sqrt{\sigma_1} \bar{A} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \]
\[ \Xi_{22} \triangleq -I_5 \otimes \rho^{-1}. \]

**Proof:** It is obvious that (19) implies (9), then the system (7) is exponentially mean-square stable. Now, let us prove that the system (7) satisfies the \( H_\infty \) constraint under the zero-initial condition.

Choosing the Lyapunov functional as (10), we have
\[ \mathbb{E}\{\Delta V_k + z_k^T z_k - \gamma^2 \omega_k^T \omega_k\} \leq \mathbb{E}\{h_{1k}^T \Pi_1 h_{1k} + 2 \bar{x}_k^T (A + \bar{a}_1 \bar{A})^T P D \omega_k + 2 \bar{x}_k^T (B + \bar{a}_1 \bar{B})^T P D \omega_k + \omega_k D^T P D \omega_k\} \]
\[ \leq \mathbb{E}\{h_{1k}^T \Pi_1 h_{1k} + 2 \bar{x}_k^T \bar{A}^T P D \omega_k + 2 \bar{x}_k^T \bar{B}^T P D \omega_k \}
\[ + 2 \bar{a}_1 \bar{x}_k^T \bar{A}^T P D \omega_k + 2 \bar{a}_1 \bar{x}_k^T \bar{B}^T P D \omega_k \]
\[ + 2 \bar{a}_1 \bar{x}_k^T \bar{A}^T P D \omega_k + 2 \bar{a}_1 \bar{x}_k^T \bar{B}^T P D \omega_k \]
\[ + \omega_k D^T P D \omega_k + \bar{x}_k^T F^T F \bar{x}_k - \gamma^2 \omega_k^T \omega_k\} \]
\[ = \mathbb{E}\{h_{2k}^T \Pi_2 h_{2k}\} \]

where
\[ h_{2k} \triangleq \begin{bmatrix} \bar{x}_k^T & \xi_k^T & \bar{x}_k^T \bar{A} & \xi_k^T \bar{B} & u_k^T & v_k^T \end{bmatrix}, \]
\[ \Pi_2 \triangleq \begin{bmatrix} \Omega_{11} & * & * & * & * & * \\ \Omega_{21} & \Omega_{22} & * & * & * & * \\ \Omega_{31} & \Omega_{32} & \Omega_{33} & * & * & * \\ \Omega_{41} & \Omega_{42} & \Omega_{43} & \Omega_{44} & * & * \\ \Omega_{51} & \Omega_{52} & \Omega_{53} & \Omega_{54} & \Omega_{55} & * \\ \Omega_{61} & \Omega_{62} & \Omega_{63} & \Omega_{64} & \Omega_{65} & \Omega_{66} \end{bmatrix}, \]
\[ \Omega_{11} \triangleq \bar{A}^T P_A + \bar{a}_1^T \bar{A}^T P_{\bar{A}} + \sum_{j=1}^{q} (\sigma - \xi + 1)R \]
\[ - \mu \tilde{G}^T \tilde{G} + \mu \delta^2 T^T T + F^T F - P, \]
\[ \Omega_{21} \triangleq \bar{B}^T P_A + \bar{a}_1^T \bar{A}^T P_{\bar{A}}, \]
\[ \Omega_{22} \triangleq \bar{B}^T P_{\mathcal{Q}} + \bar{a}_1^T \bar{B}^T P_{\bar{B}} - Q + (\sigma - \xi + 1)U, \]
\[ \Omega_{31} \triangleq \bar{a}_1 G^T P_A, \quad \Omega_{32} \triangleq \bar{a}_1 G^T P_B, \]
\[ \Omega_{33} \triangleq \bar{a}_1 G^T P_{\mathcal{Q}} + \bar{a}_1^2 \bar{A}^T P_{\bar{A}} - R, \]
\[ \Omega_{41} \triangleq \bar{a}_1 H^T P_A, \quad \Omega_{42} \triangleq \bar{a}_1 H^T P_B, \]
\[ \Omega_{43} \triangleq \bar{a}_1 H^T P_{\mathcal{Q}} + \bar{a}_1 \sigma_2^2 \bar{A}^T P_{\bar{A}}, \]
\[ \Omega_{44} \triangleq \bar{a}_1 H^T P_H + \bar{a}_1 \sigma_2^2 \bar{B}^T P_{\bar{B}} - U, \]
\[ \Omega_{51} \triangleq \bar{a}_1 \bar{a}_2 D^T P_A + \mu \bar{G}, \quad \Omega_{52} \triangleq \bar{a}_1 \bar{a}_2 D^T P_B, \]
\[ \Omega_{53} \triangleq \bar{a}_1 \bar{a}_2 D^T P_{\mathcal{Q}}, \quad \Omega_{54} \triangleq \bar{a}_1 \bar{a}_2 D^T P_H, \]
\[ \Omega_{55} \triangleq \bar{a}_1 \bar{a}_2 D^T P_D - \mu l, \quad \Omega_{61} \triangleq D^T P_A, \]
\[ \Omega_{62} \triangleq D^T P_B, \quad \Omega_{63} \triangleq \bar{a}_1 D^T P_{\mathcal{Q}}, \quad \Omega_{64} \triangleq \bar{a}_1 D^T P_H, \]
\( \Omega_{65} \triangleq \bar{a}_1 \bar{a}_2 D^T \rho \tilde{D}, \quad \Omega_{66} \triangleq D^T \rho D - \gamma^2 I. \)

By applying the Schur Complement Lemma, one can see from (19) that \( \Pi_2 \leq 0 \), which implies
\[
\mathbb{E}(\Delta V_k) + \mathbb{E}(\xi_k^T \xi_k) - \gamma^2 \mathbb{E}(\omega_k^T \omega_k) < 0. \tag{20}
\]
Summing up (20) from 0 to \( \infty \) with respect to \( k \), one has
\[
\sum_{k=0}^{\infty} \mathbb{E}(\xi_k^T \xi_k) \leq \gamma^2 \sum_{k=0}^{\infty} \mathbb{E}(\omega_k^T \omega_k), \tag{21}
\]
which completes the proof.

\[ \square \]

### 3.2. PID controller design

In this subsection, the solution to the observer-based \( H_\infty \) PID control problem is presented for linear discrete-time systems subject to hybrid cyber attacks.

**Theorem 3.3:** Let the disturbance attenuation level \( \gamma > 0 \) be given. The system (7) is said to be exponentially mean-square stable and satisfies the \( H_\infty \) performance condition (8) with \( \omega_k = 0 \) if there exist positive definite matrices \( \tilde{P}, Q_i \) (\( i = 1, 2, \ldots, q \)), \( R, U \) and matrices \( \tilde{\Sigma}_{11}, \tilde{\Sigma}_{12}, \tilde{\Sigma}_{22}, \tilde{L}, \tilde{K}_p, \tilde{K}_u, \tilde{K}_D \) as such:
\[
\tilde{\Sigma}_2 \triangleq \begin{bmatrix} \tilde{\Sigma}_{21}^1 & \tilde{\Sigma}_{21}^2 \end{bmatrix} < 0 \tag{22}
\]
where
\[
\tilde{\Sigma}_{21}^1 \triangleq \begin{bmatrix} \Lambda_{11} & 0 & 0 & \cdots & 0 \\ \Lambda_{12} & \Lambda_{13} & \Lambda_{14} & \cdots & \Lambda_{15} \end{bmatrix}, \\
\Lambda_{16} & \cdots & \Lambda_{11} \\
\end{bmatrix}
\]
\[
\tilde{\Sigma}_{21}^2 \triangleq I_5 \otimes \tilde{\Sigma}, \quad \tilde{\Sigma} \triangleq \begin{bmatrix} \tilde{P} - \mathbb{E}(\mathbf{W}) - \mathbb{E}(\mathbf{W}^T \mathbf{Y})^T \\ 0 \\ \cdots \\ 0 \\ \tilde{P} \end{bmatrix}, \tag{23}
\]

\[
\Lambda_{11} \triangleq \begin{bmatrix} \lambda_{11} \\ \lambda_{12} \\ \lambda_{13} \\ \lambda_{14} \\ \lambda_{15} \\ \cdots \\ \lambda_{16} \end{bmatrix}, \quad \lambda_{16} \triangleq \begin{bmatrix} \lambda_{11} \\ \lambda_{12} \\ \lambda_{13} \\ \lambda_{14} \\ \lambda_{15} \\ \cdots \\ \lambda_{16} \end{bmatrix}, \tag{24}
\]

Moreover, the gain matrices of the controller (2) can be calculated by
\[
\tilde{K}_p = \tilde{\Sigma}_{11}^{-1} \tilde{K}_p, \quad \tilde{K}_u = \tilde{\Sigma}_{11}^{-1} \tilde{K}_u, \\
\tilde{K}_D = \tilde{\Sigma}_{11}^{-1} \tilde{K}_D, \quad L = \tilde{P}^{-1} \tilde{L}. \tag{25}
\]

**Proof:** First, we denote
\[
\hat{\Sigma} \triangleq \begin{bmatrix} \hat{\Sigma}_1 & \hat{\Sigma}_2 \\ \hat{\Sigma}_2 & \hat{\Sigma}_3 \end{bmatrix} < 0 \tag{26}
\]

Pre- and post- multiplying inequality \( \tilde{\Sigma}_2 < 0 \) in (19) by \( \text{diag}(I, I, I, I, I, I, I, I, I, I) \) and its transposition, one has
\[
\hat{\Sigma}_2 \triangleq \begin{bmatrix} \hat{\Sigma}_{21}^1 & \hat{\Sigma}_{21}^2 \end{bmatrix} < 0 \tag{27}
\]
where
\[
\hat{\Sigma}_{21}^1 \triangleq \begin{bmatrix} \hat{\Lambda}_{11} & 0 & 0 & \cdots & 0 \\ \hat{\Lambda}_{12} & \hat{\Lambda}_{13} & \hat{\Lambda}_{14} & \cdots & \hat{\Lambda}_{15} \end{bmatrix}, \\
\hat{\Lambda}_{16} & \cdots & \hat{\Lambda}_{11} \\
\end{bmatrix}
\]
\[
\hat{\Sigma}_{21}^2 \triangleq I_5 \otimes \hat{\Sigma}, \quad \hat{\Sigma} \triangleq \begin{bmatrix} \hat{\Sigma}_{22} \hat{W}_{\tilde{p}^{-1} \tilde{W}^T \mathbf{Y}^T} \hat{\Sigma}_{22} \end{bmatrix} < 0 \tag{28}
\]

Pre- and post- multiplying inequality \( \hat{\Sigma}_3 < 0 \) in (20) by \( \text{diag}(I, I, I, I, I, I, I, I, I, I) \) and its transposition, one has
\[
\hat{\Sigma}_3 \triangleq \begin{bmatrix} \hat{\Sigma}_{31} & \hat{\Sigma}_{32} \end{bmatrix} < 0 \tag{29}
\]
where
\[
\hat{\Sigma}_{31} \triangleq \begin{bmatrix} \hat{\Lambda}_{11} & 0 & 0 & \cdots & 0 \\ \hat{\Lambda}_{12} & \hat{\Lambda}_{13} & \hat{\Lambda}_{14} & \cdots & \hat{\Lambda}_{15} \end{bmatrix}, \\
\hat{\Lambda}_{16} & \cdots & \hat{\Lambda}_{11} \\
\end{bmatrix}
\]
\[
\hat{\Sigma}_{32} \triangleq I_5 \otimes \tilde{\Sigma}, \quad \tilde{\Sigma} \triangleq \begin{bmatrix} \hat{\Sigma}_{32} \hat{W}_{\tilde{p}^{-1} \tilde{W}^T \mathbf{Y}^T} \hat{\Sigma}_{32} \end{bmatrix} < 0 \tag{30}
\]
\[
\begin{align*}
\bar{\Lambda}_{16} & \triangleq \begin{bmatrix} \Im WD \end{bmatrix}, \\
\bar{\Lambda}_{23} & \triangleq \begin{bmatrix} \sqrt{\bar{\alpha}_1} (1 - \bar{\alpha}_2) \Im WBK_a \\ 0 \end{bmatrix}, \\
\bar{\Lambda}_{24} & \triangleq \begin{bmatrix} \sqrt{\bar{\alpha}_1^2} \bar{\alpha}_2 \Im WB \end{bmatrix}, \\
\bar{\Lambda}_{25} & \triangleq \begin{bmatrix} \sqrt{\bar{\alpha}_1^2\bar{\alpha}_2^2} \Im WBK_a \end{bmatrix}, \\
\bar{\Lambda}_{35} & \triangleq \begin{bmatrix} \sqrt{\bar{\alpha}_1\bar{\alpha}_2^2} \Im WBK_b \end{bmatrix}, \\
\bar{\Lambda}_{41} & \triangleq \begin{bmatrix} -\sqrt{\bar{\alpha}_1^2} \Im WBK_a \end{bmatrix}, \\
\bar{\Lambda}_{42} & \triangleq \begin{bmatrix} -\sqrt{\bar{\alpha}_1^2} \Im WBK_b \end{bmatrix}, \\
\bar{\Lambda}_{53} & \triangleq \begin{bmatrix} -\sqrt{\bar{\alpha}_1\bar{\alpha}_2^2} \Im WBK_a \end{bmatrix}, \\
\bar{\Lambda}_{54} & \triangleq \begin{bmatrix} -\sqrt{\bar{\alpha}_1\bar{\alpha}_2^2} \Im WBK_b \end{bmatrix}.
\end{align*}
\]

Noting that
\[
\begin{align*}
\Im W + W^T \Im^T - \Im W \bar{\rho}^{-1} W^T \Im^T - \bar{\rho} &= -(\Im W - \bar{\rho}) \bar{\rho}^{-1} (\Im W - \bar{\rho})^T \leq 0, \\
\text{the inequality (24) holds if and only if} \\
\begin{bmatrix}
\Im_{11}^1 & * \\
\Im_{21}^1 & \Im_{22}^1
\end{bmatrix} < 0. \\
\end{align*}
\]

Make the following expressions:
\[
\begin{align*}
\bar{K}_P & = \Im WBK_P = \Im \begin{bmatrix} I \\ 0 \end{bmatrix} K_P = \begin{bmatrix} \Im_{11} K_P \\ 0 \end{bmatrix}, \\
\bar{K}_I & = \Im WBK_I = \Im \begin{bmatrix} I \\ 0 \end{bmatrix} K_I = \begin{bmatrix} \Im_{11} K_I \\ 0 \end{bmatrix}, \\
\bar{K}_D & = \Im WBK_D = \Im \begin{bmatrix} I \\ 0 \end{bmatrix} K_D = \begin{bmatrix} \Im_{11} K_D \\ 0 \end{bmatrix}, \\
\bar{L} & = \bar{\rho} L.
\end{align*}
\]

Therefore, taking (26) into consideration, it follows that (19) holds if (22) is true. The proof is now complete.

\textbf{Remark 3.1:} For a kind of discrete-time linear systems subject to hybrid attacks, the designed observer-based $H_\infty$ PID controller can guarantee that the closed-loop system satisfies both the exponential mean-square stability and the $H_\infty$ performance. Furthermore, the gain matrices of the PID controller could be computed conveniently via solving the LMI (22).

\textbf{Remark 3.2:} In this paper, an observer-based $H_\infty$ PID controller has been designed for discrete-time systems under hybrid cyber attacks. The novelties of this paper are displayed as follows: (1) both the FDI attack and the replay attack have been taken into consideration; and (2) the malicious signal in FDI attack is characterized by the bounded condition which caters for the practical engineering.

\section*{4. An illustrative example}

In this section, a numerical example is given to show the effectiveness of the developed observer-based $H_\infty$ PID control scheme.

Consider a system (1) whose parameters are given as follow:
\[
\begin{align*}
A & = \begin{bmatrix} 0.45 & 0.11 \\ -0.12 & 0.23 \end{bmatrix}, \\
B & = \begin{bmatrix} 0.13 \\ 0.31 \end{bmatrix}, \\
C & = \begin{bmatrix} 0.62 & -0.93 \end{bmatrix}, \\
D & = \begin{bmatrix} 0.45 \\ 0.82 \end{bmatrix}, \\
E & = 0.12, \\
F & = \begin{bmatrix} 1 & 1 \end{bmatrix}.
\end{align*}
\]

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure1.png}
\caption{Error trajectory tracking.}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure2.png}
\caption{Open-loop state trajectory.}
\end{figure}
The disturbance attenuation level $\gamma$ is set as 0.97. The occurring probability of the hybrid attacks is set to be $\alpha_1 = 0.4$ and $\alpha_2 = 0.6$ which means that the probability of the FDI attack is 0.6. The malicious signal $v_k$ is chosen as $v_k = 1.88\hat{x}_k$ which satisfies the bounded constraint (5) with $g = 1$ and $\delta = 1$. The integral length $q$ is 3. Meanwhile, the external disturbance is set as $\omega_k = e^{-0.24k}$. Using the YALMIP toolbox in Matlab to solve the matrix inequality (22), the parameters of the controller are obtained as follows:

$$K_P = [-1.2470 \quad 0.2063], \quad K_I = [0.0070 \quad -0.0856],$$
$$K_D = [0.0087 \quad -0.2757], \quad L = \begin{bmatrix} -0.4133 \\ -0.3822 \end{bmatrix}.$$  

The simulation results are plotted in Figures 1–3. Figure 1 plots the estimation error, Figure 2 shows the open-loop system state, and Figure 3 presents the closed-loop system state. The simulation results verify that the developed observer-based $H_\infty$ PID control scheme is effectiveness.

5. Conclusions

In this paper, the observer-based $H_\infty$ PID control problem has been studied for linear discrete-time systems under hybrid cyber attacks. Sufficient conditions have been established to ensure that the closed-loop system is exponentially mean-square stable and satisfied the $H_\infty$ performance. Then, the controller gains have been characterized by solving a matrix inequality. Finally, a simulation example has been conducted to demonstrate the effectiveness of the proposed control scheme. For subsequent research directions, we focus on coping with the PID control for systems with uncertainties (Liang et al., 2011), nonlinearities (Cui et al., 2018; Dong et al., 2011; Wang et al., 2017), incomplete measurements (Ding et al., 2017a; D. Zhang et al., 2017), protocols (Ding et al., 2019; X. Li et al., 2020; Zou et al., 2019), multi-rate measurements (Zou, Wang, Dong, et al., 2020), dynamic event-triggered mechanism (Zou, Wang, & Zhou, 2020, October), time-delays (J. Li et al., 2019), respectively.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported in part by the National Natural Science Foundation of China under Grants 61873058 and 62073070, the Natural Science Foundation of Heilongjiang Province of China under Grant F2018004, and the Alexander von Humboldt Foundation of Germany.

References

An, L., & Yang, G.-H. (2018, January). Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks. IEEE Transactions on Cybernetics, 49(3), 827–838. doi:10.1109/TCYB.2017.2787740
Ang, K. H., Chong, G., & Li, Y. (2005, July). PID control system analysis, design, and technology. IEEE Transactions on Control Systems Technology, 3(4), 559–576. doi:10.1109/TCST.2005.847331
Åström, K. J., Hägglund, T., Hang, C. C., & Ho, W. K. (1993, August). Automatic tuning and adaptation for PID controllers—a survey. Control Engineering Practice, 1(4), 699–714. https://doi.org/10.1016/0967-0661(93)91394-C
Bai, C.-Z., Pasqualetti, F., & Gupta, V. (2017, April). Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs. Automatica, 82, 251–260. https://doi.org/10.1016/j.automatica.2017.04.047
Basin, M. V., Ramírez, P. C. R., & Guerra-Avellaneda, F. (2018, February). Continuous fixed-time controller design for mechatronic systems with incomplete measurements. IEEE-ASME Transactions on Mechatronics, 23(1), 57–67. https://doi.org/10.1109/TMECH.2017.2700459
Basin, M. V., Yu, P., & Shitskel, Y. B. (2018, January). Hypersonic missile adaptive sliding mode control using finite- and fixed-time observers. IEEE Transactions on Industrial Electronics, 65(1), 930–941. https://doi.org/10.1109/TIE.2017.271116
Cetinkaya, A., Ishii, H., & Hayakawa, T. (2017, May). Networked control under random and malicious packet losses. IEEE Transactions on Automatic Control, 62(5), 2434–2449. https://doi.org/10.1109/TAC.2016.2612818
Chen, B., Ho, D. W. C., Hu, G., & Yu, L. (2018, June). Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. IEEE Transactions on Cybernetics, 48(6), 1862–1876. https://doi.org/10.1109/TCYB.2017.2716115
Cui, Y., Liu, Y., Zhang, W., & Alsaaedi, F. E. (2018, November). Sampled-based consensus for nonlinear multiagent systems with deception attacks: The decoupled method. IEEE Transactions on Systems, Man, and Cybernetics: Systems. https://doi.org/10.1109/TSMC.2018.2876497
Ding, D., Wang, Z., Han, Q.-L., & Wei, G. (2018, May). Security control for discrete-time stochastic nonlinear systems subject to deception attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(5), 779–789. https://doi.org/10.1109/TSMC.2016.2616544

Ding, D., Wang, Z., Han, Q.-L., & Wei, G. (2019, June). Neural-network-based output-feedback control under Round-Robin scheduling protocols. *IEEE Transactions on Cybernetics*, 49(6), 2372–2384. https://doi.org/10.1109/TCyB.2018.2827037

Ding, D., Wang, Z., Ho, D. W. C., & Wei, G. (2017a, April). Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. *Automatica*, 78, 231–240. https://doi.org/10.1016/j.automatica.2016.12.026

Ding, D., Wang, Z., Ho, D. W. C., & Wei, G. (2017b, August). Observer-based event-triggering consensus control for multi-agent systems with lossy sensors and cyber-attacks. *IEEE Transactions on Cybernetics*, 47(8), 1936–1947. https://doi.org/10.1109/TCSY.2016.2582802

Dong, H., Lam, J., & Gao, H. (2011, January). Distributed $H_{\infty}$ filtering for repeated scalar nonlinear systems with random packet losses in sensor networks. *International Journal of Systems Science*, 42(9), 1507–1519. https://doi.org/10.1080/00207721.2010.550403

Huang, C., Ho, D. W. C., & Lu, J. (2012, April). Partial-information-based distributed filtering in two-targets tracking sensor network. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 59, 820–832. https://doi.org/10.1109/TCSI.2011.2169912

Jin, X., Haddad, W. M., & Yucelen, T. (2017, November). An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems. *IEEE Transactions on Automatic Control*, 62(11), 6058–6064. https://doi.org/10.1109/TAC.2017.2652127

Li, J., Dong, H., Wang, Z., Hou, N., & Alsaaadi, F. E. (2019). On passivity and robust passivity for discrete-time stochastic neural networks with randomly occurring mixed time delays. *Neural Computing and Applications*, 31(1), 65–78. https://doi.org/10.1007/s00521-017-2980-1

Li, X., Han, F., Hou, N., Dong, H., & Liu, H. (2020, May). Set-membership filtering for piecewise linear systems with censored measurements under Round-Robin protocol. *International Journal of Systems Science*, 51(9), 1578–1588. https://doi.org/10.1080/00207712.2020.1768453

Li, Y., Shi, L., Cheng, P., Chen, J., & Quevedo, D. E. (2015, October). Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Transactions on Automatic Control*, 60(10), 2831–2836. https://doi.org/10.1109/TAC.2015.2461851

Li, J., Shen, B., Dong, H., & Lam, J. (2011, January). Robust distributed state estimation for sensor networks with multiple stochastic communication delays. *International Journal of Systems Science*, 42(9), 1459–1471. https://doi.org/10.1080/00207721.2010.550402

Lien, C. H. (2004, August). Robust observer-based control of systems with state perturbations via LMI approach. *IEEE Transactions on Automatic Control*, 49(8), 1365–1370. https://doi.org/10.1109/TAC.2004.832660

Mo, Y., Chabukswar, R., & Sinopoli, B. (2014, July). Detecting integrity attacks on SCADA systems. *IEEE Transactions on Control Systems Technology*, 22(4), 1396–1407. https://doi.org/10.1109/TCST.2013.2280899

Mousavinejad, E., Yang, F., Han, Q.-L., & Vlasic, L. (2018, November). A novel cyber attack detection method in networked control systems. *IEEE Transactions on Cybernetics*, 48(11), 3254–3264. https://doi.org/10.1109/TCYB.2018.2843358

Peng, L., Shi, L., Cao, X., & Sun, C. (2018, July). Optimal attack energy allocation against remote state estimation. *IEEE Transactions on Automatic Control*, 63(7), 2199–2205. https://doi.org/10.1109/TAC.2018.2843358

Rosinová, D., & Veselý, V. (2007). Robust PID decentralized controller design using LMI. *International Journal of Computers Communications & Control*, 2(2), 195–204. https://doi.org/10.15837/ijccc.2007.2

Silva, G. J., Datta, A., & Bhattacharyya, S. P. (2002, February). New results on the synthesis of PID controllers. *IEEE Transactions on Automatic Control*, 47(2), 241–252. https://doi.org/10.1109/9.983352

Soleymani, R., Nekoui, M. A., & Moarefianpour, A. (2020, January). Robust adaptive unknown input observer design for a class of disturbed systems. *Systems Science and Control Engineering*, 8(1), 249–257. https://doi.org/10.1080/21642583.2020.1739578

Takahashi, R. H. C., Peres, P. L. D., & Ferreira, P. A. V. (1997, October). Multijobective $H_{\infty}/H_{2}$ guaranteed cost PID design. *IEEE Control Systems Magazine*, 17(5), 37–47. https://doi.org/10.1109/37.621468

Wang, D., Mu, C., He, H., & Liu, D. (2017, July). Event-driven adaptive robust control of nonlinear systems with uncertainties through NDP strategy. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 47(7), 1358–1370. https://doi.org/10.1109/TSMC.2016.2592682

Yang, H. (2000, April). Theory and application of a novel fuzzy PID controller using a simplified Takagi-Sugeno rule scheme. *Information Sciences*, 123(3), 261–293. https://doi.org/10.1016/S0020-0255(99)00133-4

Yuan, H., & Xia, Y. (2018). Secure filtering for stochastic non-linear systems under multiple missing measurements and deception attacks. *IET Control Theory & Applications*, 12(4), 515–523. https://doi.org/10.1049/ctt.2017.124

Zhang, M., & Lin, C. (2020). Secure state estimation for cyber physical systems with state delay and sparse sensor attacks. *Systems Science and Control Engineering*. https://doi.org/10.1080/21642583.2020.1834465

Zhang, D., Song, H., & Yu, L. (2017, August). Robust fuzzy-model-based filtering for nonlinear cyber-physical systems with multiple stochastic incomplete measurements. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 47(8), 1826–1838. https://doi.org/10.1109/TSMC.2016.2551200

Zhao, D., Wang, Z., Ding, D., Wei, G., & Alsaaadi, F. E. (2018, April). PID output-feedback control under event-triggered protocol. *International Journal of General Systems*, 47(5), 432–445. https://doi.org/10.1080/03081079.2018.1459596

Zhao, D., Wang, Z., Ding, D., & Wei, G. (2020, June). $H_{\infty}$ PID control with fading measurements: The output-feedback case. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(6), 2170–2180. https://doi.org/10.1109/TSMC.2020.3022102

Zhao, D., Wang, Z., Wei, G., & Han, Q.-L. (2020, October). A dynamic event-triggered approach to observer-based PID security control subject to deception attacks. *Automatica*, 120, Article No. 109128, 13 pages. https://doi.org/10.1016/j.automatica.2020.109128

Zhao, L., & Yang, G.-H. (2020). Cooperative adaptive fault-tolerant control for multi-agent systems with deception...
attacks. *Journal of the Franklin Institute*, 357(6), 3419–3433. https://doi.org/10.1016/j.jfranklin.2019.12.032

Zhu, M., & Martínez, S. (2014, March). On the performance analysis of resilient networked control systems under replay attacks. *IEEE Transactions on Automatic Control*, 59(3), 804–808. https://doi.org/10.1109/TAC.2013.2279896

Zhuang, M., & Atherton, D. P. (1993, May). Automatic tuning of optimum PID controllers. *IEE Proceedings D-Control Theory and Applications*, 140(3), 216–224. https://doi.org/10.1049/ip-d.1993.0030

Zou, L., Wang, Z., Dong, H., & Han, Q.-L. (2020, November). Moving horizon estimation with multi-rate measurements and correlated noises. *International Journal of Robust and Nonlinear Control*, 30(17), 7429–7445. https://doi.org/10.1002/rnc.v30.17

Zou, L., Wang, Z., Han, Q.-L., & Zhou, D. (2019, December). Moving horizon estimation for networked time-delay systems under Round-Robin protocol. *IEEE Transactions on Automatic Control*, 64(12), 5191–5198. https://doi.org/10.1109/TAC.9

Zou, L., Wang, Z., & Zhou, D. (2020, October). Moving horizon estimation with non-uniform sampling under component-based dynamic event-triggered transmission. *Automatica*, 120. https://doi.org/10.1109/TAC.2019.2910167