Research on co-design of dual security control and communication for nonlinear CPS with actuator fault and FDI attacks

Li Zhao¹,², Wei Li¹ and YaJie Li¹

Abstract
In this study, a co-design method of dual security control and communication is investigated for a nonlinear cyber–physical system (CPS) with an actuator fault and false data injection (FDI) attacks. First, under the discrete event trigger communication scheme, considering the different effects of actuator fault and FDI attacks on a double-end network, a dual security control strategy with active fault-tolerance and active–passive attack-tolerance is proposed. It can accommodate an actuator fault, actively compensate an actuator FDI attack, and passively resist a sensor FDI attack, respectively, thereby establishing a new dual security control framework with fault-tolerance and attack-tolerance. Moreover, the Takagi–Sugeno (T-S) fuzzy model for the nonlinear CPS is established under this framework. Second, by constructing an appropriate Lyapunov–Krasovskii functional and introducing the time-delay theory and the affine Bessel–Legendre inequality, lesser conservative design methods of a robust augmented observer for the estimation of the state, FDI attacks, and fault as well as a dual security controller are obtained. Finally, a classical quadruple-tank model is used to show the validity and feasibility of the proposed method.

Keywords
Nonlinear cyber-physical system (CPS), false data injection (FDI) attacks, dual security control, active fault-tolerance, active-passive attack-tolerance, co-design

Introduction
A cyber–physical system (CPS) is a complex system with the highest degree of integration among cyber and physical systems; it realizes real-time perception and control using computational techniques and by communication and control.¹,² Because it is commonly applied in intelligent transportation, smart cities, micro-grids, and other fields, CPS has gained increasing interest and become a prominent topic.³ Generally, a CPS is prone to risks and can lose stability because of the following reasons: (1) The system operation needs to be accessed and controlled remotely through an open network, and cyber attacks are easy in this scenario, which increases the risks of the system information being destroyed, tampered, or blocked.⁴,⁵ (2) The actuator, as the core physical component of a CPS, is highly prone to faults because it needs to operate in a relatively harsh environment for a long time.⁶ Therefore, it is significant to study security control for a CPS under the dual threats of cyber attacks and physical faults.⁷,⁸

During application, most of the controlled plants are nonlinear. However, modeling a nonlinear system is difficult because of its complexity and particularity and the requirement of high system performance, to solve this problem, the Takagi–Sugeno (T–S) fuzzy model is an effective approach.⁹ Its basic concept is to decompose a nonlinear system into a series of linear combinations of local subsystems using IF–THEN rules, and subsequently apply the linear system theory for modeling, analysis, and synthesis. Because of its simple modeling process, it has achieved remarkable results.¹⁰–¹²

¹School of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou, P. R. China
²School of Electrical Engineering, Longdong University, Qingyang, P. R. China

Corresponding author:
Wei Li, School of Electrical and Information Engineering, Lanzhou University of Technology, No.36, Pengjiaping Road, Qilihe District, Lanzhou, Gansu 730050, China.
Email: liwei@lut.edu.cn
There are two aspects of security problems in a nonlinear CPS: physical and cyber security. Physical security refers to the safety and stability maintenance of a CPS when the physical components fail, whereas cyber security refers to the security of the communication network that supports the CPS information perception and interaction. In view of physical security, fault-tolerant control is an effective method for dealing with component faults, which has advanced in recent years. Passive, active, and active-passive hybrid fault-tolerant methods were respectively adopted in Li and Li, Lan and Patton, and Xu et al. to investigate physical security. However, the above results do not consider the issue of cyber security. Therefore, studying the dual security control problem for a nonlinear CPS based on the T–S fuzzy model is highly challenging, which is one of the motivations of this study.

With the development of CPSs, the security problems of their cyber systems are becoming constantly exposed, and frequent cyber attacks make the control system more vulnerable. In general, cyber attacks on a CPS mainly include denial-of-service (DoS) and false data injection (FDI) attacks. A DoS attack is simple to implement; however, there is no stealth in space and time; therefore, it is easy to detect and prevent. However, a FDI attack has high concealment and is difficult to detect, resulting in a greater potential threat and higher destructiveness than a DoS attack. StuxNet virus is a typical example of a FDI attack. For FDI attacks in a CPS, a static output feedback robust control strategy was studied in Su and Ye to achieve stable system operation. In An and Yang, an improved adaptive resilient controller was designed to tolerate attacks passively. In Corradini and Cristofaro, a sliding mode attack-tolerant control strategy was proposed, which effectively realizes a passive defense against FDI attacks. The strategies in Su and Ye, An and Yang, and Corradini and Cristofaro are passive in dealing with FDI attacks, having limited defensive ability, and thus, active defense strategies are more targeted than passive ones. In addition, the above studies only consider cyber attacks in a cyber system. It is well-known that CPS is a combination of physical and cyber systems. Therefore, finding approaches to adopt more active defense strategies to ensure the security of a nonlinear CPS under physical faults and cyber attacks is another research motivation of this study.

In a CPS, the rapidly increasing data generated by its intelligent devices need to be transmitted with limited bandwidth; thus, the inconsistency between the transmission of a large amount of data and the limited communication resources is becoming increasingly important. In the traditional periodic time-triggered communication scheme (PTTCS), the transmission of a large amount of redundant data aggravates the communication burden, and the control strategy design is inappropriately related with the communication. Over the past decade, to solve these problems, a self-triggered communication scheme (STCS), a discrete event-triggered communication scheme (DETCs), and an adaptive event-triggered communication scheme (AETCS) have been proposed. Among them, the AETCS is novel, and its trigger parameter can change adaptively with respect to the dynamic error of a system. However, once the physical and cyber systems in a CPS are damaged, it is difficult to realize the adaptive coordinates between communication and control under the AETCS. Because the DETCS is simple to implement and can achieve good control performance, it is the most representative trigger scheme. In Lu and Yang, based on the DETCS, a new security observer was designed to estimate a state and an attack. In Li et al., the security consensus problem was considered for multi-agent systems, and an event-triggered control scheme with state dependence was used to update the control input signal. In Gao et al., an event-triggered dynamic output feedback control problem was studied for a discrete Markov jump system, and a dual-event-triggered scheme was implemented asynchronously on the node of a sensor and a controller. The above studies were based on the DETCS, which can effectively save network resources. However, there are few results on the co-design of dual security control and communication for a nonlinear CPS. This is another motivation of this study.

Based on previous investigations, in this study, we aim to co-design dual security control and communication for a nonlinear CPS under the DETCS. The main contributions are summarized as follows:

1. A new dual security control strategy with active fault-tolerance and active-passive attack-tolerance is proposed, in which an actuator fault and an actuator FDI attack are compensated actively and a sensor FDI attack is defended passively. Furthermore, a dual security control framework is built, which lays the foundation to realize dual security control for an actual CPS with FDI attacks on the dual-end network and an actuator fault.

2. A robust augmented observer is obtained to accurately estimate the system state, FDI attacks, and actuator fault in real time using the augmented matrix method.

3. A new T–S fuzzy model of a closed-loop nonlinear CPS is established under the DETCS, which integrates a trigger condition, FDI attacks, and an actuator fault. Subsequently, a co-design method of dual security control and communication with reduced data transmission is established to achieve a balance between dual security control and communication resources.

4. In the derivation of the robust augmented observer and the dual security controller, an appropriate Lyapunov–Krasovskii function is constructed and the affine Bessel–Legendre inequality is introduced, thereby reducing the conservatism of the
The control unit calculates the control quantity with active fault-tolerance and active-passive attack-tolerance on the received data, following which the control data are transmitted to the execution unit. It can be seen that the control action is still conducted in a non-uniform periodic manner.

The execution unit includes a zero-order holder (ZOH) and an actuator. The ZOH holds the data in a non-uniform periodic manner, and it transmits the result to the actuator, which acts on the controlled plant.

**Assumption 1:** The sampling is conducted at equal periods $h$; the intelligent sensing unit is clock-driven, and the corresponding sequence is $\{i_k\}, k = 0, 1, 2, \cdots$. Both the control and execution units are event-driven. The sending period of the filtered data by the event generator is denoted as $h_0$, and the corresponding sequence is $\{i_k\}, k = 0, 1, 2, \cdots$.

**Assumption 2:** FDI attacks are detectable and separable from physical faults.

**System description**

As shown in Figure 1, the plant is continuous, and the operation of the intelligent sensing and control units is completed by the calculation of a digital quantity; therefore, the system is a typical sampling data system. Considering a class of nonlinear controlled plants, the following state equation of the fuzzy system can be obtained by adopting the T–S fuzzy model:

$$
\begin{align*}
\dot{x}(t) &= \sum_{i=1}^{N} \xi_i(\theta(t))\left[ A_i x(t) + B_i [w(t) + a^i(t)] + E_{fi}(t) \right] \\
y(i_k) &= \sum_{i=1}^{N} \xi_i(\theta(t))\left[ C_i [x(i_k) + a^i(i_k)] + E_{ui}(i_k) \right]
\end{align*}
$$

where $\xi_i(\theta(t)) = a_i(\theta(t))/\sum_{i=1}^{N} a_i(\theta(t))$, $\xi_i(\theta(t))$ represents the weight ratio of each fuzzy rule, $a_i(\theta(t)) = \prod_{j=1}^{N} M_{ij}(\theta(t))$, and $M_{ij}(\theta(t))$ is the membership function of $\theta_j(t)$ with respect to $M_{ij}$. It is assumed that $a_i(\theta(t)) > 0 (i = 1, 2, \cdots, N)$ and $\sum_{i=1}^{N} a_i(\theta(t)) > 0$; therefore $\xi_i(\theta(t)) > 0$ and $\sum_{i=1}^{N} \xi_i(\theta(t)) = 1$. $A_i, B_i, C_i, E_{fi}, E_{ui},$ and $E_d$ are known matrices with appropriate dimensions. $x(t) \in \mathbb{R}^n$ is the system state, $u(t) \in \mathbb{R}^{n_u}$ is the control input (without the sensor FDI attack), $w(t) \in \mathbb{R}^{n_w}$ is the disturbance, $y(i_k) \in \mathbb{R}^m$ is the sampled output at instant $i_k$, $n(i_k) \in \mathbb{R}^{n_s}$ is the measurement noise, and $a^i(t) \in \mathbb{R}^{n_s}$ and $a^i(i_k) \in \mathbb{R}^{n_s}$ are the FDI attacks on the double-end network called actuator.
FDI attack and sensor FDI attack, respectively. \{f_i, f_2, \ldots, f_k, \ldots\} is the sampling time sequence and \(f(t) \in \mathbb{R}^p\) is a time-varying actuator fault. The derivative norms of \(f(t)\) and \(a^T(t)\) are bounded, that is, there are constants \(f_1\) and \(a_1\) that satisfy \(||f(t)|| \leq f_1\) and \(||a^T(t)|| \leq a_1||.

**Remark 1:** In real systems, actuator fault occurs in physical devices and FDI attack comes from information networks. Although there are essential differences between real physical devices and FDI attack comes from information networks, there may be essential differences between physical devices and FDI attack comes from information networks. Although there are essential differences between real physical devices and FDI attack comes from information networks.

**Remark 2:** The actuator fault changes the control actions of the system, whereas the sensor FDI attack modifies the measurements of the sensor. They are modeled in equation (1) based on different exerting locations and influences.

To detect and estimate the FDI attacks and the system state, \(x(t)\), actuator FDI attack \(\tilde{a}(t)\), and sensor FDI attack \(\hat{a}^T(t)\) are augmented into a new state \(\eta(t)\). Thus, the following augmented state equation can be obtained:

\[
\eta(t) = \begin{bmatrix} \xi_i(\theta(t)) [\hat{A}_i \eta(t) + \tilde{B}_i \mu(t) + \tilde{E}_i f(t) + \tilde{E}_a \bar{v}(t)] \\ y(t_i) = \sum_{i=1}^{r} \xi_i(\theta(t)) [\tilde{C}_i \eta(t_i) + E_{i v} v(t_i)] \end{bmatrix}
\]

where,

\[
\eta(t) = \begin{bmatrix} x^T(t) \\ \tilde{a}^T(t) \end{bmatrix}, \tilde{E}_a = \text{diag} \{ E_{1 v} \ 1 \ 1 \}, \tilde{C}_i = [C_i \ 0 \ C_i].
\]

\[
\tilde{A}_i = \begin{bmatrix} A_i & B_i & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \tilde{B}_i = \begin{bmatrix} B_i \\ 0 \\ 0 \end{bmatrix}, \tilde{E}_i = \begin{bmatrix} E_{fi} \\ 0 \\ 0 \end{bmatrix}.
\]

**Trigger condition of DETCS**

In this study, we adopt the typical DETCS in Peng and Yang\(^{26}\) to determine whether the current sampling value needs to be transmitted.

\[
[x^T(t) - \hat{x}^T(t)] \Phi [x^T(t) - \hat{x}^T(t)] \leq \sigma \hat{x}^T(t) \Phi \hat{x}(t)
\]

where \(\sigma \in [0,1]\) is a predefined event trigger parameter that is related to the expected system performance. \(\Phi\) is the positive definite symmetric matrix to be designed.

The state estimation error is defined as \(\tilde{x}(t_k) - \hat{x}(t_k) = e(t_k)\), where \(\tilde{x}(t_k)\) represents the estimated state value by the observer. \(\hat{x}(t_k)\) represents the latest state estimation value, which is calculated by the event generator at the last moment and meets the trigger condition in equation (3), and is transmitted through the network.

**Analysis of correlated delay interval**

From the above analysis, the estimation of the observer has an equal sampling period, whereas the fault-tolerant/attack-tolerant control is associated with a non-uniform sampling period. Therefore, we treat them as sampling data systems, and subsequently adopt the time-delay theory to deal with these problems.\(^{36,37}\) Similar to the related delay analysis in Li et al.,\(^{38}\) it will not elaborate here.

The time delay function is defined as

\[
\tau_1(t) = t - n(t), 0 \leq \tau_1(t) \leq h_1 = h.
\]

where \(h\) is the sampling period.

\[
\tau_2(t) = t - n(t).
\]

The upper and lower bounds of the time delay function can be described as follows:

\[
0 < h_1 + \tau_1 + h_2 \leq \tau_2(t) \leq (h_1 + 1)h + \tau_1 + (h_1 + 1)h \\
\leq (d_k + 1)h + \tau_1 + (d_k + 1)h = (d_k + 1)h + \tau_1 + (d_k + 1)h \\
\leq h_{max} + \tau' = h_{max} + \tau' = h_{max} + \tau' = h_{max} + \tau'.
\]

\[\tau_1 + h_{max} = \tau_2(t)\] is the network transmission delay at instant \(n_k + 1\), \(h_2\) is the network transmission delay at instant \(n_k + 1\), \(h_{max}\) is the maximum transmission period filtered by the event generator, and \(\tau'\) is the upper bound of \(\tau_1 + (d_k + 1)h\).

**Design of robust \(H_\infty\) observer for estimation of state, FDI attacks, and actuator fault**

**Augmented error system**

The time delay theory is adopted to analyze the sampling characteristics of the system output in one sampling period; the discrete sampling output equation is held through the ZOH,\(^{39}\) and the measurement output can be obtained as follows:

\[
y(t) = \sum_{i=1}^{r} \xi_i(\theta(t)) [\tilde{C}_i \eta(t - \tau_1(t)) + E_{i v} v(t - \tau_1(t))]
\]

The following observer is constructed to observe the system state, FDI attacks, and the actuator fault:
tem can be obtained as follows: 
Using the augmented matrix method, an augmented observer is obtained in equation (7), which 

The following are defined: \( e_n(t) = \tilde{y}(t) - y(t) \), \( e_s(t) = \tilde{y}(t) - y(t) \), and \( e_f(t) = \tilde{f}(t) - f(t) \). The error system can be obtained as follows:

\[
\begin{align*}
\dot{e}_n(t) &= \sum_{i=1}^{r} \sum_{j=1}^{r} \xi_i(\theta(t)) \xi_j(\theta(t)) \left[ A \tilde{e}_n(t) + \tilde{E}_f e_f(t) \right] \\
&\quad - L_f \tilde{C} e_n(i_k) + L_f E_v (i_k) - \tilde{E}_w \bar{v}(t) \\
\dot{e}_s(t) &= \dot{\tilde{y}}(t) - \tilde{f}(t) + \sum_{j=1}^{r} \xi_j(\theta(t)) [\tilde{C} e_n(i_k) - E_v i(i_k)] \\
&\quad + F \tilde{E}_v (i_k) \\
\dot{e}_f(t) &= \sum_{i=1}^{r} \xi_i(\theta(t)) \left[ \tilde{C} e_n(i_k) - E_v i(i_k) \right]
\end{align*}
\]

Thus, the augmented error system with the system state, FDI attacks, and actuator fault is as follows:

\[
\begin{align*}
\dot{\tilde{e}}(t) &= \sum_{i=1}^{r} \sum_{j=1}^{r} \xi_i(\theta(t)) \xi_j(\theta(t)) \left[ \hat{A} \tilde{e}(t) - \tilde{L}_j \tilde{C} \tilde{e}(t - \tau_1(t)) \right] \\
&\quad - \tilde{E}_w \bar{v}(t) + \tilde{L}_j E_v i(t - \tau_1(t))
\end{align*}
\]

Where

\[
\hat{A}_i = \begin{bmatrix}
\hat{A}_i & \hat{E}_f \\
0 & 0
\end{bmatrix}, \quad \hat{e}(t) = \begin{bmatrix} e_n(t) \\ e_f(t) \end{bmatrix}, \quad \tilde{L}_j = \begin{bmatrix} L_j \\ F_j \end{bmatrix}, \\
\tilde{C}_i = \begin{bmatrix} \tilde{C}_i & 0 \end{bmatrix}.
\]

\[
\dot{\tilde{e}}(t - \tau_1(t)) = \begin{bmatrix} e_n(t - \tau_1(t)) \\ e_f(t - \tau_1(t)) \end{bmatrix}, \quad \tilde{E}_w = \begin{bmatrix} \tilde{E}_w \\ 0 \end{bmatrix}, \quad \bar{v}(t) = \begin{bmatrix} \bar{v}(t) \\ \tilde{f}(t) \end{bmatrix}.
\]

**Remark 3:** Using the augmented matrix method, an augmented observer is obtained in equation (7), which can observe the system state, the FDI attacks on the double-end network, and the actuator fault in real time.

**Design of robust \( H_\infty \) observer**

**Theorem 1:** Considering the error system in equation (9), for certain positive constants \( h_1 \) and \( \gamma_1 \), if there exist a symmetric positive definite matrix \( P \) and appropriate dimension matrices \( X, Y_j \) such that the following conditions hold:

\[
\begin{align*}
&\begin{bmatrix} \Pi_{11} & \Pi_{12} & \Pi_{13} & \Pi_{14} & 0 \\
* & \Pi_{22} & \Pi_{23} & \Pi_{24} & h_1 n_1 C_j^T Y_j^T \\
* & * & \Pi_{33} & \Pi_{34} & 0 \\
* & * & * & \Pi_{44} & 0 \\
* & * & * & * & -\gamma_1^2 I
\end{bmatrix} < 0 \quad (10)
\end{align*}
\]

\[
\begin{align*}
&\begin{bmatrix} \Pi_{11} + P & \Pi_{12} & \Pi_{13} & \Pi_{14} & X \\
* & \Pi_{22} & \Pi_{23} & \Pi_{24} & X \\
* & * & \Pi_{33} & \Pi_{34} & X \\
* & * & * & \Pi_{44} & X \\
* & * & * & * & -\gamma_1^2 I
\end{bmatrix} < 0 \quad (11)
\end{align*}
\]

\[
\begin{align*}
&\begin{bmatrix} \Pi_{11} + P & \Pi_{12} & \Pi_{13} & \Pi_{14} & Y_i E_i - P \tilde{E}_w \\
* & \Pi_{22} & \Pi_{23} & \Pi_{24} & 0 \\
* & * & \Pi_{33} & \Pi_{34} & 0 \\
* & * & * & \Pi_{44} & 0 \\
* & * & * & * & -\gamma_1^2 I
\end{bmatrix} < 0 \quad (12)
\end{align*}
\]

then the error system in equation (9) is asymptotically stable and satisfies the \( H_\infty \) performance index in equation (14). The augmented state observer gain matrix, \( L_j \), and the fault estimation gain matrix, \( F_j \), are obtained using \( \tilde{L}_j = \begin{bmatrix} L_j \\ F_j \end{bmatrix} \).

\[
\| \tilde{e}(t) \|^2 \leq \gamma_1^2 \left( \sum_{k=0}^{\infty} (i_k + 1 - i_k) \| v(i_k) \|^2 + \| \bar{v}(t) \|^2 \right) \quad (14)
\]
where

\[ \Pi_{11} = P \tilde{A}_i + \tilde{A}_i^T P - n_2 P + h_1n_2(P \tilde{A}_i + \tilde{A}_i^T P) \\
+ h_1n_2 \tilde{A}_i^T P \tilde{A}_i \\
- 3X - 3X^T, \Pi_{13} = 2X - 3X^T, \Pi_{14} = 6X - 3X^T, \\
\Pi_{12} = - Y_i \tilde{C}_i + n_2 P - h_1n_1 \tilde{A}_i^T Y_i \tilde{C}_i - h_1n_2 Y_i \tilde{C}_i \\
- h_1n_2 \tilde{A}_i^T P + X \\
- 3X^T, \Pi_{15} = Y_i E_{ii} + h_1n_1 \tilde{A}_i^T Y_i E_{ii} + h_1n_2 Y_i E_{ii}, \\
\Pi_{16} = - P \tilde{E}_{ii} - h_1n_1 \tilde{A}_i^T P \tilde{E}_{ii} - h_1n_2 P \tilde{E}_{ii}, \\
\Pi_{22} = - n_2 P + h_1n_2 P \\
+ h_1n_2(\tilde{Y}_i \tilde{C}_i + \tilde{C}_i^T \tilde{Y}_i^T) + X + X^T, \Omega_{23} = 2X + X^T, \\
\Pi_{24} = 6X + X^T, \Pi_{25} = - h_1n_1 \tilde{Y}_i E_{ii}, \\
\Pi_{26} = h_1n_1 \tilde{C}_i^T \tilde{Y}_i^T E_{ii} \\
+ h_1n_2 P \tilde{E}_{ii}, \Pi_{33} = 2X + 2X^T, \Pi_{34} = 6X + 2X^T, \Pi_{44} = \\
6X + 6X^T, \Pi_{66} = - \eta^T I + h_1n_1 \tilde{E}_{ii}^T P \tilde{E}_{ii}, \Pi_{11} = P \tilde{A}_i \\
+ \tilde{A}_i^T P - n_2 P - 3X - 3X^T, \Pi_{12} = - Y_i \tilde{C}_i + n_2 P \\
+ X - 3X^T, \Pi_{15} = 2X + X^T. \\
\]

**Proof:** To ensure the error system is asymptotically stable in equation (9), we first consider \( \dot{v}(t) = 0, v_i(t) = 0 \), and construct the Lyapunov–Krasovskii function as follows:

\[
V_1(t) = \tilde{e}^T(t)P \tilde{e}(t) + (h_1 - \tau(t)) \tilde{e}(t) \tilde{e}^T(t - \tau(t))Q \tilde{e}^T(t) + (h_1 - \tau(t)) \int_{t-\tau(t)}^t \tilde{e}^T(s) \tilde{R} \tilde{e}(s) ds \\
+ (h_1 - \tau(t)) \varphi_1(t) S \varphi_1(t) \\
\]

(15)

where \( \varphi_1(t) = \tilde{e}(t) - \tilde{e}(t_i) \) and \( P = P^T > 0, Q = Q^T > 0, R = R^T > 0, S = S^T > 0 \).

Differentiating along the trajectory of the system in equation (9), we obtain

\[
\dot{V}_1(t) = 2 \tilde{e}^T(t)P \dot{\tilde{e}}(t) + 2(h_1 - \tau(t)) \tilde{e}^T(t) - \tau(t))Q \tilde{e}(t) \\
- h_1 \tilde{e}^T(t - \tau(t))Q \tilde{e}(t - \tau(t)) + 2(h_1 - \tau(t)) \varphi_1(t) S \dot{\varphi}_1(t) \\
- \varphi_1^T(t) S \varphi_1(t) - \int_{t-\tau(t)}^t \tilde{e}^T(s) \tilde{R} \tilde{e}(s) ds \\
+ (h_1 - \tau(t)) \tilde{e}^T(t) \tilde{R} \tilde{e}(t) \\
\]

(16)

The integral term, \(- \int_{t-\tau(t)}^t \tilde{e}^T(s) \tilde{R} \tilde{e}(s) ds\), can be processed by the affine Bessel–Legendre inequality with reduced conservatism,\(^4\) that is,

\[
\int_{t-\tau(t)}^t \tilde{e}^T(s) \tilde{R} \tilde{e}(s) ds \leq - \psi_1^T(t) \Theta \psi_1(t) \\
\]

(17)

where

\[
\psi_1^T(t) = \left[ \tilde{e}^T(t), \tilde{e}^T(t_i), \frac{1}{\tau(t)} \Omega_0^T, \frac{1}{\tau(t)} \Omega_1^T \right]. \\
\Theta = XH_1 + H_2 X^T - \tau(t)XX^T, \Omega_0 = \int_{t-\tau(t)}^t \tilde{e}(s) ds, \\
\Omega_1 = \int_{t-\tau(t)}^t \left( \frac{s - t + \tau(t)}{\tau(t)} - 1 \right) \dot{e}(s) ds, \\
H_1 = \begin{bmatrix} 1 & -1 & 0 & 0 \\
1 & 1 & -2I & 0 \\
1 & -1 & 0 & -6I \end{bmatrix}, \\
R = \text{diag} \left\{ R^{-1} \frac{1}{3} R^{-1} \frac{1}{3} R^{-1} \right\}. \\
\]

Substituting the inequality in equation (17) into \( \dot{V}_1(t) \), we define

\[
M_{11} = [1 \ 0 \ 0 \ 0], M_{12} = [1 \ -I \ 0 \ 0], \]

\[
M_{13} = [\tilde{A}_i \ -L_{i} \tilde{C}_i \ 0 \ 0], M_{14} = [0 \ 1 \ 0 \ 0] \\
\]

Thus, \( \varphi_1(t) = M_{12} \psi_1(t), \dot{\psi}_1(t) = M_{13} \dot{\psi}_1(t), \tilde{e}(t) = M_{14} \dot{\psi}_1(t) \).

We can further obtain \( V_1(t) \leq \psi_1^T(t) \Sigma_{11} + (h_1 - \tau(t)) \Sigma_{12} + \tau(t) \Sigma_{13} \psi_1(t) \), where

\[
\Sigma_{11} = 2M_{11}^T P M_{13} - M_{12}^T S M_{12} - XH_2 - H_2^T X^T - h_1 M_{14}^T Q M_{14}, \\
\Sigma_{12} = 2M_{12}^T S M_{13} + M_{13}^T R M_{13} + 2M_{14}^T Q M_{14}, \\
\Sigma_{13} = XX^T. \\
\]

If \( \Sigma_{11} + (h_1 - \tau(t)) \Sigma_{12} + \tau(t) \Sigma_{13} < 0 \), then \( \dot{V}_1(t) < 0 \); therefore, the error system in equation (9) is asymptotically stable. According to the linear convex combination lemma in Park et al.,\(^4\) the necessary and sufficient conditions for \( \Sigma_{11} + (h_1 - \tau(t)) \Sigma_{12} + \tau(t) \Sigma_{13} < 0 \) are

\[
\Sigma_{11} + h_1 \Sigma_{12} < 0, \Sigma_{11} + h_1 \Sigma_{13} < 0 \\
\]

(18)

Under zero initial conditions, when \( \dot{w}(t) \neq 0, v_i(t) \neq 0 \), and considering the following \( H_1 \) performance index function:
we define

\[
\begin{align*}
\phi_{2}^{T}(t) &= \left[ \begin{array}{c}
\bar{e}^{T}(t) \\
\bar{e}^{T}(t-\tau_{1}(t)) \\
\bar{e}^{T}(t-\tau_{2}(t))
\end{array} \right], \\
M_{21} &= [1 0 0 0 0 0], \\
M_{22} &= [1 -1 0 0 0 0], \\
M_{23} &= [A_{i} -L_{j}C_{j} 0 0 L_{j}E_{\alpha i} -E_{\alpha i}], \\
M_{24} &= [0 1 0 0 0 0], \\
M_{25} &= [1 0 0 0 0 0], \\
M_{26} &= [0 1 0 0 0 0].
\end{align*}
\]

\(\Omega_{0}, \Omega_{1}\) are similar to (17); thus, \(\bar{e}(t) = M_{21}\phi_{2}(t)\),
\(\phi_{1}(t) = M_{22}\phi_{2}(t)\), \(\bar{e}(t-\tau_{1}(t)) = M_{23}\phi_{2}(t)\),
\(\phi_{1}(t) = M_{25}\phi_{2}(t), [v^{T}(t_{k}) \bar{w}^{T}(t)]^{T} = M_{26}\phi_{2}(t)\).

Furthermore, the following equation can be obtained:

\[
J_{1} = \phi_{2}^{T}(t)\Sigma_{21} + (h_{1} - \tau_{1}(t))\Sigma_{22} + \tau_{1}(t)\Sigma_{23}\phi_{2}(t) < 0
\]  
(20)

where

\[
\Sigma_{21} = 2M_{22}^{T}PM_{23} - h_{1}M_{22}^{T}QM_{24} - M_{22}^{T}SM_{22} - M_{22}^{T}(XH_{2} + H_{2}^{T}X^{T})M_{25} + M_{22}^{T}M_{21} - \gamma_{1}^{2}M_{26},
\]

\[
\Sigma_{22} = 2M_{22}^{T}SM_{23} + M_{23}^{T}RM_{23} + 2M_{24}^{T}QM_{24},
\]

\[
\Sigma_{23} = M_{25}^{T}XRX^{T}M_{25}.
\]

It can be seen from the linear combination lemma that \(J_{1} < 0\) is equivalent to

\[
\Sigma_{21} + h_{1}\Sigma_{22} < 0, \Sigma_{21} + h_{1}\Sigma_{23} < 0
\]  
(21)

Because the inequalities in equations (18) and (21) are nonlinear, let \(R = n_{1}P, S = n_{2}P, Q = n_{3}P, Y_{1} = PL_{j}\); thus, the nonlinear matrix inequalities can be converted into linear matrix inequalities by applying the Schur complement lemma. Furthermore, the inequalities in equations (10)–(13) can be obtained using the Linear matrix inequality (LMI) toolbox. Among them, parameters \(L_{j}, F_{j}\) can be designed by solving \(\bar{L}_{j} = P^{-1}Y_{j}\).

Integrating equation (19) from 0 to \(+\infty\), we obtain

\[
V_{j}(+\infty) - V_{j}(0) \leq - \int_{0}^{+\infty} \bar{e}^{T}(s)\bar{e}(s)ds + \gamma_{1}^{2}\]

\[
\int_{0}^{+\infty} \bar{w}^{T}(s)\bar{w}(s)ds
\]

\[
+ \gamma_{1}^{2} \sum_{k=0}^{+\infty} [(t_{k+1} - t_{k})v^{T}(t_{k})v(t_{k})],
\]

where \(\bar{w}(t) \in L_{2}[0, +\infty), v(t_{k}) \in L_{2}[0, +\infty],\) and \(V_{j}(0) = 0, V_{j}(+\infty) \geq 0\).

Thus, \(\|\bar{e}(t)\|_{2}^{2} \leq \gamma_{1}^{2}\sum_{k=0}^{+\infty} [(t_{k+1} - t_{k})v^{T}(t_{k})v(t_{k})]^{1/2} + \|\bar{w}(t)\|_{2}^{2}\)

is true. Consequently, the relevant \(H_{\infty}\) performance index is verified.

Remark 4: When dealing with the integral term, the affine Bessel-Legendre inequality is used in the paper, which reduces the conservativeness of the final result and increases the solution space, resulting in improved system performance and enhanced defense against actuator fault and FDI attacks.

**Co-design of robust \(H_{\infty}\) dual security control and communication**

The control input can be updated to apply the following equation:

\[
u(t) = \sum_{j=1}^{r} \sum_{i=1}^{r} \xi_{i}(\theta(t))\xi_{j}(\theta(t)) \left[ K_{ij}\bar{x}(t_{k}) - B_{ij}^{*}E_{\beta j}\bar{f}(t_{k}) \right]
\]

(22)

where \(t \in [t_{k}, t_{k+1}]\) and \(\{t_{1}, t_{2}, \cdots, t_{k}, \cdots\}\) is a sequence of the transmitted data in the event generator backend. \(\bar{x}(t_{k}), \bar{f}(t_{k})\), and \(\bar{a}^{\alpha}(t_{k})\) are the estimation of the system state, actuator fault, and actuator FDI attack, respectively, which are estimated by the observer. \(K_{ij} \in R^{m \times n}\) is the designed controller gain matrix. \(B_{ij}^{*} \in R^{n \times n}\) is the fault adjustment matrix, and it satisfies \((I - B_{ij}^{*})E_{\beta j} = 0, \text{rank}(B_{ij}^{*}E_{\beta j}) = \text{rank}(B_{ij})\).

Remark 5. For the actuator fault, an active fault-tolerant control strategy is adopted. For the FDI attacks on the double-end network, different countermeasures are adopted according to their different exerting locations. Specifically, the actuator FDI attack is defended by active compensation, and the sensor FDI attack is passively defended to robustly deal with it by dynamic output feedback control. The combination of
active and passive can be called as active-passive attack-tolerant control.

Substituting the control input in equation (22) into the controlled plant model in equation (1), the closed-loop nonlinear CPS model with the actuator fault and the FDI attacks can be obtained as follows:

\[
\begin{aligned}
\dot{x}(t) &= \sum_{i=1}^{r} \sum_{j=1}^{r} \xi(\theta(t))\xi(\theta(t))\left(A_i x(t) + B_i K_i \dot{x}(t_k)\right) \\
&\quad - B_i^* E_i \tilde{f}(t_k) - B_i^* B_i \tilde{d}(t_k) + B_i \eta(t) + E_i \omega(t) + E_i \nu(t) \\
\dot{y}(t_k) &= \sum_{i=1}^{r} \xi(\theta(t))\left(C_i x(t_k) + \alpha_i(t_k) + E_i \nu(t_k)\right)
\end{aligned}
\]

Furthermore, equation (23) can be written as follows:

\[
\begin{aligned}
\dot{x}(t) &= \sum_{i=1}^{r} \sum_{j=1}^{r} \xi(\theta(t))\xi(\theta(t))\left(A_i x(t) + B_i K_i x(t - \tau_2(t))\right) \\
&\quad + B_i K_i \tau_2(t) - \tau_2(t) E_i \dot{f}(t) + \tau_2(t) E_i \nu(t) - B_i \dot{d}(t) + \tau_2(t) B_i \dot{d}(t) + E_i \omega(t) + E_i \nu(t) \\
\dot{y}(t_k) &= \sum_{i=1}^{r} \xi(\theta(t))\left(C_i x(t_k) + \alpha_i(t_k) + E_i \nu(t_k)\right)
\end{aligned}
\]

(23)

**Remark 6:** Theorem 1 ensures that estimation errors \(e_c(t - \tau_2(t)), e_f(t - \tau_2(t)), e_{\omega}(t - \tau_2(t))\) are asymptotically convergent for the system state, actuator fault, and actuator FDI attack, whereas \(\tau_2(t) E_i \dot{f}(t)\) and \(\tau_2(t) B_i \dot{d}(t)\) are norm-bounded; therefore, they can be treated as external disturbances. In addition, the sensor FDI attack is considered as a special type of disturbance to be tolerated passively in a robust manner.

**Remark 7:** In the design of the controller, we consider the dual security control for the actuator fault and the FDI attacks, and it is insensitive to various types of disturbances. In fact, it is a robust controller with active fault-tolerance and active-passive attack-tolerance; therefore, it can be referred to as a dual security controller.

**Design goals**

Under the DETCS, for the nonlinear CPS with the actuator fault and the FDI attacks, the co-design goals of fault-tolerance and attack-tolerance and communication are as follows:

1. In the case of no attack and disturbance, we cooperatively obtain security control matrix \(K_i\) and event trigger matrix \(\Phi\), such that the closed-loop nonlinear CPS in equation (24) is asymptotically stable;

\[
\begin{aligned}
\Psi_{11} &\quad \Psi_{12} &\quad \Psi_{13} &\quad \Psi_{14} &\quad 0 &\quad 0 &\quad \begin{bmatrix} h_{22} & K_{1j}^T \end{bmatrix} < 0 &\quad (25) \\
\odot &\quad * &\quad \Sigma_{22} &\quad \Sigma_{23} &\quad \Sigma_{24} &\quad \Sigma_{25} &\quad \begin{bmatrix} \sum_{i=1}^{n} a_i \end{bmatrix} &\quad < 0 &\quad (26) \\
\odot &\quad * &\quad * &\quad * &\quad \Sigma_{33} &\quad \Sigma_{34} &\quad X &\quad 0 &\quad \begin{bmatrix} \sum_{i=1}^{n} a_i \end{bmatrix} &\quad \begin{bmatrix} h_{22} & K_{26} \end{bmatrix} &\quad < 0 &\quad (27) \\
\odot &\quad * &\quad * &\quad * &\quad * &\quad * &\quad \Sigma_{44} &\quad X &\quad 0 &\quad \begin{bmatrix} \sum_{i=1}^{n} a_i \end{bmatrix} &\quad \begin{bmatrix} h_{22} & K_{26} \end{bmatrix} &\quad < 0 &\quad (28)
\end{aligned}
\]

Theorem 2 Under the DETCS, for certain positive constants \(h_2, \sigma, \gamma_2, n_1, n_2, n_3, m_1, m_2, m_3, m_4, m_5, m_6, \) and \(\sigma \in [0, 1]\), for the system with time-varying actuator fault \(f(t)\) and FDI attacks \(d(t), d(i_k)\) in equation (24), if there exist symmetric positive definite matrix \(P\) and appropriate dimension matrices \(X, K, Q, L, Q, L, Q, L, Q, L, Q, L, Q, L\), such that the following conditions hold:
\[
\begin{align*}
\begin{bmatrix} Q_2 & E_{1}^{T}P' \\ * & m_1P' \end{bmatrix} > 0, & \quad \begin{bmatrix} Q_4 & n_1E_{1}^{T}P' \\ * & m_2P' \end{bmatrix} > 0, & \quad \begin{bmatrix} Q_6 & n_2E_{1}^{T}P' \\ * & m_3P' \end{bmatrix} > 0, \\
\begin{bmatrix} Q_2 & B_{1}^{T}P' \\ * & m_1P' \end{bmatrix} > 0, & \quad \begin{bmatrix} Q_4 & n_1B_{1}^{T}P' \\ * & m_2P' \end{bmatrix} > 0, & \quad \begin{bmatrix} Q_6 & n_2B_{1}^{T}P' \\ * & m_3P' \end{bmatrix} > 0.
\end{align*}
\]

(29)

then the system in equation (24) is asymptotically stable, and it meets the \( H_\infty \) performance index in equation (30). Dual security controller gain \( K_i = (P'B_i)^{-1}K_{ij} \) and event trigger matrix \( \Phi \) can be obtained cooperatively.

\[
\begin{align*}
\|x(t)\|_2^2 & \leq \gamma^2 \left[ \|w(t)\|_2^2 + \sum_{k=0}^{\infty} (t_{k+1} - t_k) \left( \|e_q(t_k)\|_2^2 + \|e_p(t_k)\|_2^2 \right) \right] \\
\|e_p(t_k)\|_2^2 & + \|e_q(t_k)\|_2^2
\end{align*}
\]

(30)

where \( \Xi_{11} = P'A_i + A_i^TP' - n_1P' \)

\[
= \frac{h_2^2}{4}(m_2 + m_3)P' - 3X',
\]

\( \Xi_{13} = 2X' - 3X'T, \)

\( \Xi_{14} = 6X' - 3X'T, \)

\( \Xi_{21} = 2X' + X'T, \)

\( \Xi_{23} = 6X' + X'T, \)

\( \Xi_{22} = -n_1P' + h_2n_3P' + \frac{h_2^2}{4}(m_2 + m_3)P' + X' + X'T, \)

\( \Xi_{55} = \frac{h_2^2}{4}(m_3 + m_6)P', \)

\( \Psi_{11} = \Xi_{11} + h_2n_1 \)

\( (P'A_i + A_i^TP') + h_2n_2A_i^TP'A_i, \)

\( \Psi_{12} = \Xi_{12} + h_2n_1K_{ij} - h_2n_1A_i^TP' + h_2n_2A_i^TK_{ij}, \)

\( \Xi_{44} = 6X' + 6X^T, \)

\( \Psi_{11}' = \Psi_{11} + I, \)

\( \Psi_{12}' = \Psi_{12}, \)

\( \Xi_{13}' = \Xi_{13}, \)

\( \Xi_{14}' = \Xi_{14}, \)

\( \Psi_{11}' = \Xi_{11} + h_2(m_1 + m_4)P', \)

\( \Psi_{22}' = \Xi_{22} - h_2n_1(K_{ij} + K_{ij}^T), \)

\( \Xi_{35} = \frac{h_2^2}{4}(m_3 + m_6)K_{ij}^T, \)

\( \Xi_{33} = 2X' + 2X^T, \)

\( \Xi_{34} = 6X' + 2X^T, \)

\( \Psi_{26}' = \frac{h_2^2}{4}(m_3 + m_6)K_{ij}^T, \)

\( \Psi_{66}' = -\frac{h_2^2}{4}(m_3 + m_6)P', \)

\( \Psi_{55}' = \Xi_{55}' + h_2n_2A_i^TK_{ij} + h_2n_1K_{ij}, \)

\( \Psi_{25}' = \Xi_{25} - \Xi_{22}, \)

\( \Psi_{53}' = \Xi_{53}, \)

\( \Psi_{35}' = \Xi_{35}, \)

\( \Psi_{36}' = \Xi_{36} + h_2n_1P'E_{fi}, \)

\( \Psi_{26}' = \Xi_{26} - h_2n_2A_i^TP'B_i - h_2n_1P'B_i, \)

\( \Psi_{44}' = \Xi_{44}, \)

\( \Psi_{55}' = \Xi_{55}, \)

\( \Psi_{56}' = \Xi_{56} - h_2n_2K_{ij}^TE_{fi}, \)

\( \Psi_{35}' = \Xi_{35}, \)

\( \Psi_{56}' = \Xi_{56}, \)

\( \Psi_{58}' = \Xi_{58} + h_2n_2K_{ij}^TE_{sei}, \)

\( \Psi_{38}' = \Xi_{38}, \)

\( \Psi_{58}' = \Xi_{58} - h_2n_2E_{fi}'P'B_i, \)

\( \Psi_{46}' = \Xi_{46} + h_2n_1P'E_{fi}, \)

\( \Psi_{78}' = \Xi_{78}, \)

\( \Psi_{78}' = \Xi_{78}, \)

\( \Psi_{88}' = \Xi_{88} + h_2n_2E_{sei}'P''E_{sei}, \)

\( \Xi_{311} = \Xi_{311} + \Xi_{312} = \Xi_{312} - h_2n_2K_{ij}^T, \)

\( \Psi_{11}' = \Xi_{11} + I, \)

\( \Psi_{12}' = \Xi_{12}, \)

\( \Xi_{13}' = \Xi_{13}, \)

\( \Xi_{14}' = \Xi_{14}, \)

\( \Psi_{12}' = \Xi_{12}, \)

\( \Xi_{13}' = \Xi_{13}, \)

\( \Xi_{14}' = \Xi_{14}, \)

\( \Psi_{15}' = K_{ij} + \frac{h_2^2}{4}(m_3 + m_6)A_i^TK_{ij}, \)

\( \Psi_{68}' = -P'E_{fi}' - \)

\( \frac{h_2^2}{4}(m_3 + m_6)A_i^TP'B_i - P'B_i, \)
In the simulation, \( x_i (i = 1, 2, 3, 4) \) represents the water level variations of the Nth tank and \( y_i \) denotes the observation of the variation. The tank is supplied by two pumps, and \( u_1 \) and \( u_2 \) are the voltages applied to them, respectively. The disturbance, \( w(t) \), and the noise, \( v(i) \), are the independent white noise processes that obey \( N(0, 1, 0.01) \). The initial state is \( x(0) = [4 \ 4 \ 2 \ 2]^T \), and the sampling period is \( h_1 = 0.1s \).

The fuzzy membership function is assumed to be

\[ M_1(x_4) = \sin^2 x_4, \quad M_2(x_4) = \cos^2 x_4, \quad M_3(x_4) = \sin^2 x_4, \quad M_4(x_4) = \cos^2 x_4, \]

and the nonlinear system is expressed as a T-S fuzzy system with four rules.

\[ \begin{align*}
\dot{x}(t) &= A_1x(t) + B_1w(t) + E_0f(t) + E_1w(t) \\
y(i) &= C_1x(i) + E_2w(i)
\end{align*} \]

Rule 1: if \( x_i \) is \( M_i \), \( i = 1, 2, 3, 4 \), then

\[ A_1 = \begin{bmatrix} -0.016 & 0 & 0.42 & 0 \\ 0 & -0.011 & 0 & 0.33 \\ 0 & 0 & -0.042 & 0 \\ 0 & 0 & 0 & -0.33 \end{bmatrix}, \]

\[ B_1 = \begin{bmatrix} 0.083 \\ 0 \\ 0.031 \end{bmatrix}, \]

\[ C_1 = \begin{bmatrix} 0.1246 \\ 0 \\ 0.045 \end{bmatrix}, \]

\[ E_0 = \begin{bmatrix} 0.165 \\ 0 \\ 0.063 \end{bmatrix}, \]

\[ E_1 = \begin{bmatrix} 0.016 \\ 0.016 \\ 0.016 \end{bmatrix}, \]

\[ E_2 = \begin{bmatrix} 0.2076 \\ 0.1576 \\ 0.0776 \end{bmatrix}, \]

\[ E_3 = \begin{bmatrix} 0.02 \\ 0.02 \\ 0.02 \end{bmatrix}. \]
\[
E_{a1} = \begin{bmatrix} 0.024 \\ 0.024 \\ 0.024 \\ 0.024 \end{bmatrix}, \quad E_{a2} = -[0.083 \ 0 \ 0 \ 0.031]^T, \\
E_{a3} = -[0.1246 \ 0 \ 0 \ 0.0464]^T, \\
E_{a4} = -[0.167 \ 0 \ 0 \ 0.061]^T, \\
E_{a5} = -[0.2076 \ 0 \ 0 \ 0.0774]^T, \\
C_1 = \text{diag}\{0.5 \ 0.5 \ 0.5 \ 0.5\}, \quad C_2 = \text{diag}\{0.48 \ 0.48 \ 0.48 \ 0.48\}, \quad C_3 = \text{diag}\{0.46 \ 0.46 \ 0.46 \ 0.46\}, \quad C_4 = \text{diag}\{0.52 \ 0.52 \ 0.52 \ 0.52\}, \\
E_{d1} = [0.015 \ 0 \ 0.015 \ 0.015]^T, \\
E_{d2} = [0.0224 \ 0 \ 0.0224 \ 0.0224]^T, \\
E_{d3} = [0.030 \ 0 \ 0.025 \ 0.027]^T, \\
E_{d4} = [0.0374 \ 0 \ 0.031 \ 0.0326]^T, \\
L_1 = \begin{bmatrix} 2.8710 & 0.5154 & -0.2426 & 0.5969 \\ 0.3479 & 2.7649 & 0.7053 & -0.1668 \\ -0.0821 & 1.6116 & 0.6325 & -0.0629 \\ 0.8670 & 0.4102 & -0.2061 & 0.7224 \\ 0.8554 & 0.0738 & -0.1027 & 1.2795 \\ -0.0622 & 3.2076 & 1.7437 & -0.1811 \\ 0.2302 & -0.4159 & 0.2273 & -0.4186 \\ -0.3291 & 0.3666 & -0.6108 & 0.1823 \\ 0.0791 & -1.5287 & 2.3747 & 0.0560 \\ -0.8352 & -0.3990 & 0.1995 & 2.2851 \end{bmatrix}, \\
L_2 = \begin{bmatrix} 2.8823 & 0.4989 & -0.2577 & 0.6072 \\ 0.3646 & 2.8056 & 0.7348 & -0.1610 \\ -0.0628 & 1.6379 & 0.6538 & -0.0688 \\ 0.8362 & 0.4206 & -0.2103 & 0.7527 \\ 0.8651 & 0.0759 & -0.1099 & 1.2083 \\ -0.0427 & 3.2158 & 1.7477 & -0.1883 \\ 0.2365 & -0.4073 & 0.2235 & -0.4034 \\ -0.3437 & 0.4649 & -0.6309 & 0.1786 \\ 0.0598 & -1.5451 & 2.4820 & 0.0593 \\ -0.8049 & -0.4076 & 0.1996 & 2.3784 \end{bmatrix}, \\
L_3 = \begin{bmatrix} 2.4360 & 0.4444 & -0.1796 & 0.5654 \\ 0.2824 & 2.3767 & 0.5576 & -0.1256 \\ -0.0585 & 1.3831 & 0.5124 & -0.0588 \\ 0.6865 & 0.3584 & -0.1464 & 0.6607 \\ 0.7270 & 0.0553 & -0.0958 & 1.0525 \\ -0.0426 & 2.6693 & 1.3866 & -0.1620 \\ 0.2097 & -0.3514 & 0.1865 & -0.3711 \\ -0.2683 & 0.4371 & -0.0139 & 0.1432 \\ 0.0651 & -1.3403 & 2.2300 & 0.0466 \\ -0.6698 & -0.3475 & 0.1351 & 2.0881 \end{bmatrix}, \\
L_4 = \begin{bmatrix} 2.6355 & 0.4829 & -0.2241 & 0.5439 \\ 0.3320 & 2.6460 & 0.6552 & -0.1770 \\ -0.0924 & 1.5548 & 0.5863 & -0.0603 \\ 0.8471 & 0.3874 & -0.1849 & 0.6825 \\ 0.7107 & 0.1025 & -0.1288 & 1.3247 \\ -0.0696 & 3.1329 & 1.7009 & -0.1940 \\ 0.1856 & -0.4020 & 0.2143 & -0.3981 \\ -0.3127 & 0.2842 & -0.5992 & 0.1661 \\ 0.9434 & -1.5113 & 2.2896 & 0.0464 \\ -0.8176 & -0.3989 & 0.1762 & 2.1892 \end{bmatrix}, \\
F_1 = \begin{bmatrix} -1.2716 & -0.6144 & 0.2420 & -1.5065 \end{bmatrix}, \quad F_2 = \begin{bmatrix} -1.1902 & -0.6781 & 0.2930 & -1.5697 \end{bmatrix}, \\
F_3 = \begin{bmatrix} -1.1059 & -0.6915 & 0.3017 & -1.6578 \end{bmatrix}, \quad F_4 = \begin{bmatrix} -0.8862 & -0.5902 & 0.2100 & -1.3947 \end{bmatrix}, \\
K_1 = \begin{bmatrix} 0.5009 & 0.2171 & -0.1319 & 2.5949 \\ 0.1105 & 0.3758 & 2.0049 & -0.1598 \end{bmatrix}, \\
K_2 = \begin{bmatrix} 0.6119 & 0.2112 & -0.1395 & 2.7603 \\ 0.0992 & 0.3786 & 2.0347 & -0.1979 \end{bmatrix}, \\
K_3 = \begin{bmatrix} 0.4413 & 0.2260 & -0.1040 & 2.5043 \\ 0.1238 & 0.3623 & 1.9801 & -0.1368 \end{bmatrix}, \\
K_4 = \begin{bmatrix} 0.5016 & 0.2386 & -0.0354 & 2.5823 \\ 0.1314 & 0.3052 & 1.8374 & -0.1476 \end{bmatrix}, \\
\Phi = \text{diag}\{0.2551 \ 0.2551 \ 0.2551 \ 0.2551\}
\]

Let \( n_1 = 0.01, m_2 = 0.5, n_3 = 0.01, \) and \( \gamma_1 = 7.3, \) then observer gain matrix \( L_j \) and fault estimation gain matrix \( F_j \) can be obtained by Theorem 1.

In Theorem 2, let \( n_1 = 6, m_2 = 0.01, n_3 = 0.2, \)
\( m_1 = m_2 = m_3 = m_4 = m_5 = m_6 = 0.01, \quad \delta = 0.001, \)
\( h_2 = 1.9, \gamma_1 = 5.2, \) the state feedback gain matrix, \( K_j, \)
and the event trigger weight matrix, \( \Phi, \) can be obtained cooperatively using Theorem 2.
Estimation of state, actuator fault, and FDI attacks

In the simulation, we consider the worst case in which the actuator fault and the FDI attacks occur simultaneously.

Suppose that the fault occurs in the first channel, then the time-varying fault of the system is as follows:

\[
f(t) = \begin{cases} 
0, & t \leq 100 \\
2 + 2 \sin 0.01\pi(t - 100), & 100 < t \leq 800 
\end{cases}
\]

For the actuator FDI attack, we assume that its first channel is constant at zero, and the second channel satisfies the following equation:

\[
a^a(t) = \begin{cases} 
0, & t \leq 100 \\
1 + \sin 0.01\pi(t - 100), & 100 < t \leq 800 
\end{cases}
\]

For the sensor FDI attack, we assume that each channel satisfies the following equation:

\[
a^s(t) = \begin{cases} 
0, & t \leq 100 \\
1 + \sin 0.01\pi(t - 100), & 100 < t \leq 800 
\end{cases}
\]

To observe the above system fault and FDI attacks more clearly, the estimations and corresponding errors of the fault and the actuator and sensor FDI attacks are respectively shown in Figures 2 to 9.

It can be seen from Figures 2 to 9 that the estimation errors of the fault, actuator FDI attack, sensor FDI attack, and state have a larger fluctuation at 100s when the FDI attacks and the actuator fault are exerted. The remaining time they are within the normal range. Among them, the fault estimation error does not exceed ±0.05, and the estimation error of the actuator FDI attack does not exceed ±0.1. The estimation error of the sensor FDI attack fluctuates between ±0.02, and the state estimation error fluctuates between ±0.01. These results show that the designed robust observer using the proposed method can timely and accurately estimate the state, FDI attacks, and actuator fault.

Analysis of impact of event-trigger parameters on CPS security and communication resource

To further analyze the influence of the trigger parameter on the CPS security and communication resources, the data transmission amount and the system security state under different trigger parameters are listed in Table 1.

where \( n \) is data transmission amount, \( \bar{n} \) is data transmission rate, and \( \bar{h} \) is average transmission period.

It can be seen that with the increase in trigger parameter \( \delta \), data transmission amount \( n \) is decreased and average transmission period \( \bar{h} \) is increased; however, the system becomes unstable when \( \delta = 0.0012 \). Therefore, although the increase in \( \delta \) reduces the amount of data transmission and the network resources are saved, it is
at the expense of system security. Therefore, it is significant to choose the appropriate trigger parameter $\delta$ to balance the relationship between system security and network resources. In this study, trigger parameter $\delta = 0.001$ is selected based on the trade-off between them.

**Comparison of different control methods**

In the following, the active–passive attack tolerance method proposed in this paper and the passive attack tolerance method in Li et al. [38] (to tolerate FDI attacks on double-end network passively and actuator fault actively) are adopted. The output responses with these different attack-tolerance methods are presented in Figure 10(a) and (b). In addition, the data transmission amounts are specified in Table 2.

It can be seen that the system output in Figure 10(a) remains stable after 400 s, whereas that in Figure 10(b) becomes divergent after 500 s, which suggests that the method proposed in this paper is more effective in defending FDI attacks than that proposed in Li et al. [38] Table 2 shows that the amount of data transmission is lesser by the method proposed in this paper than that by the other methods. This shows that the former method is also more effective in saving network communication resources than the latter.

The reason is that the method in Li et al. [38] regards FDI attacks on double-end network as types of special disturbances and suppresses them passively in a robust manner. The control strategy proposed in this paper is different; specifically, a highly targeted active compensation is made for the actuator FDI attack according to its estimation, and the passive attack tolerance method...

---

**Figure 5.** Estimation error of actuator FDI attack.

**Figure 7.** Estimation error of sensor FDI attack.

**Figure 6.** Sensor FDI attack and its estimation.

**Figure 8.** States and their estimations.
is used only for the sensor FDI attack. Therefore, for a highly serious FDI attack, in terms of both the defense ability and the saving of communication resources, the system performance with the method proposed in this paper is better than that by the other method.

Compared to the PTTCS, which needs to transmit 8000 data, the DETCS only transmits 652 data in Table 2, with transmitted data rate of 8.15% and an average transmission period of $\bar{h} = 1.227s$. This result further shows that the method proposed in this paper not only ensures excellent performance but also effectively saves the network communication resources and achieves a trade-off between dual security control and communication resource.

**Conclusion**

Based on the DETCS, this study investigated a co-design method of dual security control and communication for a nonlinear CPS with an actuator fault and FDI attacks. First, a dual security control framework with active fault-tolerance and active–passive attack-tolerance was built, and a T–S fuzzy model of a closed-loop CPS was established, which integrated a trigger condition, the actuator fault, and the FDI attacks. Second, by introducing the appropriate Lyapunov–Krasovskii function, time delay theory, affine Bessel–Legendre inequality, and LMI technique, a robust observer for the estimation of the state, FDI attacks, and fault as well as a dual security controller with active fault-tolerance and active–passive attack-tolerance were obtained. This consequently achieved the co-design goal of dual security control and communication. Finally, a simulation of a quadruple-tank was conducted. It showed that the method proposed in this paper can timely and accurately estimate the system state.

**Table 1.** Comparison of data transmission amount and system state under different trigger parameters.

| $\bar{\delta}$ | $\bar{n}$ | $\bar{n}$ (%) | $\bar{h}$ (s) | System state |
|---------------|---------|--------------|--------------|--------------|
| 0.006         | 716     | 8.95         | 1.117        | Stable       |
| 0.008         | 693     | 8.66         | 1.154        | Stable       |
| 0.001         | 652     | 8.15         | 1.227        | Stable       |
| 0.0012        | 639     | 7.99         | 1.252        | Unstable     |

**Table 2.** Comparison of data transmission amounts with different attack-tolerance methods.

| Methods                   | $\bar{n}$ | $\bar{n}$ (%) | $\bar{h}$ (s) |
|---------------------------|-----------|---------------|---------------|
| Passive attack tolerance  | 1564      | 19.5          | 0.5115        |
| Active-passive attack tolerance | 652     | 8.15          | 1.227         |

**Figure 9.** State estimation errors.

**Figure 10.** System output responses with different control methods: (a) system output response with active-passive attack-tolerant and (b) system output response with passive attack-tolerant.
state, actuator fault, and FDI attacks as well as tolerate the fault actively and the FDI attacks actively-passively, simultaneously saving the network communication resources effectively. The proposed results can also provide a theoretical basis for dual security design of a nonlinear CPS in practical engineering. Particularly when a system is subject to FDI attacks and actuator fault simultaneously, the active–passive attack tolerance strategy is expected to be an effective defense method.

However, this study deals with the FDI attack at the sensor-end passively, and the defense capability of passive attack-tolerance is very limited. Therefore, how to establish a more effective defense strategy to actively deal with FDI attacks on a double-ended network and further improve the CPS security defense capability will be investigated in the next research study.

**Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding**

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This study was financially supported by the National Natural Science of China (Grant Nos. 62163022, 61763027), Higher Innovation Education Capacity Improvement Project of Gansu in China (Grant No. 2019B-152), and Youth Science and Technology Fund of Gansu Province (Grant Nos. 21JR1RM339, 21JR7RM192).

**ORCID iD**

Li Zhao https://orcid.org/0000-0002-1261-1429

**References**

1. Zhang D, Wang QG, Feng G, et al. A survey on attack detection, estimation and control of industrial cyber-physical systems. *ISA Trans* 2021; 116: 1–16.
2. Kim K and Kumar PR. Cyber–physical systems: a perspective at the centennial. *Proc IEEE* 2012; 100(13): 1287–1308.
3. Colombo AW, Karnouskos S, Kaynak O, et al. Industrial cyber-physical systems: a backbone of the fourth industrial revolution. *IEEE Ind Electron Mag* 2017; 11(1): 6–16.
4. Aydos M, Vural Y and Tekerek A. Assessing risks and threats with layered approach to Internet of Things security. *Meas Control* 2019; 52(5–6): 338–353.
5. Wan Y, Long C, Deng R, et al. Distributed event-based control for thermostatically controlled loads under hybrid cyber attacks. *IEEE Trans Cybern* 2021; 51(11): 5314–5327.
6. Wolf M and Serpanos D. Safety and security in cyber-physical systems and internet-of-things systems. *Proc IEEE* 2018; 106(1): 9–20.
7. Dibaji SM, Pirani M, Flamholz DB, et al. A systems and control perspective of CPS security. *Annu Rev Control* 2019; 47: 394–411.

8. Ge H, Yue D, Xie X, et al. A unified modeling of multi-sources cyber-attacks with uncertainties for CPS security control. *J Franklin Inst* 2021; 358(1): 89–113.
9. Takagi T and Sugeno M. Fuzzy identification of systems and its applications to modeling and control. *IEEE Trans Syst Man Cybern* 1985; 15(1): 116–132.
10. Chaibi R, El Aiss H, El Hajjaji A, et al. Stability analysis and robust $\mathcal{H}\infty$ controller synthesis with derivatives of membership functions for T-S fuzzy systems with time-varying delay: input-output stability approach. *Int J Control Autom Syst* 2020; 18(7): 1872–1884.
11. Wang L and Lam HK. $\mathcal{H}\infty$ control for continuous-time Takagi-Sugeno fuzzy model by applying generalized Lyapunov function and introducing outer variables. *Automatica* 2021; 125: 109409.
12. Ge C, Shi Y, Park JH, et al. Robust $\mathcal{H}\infty$ stabilization for T-S fuzzy systems with time-varying delays and memory sampled-data control. *Appl Math Comput* 2019; 346: 500–512.
13. Liu T, Tian J, Wang JZ, et al. Integrated security threats and defense of cyber-physical systems. *Zidonghua Xuebao* 2019; 45(1): 5–24.
14. Mahmoud MS, Hamdan MM and Baroudi UA. Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges. *Neurocomputing* 2019; 338(21): 101–115.
15. Li YJ and Li W. Co-design between $\alpha/\mathcal{H}_\infty$ fault-tolerant control of networked control system and network communication. *J Jilin Univ (Eng Technol Ed)* 2016; 46(6): 2010–2020.
16. Lan J and Patton RJ. A new strategy for integration of fault estimation within fault-tolerant control. *Automatica* 2016; 69: 48–59.
17. Xu F, Tan J, Wang X, et al. Mixed active/passive robust fault detection and isolation using set-theoretic unknown input observers. *IEEE Trans Autom Sci Eng* 2018; 15(2): 863–871.
18. Zhao L and Li W. Co-design of dual security control and communication for nonlinear CPS under DoS attack. *IEEE Access* 2020; 8: 19271–19285.
19. Wang M, Liu Y and Xu B. Observer–based $\mathcal{H}_\infty$ control for cyber–physical systems encountering DoS jamming attacks: an attack-tolerant approach. *ISA Trans* 2020; 104: 1–14.
20. Ma Y, Che WW and Deng C. Dynamic event-triggered model-free adaptive control for nonlinear CPSs under aperiodic DoS attacks. *Inf Sci* 2022; 589: 790–801.
21. Li F and Tang Y. False data injection attack for cyber-physical systems with resource constraint. *IEEE Trans Cybern* 2020; 50(2): 729–738.
22. Zhang TY and Ye D. False data injection attacks with complete stealthiness in cyber–physical systems: a self-generated approach. *Automatica* 2020; 120: 109117.
23. Langner R. Stuxnet: dissecting a cyberwarfare weapon. *IEEE Secur Priv* 2011; 9(3): 49–51.
24. Su L and Ye D. Static output feedback control for discrete-time hidden Markov jump systems against deception attacks. *Int J Robust Nonlinear Control* 2019; 29(18): 6616–6637.
25. An L and Yang GH. Improved adaptive resilient control against sensor and actuator attacks. *Inf Sci* 2018; 423: 145–156.
26. Corradini ML and Cristofaro A. Robust detection and reconstruction of state and sensor attacks for cyber-
physical systems using sliding modes. *IET Control Theory Appl* 2017; 11(11): 1756–1766.

27. Anta A and Tabuada P. To sample or not to sample: self-triggered control for nonlinear systems. *IEEE Trans Automat Contr* 2010; 55(9): 2030–2042.

28. Peng C and Yang TC. Event-triggered communication and $H_\infty$ control co-design for networked control systems. *Automatica* 2013; 49(5): 1326–1332.

29. Zhang J, Peng C, Du D, et al. Adaptive event-triggered communication scheme for networked control systems with randomly occurring nonlinearities and uncertainties. *Neurocomputing* 2016; 174: 475–482.

30. Li ZX, Yan J, Yu WW, et al. Adaptive Event-triggered control for unknown second-order nonlinear multi-agent systems. *IEEE Trans Cybern* 2021; 51(12): 6131–6140.

31. Lu AY and Yang GH. Event-triggered secure observer-based control for cyber-physical systems under adversarial attacks. *Inf Sci* 2017; 420: 96–109.

32. Li XM, Zhou Q, Li P, et al. Event-triggered consensus control for multi-agent systems against false data-injection attacks. *IEEE Trans Cybern* 2020; 50(5): 1856–1866.

33. Gao J, Zhao Z, Wang J, et al. Event-triggered output feedback control for discrete markov jump systems under deception attack. *J Franklin Inst* 2020; 357(11): 6435–6452.

34. Peng DT, Dong JM, Cui ZM, et al. On the stability of cyber-physical systems under false data injection attacks. *Acta Automatica Sinica* 2019; 45(1): 196–205.

35. Bezzaoucha Rebaï S, Voos H and Darouach M. Attack-tolerant control and observer-based trajectory tracking for cyber-physical systems. *Eur J Control* 2019; 47: 30–36.

36. Xiao HQ, He Y, Wu M, et al. Output tracking control for sampled-data networked control systems in T-S fuzzy model. *Acta Autom Sin* 2015; 41(3): 661–668.

37. Fridman E. A refined input delay approach to sampled-data control. *Automatica* 2010; 46(2): 421–427.

38. Li W, Shi Y and Li Y. Research on secure control and communication for cyber-physical systems under cyber-attacks. *Trans Inst Meas Contr* 2019; 41(12): 3421–3437.

39. Qiu AB, Ji HG and Gu JP. Optimal integrated design of time-varying fault estimation and accommodation for non-uniform sampled data systems. *Acta Autoatica Sinica* 2014; 40(7): 1493–1504.

40. Lee WI, Lee SY and Park P. Affine Bessel–Legendre inequality: application to stability analysis for systems with time-varying delays. *Automatica* 2018; 93: 535–539.

41. Park P, Ko JW and Jeong C. Reciprocally convex approach to stability of systems with time-varying delays. *Automatica* 2011; 47: 235–238.

42. Johansson KH. The quadruple-tank process: a multivariable laboratory process with an adjustable zero. *IEEE Trans Control Syst Technol* 2000; 8(3): 456–465.