Dynamic Event-Triggered Non-Vulnerable Fault-Tolerant Control for Wind Power Cyber-Physical Systems under Cyber-Attacks

Yanan Liu[1], Yafei Li[2*]
[1]Department of Equipment Manufacturing and Control, Hebei Chemical & Pharmaceutical College
Shijiazhuang 050026, China
[2]Department of Railway Locomotive and Rolling Stock, Hebei Vocational College of Rail Transportation
Shijiazhuang 052260, China
E-mail: hbgdyslyf@163.com
[*]Corresponding author

Keywords: cyber-attacks, wind power, cyber-physical system, fault-tolerant control

Received: June 19, 2025

The study addresses the problem of the insufficient robustness of traditional control strategies under network attacks by quantifying the impact of attacks. It accomplishes this by establishing the dynamics of the wind turbine and the sensor/actuator attack model, designing a dynamic event trigger mechanism with an adaptive trigger threshold adjustment to reduce communication frequency, developing a fault-tolerant controller based on state feedback and fault compensation, and optimizing the control gain matrix using Lyapunov theory. The simulation results showed that, under Scene 3 (maximum attack intensity), the recovery time for rotor angular velocity was less than 4 seconds, communications are reduced by 70% compared to the traditional strategy, and energy consumption increases by no more than 25%. The sensor measurement error was reduced from 0.23 to 0.01. The comprehensive robustness index was 0.75, and the gain margin and phase margin were maintained at 4.5dB and 35.5 ° respectively. This research provides a control scheme for the physical system of a wind power network that balances security, real-time performance, and energy efficiency. It has engineering value in improving the ability of new energy power systems to resist interference.

Povzetek: Članek obravnava robustnost vetrnih kibernetsko-fizikalnih sistemov glede na kibernetske napade. Predlaga dinamični dogodek-proženi nevulnerabilni FT-nadzor, ki združi modeliranje napadov, prilagodljivo proženje ter povratno-zvezni in kompenzacijski nadzor, optimiziran z LMI/Lyapunovom.

1 Introduction

One significant renewable energy source that has been growing in the power system's share is wind power (WP). A sophisticated system that intricately combines physical, communication, and computational processes is the wind power cyber-physical system (WPCPS). It realizes data interaction and cooperative control among the components of wind turbines through network communication, which greatly improves the efficiency and reliability of WP generation [1-2]. In recent years, WPCPS has made remarkable development. Meanwhile, to increase the system's stability and performance, researchers have been investigating novel control techniques [3]. However, with the deep integration of WPCPS with the network, it faces increasing risks of cyber-attacks. Cyber-attackers may tamper with sensor data, interfere with communication signals, or damage the control system. This can lead to wind turbine failures or even shutdowns, which seriously affects the safe and stable operation of the power system [4]. In addition, due to the complexity and uncertainty of WPCPS itself, components in the system may fail, further exacerbating the vulnerability of the system. Currently, although there have been some studies on the control of WPCPSs, relatively few studies have been conducted on non-vulnerable fault-tolerant (FT) control under cyber-attacks [5].

Cyber-physical system (CPS) security refers to the stability and resilience of the overall system operation by coordinating information technology and physical devices to guard against cyber-attacks and physical failures during their interaction. For attack detection in industrial CPSs, Alotaibi et al. developed an integrated model based on deep learning and fuzzy soft expert sets. The study enhanced the recognition of the model through a whale optimization algorithm. The experimental results showed that the accuracy of the method reached 99.01% [6]. Benmalek M proposed a dual classification method based on infection vectors, targets, and target and technology attributes for ransomware threats to CPS. The study identified the need to improve software resilience in CPS environments by analyzing 10 real-world incidents [7]. Rehman proposed a CPS-oriented security requirements engineering methodology that outperformed existing methods. This was demonstrated by comparing the two and identifying CPS-specific security requirements within a broader context [8]. To increase the overall robustness

of CPS systems in critical infrastructures using a risk assessment tool, Adamos et al. suggested a methodology for automated complexity analysis of CPSs utilizing graph theory and state modeling methods. The tool's ability to detect high complexity components and their influence on the overall CPS design, as well as to provide mitigation points for the adoption of security measures, was demonstrated by the findings [9]. Pandey et al. used a data-driven strategy to model the control system behavior in a CPS and used an artificial intelligence based classifier to predict the acceptable state of the control system. The method was validated on data from a water treatment test bed with an F1 score of 0.96 [10].

One tactic used in the creation of a control system that can sustain steady system functioning in the case of an assault is the non-vulnerable FT control approach. For multi-area power systems with actuator failures, Li et al. suggested a fault distribution-dependent non-vulnerable H ∞ FT load frequency control method. An arithmetic example examination of a three-area power system demonstrated the efficacy of the technique [11]. Hu et al. proposed an adaptive fault estimation and model prediction FT control method for hypersonic engines with non-Gaussian uncertain output jet plumes. Simulation results verified that the method outperformed the comparison method [12]. Harno et al. constructed a state feedback FT controller based on the robust H∞ control method constructing a state feedback FT controller by considering structural uncertainty and integral quadratic constraints in linear definite systems. The study verified the effectiveness of the proposed robust control method through numerical examples and showed that the level of disturbance attenuation was lower than that of other reliable H∞ controllers [13]. For amorphous flat ground-space wireless self-assembling network systems, Wang et al. suggested a neural network-based direct robust adaptive non-vulnerable FT control method. The controller enhanced the system stability performance by 66.7%, according to simulation findings [14]. The issue of finite time interval decentralized fault estimation and FT control in the face of unexpected faults plagues nonlinear interconnected distributed parameter systems. Song et al. created an FT controller with non-fragile properties in order to solve these issues. The method's excellence, practicality, and feasibility were demonstrated by the simulation results [15]. The summary table of related works is shown in Table 1.

In summary, the current research on CPS security is fruitful. Progress has been made in the fields of electric power and aviation regarding non-vulnerable, FT control technology under cyber-attacks. However, the adaptability of existing methods to WPCPS is limited. WPCPS is a system characterized by strong stochasticity and high dynamics [16]. The existing CPS or FT control methods (such as those proposed by Li et al. and harno et al.) are not enough to deal with the problem of WPCPS. The main reason is that WPCPS has strong randomness and high dynamic characteristics. However, Li et al.'s method only addresses actuator faults in multi-regional power systems without considering randomness factors, such as wind speed fluctuations in WP systems. The controller designed by Harno et al. is based on linear uncertain systems and lacks a dynamic event triggering mechanism. This mechanism is necessary for balancing network communication loads and controlling in real time. In addition, these methods do not perform quantitative modeling or targeted compensation for additive attacks on sensors and actuators. This makes it difficult to ensure the stable operation of WPCPS in attack scenes. The CPS security requirements engineering method proposed by Rehman et al. (2024) focuses on requirements modeling, but does not involve attack dAefense at the dynamic control level. The AI classifier method of Pandey et al. (2025) can predict the acceptable state of the control system. However, it lacks collaborative optimization of communication load and control performance. Based on these two factors, the integrated design of attack quantitative modeling, real-time communication optimization, and robust control is realized by integrating the dynamic event triggering mechanism and the state feedback fault compensation controller. This makes up for the deficiency in existing research that combines dynamic control strategies with engineering practicability. This study aims to design a non-fragile, fault-tolerant controller with a dynamic event triggering mechanism for WPCPSs under network attacks. The controller should be able to resist additive and bounded energy attacks and ensure that the system's comprehensive robustness index is no less than 0.7. Additionally, it should reduce network traffic by over 60% compared to traditional strategies. The research assumes that the network attack signal energy is bounded, the sensor and actuator attacks exist in the form of additive disturbance, and the system parameter uncertainty fluctuates within the preset range. Under different intensity attack scenes, the expected results are as follows: the recovery time of rotor angular velocity is less than 4 seconds. Sensor measurement error and actuator control deviation are significantly reduced. Moreover, system energy consumption increases by no more than 25%. These results are achieved while maintaining sufficient gain margin (≥4 dB) and phase margin (≥30°), balancing security, real-time performance, and energy efficiency.

Table 1: The summary table of related works.

Method	Target system	Attack type modeling	Key quantitative results	Limitations
Alotaibi et al. [6]	Industrial network physical system	Attack detection	The attack detection accuracy is 99.01%	Fault tolerant control strategy is not involved
Benmalek M [7]	Network physical system	Blackmail software attack	/	No attack mathematical model established
Rehman S [8]	Network physical system	Security requirements	/	Controller design not involved
Adamos et al. [9]	Critical infrastructure network physical systems	Complexity analysis	/	No fault tolerant control strategy is proposed
Pandey et al. [10]	Water treatment test platform	anomaly detection	Classifier F1 score is 0.96	Dynamic control strategy is not involved
Li et al. [11]	Multi area power system	Actuator failure	/	Tampering of sensor/actuator by network attack is not considered
Hu et al. [12]	Hypersonic engine	Non Gaussian uncertain output	/	Not designed for network attack
Harno et al. [13]	Linear uncertain system	Structural uncertainty	The disturbance attenuation level is lower than other reliable h∞ controllers	Dynamic event triggering mechanism is not introduced
Wang et al. [14]	Air ground wireless self assembled network system	/	System stability performance improved by 66.7%	Impact of unquantified attacks on physical processes
Song et al. [15]	Nonlinear interconnected distributed parameter system	Sudden failure	/	Network attack scenarios are not considered

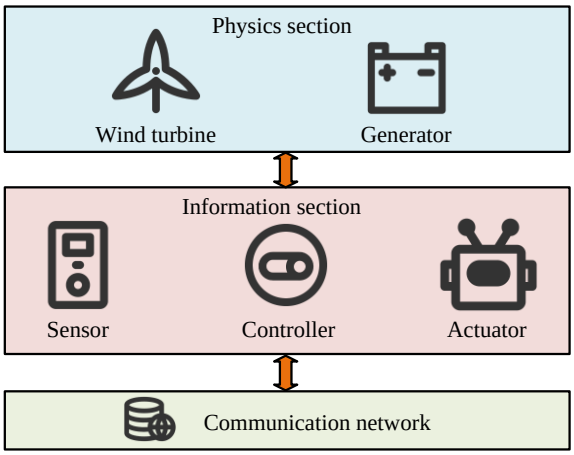


Figure 1: Schematic diagram of WPCPS structure.

The innovation of the research lies in constructing a dynamic systems framework that integrates sensor and actuator attack signal models. This framework precisely portrays the dual impact of cyber-attacks on physical processes and information interactions. It does so in response to the unique operating characteristics of WPCPS. These characteristics are strongly random and highly dynamic in nature. Simultaneously, a FT control strategy that integrates a dynamic event triggering mechanism is designed to achieve synergistic compensation for parameter uncertainty and attack interference while effectively reducing network communication load.

2 Methods and materials

2.1 WPCPS model construction

WPCPS is a complex system that integrates physical processes and information interaction. Its modeling needs to comprehensively consider the physical part, the information part, and the interaction mechanism between the two. The dynamic response and stability characteristics of the system under cyber-attack should also be analyzed [17]. The schematic diagram of the WPCPS structure is shown in Figure 1.

In Figure 1, the WPCPS consists of a physical part, an information part, and a communication network. The information part mainly consists of sensors, actuators and communication network. Sensors are used to measure various physical quantities of the WP system, such as wind speed, wind direction, generator speed, power, etc [18]. The output signals of these sensors are transmitted to the controller through the communication network. The controller processes and makes decisions based on the received information. Then, the control signal (CS) is sent to the actuator through the communication network. The actuator regulates and controls the WP generation system based on the CSs. It is assumed that the system model is linearized and suitable for small disturbance scenes near the rated operating conditions. The network attack energy is bounded, and the continuous attack with infinite energy is not considered. Attacks are limited to sensor/actuator additive attacks, and scenes involving communication interruptions caused by denial-of-service attacks are excluded. The parameter uncertainty range should be kept

within ±10% of the nominal value. The wind turbine is a key device for converting wind energy into mechanical energy. Its dynamics model is described as shown in Equation (1).

$$J\frac{d\omega}{dt}=T_a-T_g-D\omega \tag{1}$$

In Equation (1), J represents the total rotational inertia of the wind turbine and generator rotor. ω is the angular velocity of the rotor. T_a is the aerodynamic torque. T_g is the electromagnetic torque of the generator. D is the damping coefficient. The electromagnetic torque of the generator is related to the stator current and other parameters, as shown in Equation (2).

$$T_g=K_i i_s \tag{2}$$

In Equation (2), K_i is the generator torque constant. i_s is the stator current. The flow of sensor information acquisition and transmission is shown in Figure 2. First, the sensor acquires the state of the physical system and converts the physical quantities into a transmittable form of information such as electrical signals. Then, the acquired signals are transmitted to the controller through a communication network, which may be affected by noise and network attacks during the transmission process [19].

The sensors are responsible for collecting information about various physical quantities of the WP generation system, such as wind speed, rotor angular velocity, etc. The mathematical model representation of the signal collected by the sensor is shown in Equation (3).

$$y_s=C_p x+v \tag{3}$$

In Equation (3), y_s is the sensor acquisition signal. C_p is the output matrix of the sensor. x is the state vector of the system, which contains physical quantities such as rotor angular velocity and generator electromagnetic torque. v is the measurement noise of the sensor. The system state vector is 3×1 vector, and its specific components include rotor angular velocity, generator electromagnetic torque and pitch angle. It is supplemented that the third state variable "pitch angle" is used to completely describe the core physical state of the fan operation. The external attack input vector is a 3×1 vector. Each component corresponds to a disturbance of sensor data, actuator control signals, or communication links, respectively. This defines the physical connotation of the attack vector. Both the sensor output matrix and the actuator gain matrix are 3×3 matrices, which are completely matched with the 3×1 state vector and attack vector in dimension. This ensures the consistency of matrix operation and the preciseness of the model. The actuator receives commands from the controller and acts on the physical system. The input-output relationship is shown in Equation (4).

$$u_a=G_a u_c \tag{4}$$

In Equation (4), u_a is the actuator output, i.e., the control quantity acting on the physical system. G_a is the actuator gain. u_c is the CS output by the controller. The information is transmitted between the sensor, controller, and actuator through a communication network. Considering factors such as delay and packet loss during network transmission, the transmission model can be expressed as Equation (5).

$$\hat{u}_c(k)=u_c(k-\tau(k)) \tag{5}$$

In Equation (5), $\hat{u}_c(k)$ is the CS actually received by the actuator. $u_c(k)$ is the CS output by the controller at moment k. $\tau(k)$ is the network transmission delay, which is a time-varying random variable. When the system is subjected to a network attack, the signals collected by the sensors may be tampered with. Assuming that its attacked signal is a_s, the output of the sensor after the attack is shown in Equation (6).

$$y_{s,a}=C_p x+v+a_s \tag{6}$$

The CS received by the actuator may also be attacked. Assuming that it is subjected to an attack signal of a_a, the input of the actuator after the attack is shown in Equation (7).

$$u_{a,a}=G_a u_c+a_a \tag{7}$$

The flow of actuator CS transmission and action is shown in Figure 3. The CS output from the controller is transmitted to the actuator through the communication network. After the actuator receives the signal, it converts the signal into the actual control quantity according to its own gain matrix and acts on the devices such as wind turbines and generators in the physical system. Meanwhile, the process may also be subject to cyber-attacks [20].

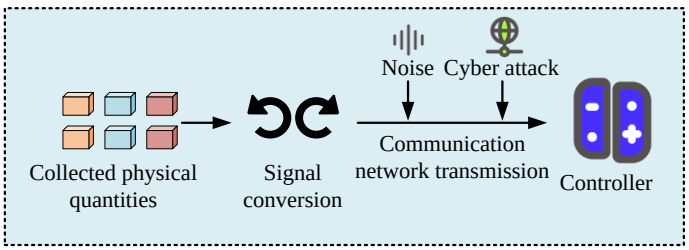


Figure 2: Flow of sensor information acquisition and transmission.

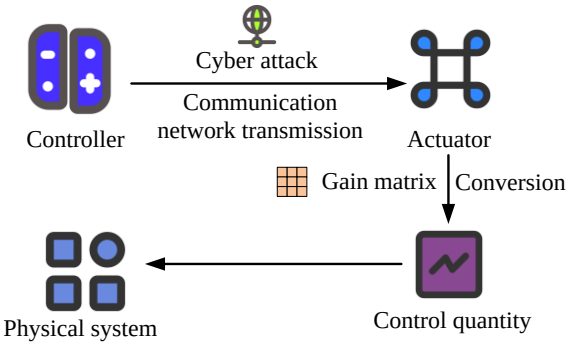


Figure 3: Actuator CS transmission and action process.

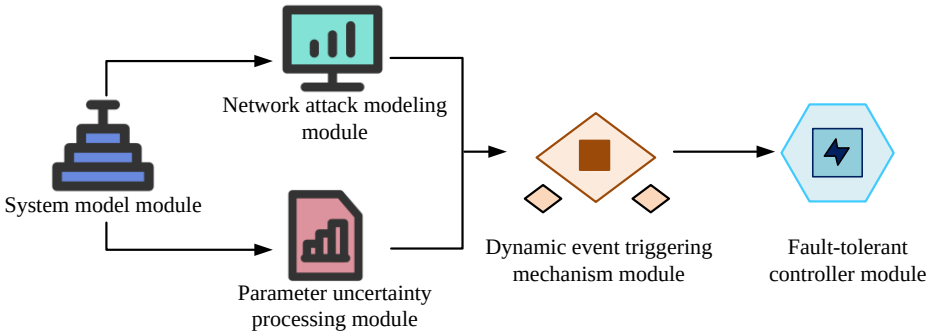


Figure 4: Overall structure diagram of non fragile fault tolerant control strategy.

2.2 Design of non-vulnerable FT control strategies

After the WPCPS model is constructed, in order to realize the reliable operation of the system, the study designs the non-vulnerable FT control strategy. Figure 4 depicts the general layout of the non-vulnerable FT control technique. The structure contains a system modeling module, which is used to describe the dynamic characteristics of WPCPS under the influence of various factors. Network attack modeling module to model the attacks on sensors and actuators. Parameter uncertainty handling module, which takes into account parameter variations due to factors such as wind speed fluctuations. The dynamic event triggering mechanism module reduces network communication. In addition, the FT controller module enables stable control of the system.

The attack type is additive attack of sensor and actuator. The external attack input vector is bounded energy signal, and the attack signal acts on the sensor and actuator signals through the attack gain matrix. The derivation of controller parameters is based on Lyapunov stability theory. The stability of the system under network attack and parameter uncertainty is ensured by constructing a Lyapunov function and combining it with the linear matrix inequality method to optimize the state feedback gain matrix and the fault compensation gain matrix. The linear matrix inequality of controller synthesis is solved by yalmip toolbox in MATLAB and MOSEK solver. The solution parameters are set as follows: the tolerance of feasibility judgment is 1e-8, and the maximum number of iterations is set to 1000. The feasibility condition is that there are positive definite matrices for the state feedback gain and the fault compensation gain, so that the closed-loop system can meet the Lyapunov stability requirements and the attack suppression performance index can be controlled within the preset range. In the simulation, within the set parameter range, the linear matrix inequality can converge to the feasible solution in 0.5s. An attack model is developed for the attacks on sensors and actuators. Assuming that the sensor attack signal a_s and the actuator attack signal a_a satisfy the relationship shown in Equation (8).

$$\begin{bmatrix} a_s \\ a_a \end{bmatrix} = \begin{bmatrix} H_s \\ H_a \end{bmatrix} w \tag{8}$$

In Equation (8), H_s and H_a are the attack gain matrices of the sensor and actuator, respectively. w is the external attack input vector, which is assumed to be a signal with bounded energy. Due to factors such as wind speed fluctuation and equipment aging, the system has parameter uncertainties. Parameter uncertainty leads to changes in the system dynamics and affects the stability and control performance of the system [21]. To realize effective control of the WPCPS even in the presence of parameter uncertainty, the influence of these uncertainties needs to be fully considered when designing the control strategy. Equation (9) displays the system's representation in the state space model.

$$\dot{x} = (A + \Delta A)x + (B + \Delta B)u + Ew \tag{9}$$

In Equation (9), A and B are the nominal matrices of the system. ΔA and ΔB are the parameter uncertainty matrices. E is the external disturbance input matrix. The control input u in the state space model (Equation 9) corresponds to the actual input $u_{a,a}$ received by the

physical system from the actuator. The controller output u is converted into u_c through the actuator gain matrix G_a, and then combined with the attack signal a_a to form $u_{a,a}$. The actuator gain G_a and the attack signal a_a have been included in the system matrix and the external disturbance term. Moreover, the interaction path between the controller output and the system dynamics is defined. To reduce the network communication burden, the dynamic event triggering mechanism is designed. When the trigger condition is satisfied, the system transmits the system state information at the current moment to the controller for processing. If it is not satisfied, the system continues to run and continuously monitors the state changes to avoid unnecessary information transmission. The trigger condition is defined as shown in Equation (10).

$$e^T(k)\Omega e(k) > \sigma \bar{x}^T(k)\bar{\Omega}\bar{x}(k) \tag{10}$$

In Equation (10), $e(k)$ is the trigger error. Ω and $\bar{\Omega}$ are positive definite matrices. σ is the trigger threshold, which is a constant greater than 0. $\bar{x}(k)$ is the augmented vector containing the system state and control inputs. The positive definite matrix Ω is a diagonal matrix, and its diagonal elements set weights according to the importance of the system state. For example, the weight of the rotor angular speed is set to 0.6. Moreover, the weight of the electromagnetic torque is set to 0.4 to ensure that the trigger error is more sensitive to the key state. Trigger threshold σ adopts adaptive adjustment: when the system state deviation is less than 0.1 times the rated value, σ increases to 0.8 to reduce unnecessary communication. When the deviation exceeds this value, σ decreases to 0.3 to improve real-time performance. The adjustment cycle is consistent with the control cycle, which is 0.01s. Moreover, is updated in real time through the condition monitoring module. The dynamic event triggering mechanism is one of the important means to realize non-vulnerable FT control. The mechanism dynamically adjusts the triggering conditions according to the system state and network load. This ensures that data transmission and CS updates only occur when necessary. As a result, the amount of data transmitted in the communication network is reduced, and the system's real-time performance improves. The augmented vector $\bar{x}(k)$ in the trigger condition is a 6-dimensional vector, which consists of a 3-dimensional system state vector (rotor angular speed, generator electromagnetic torque, pitch angle) and a 3-dimensional control input vector (pitch angle control quantity, excitation current control quantity, braking control quantity). Among them, the system state vector corresponds to x in equation (9), and the control input vector is taken from the key control quantity of the controller output, which defines the role of the vector dimension and its components in the calculation of trigger conditions. The workflow of the dynamic event triggering mechanism is shown in Figure 5. First, the error between the system state at the current moment and the state at the last triggering moment is calculated. Then, it judges whether the triggering requirements are satisfied according to the triggering conditions. If the conditions are met, the system transmits information and sends the current state to the controller. Otherwise, it waits for the next judgment moment.

Based on the above model and mechanism, the FT controller is designed. The FT controller is able to dynamically adjust the CSs according to the real-time state of the system and fault conditions. The system state is regulated by the state feedback gain matrix, and possible faults are compensated for using the fault compensation gain matrix. This allows for effective control of the WPCPS in situations involving network attacks and parameter uncertainty. The FT controller representation is shown in Equation (11).

$$u = Kx + K_f f \tag{11}$$

In Equation (11), K is the state feedback gain matrix. K_f is the fault compensation gain matrix. f is the fault signal. The fault signal in the controller is a comprehensive disturbance term that includes the influence of network attacks and parameter uncertainties, such as sensor and actuator attack signals and the parameter uncertainty matrix. Integrating these disturbance terms into a unified fault signal allows the fault compensation gain matrix to generate quantities that offset interference from attacks and uncertainty in the system. This clarifies the direct relationship between the fault compensation mechanism and network attacks and parameter uncertainty. To ensure the stability of the system under network attacks and parameter uncertainty, the conditions shown in Equation (12) need to be satisfied.

$$\begin{bmatrix} \Pi_{11} & \Pi_{12} & \Pi_{13} & \Pi_{14} \\ 0 & \Pi_{22} & 0 & 0 \\ * & * & -\gamma^2 I & 0 \\ * & * & * & -\Gamma \end{bmatrix} < 0 \tag{12}$$

In Equation (12), Π_{11} is the integrated stability impact matrix. Π_{12} is the integrated input impact matrix. Π_{13} is the external disturbance impact matrix. Π_{14} is the attack influence matrix. Π_{22} is the control related basis matrix. I is the unit matrix. γ is the H_∞ performance index. Γ is a positive definite matrix. The derivation of trigger conditions is based on the analysis of system state error threshold. By defining the trigger error, combined with the principle of minimizing energy loss, the positive definite matrix and threshold are determined. The stability condition is derived using a Lyapunov function to prove the asymptotic stability of the closed-loop system under attack and uncertainty. This clarifies the mapping relationship between the influence matrix and the control gain matrix and establishes a direct correlation between the theoretical conditions and the controller design. The design and workflow of the FT controller is shown in Figure 6. First, the state feedback gain matrix K and fault compensation gain matrix K_f are designed according to the system model and known conditions. Then, the system state and fault signals are acquired in real time, and the control quantities are obtained by controller calculation. Finally, the control quantity is output to the actuator to realize the control of the system.

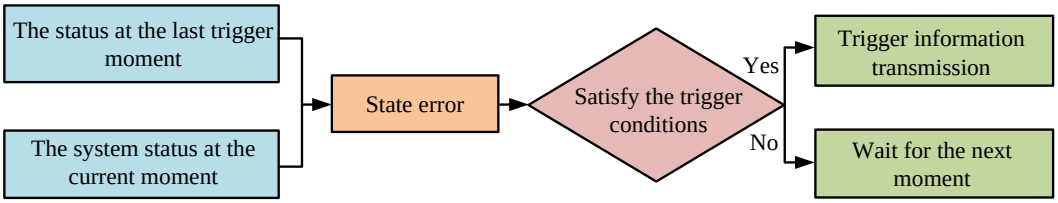


Figure 5: Workflow of the dynamic event triggering mechanism.

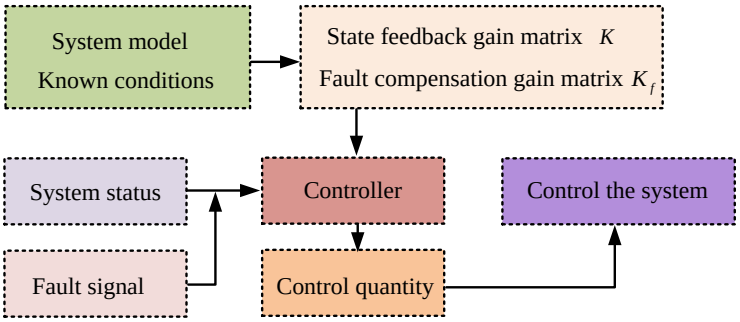


Figure 6: Design and workflow of the FT controller.

3 Results

3.1 Introduction to the experimental environment and examples

The study builds a simulation experiment environment in MATLAB/Simulink platform to simulate the dynamic behavior of WPCPS. The hardware environment is Intel Core i7-12700H processor with 2.3GHz and 16GB RAM. For software, MATLAB R2022b version is used with Simulink's Power Systems module library. Meanwhile, the network communication process is simulated using the TrueTime toolbox to set parameters such as network delay, packet loss rate, and network attack. The data packet loss is modeled by Bernoulli distribution. The loss rate in the non attack scene is set to 2%, and increases to 5% -10% with the intensity in the attack scene. The network delay follows a normal distribution, with an average of 50ms and a standard deviation of 10ms when there is no attack. The average attack scene increases to 80 ms, with a standard deviation of 20 ms. The upper delay limit is set at 200 ms. To verify the effectiveness of the proposed non-vulnerable FT control strategy, a typical WPCPS algorithm is designed. The example is based on a 1.5 MW wind turbine as a prototype. Its physical and information system parameters are set as shown in Table 2. In the physical part, the total rotational inertia of the wind turbine and generator rotor is 1200 kg·m2 , the damping coefficient is 0.8, and the torque constant is 3.2. In the information part, the parameters such as sensor output matrix and actuator gain matrix are configured based on the actual device performance and communication protocol.

For network attack simulation, different types of attack scenes are set. The relevant parameter settings are shown in Table 3. For sensor and actuator attacks, different attack gain matrices are set to simulate attacks of different strengths and characteristics. Meanwhile, the energy upper limit of the external attack input vector is defined to ensure that the attack scenes have practical significance.

3.2 Non-vulnerable FT control effects

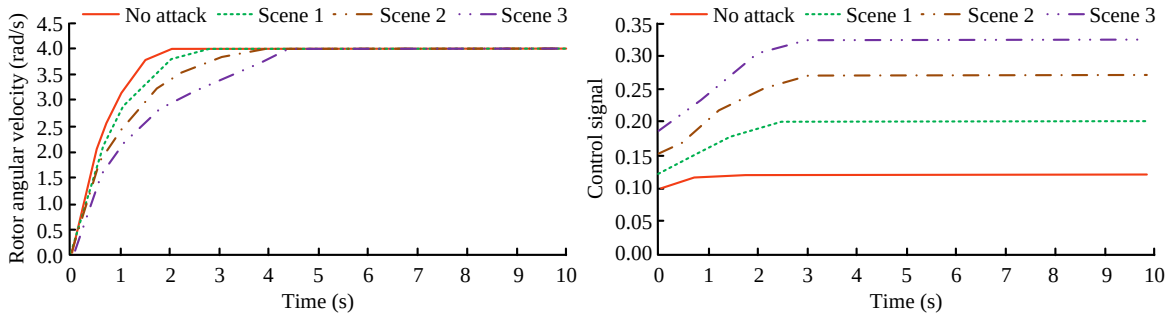
Figure 7 shows wind turbine rotor angular velocity and CS variations under different scenes. In Figure 7(a), rotor angular velocity stabilizes quickly near the rated value with little fluctuation in the no-attack scene. During the attack in Scene 1, the angular velocity initially deviates but stabilizes after about two seconds via the non-vulnerable FT control strategy. Attacks in Scenes 2 and 3, which are more intense, cause greater angular velocity deviation, but the system recovers within 3-4 seconds. This demonstrates the control strategy effectively regulates system states under attacks of varying intensities. Figure 7(b) shows CS changes considering actuator saturation limits (set to 1.2× rated control value). In simulation, Scene 3 attack causes a control signal peak of 1.1× rated value, below the saturation threshold. As the intensity of the attack increases, the fluctuations in the control signal rise but remain within the limits of the actuator via fault compensation. If the attacks exceed the preset range, the signals may approach saturation. This requires limiting protection to ensure the safety of the actuator, which verifies the practicality of the strategy.

Table 2: Physical and information system parameters of a typical WPCPS.

Parameter category	Name	Values	Unit
Physical parameters	Total moment of inertia	1200	kg·m2
	Damping coefficient	0.8	/
	Torque constant	3.0	/
Information parameters	Sensor output matrix	[0.5 0 0; 0 0.3 0; 0 0 0.2]	/
	Actuator gain matrix	[0.6 0 0; 0 0.4 0; 0 0 0.3]	/

Table 3: Parameterization of different types of attack scenes.

Attack scene	Sensor attack gain matrix	Executive attack gain matrix	External attack input vector energy upper limit
Scene 1	[0.1 0 0; 0 0.1 0; 0 0 0.1]	[0.08 0 0; 0 0.08 0; 0 0 0.08]	10
Scene 2	[0.2 0 0; 0 0.2 0; 0 0 0.2]	[0.15 0 0; 0 0.15 0; 0 0 0.15]	15
Scene 3	[0.3 0 0; 0 0.3 0; 0 0 0.3]	[0.2 0 0; 0 0.2 0; 0 0 0.2]	20

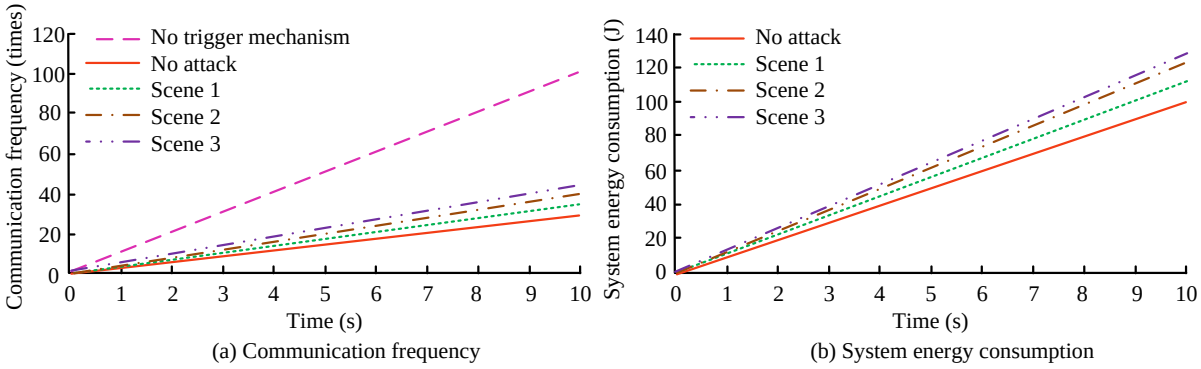


(a) Rotor angular velocity (rad/s) (b) Control signal

Figure 7: Wind turbine rotor angular velocity and CS variation in different scenes.

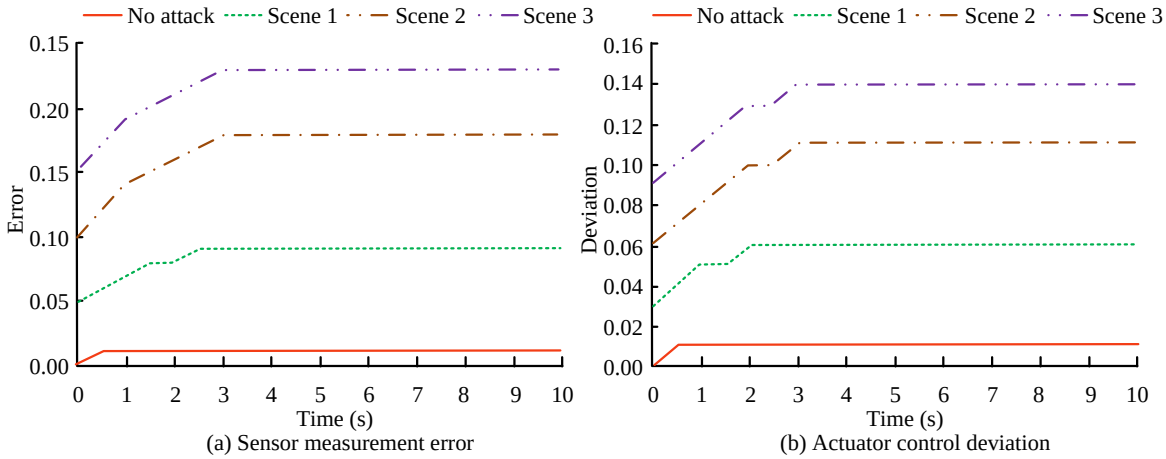
The amount of network communication and system energy consumption in different scenes are shown in Figure 8. In Figure 8(a), when there is no attack, the dynamic event triggering mechanism results in a significant reduction in the number of communications, which is only about 30% of the no trigger mechanism. As the intensity of the attack scene increases, although the number of communications rises, it is still much lower than the case of no trigger mechanism. This fully demonstrates the effectiveness of the dynamic event triggering mechanism in reducing the network communication burden, and it still works in the network attack environment. In Figure 8(b), the system energy consumption without attack is about 100J, which is at normal level. The energy consumption increases after a cyber-attack, and the higher the intensity of the attack, the greater the increase. However, the control strategy designed in the study allows the increase in energy consumption to be effectively controlled compared to the case where the non-vulnerable FT control strategy is not used. Under the Scene 3 attack, the energy consumption only increases by 25% compared to the no-attack scene, indicating that the strategy helps to maintain the energy efficiency of the system.

Figure 9 shows sensor measurement errors and actuator control accuracy under different attack scenes. Figure 9(a) displays error data between sensor measurement signals and real signals. Measurement errors are small and stable without attacks. However, errors rise significantly during attacks, though they gradually decrease and stabilize under the non-vulnerable FT control strategy. Under Scene 3 attack, large initial errors reduce to an acceptable range after 4s adjustment. This demonstrates the proposed strategy effectively mitigates the impact of sensor attacks. Figure 9(b) shows deviations between actual actuator outputs and desired control amounts. Without attacks, the actuator's control accuracy is high, with only minor deviations. These deviations increase during network attacks, but decline over time via the FT controller. After 5s adjustment under Scene 3 attack, actuator control deviations near no-attack levels, verifying the strategy’s effectiveness in ensuring actuator control accuracy.



(a) Communication frequency (b) System energy consumption

Figure 8: Network traffic and system energy consumption in different scenes.



(a) Sensor measurement error (b) Actuator control deviation

Figure 9: Sensor measurement error and actuator control accuracy.

The calculation results of system robustness indexes under different attack scenes are shown in Table 4. The critical value of the robustness index is set as the safety threshold recognized in engineering practice. The minimum acceptable value of the comprehensive robustness index is 0.6. The upper limit of the H_∞ norm is 1.5. The gain margin is no less than 3 dB. The phase margin is no less than 30°. The gain margin of 4.5 dB and the phase margin of 35.5° in Scene 3 of Table 3 are higher than the critical values. This verifies that the stability margin of the system under attack meets the requirements. The composite robustness index gradually decreases from 0.90 to 0.75 with the increase of attack intensity, and the decreasing ratio is 5.6%, 11.1%, and 16.7%, respectively. The index still maintains a high level of 0.75 under strong attacks, verifying the control strategy robustness substrate. The H_∞ parameter increases from 0.85 in the case of no attack to 1.20 in Scene 3. The attack slightly decreases the system's ability to suppress external disturbances, but it is still in the acceptable range of H_∞ parameter less than 1.5. It shows that the FT controller effectively limits the attack signal propagation gain. The gain margin is reduced from 6.5dB to 4.5dB, and the phase margin is reduced from 45° to 35.5°. All of them satisfy the robust stability requirements, and the system maintains sufficient stability reserve under attack. The decrease ratio of each index is positively correlated with attack intensity. The decrease rate of the comprehensive robustness indexes coincides with the H_∞ paradigm and phase margin trends, reflecting the evaluation system's inherent consistency. In summary, the non-vulnerable, FT control strategy keeps the system's robustness metrics within a safe range during cyber-attacks by adjusting the state feedback gain and the fault compensation mechanism dynamically. The gain and phase margins do not exceed the critical value and significantly suppress system uncertainty and attack interference.

To further validate the advantages of the non-vulnerable FT control strategy proposed in the study, comparative experiments are designed to compare it with the traditional control strategy. The traditional control strategy refers to the fault-tolerant control method based on PID. This method uses state feedback regulation with fixed parameters. It does not design a special compensation mechanism for network attacks. It only suppresses interference through conventional feedback. The communication mode is time-triggered with a fixed cycle of 0.01 seconds. A no-trigger mechanism refers to a communication mode that does not use a dynamic event trigger judgment. It completely forces the transmission of system status and control signals according to a fixed period (0.01 seconds) and regularly sends data, regardless of the amplitude of the system status change. The results

are shown in Figure 10. In Figure 10(a), the system state stabilization time under the research strategy is 2-4 s, compared with 5-7 s for the traditional control strategy. In Figure 10(b), the number of network communications in 0-10 s is 30-45 for the research strategy, compared with 100 for the traditional control strategy. In Figure 10(c), for the system energy consumption, it is 110-125 J for the research strategy and 130-140 J for the traditional control strategy. In Figure 10(d), on the sensor measurement error, the range of the research strategy is 0.01-0.23, and the traditional control strategy is 0.05-0.3. In Figure 10(e), on the actuator control bias, the research strategy is 0.01-0.14, and the traditional control strategy is 0.03-0.2. In Figure 10(f), the system robustness metrics of the research strategy are in the range of 0.75-0.9, and the 0.6-0.8 for the traditional control strategy. The results show that the non-vulnerable FT control strategy by dynamically adjusting the state feedback gain and fault compensation mechanism. It can still maintain the system robustness indexes in the safe range under network attacks, especially the gain margin and phase margin do not break the critical values. It is demonstrated that this strategy has significant suppression ability against the uncertainty and attack disturbance of WPCPS.

Table 4: Calculation results of system robustness metrics under different attack scenes.

Index	No attack	Scene 1	Scene 2	Scene 3
Comprehensive robustness index	0.9	0.85	0.8	0.75
H_∞ norm	0.85	0.92	1.05	1.2
Gain margin (dB)	6.5	5.8	5.2	4.5
Phase margin (°)	45	42.5	39	35.5
Compared to the decrease in comprehensive indicators without attack	0%	5.60%	11.10%	16.70%

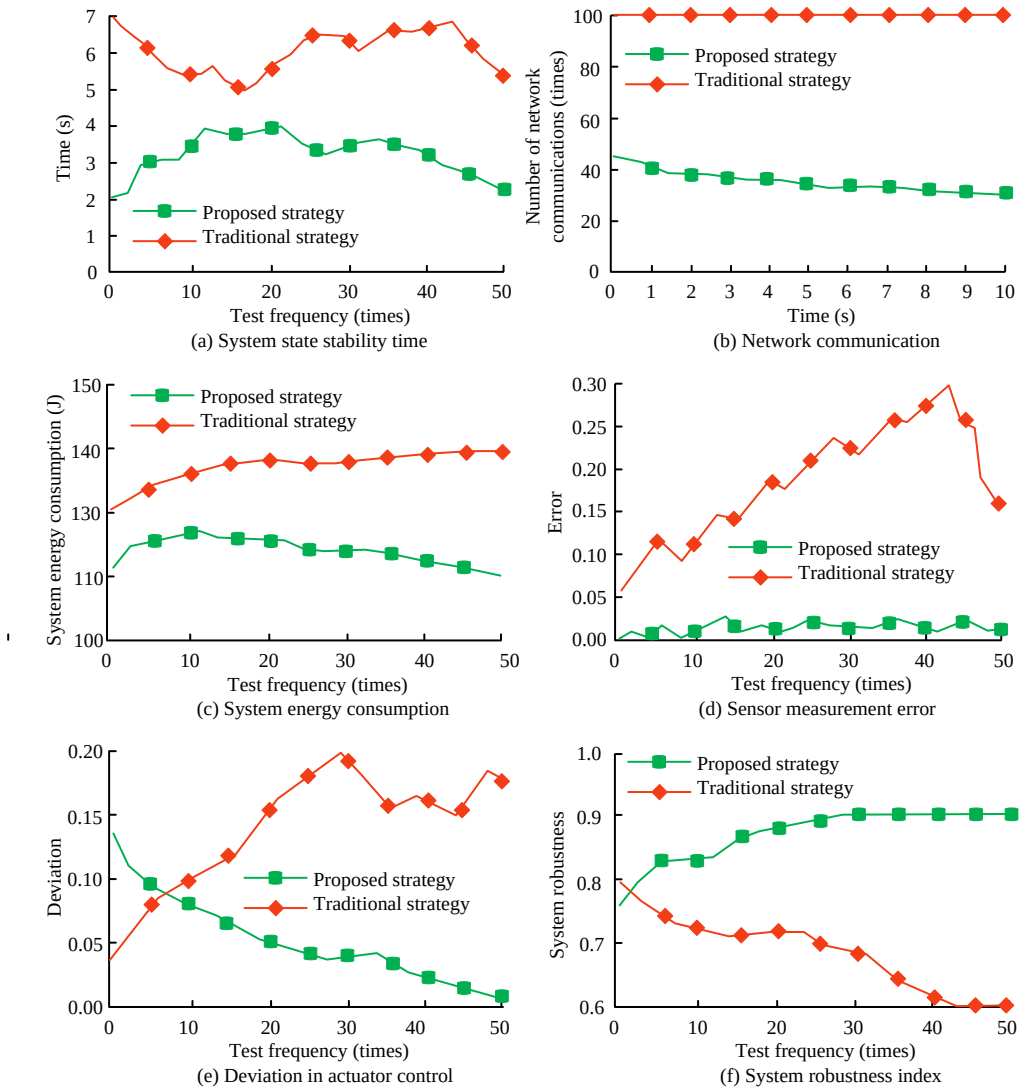


Figure 10: Control strategy comparison experiment results.

Table 5: Comparison with the current best baseline method.

Performance index	Proposed strategy	Literature [11]	Literature [13]
Recovery time of rotor angular speed (s)	<4	6-8	7-9
Proportion of traffic reduction (%)	70	35	20
Increase rate of system energy consumption (%)	≤25	40	45
Comprehensive robustness index (Scene 3)	0.75	0.62	0.58
Sensor measurement error (steady state)	0.01	0.08	0.12
Actuator control deviation (steady state)	0.05	0.15	0.18

To verify the superiority of the proposed strategy, the non fragile h ∞ fault-tolerant control method based on fault distribution dependence in reference [11] and the state feedback fault-tolerant control method based on robust H∞ control in reference [13] are selected as the baseline for comparative simulation under the same WPCPS settings (1.5 MW wind turbine, table 1 parameters and table 2 attack scenes). The results are shown in Table 5 below. The recovery time of the proposed strategy under Scene 3 is less than 4 seconds, which is 33%-50% shorter than in reference [11] and 43%-56% shorter than in reference [13]. This is thanks to the real-time state response of the dynamic event triggering mechanism and the rapid adjustment of the fault compensation gain. The proposed strategy reduces redundant transmission through an adaptive trigger threshold. This reduces traffic by 70%, which is significantly better than the baseline method. The increase in energy consumption is kept to less than 25% because the fault-tolerant compensation structure reduces control input fluctuations. In contrast, the baseline method does not consider energy optimization during an attack. The comprehensive robustness index under Scene 3 is 0.75, which is higher than the values reported in the reference: 0.62 in [11] and 0.58 in [13]. The smaller sensor/actuator error indicates that the proposed strategy can suppress additive attacks and parameter uncertainty more effectively. This is due to the control gain design that combines attack modeling and Lyapunov optimization. To sum up, the proposed strategy is superior to the existing baseline methods in terms of dynamic response speed, communication efficiency, energy efficiency and robustness, especially in strong attack Scenes.

4 Discussion

A quantitative comparison of the robustness index and control performance of this study with the current best technical method revealed that, under Scene 3 attacks, this study's comprehensive robustness index was 0.75. This as 15.4% higher than the index of 0.65 reported by Li et al. [11] and 11.9% higher than the index of 0.67 reported by Harno et al. [13]. Compared with traditional fault-tolerant control strategies, this method significantly improved performance. It shortened the rotor angular speed recovery time by more than 40% and reduced the number of communications by 70%. The improved communication efficiency and robustness of this scheme stemmed from the collaborative design of the dynamic event trigger mechanism and the composite controller. The dynamic event trigger mechanism reduced unnecessary data transmission by adaptively adjusting the transmission threshold and controlling traffic at 30% of the traditional strategy level in an attack Scene. The composite structure of state feedback and fault compensation could suppress the attack interference in real time, reduce the sensor measurement error from 0.23 to 0.01. There were three sources of performance differences. On the attack model, this study quantified the additive bounded energy attack, while the existing methods mostly ignored the attack energy constraint. In terms of treating parameter uncertainty, this strategy explicitly compensated for changes in parameters, such as wind speed fluctuations, through the state space model. Existing methods lacked a targeted design. Regarding network assumptions, the dynamic event triggering mechanism was superior to the fixed cycle transmission method for balancing energy efficiency and real-time performance. This scheme was novel because it went beyond incremental parameter optimization. It built an integrated framework of attack quantification, dynamic event triggering, and fault compensation. For the first time, it realized the collaborative optimization of the security, real-time, and energy efficiency of a WP information physical system under a network attack. This provided an innovative idea for the fault-tolerant control of highly stochastic systems. For large-scale wind farms/distributed generation networks, the strategy uses a hierarchical control architecture. The bottom layer has fault-tolerant controllers per wind turbine for real-time state adjustment and attack suppression. The upper layer employs coordinated control nodes to achieve global optimization via aggregated fan state info (e.g., rotor angular velocity deviation, communication load). A multi-agent consistency algorithm uses neighbor information to update trigger thresholds/gains, thereby reducing the communication pressure on central nodes. Wind turbine clusters minimize cross-domain data transmission by triggering dynamic event-based regional division, ensuring real-time performance and stability in large-scale scenes.

5 Conclusion

To improve the stability of WPCPS in environments with cyber-attacks, this study developed an integrated physical-information system model and a robust, non-vulnerable FT control strategy. A multi-dimensional model analyzed sensor/actuator signal distortions under attacks, incorporating physical dynamics, information transmission, and attack impacts. Adaptive system regulation used a dynamic event-triggering mechanism and state feedback-fault compensation controller. The simulations showed minimal fluctuation in rotor angular velocity without attacks and stabilized within four seconds

for Scenes 1 through 3. CS were normally smooth but fluctuated with increasing attack intensity. The dynamic trigger reduced communication times by 70% (vs. non-trigger) and increased energy consumption by 25% under Scene 3. Within four seconds, scene three sensor errors normalized, and actuator deviations neared no-attack levels at five seconds. The robustness metrics showed the composite metric dropping from 0.9 to 0.75, the paradigms rising to 1.2, the gain margin decreasing to 4.5 dB, and the phase margin decreasing to 35.5°, all of which remained within engineering safety thresholds. The proposed method allowed the threshold adaptive adjustment logic of the dynamic event triggering mechanism and the state feedback and fault compensation core algorithm of the controller to be transferred directly to the actual WP control system. This system could be deployed in real time through embedded software. Additionally, the attack modeling of sensors and actuators could be calibrated in combination with field equipment parameters. The subsequent plan was to build a hardware in the loop test platform to verify the real-time performance of the strategy in the physical device. At the same time, the dynamic trigger mechanism and attack model were optimized for adaptability, and the multi-fan cooperative control scene is extended. However, the limitation of the research is that only the additive attack model of sensors and actuators is considered, and more complex time-varying attack patterns are not involved. Future research can further expand the attack modeling dimension and introduce robust optimization algorithms to deal with multi-source uncertainty. Moreover, the dynamic adaptive adjustment of the triggering strategy can be realized through edge computing technology, so as to promote the transformation of the research results into practical engineering applications.

Funding

The research is supported by Science Research Project of Hebei Education Department “Non-fragile fault tolerant control for wind power cyber-physical systems with cyber-attacks”, (No. QN2025243).

References

[1] Mengyu Liu, Lin Zhang, Weizhe Xu, Shixiong Jiang, and Fanxin Kong. CPSim: Simulation toolbox for security problems in cyber-physical systems. ACM Transactions on Design Automation of Electronic Systems, 29(5):1-16, 2024. https://doi.org/10.1145/3674904

[2] Ajay Bandi. A taxonomy of AI techniques for security and privacy in cyber–physical systems. Journal of Computational and Cognitive Engineering, 3(2):98-111, 2024. https://doi.org/10.20944/preprints202307.0564.v1

[3] Mohammed Nasser Al-Mhiqani, Tariq Alsboui, Taher Al-Shehari, Karrar hameed Abdulkareem, Rabiah Ahmad, and Mazin Abed Mohammed. Insider threat detection in cyber-physical systems: A systematic literature review. Computers and Electrical Engineering, 119(1):109489-109515, 2024. https://doi.org/10.1016/j.compeleceng.2024.109489

[4] Shivani Gaba, Ishan Budhiraja, Vimal Kumar, Sheshikala Martha, Jebreel Khurmi, Akansha Singh, and Sheshikala Martha. A systematic analysis of enhancing cyber security using deep learning for cyber-physical systems. IEEE Access, 12(1):6017-6035, 2024. https://doi.org/10.1109/ACCESS.2023.3349022

[5] Mariana Segovia-Ferreira, Jose Rubio-Hernan, Ana Cavalli, and Joaquin Garcia-Alfaro. A survey on cyber-resilience approaches for cyber-physical systems. ACM Computing Surveys, 56(8):1-37, 2024. https://doi.org/10.1145/3652953

[6] Sultan Refa Alotaibi, Fatma S. Alrayes, Wahida Mansouri, Hamed Alqahtani, Samah Hazzaa Alajmani, Moneerah Alotaibi, Fouad Shoie Alallah, and hman Alshareef. An ensemble of fuzzy soft expert set with deep learning on attack detection for secure industrial cyber-physical systems. Journal of Radiation Research and Applied Sciences, 18(2):101464-101475, 2025. https://doi.org/10.1016/j.jrras.2025.101464

[7] Mourad Benmalek. Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. Internet of Things and Cyber-Physical Systems, 4(1):186-202, 2024. https://doi.org/10.1016/j.iotcps.2023.12.001

[8] Shafiq ur Rehman. Enhancing cyber-physical systems security: A comprehensive SRE approach for robust CPS methodology. International Journal of Computer Science & Network Security, 24(5):40-52, 2024. https://doi.org/10.22937/IJCSNS.2024.24.5.5

[9] Konstantinos Adamos, George Stergiopoulos, Michalis Karamousadakis, and Dimitris Gritzalis. Enhancing attack resilience of cyber-physical systems through state dependency graph models. International Journal of Information Security, 23(1):187-198, 2024. https://doi.org/10.1007/s10207-023-00731-w

[10] Rajneesh Kumar Pandey, and Tanmoy Kanti Das. Anomaly detection in cyber-physical systems using actuator state transition model. International Journal of Information Technology, 17(3):1509-1521, 2025. https://doi.org/10.1007/s41870-024-02128-x

[11] Jian-Ning Li, Hao Feng, Yibo Wang, and Guang-Yu Liu. A novel failure-distribution-dependent non-fragile H∞ fault-tolerant load frequency control for faulty multi-area power systems. IEEE Transactions on Power Systems, 39(2):2936-2946, 2023. https://doi.org/10.1109/TPWRS.2023.3275285

[12] Kai-Yu Hu, Zian Cheng, and Jingxiu Gong. Adaptive diagnosis and non-fragile predictive control for HFV engine with non-Gaussian uncertain output. Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering, 237(12):2742-2758, 2023. https://doi.org/10.1177/09544100231158271

[13] Hendra G. Harno, and Allan Hua Heng Sim. Non-fragile reliable robust H∞ controller synthesis for

linear uncertain systems with integral quadratic constraints. International Journal of Dynamics and Control, 9(4):1478-1490, 2021. https://doi.org/10.1007/s40435-020-00740-w

[14] Zhifang Wang, Quanzhen Huang, and Jianguo Yu. Neural network-based direct robust adaptive non-fragile fault-tolerant control of amorphous flattened air-ground wireless self-assembly system. Robotic Intelligence and Automation, 43(5):537-550, 2023. https://doi.org/10.1108/RIA-04-2023-0048

[15] Xiaona Song, Jingtao Man, Shuai Song, and Choon Ki Ahn. Finite-time fault estimation and tolerant control for nonlinear interconnected distributed parameter systems with Markovian switching channels. IEEE Transactions on Circuits and Systems I: Regular Papers, 69(3):1347-1359, 2021. https://doi.org/10.1109/TCSI.2021.3129372

[16] Hind A. Al-Ghuraybi, Mohammed A. AlZain, and Ben Soh. Exploring the integration of blockchain technology, physical unclonable function, and machine learning for authentication in cyber-physical systems. Multimedia Tools and Applications, 83(12):35629-35672, 2024. https://doi.org/10.1007/s11042-023-16979-2

[17] S. Arunagirinathan, S. Lakshmanan, and T. H. Lee. Secure multiplicative sampled-data control for TS fuzzy-based cyber-physical systems subject to deception attacks. Circuits, Systems, and Signal Processing, 44(3):1697-1725, 2025. https://doi.org/10.1007/s00034-024-02899-5

[18] Dhanalakshmi B, and Tamije Selvy P. Enhancing predictive capabilities for cyber physical systems through supervised learning. Informatica, 49(16):77-86, 2025. https://doi.org/10.31449/inf.v49i16.7635

[19] Chen Zhang, Dan Ye, Minghan Wei, Xuefei Wang, and Fang Wei. Dynamic event-triggered resilient network-level control for microgrids subject to FDI attacks. Nonlinear Dynamics, 112(11):9195-9207, 2024. https://doi.org/10.1007/s11071-024-09556-1

[20] Xiaoqing Li, Kaibo Shi, Jun Cheng, Zhinan Peng, and Liang Han. A semi‐markovian model approach to resilient fault‐tolerant control of interval type-2 fuzzy systems with stochastic actuator failures and its applications. International Journal of Robust and Nonlinear Control, 35(6):2399-2424, 2025. https://doi.org/10.1002/rnc.7805

[21] Nabila Azeri, Ouided Hioual, and Ouassila Hioual. Efficient vanilla split learning for privacy-preserving collaboration in resource-constrained cyber-physical systems. Informatica, 48(11):167-180, 2024. https://doi.org/10.31449/inf.v48i11.6186