Adaptive Resilient Control Strategy for Wind Turbines Against Replay Attacks

Shiyi Zhao[1], Jinhui Xia[2], Ruilong Deng[1], Peng Cheng[1], Qinmin Yang[1], and Yuanchao Shu[1]

[1a]College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China
[1b]State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China
[2]School of Automation, Southeast University, Nanjing 210096, China

***Abstract*—As the wind power generation capacity increases continuously, the vulnerability of the wind turbine communication system is gradually exposed. In particular, the Ethernet-based communication link is easily utilized by attackers to implement replay attacks, leading to erroneous transmission of measurement signals. This paper presents a resilient control strategy based on a switching mechanism to address the problem of replay attacks on rotor speed measurement signals in wind turbines. Firstly, the dynamics of wind turbine system and replay attack model are established. Then, a neural network-based state estimator is developed to compensate for the erroneous rotor speed measurement signal caused by the attack. Finally, a switching-type resilient control algorithm is presented to mitigate the effect of the attack, and comprehensive studies are executed on a 1.5 MW wind turbine in FAST software. The simulation results illustrate the efficacy of the developed resilient control scheme in mitigating the effects of the replay attack and maintaining the expected performance of wind turbines.**

***Index Terms*—wind turbine, rotor speed, replay attack, resilient control**

I. Introduction

As the wind energy industry continues to expand globally, the cyberphysical security of wind turbines is critical to ensuring the safety and stability of the entire power grid [1]–[3]. In response to the vulnerability of the wind turbine control system, the attacker can utilize the Ethernet-based communication link to gain access to the control network and implement a replay attack to cause an incorrect transmission of information on the sensor-controller link, which may lead to possible failures, shutdowns, and damages to the physical processes of wind turbines [4]–[6]. Currently, there have been exploratory studies on analyzing the communication vulnerability and the impact of several common attacks on wind turbines [6]–[8]. To mention a few, it was demonstrated in [6] that the attacker could easily access a wind turbine or wind farm control network and conduct a cyber-attack on wind turbine by issuing control commands, which ultimately resulted in the slowdown and stopping of the wind turbines. The authors in [7] illustrated the scenario in which the sensor-controller communication link utilizing the Ethernet protocol in a wind turbine was exploited by an attacker to implement the time-delay attack, and the corresponding impacts of attack were analyzed. In [8], cyber attack scenarios involving cyber components or networks were taken into account in the architecture of the integrated SCADA/EMS system of wind farm, which subsequently affected the overall reliability and performance of the power system.

To mitigate the impact of cyber attacks and guarantee the restoration of system operation, considerable researches [9]–[14] have been conducted on defense control based on conventional control and compensation methods. For example, an adaptive resilient control scheme was introduced in [9] for wind turbines in the low-speed operating region, specifically to mitigate the impact of false data injection (FDI) attacks. In [10], the authors introduced a modified receding-horizon control law to counteract replay attacks and examined the resulting degradation in system performance. A dual-triggered resilient torque control strategy was designed in [11] for wind turbines to defend against denial-of-service (DoS) attacks. Liu *et al.* in [12] introduced a proactive distributed detection and localization framework to defend against the stealthy deception attacks in DC microgrids. However, the aforementioned research findings primarily concentrated on attack behaviors that include FDI and DoS attacks on wind turbines or other attacks on power systems, and there is still a lack of impact analysis of replay attacks and the construction of corresponding protection measures in wind turbines.

Based on the above discussions, this paper aims to establish a resilient control scheme for wind turbine against replay attacks, and the main contributions can be summarized as follows:

1) Based on the system dynamics and communication vulnerability of wind turbine control system, a replay attack model aiming at causing measurement signal errors is constructed in this paper.
2) A neural network-based state estimator is designed to compensate for abnormal rotor speed signals, which can

This work was supported in part by the National Natural Science Foundation of China under Grants 62403418, 92467301, and U21A20478, in part by the China Postdoctoral Science Foundation under Grant 2023M743007, in part by the Postdoctoral Fellowship Program of CPSF under Grant GZC20232289, in part by the National Key R&D Program of China under Grant 2021YFD1400200, in part by the Frontier Technologies R&D Program of Jiangsu under Grant BF2024065, in part by the Natural Science Foundation of Zhejiang Province under Grant LR23F030001, in part by the Zhejiang High-Level Talents Special Support Program under Grant 2021R52002, in part by the State Key Laboratory of Industrial Control Technology under Grant ICT2024A13, and in part by the Baima Lake Laboratory Joint Funds of the Zhejiang Provincial Natural Science Foundation of China under Grant LBMHD24F030001.

solve the problem of real-time signal compensation in the control system of the wind turbine with nonlinear dynamics.

3) The resilient control algorithm based on the switching mechanism is established to achieve the improvement of output tracking performance and system operation safety of the wind turbine, and the simulation results are provided to demonstrate the effectiveness of the proposed scheme.

II. Problem Statement

TABLE I
Symbol Description

Notations	Descriptions
A_T	Aerodynamic torque
ρ	Air density
D_c	Damping factor
G_T	Electromagnetic torque
M_c	Equivalent moment of inertia
β	Pitch angle
$C_P(\lambda,\beta)$	Power coefficient
$C_{P\max}$	Maximum power factor
R	Rotor radius
ξ_r	Rotor speed
λ	Tip speed ratio
v	Wind speed

A. System Model

The physical structure of the wind turbine shown in Fig. 1 is considered in this paper, which is mainly composed of rotor, generator, and drive-train, etc. The main operating process can be summarized as follows: 1) The wind turbine utilizes wind power to rotate and convert wind energy into mechanical energy; 2) The drive-train is used to increase the speed and drive the generator to produce electricity; 3) The generator converts mechanical energy into electrical energy and feeds it into the grid.

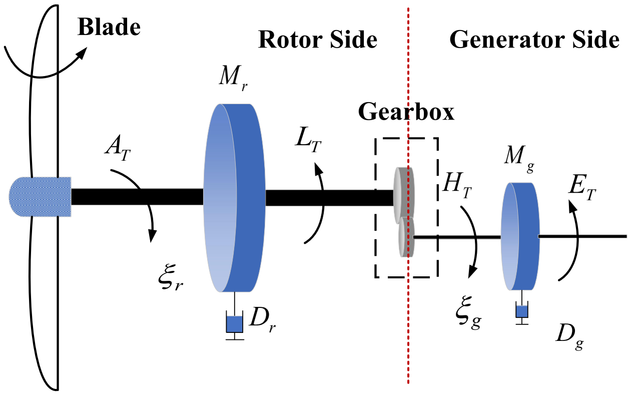

Fig. 1. The wind turbine structure with a drive-train.

By mathematically modeling the above wind turbine, the captured power is represented by the expression of

$$P_a = \frac{1}{2}\rho\pi R^2 C_P(\lambda,\beta)v^3 \tag{1}$$

Furthermore, the output power of the wind turbine can be expressed as

$$P_a = \xi_r A_T \tag{2}$$

with $A_T = \frac{1}{2\lambda}\rho\pi R^3 C_P(\lambda,\beta)v^2$.

The dynamic behavior of the rotor and generator system can be modeled as

$$\begin{cases} M_r\dot{\xi_r} = A_T - D_r\xi_r - L_T \\ M_g\dot{\xi_g} = H_T - D_g\xi_g - E_T \end{cases} \tag{3}$$

Let $r_g = \xi_g/\xi_r = L_T/H_T$ denote the gear box ratio, the system dynamics of wind turbine can be expressed as

$$M_c\dot{\xi_r} = A_T - D_c\xi_r - G_T \tag{4}$$

where $M_c = M_r + n_g^2 M_g$, $D_c = D_r + r_g^2 D_g$, and $G_T = r_g E_T$.

B. Threat Model

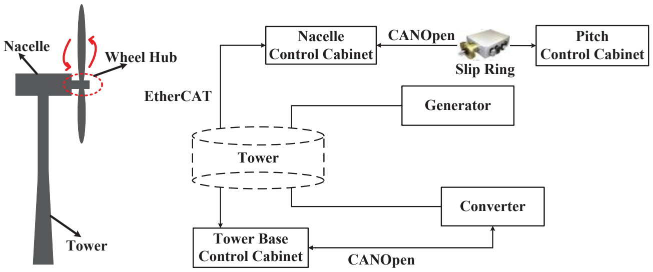

Fig. 2. Communication architecture in the wind turbine control loop.

According to the operating principles of the wind turbine, the optimal torque control strategy with fixed pitch angle is applied to the wind turbine operating in the low-speed region, and the generator torque is adjusted according to the rotor speed to realize the maximum capture of wind energy. Based on the communication framework in the control loop of the wind turbine (see Fig. 2), the typical EtherCAT communication protocol employed in the control loop can be parsed and exploited by the attacker to replay the rotor speed data. Therefore, the presence of replay attacks in the measurement channel is considered in this paper. According to the operational characteristics of wind turbine, the considered replay attacks may cause overloading of the drive-train, decrease the generated power, or even jeopardize the operational safety of the wind turbines. Such replay attacks that lead to erroneous measurement signals can be constructed as

$$O_a(t) = \begin{cases} \xi_r(t), & \text{no attack} \\ \xi_r(t-t_a), & \text{replay attack} \end{cases} \tag{5}$$

where $\xi_r(t-t_a)$ denotes the measurement signal being replayed, and t_a represents the replayed time length.

C. Problem Statement and Control Objective

Considering the wind turbine dynamics (4) with $O(t) = \xi_r(t)$ and G_T being the output and input of the system, the aim of this research is to develop a resilient control framework for wind turbines operating in low-wind-speed environments to counteract the effects of replay attacks. For the considered wind turbines, the generator torque is regulated to optimize wind energy capture, which can be expressed as

$$P_d = \frac{1}{2}\rho\pi R^2 C_{P\,\max} v^3 \tag{6}$$

The system error is defined as $\varrho(t) = O(t) - O_d(t)$, where $O_d(t) = \xi_{ropt}(t)$ denotes the optimum output value. The tracking objective can be attained if there exists a convergence rate $A_m > 0$ that satisfies

$$||O(t) - O_d(t)||^2 \le \varrho^{-A_m(t-t_0)} ||\varrho(t_0)||^2 + \Omega \tag{7}$$

where $\Omega > 0$ is a constant.

The primary restriction imposed on the expected tracking reference is elaborated in the subsequent assumption.

Assumption 1: The ideal value of the system output and its time derivative are kept within the bounds of $|O_d(t)| < \bar{O}_d$ and $|\dot{O}_d(t)| < \bar{O}_{d1}$, with the unknown constants $\bar{O}_d > 0$ and $\bar{O}_{d1} > 0$.

III. Main Results

A. Neural Network-based State Estimator Design

Considering that the occurrence of replay attacks can lead to erroneous measurement signal ξ_r and the variation of A_T, a neural network-based state estimation architecture is used and enables real-time reconstruction of A_T in wind turbines.

The neural network output is expressed as

$$W(X) = \Phi^T \Lambda(H^T X) \tag{8}$$

where X is the input of neural network, $\Lambda(\cdot)$ denotes the activation function, H and Φ represent the weights of hidden layer and output layer.

The approximation ability of neural networks has been demonstrated by many existing results and can be specified as Lemma 1 in [11]. Furthermore, the smooth function A_T with respect to the rotor speed ξ_r can be approximated using a neural network as

$$A_T(\xi_r) = \Phi^T \Lambda(\xi_r) + \iota(\xi_r),\ |\iota(\xi_r)| \le \epsilon \tag{9}$$

where the ideal weight vector Φ is difficult to obtain directly and will be estimated as $\hat{\Phi}$ for the purpose of controller design, $\Lambda(\xi_r)$ is a hyperbolic tangent function and satisfies $\Lambda^T(\xi_r)\Lambda(\xi_r) \le N$ with N representing the number of neural network nodes, $\iota(\xi_r)$ represents the estimated error, and $\epsilon > 0$ is a constant.

Based on the approximation capability of neural network and the dynamics of wind turbine, the following state estimator is designed to estimate the sensor information.

$$\begin{cases} M_c\dot{\hat{\xi}}_r = \hat{A}_T(\hat{\xi}_r(t)) - D_c\hat{\xi}_r(t) - G_T + G(O_a(t) - \hat{\xi}_r(t)), \\ \hat{O}(t) = \hat{\xi}_r(t) \end{cases} \tag{10}$$

where $\hat{\xi}(t)$ denotes the estimation of $\xi_r(t)$ with the error being $\vartheta(t) = \xi_r(t) - \hat{\xi}_r(t)$, $\hat{A}_T(\hat{\xi}_r(t)) = \hat{\Phi}^T\Lambda(\hat{\xi}_r)$ represents the estimation of $A_T(\xi_r(t))$, $\hat{\Phi}$ denotes the estimation of Φ with $\tilde{\Phi} = \Phi - \hat{\Phi}$ as the estimated error, and $G > 0$ is a coefficient.

B. Switching Resilient Control Strategy

Considering the attack model (5) with $\xi_r(t - t_a)$ as the replayed rotor speed information, the whole operation process of wind turbine from t_0 to t_∞ can be categorized into two cases.

Case 1: When the wind turbine operates with a reliable communication environment without attack, the system dynamic of wind turbine can be expressed as

$$\begin{cases} M_c\dot{\xi}_r(t) = A_T(\xi_r(t)) - D_c\xi_r(t) - G_T(t), \\ O(t) = \xi_r(t) \\ O_a(t) = \xi_r(t) \end{cases} \tag{11}$$

The feedback torque controller is established with the form of

$$G_T(t) = A_T(\xi_r(t)) - D_c\xi_r(t) - M_c\dot{O}_d(t) + \kappa_1\varrho(t) \tag{12}$$

where $\kappa_1 > 0$ is the controller coefficient.

Case 2: When an attacker intercepts the rotor speed measurement information and replays it, the system controller receives the replayed data of the rotor speed. The compromised system can be described in terms of its dynamics as

$$\begin{cases} M_c\dot{\xi}_r(t) = A_T(\xi_r(t)) - D_c\xi_r(t) - G_T(t), \\ O(t) = \xi_r(t) \\ O_a(t) = \xi_r(t - t_a) \end{cases} \tag{13}$$

To compensate for the attacked rotor speed signal, the neural network-based state estimator (10) is adopted, and the dynamics of estimated error $\vartheta(t)$ is expressed as

$$\begin{aligned} \dot{\vartheta}(t) \ &= \ \frac{1}{M_c}\Big[A_T(\xi_r(t)) - \hat{A}_T(\hat{\xi}_r(t)) - D_c\vartheta(t) \\ &\quad -G(O_a(t) - \hat{\xi}_r(t))\Big] \end{aligned} \tag{14}$$

Construct the torque controller and adaptive law in the form of

$$\begin{aligned} G_T(t) \ &= \ \hat{A}_T(\hat{\xi}_r(t)) + G\hat{\xi}_r(t) - D_cO_d(t) - M_c\dot{O}_d(t) \\ &\quad +\kappa_2(\hat{\xi}_r(t) - O_d(t)) \end{aligned} \tag{15}$$

$$\dot{\hat{\Phi}}(t) \ = \ \frac{1}{M_c}(\hat{\xi}_r(t) - O_d(t))\Lambda(\hat{\xi}_r(t)) + \kappa_3\hat{\Phi}(t) \tag{16}$$

where $\kappa_2 > 0$ and $\kappa_3 > 0$ denote the gains of controller and adaptive law, respectively.

C. Stability Analysis

Based on the system dynamic (4), the derivative of system error $\varrho(t) = O(t) - O_d(t)$ can be obtained by

$$\dot{\varrho}(t) = \frac{1}{M_c}(A_T(\xi_r(t)) - D_c\xi_r(t) - G_T(t)) - \dot{O}_d(t) \tag{17}$$

Theorem 1: Consider the dynamics of wind turbine (4) and the desired rotor speed reference O_d, by adopting the proposed switching resilient control laws (12) and (15), and with the parameters satisfying $2D_c - 2G - \kappa_2 - 5 > 0$ and $\kappa_3 > 2N/M_c$, as well as the estimator (10) and adaptive law (16), the wind turbine can realize the expected control objective while being subjected to a replay attack.

Proof 1: See Appendix.

IV. Simulation Validations

To evaluate the ability of the proposed controller to address the adverse effects of attacks and restore secure operation of the wind turbine, a 1.5MW wind turbine is replicated using the FAST code with its characteristics detailed in Table II.

TABLE II
Wind Turbine Configurations

Parameters	Values
Rated power (P_N)	1.5 MW
Air density (ρ)	1.225 kg/m^3
Rotor radius (R)	35 m
Number of blades	3
External rotor damping (D_r)	45.52 N·m/(rad·s)
Rotor inertia (M_r)	4950000 kg·m^2
Gear box ratio (r_g)	87.965
External generator damping (D_g)	0.4 N·m/(rad·s)
Generator inertia (M_g)	90 kg·m^2
Maximum power ratio ($C_{P\,\max}$)	0.412

In this paper, TurbSim is utilized to generate Kaimal turbulent wind speed data with the average speed and the turbulence intensity set to 6 m/s and 10% (see Fig. 3). The relevant parameters in the control algorithm are configured as $\kappa_1 = 5$, $\kappa_2 = 0.005$, $\kappa_3 = 0.001$, $G = 0.001$, and the sampling period is 0.01s.

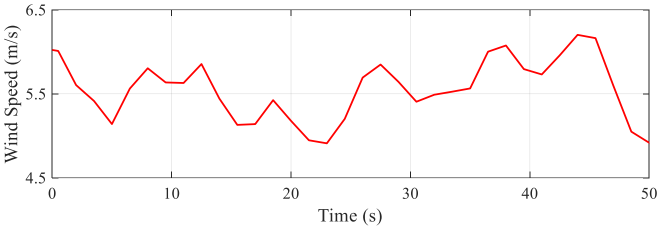

Fig. 3. Wind speed profile.

A. Wind Turbine Operation Without Attack

This section considers an operational scenario in which no attack occurs in the wind turbine control system. The simulation results regarding the system output and control performance are displayed in Fig. 4.

As depicted in Fig. 4, the output of wind turbine consistently tracks its expected trajectory throughout the full running process (see Fig. 4(a)), and the rotor speed tracking error and generator torque vary smoothly with acceptable fluctuations (see Figs. 4(b) and 4(c)).

B. Validations of the Switching Resilient Control Algorithm Under Replay Attacks

1) Intermittent Attack: To verify the performance of the proposed controller against replay attacks, two sets of attack parameters are considered with start times being 3s and 4s, durations being 10s and 16s, and replayed steps being 100 and 200, respectively. The output performance of the wind turbine under two attack conditions is depicted in Figs. 5-6, respectively.

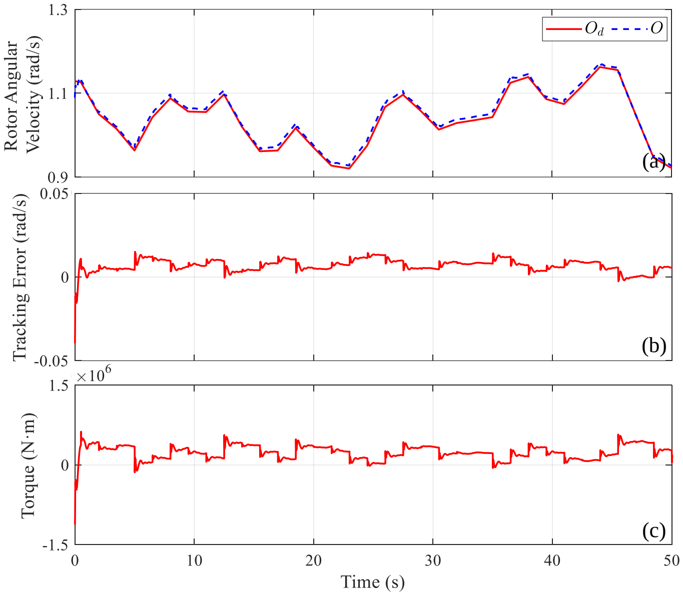

Fig. 4. Results of the wind turbine without attack. (a) System output and the desired reference. (b) Output tracking error. (c) Torque control performance.

Firstly, the attack with replayed time step being 100 is considered with the results shown in Fig. 5. It can be concluded from Fig. 5 that the resilient controller ensures higher tracking accuracy of the system output compared to the conventional method (see Fig. 5(a)), with the error scopes of 0.05 rad/s and 0.2 rad/s, respectively (see Fig. 5(b)). As shown in Fig. 5(c), the controller exhibits smooth variations within a small range under the proposed control method, whereas it experiences abrupt changes at the termination of the attack when using the traditional feedback control method.

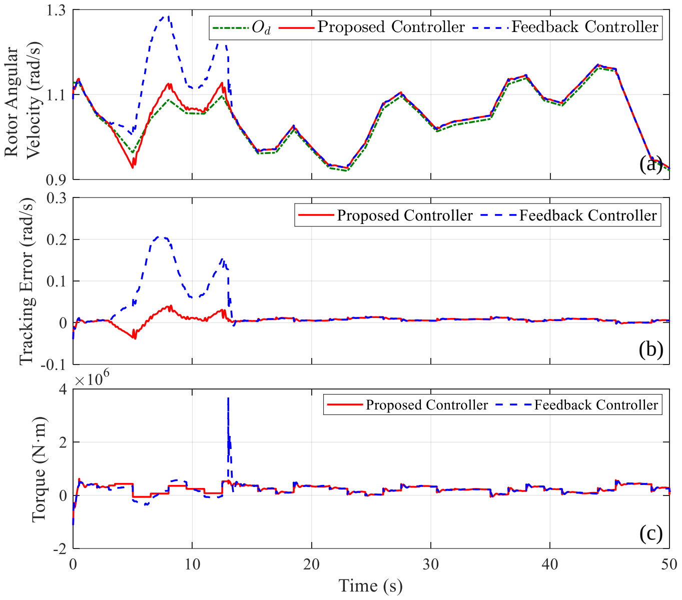

Fig. 5. Results of control methods against replay attack with replayed time step being 100. (a) System output and the desired reference. (b) Output tracking error. (c) Torque control performance.

To further assess the proposed scheme, this section also examines an attack scenario where the replayed time step is set to 200, and the results are presented in Fig. 6. A comparison of the results in Figs. 5 and 6 reveals that when the attack intensity increases, the proposed method still ensures that the output tracking error and generator torque remain within the expected range. However, the output error and generator torque are both doubled when using the traditional control method.

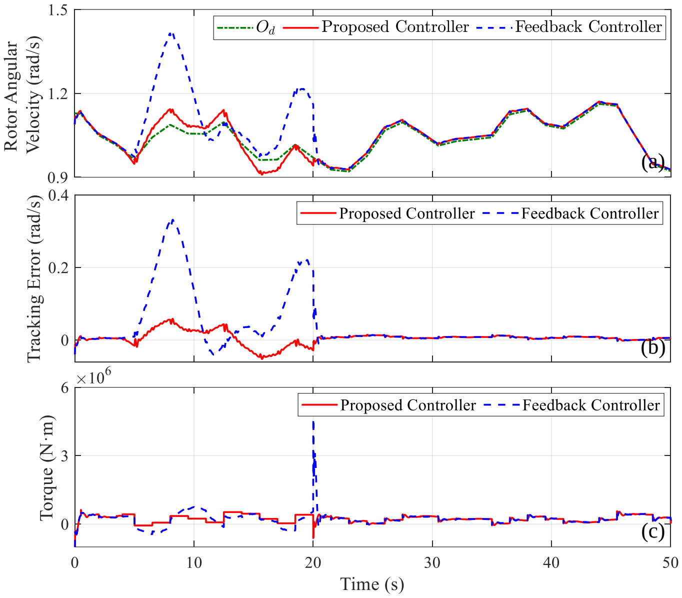

Fig. 6. Results of control methods against replay attack with replayed time step being 200. (a) System output and the desired reference. (b) Output tracking error. (c) Torque control performance.

2) Persistent Attack: To evaluate the ability of the proposed control method to enhance the resilience and recovery of wind turbines against the replay attacks, five persistent attacks with different replayed time steps are considered in this section, and comparative simulation results for the resilient and feedback control methods are given in Table III.

In this section, the full operation time is set to 200s with a sampling period of 0.01s. As shown in Table III, for the wind turbines subjected to the five types of attacks, the proposed resilient control method ensures full-time operation of the system and significantly extends the operation time as opposed to the conventional feedback control approach. In contrast, the conventional feedback controller fails to mitigate the impact of the replay attacks, leading to system faults or shutdowns that halt the operation of the wind turbine.

Therefore, it is evident that the proposed control method surpasses the traditional control method with regard to mitigating the impact of attacks and restoring operational performance for the wind turbines facing replay attacks.

TABLE III
PERFORMANCE COMPARISON (OPERATING STATUS) WITH RESILIENT/FEEDBACK CONTROL METHODS FOR WIND TURBINE AGAINST PERSISTENT REPLAY ATTACKS

Attack Situations (Replayed Time Step)	Operating Status	
	Resilient Control (Extended Operation Time)	Feedback Control (Early Termination)
200	177.5s	Fault Alert
400	176.41s	
600	172.64s	
800	165.27s	
1000	138.63s	Shutdown

V. Conclusion

In this paper, a switching-type resilient control strategy has been proposed for the wind turbine with the rotor speed measurement signal being attacked. Firstly, a replay attack model leading to the unreliable data transmission over the sensor-controller link in wind turbine has been established. Then, a neural network-based state estimator has been developed to correct the compromised data, and a switching-type resilient control algorithm has been proposed to realize the desired control objective for wind turbine. Finally, simulation results have confirmed the capability of the presented control method to retain the desired operation of the wind turbine subjected to the replay attack.

Appendix

Proof of Theorem 1

Choose the Lyapunov function given by

$$P(t) = \begin{cases} P_1(t), & \text{no attack} \\ P_2(t), & \text{attack occurs} \end{cases} \tag{18}$$

where $P_1(t) = \frac{1}{2}\varrho^2(t)$, $P_2(t) = \frac{1}{2}\varrho^2(t) + \frac{1}{2}\vartheta^2(t) + \frac{1}{2}\tilde{\Phi}^T(t)\tilde{\Phi}(t)$.

Case 1: When the wind turbine operates under reliable communication without attack, the Lyapunov function becomes

$$P(t) = P_1(t) = \frac{1}{2}\varrho^2(t) \tag{19}$$

Based on (12), the time derivative of (19) can be derived by

$$\begin{aligned} \dot{P}_1(t) &= -\frac{\kappa_1}{M_c}\varrho^2(t) \\ &\leq -A_1 P_1(t) + B_1 \end{aligned} \tag{20}$$

where $A_1 = \frac{2\kappa_1}{M_c}$, $B_1 = 0$.

Case 2: When the replay attack is implemented, the controller receives the wrong rotor speed information, and the Lyapunov function $P(t)$ in (18) becomes

$$P(t) = P_2(t) = \frac{1}{2}\varrho^2(t) + \frac{1}{2}\vartheta^2(t) + \frac{1}{2}\tilde{\Phi}^T(t)\tilde{\Phi}(t) \tag{21}$$

In terms of (10) and (15), differentiating (21) with time t yields

$$\begin{aligned} \dot{P}_2(t) = &\frac{1}{M_c}[\varrho(t)+\vartheta(t)] \times \left[A_T(\xi_r(t)) - \hat{A}_T(\hat{\xi}_r(t))\right] \\ &-\frac{G}{M_c}\left[\varrho(t)\hat{\xi}_r(t) + \vartheta(t)(O_a(t) - \hat{\xi}_r(t))\right] \\ &-\frac{\kappa_2}{M_c}\varrho(t)\left[\hat{\xi}_r(t) - O_d(t)\right] - \tilde{\Phi}^T(t)\dot{\hat{\Phi}}(t) \\ &-\frac{D_c}{M_c}\left[\varrho^2(t) + \vartheta^2(t)\right] \end{aligned} \tag{22}$$

Based on the relationship between the variables and Young's inequality, the following relationships are obtained.

$$-\frac{G}{M_c}\left[\varrho(t)\hat{\xi}_r(t)+\vartheta(t)(O_a(t)-\hat{\xi}_r(t))\right] \le \frac{G}{M_c}\left(\vartheta^2(t)+\bar{O}_d^2+\xi_N^2\right) \quad (23)$$

$$-\frac{\kappa_2}{M_c}\varrho(t)\left[\hat{\xi}_r(t)-O_d(t)\right] \le \frac{\kappa_2}{2M_c}\left(-\varrho^2(t)+\vartheta^2(t)\right) \quad (24)$$

where $\xi_N > 0$ denotes the rated value of the rotor speed. Combining the above two inequalities, $\dot{P}_1(t)$ can be calculated as

$$\begin{aligned}\dot{P}_2(t) \le & -\frac{2D_c+\kappa_2}{2M_c}\varrho^2(t)-\tilde{\Phi}^T(t)\dot{\hat{\Phi}}(t)+\frac{1}{M_c}\left(\varrho(t)+\vartheta(t)\right)\times \\ & \left[\tilde{\Phi}^T\Lambda(\hat{\xi}_r(t))+\Phi^T\Lambda(\xi_r(t))-\Phi^T\Lambda(\hat{\xi}_r(t))+\iota(\xi_r(t))\right] \\ & -\frac{2D_c-2G-\kappa_2}{2M_c}\vartheta^2(t)+\frac{G}{M_c}\left(\bar{O}_d^2+\xi_N^2\right) \quad (25)\end{aligned}$$

Based on (16) and the following inequalities

$$\begin{aligned}&\frac{1}{M_c}\left(\varrho(t)+\vartheta(t)\right)\times\left[\Phi^T\Lambda(\xi_r(t))-\Phi^T\Lambda(\hat{\xi}_r(t))+\iota(\xi_r(t))\right] \\ &\qquad \le \frac{3}{2M_c}\left(\varrho^2(t)+\vartheta^2(t)\right)+\frac{2N}{M_c}||\Phi||^2+\frac{1}{M_c}\epsilon^2 \quad (26)\end{aligned}$$

$$\begin{aligned}&\frac{1}{M_c}\Big(\varrho(t)+\vartheta(t)-\hat{\xi}_r(t)+O_d(t)\Big)\tilde{\Phi}^T\Lambda(\hat{\xi}_r(t)) \\ &\qquad \le \frac{1}{M_c}\vartheta^2(t)+\frac{N}{M_c}||\tilde{\Phi}||^2 \quad (27)\end{aligned}$$

$$\kappa_3\tilde{\Phi}\hat{\Phi} \le -\frac{\kappa_3}{2}||\tilde{\Phi}||^2+\frac{\kappa_3}{2}||\Phi||^2 \quad (28)$$

(25) can be derived by

$$\begin{aligned}\dot{P}_2(t) \quad \le \quad & -\frac{2D_c+\kappa_2-3}{2M_c}\varrho^2(t)-\frac{2D_c-2G-\kappa_2-5}{2M_c}\vartheta^2(t) \\ & -(\frac{\kappa_3}{2}-\frac{N}{M_c})||\tilde{\Phi}||^2+(\frac{2N}{M_c}+\frac{\kappa_3}{2})||\Phi||^2+\frac{1}{M_c}\epsilon^2 \\ & +\frac{G}{M_c}\left(\bar{O}_d^2+\xi_N^2\right) \\ \le \quad & -A_2P_2(t)+B_2 \quad (29)\end{aligned}$$

where $A_2=\min\{\frac{2D_c+\kappa_2-3}{M_c},\frac{2D_c-2G-\kappa_2-5}{M_c},\kappa_3-\frac{2N}{M_c}\}$, $B_2=(\frac{2N}{M_c}+\frac{\kappa_3}{2})||\Phi||^2+\frac{1}{M_c}\epsilon^2+\frac{G}{M_c}\left(\bar{O}_d^2+\xi_N^2\right)$.

Based on the above analysis, in combination with the two cases of the wind turbine, the following relation of $\dot{P}(t)$ holds

$$\dot{P}(t) \le -A(t)P(t)+B(t) \quad (30)$$

where

$$A(t)=\begin{cases} A_1, & \text{no attack} \\ A_2, & \text{attack occurs}\end{cases}$$

$$B(t)=\begin{cases} 0, & \text{no attack} \\ B_2, & \text{attack occurs}\end{cases}$$

Iterating over (30), there has

$$P(t) \le (\frac{1}{2})^2\varrho^{-A_m(t-t_0)}P(t_0)+\frac{B_M}{A_m} \quad (31)$$

where $A_m=\min\{A_1,A_2\}$, $B_M=B_2$. For $t\in[t_0,t_\infty]$, based on (18) and (31), the following relation can be obtained:

$$\varrho^2(t) \le \varrho^{-A_m(t-t_0)}||\varrho(t_0)||^2+\frac{2B_M}{A_m} \quad (32)$$

As seen in (32), the control objective of the proposed scheme (7) holds, with $\Omega=\frac{2B_M}{A_m}$.

Theorem 1 has been proved.

References

[1] "Roadmap for wind cybersecurity," U.S. Department of Energy, Jul. 2020. https://www.energy.gov/eere/wind/articles/roadmap-wind-cybersecurity.

[2] "Global wind report 2024," GWEC, 2024. https://www.gwec.net/reports/globalwindreport.

[3] "Distributed Wind Market Report: 2023 Edition," U.S. Department of Energy, 2023. https://www.energy.gov/eere/wind/articles/distributed-wind-market-report-2023-edition.

[4] S. Zhao, J. Xia, R. Deng, P. Cheng, and Q. Yang, "Anomaly observer based cyber-resilient torque control against hybrid attacks in wind turbines," IEEE Transactions on Smart Grid, vol. 15, no. 6, pp. 6080-6091, Nov. 2024.

[5] M. Mohammadpourfard, A. Sami, and Y. Weng, "Identification of false data injection attacks with considering the impact of wind generation and topology reconfigurations," IEEE Transactions on Sustainable Energy, vol. 9, no. 3, pp. 1349-1364, Jul. 2018.

[6] J. Staggs, D. Ferlemann, and S. Shenoi, "Wind farm security: attack surface, targets, scenarios and mitigation," International Journal of Critical Infrastructure Protection, vol. 17, pp. 3-14, Jun. 2017.

[7] S. Zhao, J. Xia, R. Deng, P. Cheng, and Q. Yang, "Adaptive observer-based resilient control strategy for wind turbines against time-delay attacks on rotor speed sensor measurement," IEEE Transactions on Sustainable Energy, vol. 14, no. 3, pp. 1807-1821, Jul. 2023.

[8] Y. Zhang, Y. Xiang, and L. Wang, "Power system reliability assessment incorporating cyber attacks against wind farm energy management systems," IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2343-2357, Sep. 2017.

[9] S. Zhao, Q. Yang, P. Cheng, R. Deng, and J. Xia, "Adaptive resilient control for variable-speed wind turbines against false data injection attacks," IEEE Transactions on Sustainable Energy, vol. 13, no. 2, pp. 971-985, Apr. 2022.

[10] M. Zhu, and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," IEEE Transactions on Automatic Control, vol. 59, pp. 804-808, Mar. 2014.

[11] S. Zhao, J. Xia, R. Deng, P. Cheng, Q. Yang, and X. Jiao, "Dual-triggered adaptive torque control strategy for variable-speed wind turbine against denial-of-service attacks," IEEE Transactions on Smart Grid, vol. 14, no. 4, pp. 3072-3084, Jul. 2023.

[12] M. Liu, C. Zhao, J. Xia, R. Deng, P. Cheng and J. Chen, "PDDL: Proactive Distributed Detection and Localization Against Stealthy Deception Attacks in DC Microgrids," IEEE Transactions on Smart Grid, vol. 14, no. 1, pp. 714-731, Jan. 2023.

[13] S. Liu, X. Cheng, H. Yang, Y. Shu, X. Weng, P. Guo, K. Zeng, G. Wang, and Y. Yang, "Stars Can Tell: A robust method to defend against GPS spoofing attacks using off-the-shelf chipset," 30th USENIX Security Symposium (USENIX Security 21), pp. 3935-3952, Aug. 2021.

[14] X. Guo, L. Tan, T. Chen, C. Gu, Y. Shu, S. He, Y. He, J. Chen, and L. Shangguan, "Exploring biomagnetism for inclusive vital sign monitoring: Modeling and implementation," 30th Annual International Conference on Mobile Computing and Networking (ACM MobiCom 24), pp. 93–107, Nov. 2024.