Journal of Electronic Research and Application, 2026, Volume 10, Issue 3
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

A Zero-Dynamics Attack Detection Method for Offshore Wind Power Systems

Kaige Chen, Hongran Li, Zeyu Zhang, Zhaoman Zhong, Lei Hu

School of Computer Engineering, Jiangsu Ocean University, Lianyungang 222005, Jiangsu, China

Abstract: With the increase in the scale and complexity of offshore wind power systems, zero-dynamics attacks pose a severe threat to the cyber security of such systems. Their concealment makes them difficult to detect using traditional output observation-based methods. To address this problem, this paper proposes a zero-dynamics attack detection framework integrating adaptive watermarking and Kalman filtering, which achieves effective attack identification by embedding an adaptive watermark into the system input and conducting residual analysis. Simulation results show that the proposed method can quickly detect zero-dynamics attacks without affecting the normal operation of the system.

Keywords: Zero-dynamics attack; Adaptive watermarking; Kalman filtering; Residual detection

Online publication: April 22, 2026

1. Introduction

With the growth of global energy demand, offshore wind power has become an important direction for energy transition. The increase in the scale and complexity of offshore wind power systems has brought new cyber security challenges [1].

In cyber-physical systems (CPS), attackers can threaten infrastructure by manipulating control systems [2,3]. In smart grids, cyber-physical attacks mainly include false data injection and denial-of-service attacks. As a type of covert attack, zero-dynamics attacks can manipulate the internal states of a system without significantly altering its output, making it difficult for traditional output observation-based detection methods to identify such attacks in a timely manner [4–7].

Existing research has mainly focused on false data injection and denial-of-service attacks, with relatively few studies on zero-dynamics attacks [8,9]. Hoehn *et al.* enhances attack detectability by introducing a modulation matrix but alters the system structure [10]. Wang *et al.* constructs an output prediction model based on the Byrnes-Isidori normal form, which is complex to implement and relies on a complete system model [11].

To solve the above problems, this paper proposes a zero-dynamics attack detection framework integrating adaptive watermarking and Kalman filtering, which realizes the rapid identification of zero-dynamics attacks

through residual analysis without affecting the normal operation of the system.

2. Offshore wind power generation systems

2.1. Structure of offshore wind power generation systems

An offshore wind power system consists of a wind turbine array, an offshore substation and a control center, as shown in **Figure 1**, and its monitoring and control are realized through a SCADA system [12]. The introduction of communication networks also brings security risks, as attackers may inject malicious signals through the network to interfere with system operation [13].

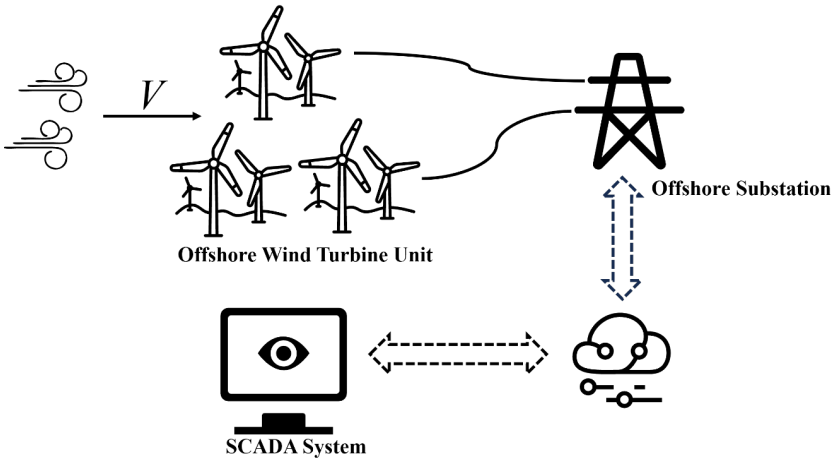

Figure 1. Structure of offshore wind power generation system.

1.2 Model of offshore wind power generation systems

To analyze the impact of attack signals on offshore wind power systems, an equivalent circuit model of the offshore wind power system is constructed based on the findings of Le *et al.*, as shown in **Figure 2** [14]. The branch voltage balance equation is given by:

$$U = U_C - i_L R_2 - L\frac{di_L}{dt} \tag{1}$$

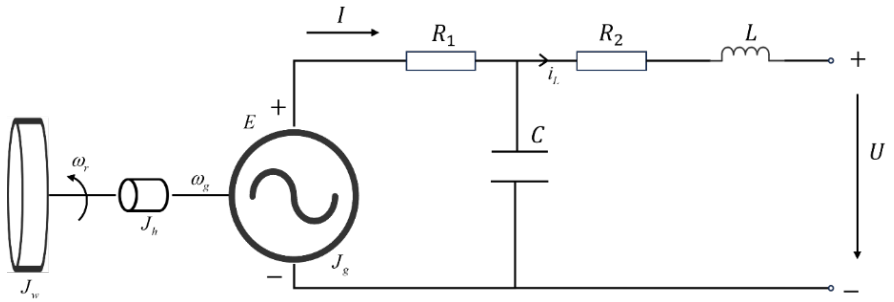

Figure 2. Equivalent circuit of the offshore wind power system.

Based on Kirchhoff's voltage and current laws, we obtain:

$$U_C = E - U_{R1} \tag{2}$$

$$i_L = I - i_C \tag{3}$$

The generator is modeled as an internal voltage source, whose induced electromotive force is proportional to the rotational speed:

$$E = K_g \omega_g \tag{4}$$

The torque balance equation is:

$$J\frac{d\omega_g}{dt} = K_t I \tag{5}$$

where K_t and K_g are the electromagnetic torque constant and back electromotive force constant, respectively; i is the current; J is the total moment of inertia, and:

$$J = J_w + J_g + J_h \tag{6}$$

Substituting **Equation (2)** and **(3)** into **Equation (1)**, we get:

$$U = K_g\left(a_0\frac{d\omega_g}{dt} + a_1\frac{d^2\omega_g}{dt^2} + a_2\frac{d^3\omega_g}{dt^3} + \omega_g\right) \tag{7}$$

where $a_0 = \frac{R_2CK_tK_g - J(R_1+R_2)}{K_tK_g}$, $a_1 = \frac{LCK_tK_g - JL - JCR_1R_2}{K_tK_g}$, $a_2 = -\frac{JLCR_1}{K_tK_g}$.

Applying the Laplace transform to **Equation (7)** and simplifying it, the system transfer function is obtained as:

$$G_1(s) = \frac{\omega(s)}{U(s)} = \frac{K}{a_2s^3 + a_1s^2 + a_0s + 1} \tag{8}$$

where is the system gain.

After introducing a PI controller $G_2(s) = \frac{k_ps + k_i}{s}$, the system model is expressed as:

$$G(s) = \frac{G_1G_2}{1 + G_1G_2} = \frac{K(k_ps + k_i)}{a_2s^4 + a_1s^3 + a_0s^2 + (Kk_p + 1)s + Kk} \tag{9}$$

Rewriting **Equation (9)** in the continuous-time state-space form:

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{10a}$$

$$y(t) = Cx(t) \tag{10b}$$

Where $A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -Kk_i & -Kk_p - 1 & -a_0 & -a_1 \end{bmatrix}$, $B = [0 \quad 0 \quad 0 \quad 1]^T, C = [Kk_i \quad Kk_p \quad 0 \quad 0]$.

The discrete-time state-space model is derived by discretizing **Equation (10)** using the zero-order hold method:

$$x[k+1] = A_dx[k] + B_du[k] \tag{11a}$$

$$y[k] = C_dx[k] \tag{11b}$$

where $A_d = e^{AT}$, $B_d = A^{-1}(e^{AT} - I)B$.

2. Zero-dynamics attack mechanism

A prerequisite for implementing a zero-dynamics attack is the existence of unstable zeros in the system. It can be seen from **Equation (9)** that the relative degree of the system is 3. According to Weller *et al.*, at least one unstable sampling zero will be inevitably introduced after discretization when the system meets specific conditions [15]. Therefore, the system described by **Equation (9)** is vulnerable to zero-dynamics attacks.

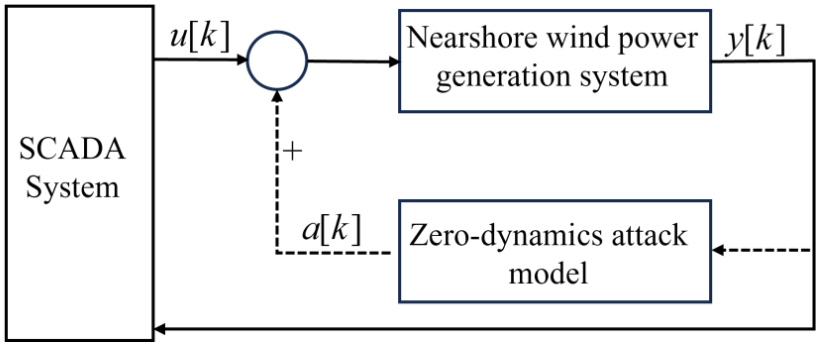

Figure 3. Zero-dynamics attack mechanism.

As shown in **Figure 3**, the attacker generates an attack signal by constructing an auxiliary internal state for zero-dynamics and injects it into the system input. Thus, the attacker usually constructs the following zero-dynamics attack model:

$$z[k+1] = A_i z[k] \tag{12a}$$

$$a[k] = C_i z[k] \tag{12b}$$

After the attack, **Equation (11)** become:

$$x[k+1] = A_d x[k] + B_d(u[k] + a[k]) \tag{13a}$$

$$y[k] = Cx[k] \tag{13b}$$

3. Real-time detection based on adaptive watermarking

3.1. Adaptive watermark injection strategy

In the detection framework, the adaptive watermark adjusts the control input by $u[k]$ introducing a perturbation $\Delta u[k]$:

$$u'[k] = u[k] + \Delta u[k] \tag{14}$$

where w(k) is the adaptive watermark perturbation.

The intensity of the watermark perturbation is adjusted according to the mean square value of the input signal:

$$V_k = \frac{1}{|I_k|}\sum_{i\in I_k} u[i]^2 \tag{15}$$

The variance of the watermark noise is:

$$\sigma_k^2 = \alpha V_k \tag{16}$$

where α>0 is the watermark coefficient.

The watermark perturbation $\Delta u[k]$ is generated following a Gaussian distribution:

$$\Delta u[k] \sim N(0, \sigma_k^2) \tag{17}$$

3.2. Output prediction based on steady-state Kalman filtering

To characterize modeling errors and measurement noise, process noise $w[k]$ and measurement noise $v[k]$ are introduced on the basis of **Equation (11)** to establish the Kalman filter model:

$$x[k+1] = A_d x[k] + B_d u'[k] + w[k] \tag{18}$$

$$y[k] = C_d x[k] \tag{19}$$

where $w[k] \sim N(0, Q_k)$, $v[k] \sim N(0, R_k)$.

The steady-state Kalman gain is obtained by solving the Riccati equation:

$$P = A_d P A_d^T + Q_k - A_d P {C_d}^T ({C_d P {C_d}^T + R_k})^{-1} C_d P A_d^T \tag{20}$$

$$K = P {C_d}^T ({C_d P {C_d}^T + R_k})^{-1} \tag{21}$$

Based on this filter, the system state and output are predicted:

$$x[k+1|k] = A_d x[k|k] + B_d u'[k] \tag{22a}$$

$$\overline{y}[k+1|k] = C_d \overline{x}[k+1|k] \tag{22b}$$

The deviation is calculated to correct the state:

$$\tilde{y}[k+1] = y[k+1] - \overline{y}[k+1|k] \tag{23}$$

$$x[k+1|k+1] = x[k+1|k] + K\tilde{y}[k+1] \tag{24}$$

Since the attacker cannot synchronize the watermark perturbation, a deviation arises between the actual output $y_{u'+a}[k]$ and the predicted output $\overline{y}[k]$ after the attack. The residual is defined as:

$$r[k] = \overline{y}[k] - y_{u'+a}[k] \tag{25}$$

3.3. Residual processing and statistical detection

Amplitude limiting filtering is used to constrain the residual, and recursive median filtering is applied to smooth the residual, yielding the final smoothed residual statistic:

$$\tilde{r}[k] = \frac{1}{w-2} \sum_{i=2}^{w-1} \overline{r}[i] \tag{26}$$

where N is the window length of the median filter.

The covariance matrix of the Kalman filter residual is:

$$S = C_d P_1 C_d^T + R \tag{27}$$

The residual statistic is constructed as:

$$g[k] = \sum_{i=k-w+1}^{k} \tilde{r}[i]^T S^{-1} \tilde{r}[i] \tag{28}$$

In the absence of an attack, $\tilde{r}[k]$ approximately follows a zero-mean Gaussian distribution, so $g[k]$

asymptotically follows a chi-square distribution with $w \cdot n_y$ degrees of freedom, where n_y is the output dimension. Given a significance level α, the detection threshold is set as:

$$\delta = \chi^{-1}_{1-\alpha}(w \cdot n_y) \tag{29}$$

When $g[k] > \delta$, the system is judged to be under a zero-dynamics attack.

4. Simulation experiments

4.1. Performance of the offshore wind power system under zero-dynamics attacks

The simulation parameters are shown in **Table 1**. **Figure 4** shows that the external output and internal dynamics of the system gradually stabilize without the introduction of adaptive watermarking.

Table 1. System parameters

Parameter/unit	Value
Rotor inertia J_d/(kg·m²)	2.137\times10^{-5}
Generator inertia J_m/(kg·m²)	4\times10^{-6}
Gearbox inertia J_h/(kg·m²)	6.5\times10^{-7}
Resistance R_1/Ω	4.6
Resistance R_2/Ω	5.4
Inductance L/H	4.3
Capacitance C/F	1.3

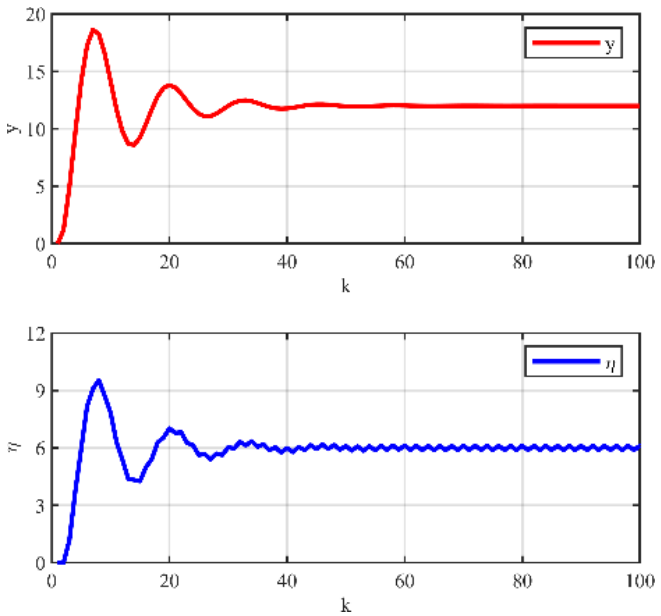

Figure 4. Normal operation of the offshore wind power system.

The zero-dynamics attack model proposed by Wang *et al.* is adopted [11]:

$$z[k+1] = G_0 z[k] \tag{30a}$$

$$a[k] = C_0 z[k] \tag{30b}$$

The initial state $||G_0|| = -2$ is set, and the attack is applied to the system with embedded adaptive watermarking. The attack is set to occur at the 80th time step, with a total simulation duration of 100 time steps. **Figure 5** shows that the external output remains stable for a short time after the attack, while the internal dynamics diverge immediately, reflecting the concealment and destructiveness of zero-dynamics attacks.

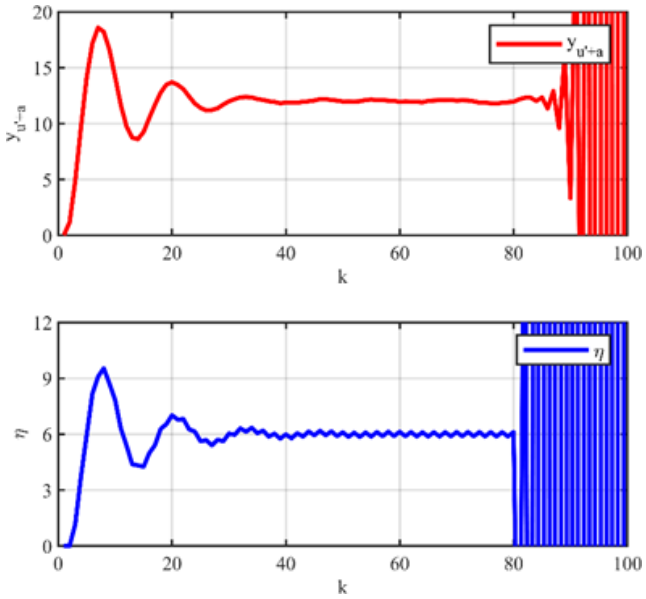

Figure 5. Offshore wind power system under zero-dynamics attack.

4.2. Simulation results of the adaptive-Kalman filter detection framework

The Kalman filter is used to predict the system output with embedded watermarking. **Figure 6** shows that the predicted output is highly consistent with the actual output under normal operating conditions.

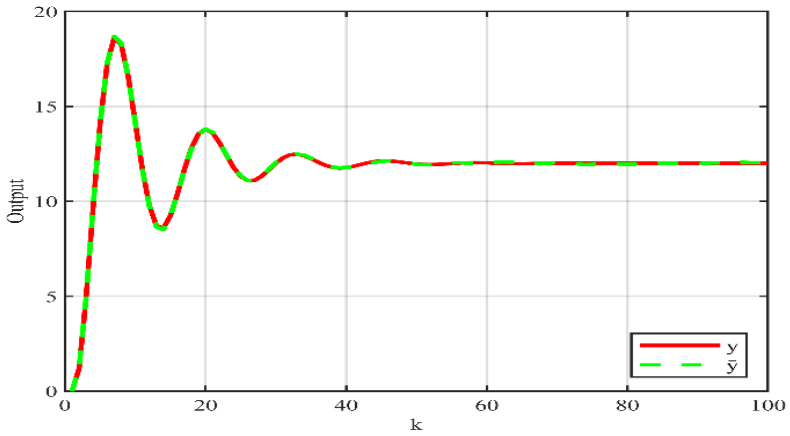

Figure 6. Comparison between the Kalman filter predicted output and the actual output.

The window length is set, and at a significance level of , the detection threshold . As shown in **Figure 7**, crosses the threshold rapidly after the attack occurs, realizing the fast identification of the zero-dynamics attack. The results verify that the proposed detection framework has good detection performance without affecting the

normal operation of the system.

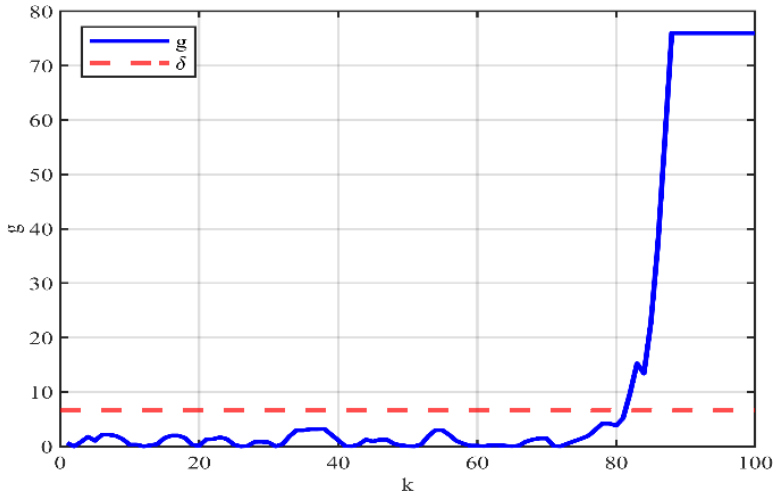

Figure 7. Detection result of zero-dynamics attacks based on the Chi-square statistic.

5. Conclusion

Aiming at the problem of zero-dynamics attacks on offshore wind power systems, this paper proposes a two-layer detection framework integrating adaptive watermarking and Kalman filtering. Simulation results show that the method can quickly identify attacks without affecting the normal operation of the system and effectively improve the security of offshore wind power systems.

Disclosure statement

The author declares no conflict of interest.

References

[1] Knack A, Syn Y, Tam K, 2021, Enhancing the Cyber Resilience of Offshore Wind. Energy Systems Catapult, 2021: 47.

[2] Lee S, Huh J, 2019, An Effective Security Measures for Nuclear Power Plant using Big Data Analysis Approach. Journal of Supercomputing, 75(8): 4251–4267.

[3] Davis R, Keskin O, 2024, Cyber Threat Modeling for Water and Wastewater Systems: Contextualizing STRIDE and DREAD with the Current Cyber Threat Landscape, 2024 Systems and Information Engineering Design Symposium (SIEDS), 1–6.

[4] Mukherjee D, 2022, Data-Driven False Data Injection Attack: A Low-Rank Approach. IEEE Transactions on Smart Grid, 13(3): 2479–2482.

[5] Shim H, Back J, Eun Y, et al., 2022, Zero-Dynamics Attack, Variations, and Countermeasures, 117–140.

[6] Pasha S, Ayub A, 2021, Zero-Dynamics Attacks on Networked Control Systems. Journal of Process Control, 2021(105): 99–107.

[7] Li X, Jiang C, Du D, et al., 2023, A Novel State Estimation Method for Smart Grid under Consecutive Denial of Service Attacks. IEEE Systems Journal, 17(1): 513–524.

[8] Zheng C, Wang X, Luo X, et al., 2022, An OpenPLC-based Active Real-Time Anomaly Detection Framework for Industrial Control Systems, 2022 China Automation Congress (CAC), 6028–6033.

[9] Jin S, 2024, False Data Injection Attack Against Smart Power Grid based on Incomplete Network Information. Electric Power Systems Research, 2024(230): 110294.

[10] Hoehn A, Zhang P, 2016, Detection of Covert Attacks and Zero Dynamics Attacks in Cyber-Physical Systems, 2016 American Control Conference (ACC), 396–401.

[11] Wang Z, Zhang H, Cao X, et al., 2024, Modeling and Detection Scheme for Zero-Dynamics Attack on Wind Power System. IEEE Transactions on Smart Grid, 15(1): 934–943.

[12] Sheng L, Li C, Gao M, et al., 2025, A Review of SCADA-based Condition Monitoring for Wind Turbines via Artificial Neural Networks. Neurocomputing, 2025(633): 129830.

[13] Amin M, El-Sousy F, Aziz G, et al., 2021, CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review. IEEE Access, 2021(9): 38571–38601.

[14] Le H, Dang P, Pham A, et al., 2020, System Identifications of a 2DOF Pendulum Controlled by QUBE-Servo and its Unwanted Oscillation Factors. Archive of Mechanical Engineering, 67(3): 435–450.

[15] Weller S, Moran W, Ninness B, et al., 2001, Sampling Zeros and the Euler-Frobenius Polynomials. IEEE Transactions on Automatic Control, 46(2): 340–343.