applied sciences

MDPI

Article

Zero-Dynamics Attack on Wind Turbines and Countermeasures Using Generalized Hold and Generalized Sampler

Daehan Kim, Kunhee Ryu and Juhoon Back *

School of Robotics, Kwangwoon University, Seoul 01897, Korea; 2018124101@kw.ac.kr (D.K.); ryuhhh@kw.ac.kr (K.R.)
* Correspondence: backhoon@kw.ac.kr

Abstract: Most wind turbines are monitored and controlled by supervisory control and data acquisition systems that involve remote communication through networks. Despite the flexibility and efficiency that network-based monitoring and control systems bring, these systems are often threatened by cyberattacks. Among the various kinds of cyberattacks, some exploit the system dynamics so that the attack cannot be detected by monitoring system output, the zero-dynamics attack is one of them. This paper confirms that the zero-dynamics attack is fatal to wind turbines and the attack can cause system breakdown. In order to protect the system, we present two defense strategies using a generalized hold and a generalized sampler. These methods have the advantage that the zeros can be placed so that the zero dynamics of the system become stable; as a consequence, the zero-dynamics attack is neutralized. The effects of the countermeasures are validated through numerical simulations and the comparative discussion between two methods is provided.

Keywords: wind energy; system security; zero-dynamics attack

Citation: Kim, D.; Ryu, K.; Back, J. Zero-Dynamics Attack on Wind Turbines and Countermeasures Using Generalized Hold and Generalized Sampler. *Appl. Sci.* **2021**, *11*, 1257. https://doi.org/10.3390/app11031257

Received: 30 November 2020
Accepted: 25 January 2021
Published: 29 January 2021

1. Introduction

Wind energy has been recognized as one of the major renewable energy sources for over two decades. As of 2019, the global wind power capacity reaches 60 GW, including onshore and offshore plants [1]. Nowadays, it is typical to install multiple turbines in the same area where wind energy is abundant, this is called a wind farm. To manage a wind farm consisting of several to hundreds of turbines efficiently, a network-based monitoring and control scheme is needed, such as supervisory control and data acquisition (SCADA) systems. By virtue of SCADA systems, it is possible to acquire the condition of the wind turbines installed over a wide area and manage them efficiently.

However, network-based control and monitoring systems, including SCADA systems, are frequently targeted by cyberattacks due to the presence of the network. Recently, several attempts of cyberattacks on network-controlled plants have been reported, including a German steel mill [2], Iranian and American nuclear facilities [3], Ukrainian power plant [4], among others. These cases imply that many systems using network-based control and monitoring systems, including the wind turbine systems, are not free from cyberattacks. In order to secure the networked control systems from possible cyberattacks, researches on cyberattacks and defense strategies have drawn attention, see, e.g., [5–8], surveys [9–11] and the references therein.

Cyberattacks on systems controlled through networks can be classified into two categories, model-free attacks and model-based attacks. The model-free attacks are basically accomplished in the form of overloading the system through superfluous requests or stealing information from network lines. A most well-known model-free attack is DoS (denial-of-service) [12]. An attacker running DoS may overload or possess the network and system resources by sending numerous requests to the target system, disturbing the normal operation of systems. DDoS (distributed denial-of-service) [13], which conducts DoS attacks in a distributed form, and PSDoS (power save denial-of-service) [14] methods

that can conduct DoS attacks with relatively small attack resources, are variants of DoS. Eavesdropping [15] is another instance of model-free attacks, which is accomplished by occupying part of the network lines. The eavesdroppers collect information by intercepting data or signals that are sent over the network. A Replay attack [16] is performed by combining the above two attacks. An attacker running the replay attack steals data being transmitted and sends it to the system repeatedly, pretending that the requests are from the valid user.

The model-based attacks are another category of cyberattack that include covert false-data injection attacks [17], zero-dynamics attacks (ZDAs) [8], robust zero-dynamics attacks [18], and pole-dynamics attacks [19]. An attacker performing the covert false-data injection attack, targeting a system that has known dynamics, can make the remote monitoring system or controller recognize that the system is under normal operation, even though it is not. ZDA is another model-based attack that manipulates the input signal only with the knowledge of the system dynamics. The attacker of ZDA can make the internal states of the system become unbounded while making the impact of the attack hardly visible on the output. The pole-dynamics attack is an attack that a malicious signal is injected into the output of the system. One of the major features of the model-based attack is that it allows more sophisticated and clever attacks. The attack signals, generated by using knowledge of the target systems, lead the remote monitoring system to be mistaken as a normal operation, which implies that the attacks are stealthy.

In this paper, we are particularly interested in the zero-dynamics attack on wind turbine systems. ZDA is known as one of the most fatal cyberattacks and this is mainly because the attack exploits the system model and very hard to detect. This attack requires a high level of model knowledge and has the character of disruption resources in the attack space of [8]. Suppose that a dynamic system that is represented by a transfer function and is stabilized by a controller, e.g., Proportional–Integral–Differential (PID) type. If the zero dynamics (which corresponds to the zeros of the transfer function) is unstable, then there exists an input signal that drives some internal variable of the system to be unbounded while unnoticed by monitoring the system output. Exploiting this fact, one can construct an undetectable cyberattack by copying the zero dynamics of the system. If this attack is applied to the system, then, by stability, the internal variable will approach the attack signal while the change of the output can hardly be detected [8].

As one might have noticed, ZDA is ineffective if the system has stable zero dynamics, since the attack is generated from a copy of the zero dynamics and thus converges to zero, meaning that the attack signal diminishes. Unfortunately, this does not mean that this system is safe from ZDA. In fact, most of the modern control systems are operated by digital controllers and it is quite often the case that the sampled-data system of the original continuous-time system has unstable zero dynamics; if the system has a relative degree greater than two, then at least one zero is unstable [20]. This means that even if the continuous-time system has stable zero dynamics, it can happen under ZDA that the sampled output remains constant while its continuous counterpart or some internal states diverge. In the first part of this paper, we demonstrate that the sampled-data model of the wind turbine system has unstable zero dynamics and thus, is vulnerable to ZDA; a ZDA is constructed so that the generator angular velocity diverges but its sampled values remain almost constant. Thus, from the input/output data of the wind turbine collected by the SCADA system, the system appears to be operating normally until some variable of the system reaches its hardware limit.

Recognizing the lethality of ZDA, several strategies to protect the system have been developed [7,21–24]. Authors in [7] proposed defense strategies to defend against such an attack by modifying the system structures including the input gain matrix, output matrix, and the system matrix. For example, the input gain matrix can be modified by adding and removing actuators or by introducing a perturbation. In [21], a modulation-matrix-based detection method was proposed, which is another structure-modifying method. These methods focus on the fact that the modification of the system structure leads to a change in

zero dynamics. If the attacker does not know about the change of the system and injects the attack signal generated based on the system before the modification, the effect of the attack can be detected. However, if the attacker knows the modified system's information, a stealthy attack is still possible. Thus, the information on the modified system should be hidden.

Another defense strategy is to make all zeros of the system become stable. Since ZDA is effective to a system that has at least one unstable zero, the methods under this strategy focus on proactively blocking the threat of attacks. Provided that the zero dynamics is stable, the attack signal based on the dynamics converges to zero. In [25], authors proposed an attack neutralizing method by measuring the output several times during one sampling interval. Then, the lifted system with new measurements has no unstable zero.

Recently, a generalized hold (GH)-based zero-assignment method was introduced in [23], and a method with a generalized sampler (GS) was proposed in [24]. The GH is an interfacing device between discrete-time signals and continuous-time signals, generating a continuous-time signal based on the predetermined hold function (or weights). By using GH instead of zero-order hold (ZOH), the zeros of the plant can be located in the stable region [20]. However, the GH-based defense method may cause undesirable intersample behavior, since the signal generated by GH is typically uneven.

The strategy employing GS is a more recently introduced method that overcomes the shortcomings of intersample behavior of the GH-based defense method. The GS constructs a new output by taking a weighted average of multiple output measurements from one sampling interval [20,24], replacing the simple sampler. It is shown that the zeros can be assigned arbitrarily by using GS, hence, it can be used as a countermeasure against ZDA. Since the operation of GS does not affect the plant input, undesirable intersample behavior no longer occurs. The output of GS, however, may differ from that of a simple sampler and can be sensitive to the sensor noise.

Most recently, cyberattacks including ZDA and their countermeasures are developed for more general systems having multiple agents. In [26], the concept of ZDA is generalized to a cooperative attack on multiagent systems considering network switching and a defense strategy involving the design of a series of network switching and the Luenberger observer has been proposed. In addition, the detection of cyberattacks including the false-data injection attack and replay attack is studied and applied to DC microgrids in [27], where the Luenberger observer and the unknown input observer are used to estimate the states of an agent and its neighbors.

In this paper, we apply two security strategies based on GH and GS to wind turbine systems. Firstly, a GH is designed so that all the zeros of the sampled-data model of the wind turbine system are located inside the unit circle. It is shown through numerical simulations that the presence of the ZDA that has been designed using the unstable sampling zero is revealed shortly after the attack is injected. The effect of GH on the intersample behavior of the generator angular velocity is also discussed. Secondly, we shift the unstable sampling zero into the stable region by employing the GS, which reveals the presence of ZDA clearly. It is emphasized that the undesirable intersample behavior does not appear anymore. In addition to this advantage, the numerical simulations demonstrate that sensitivity to noise can be reduced substantially by properly choosing the zeros.

The rest of this paper is organized as follows. In Section 2, we briefly describe the wind turbine's modeling. Section 3 addresses that the digitally controlled wind turbine system is vulnerable to ZDA. Section 4 briefly explains how to change the zeros of a system by using GH and GS. In Section 5, we apply the design of GH and GS against ZDA and demonstrate that ZDA can be neutralized via numerical simulations. Finally, Section 6 concludes the paper.

2. Dynamic Model of Wind Turbine

In this section, we briefly review the dynamics of a wind turbine. Key components of a wind turbine are the rotor blade, drivetrain, generator, and interface to the main grid.

The rotor blade is modeled as a static function that produces the mechanical torque T_a that is applied to the drivetrain. We model the drivetrain as a dynamic system with three state variables. The dynamics of the generator are not considered but it is assumed that it can apply generating torque T_g to the drivetrain.

Based on the wind turbine model, we derive a linear model and its discrete-time approximation around an operating point. Through numerical simulations, it is seen that the closed-loop system converges to the steady state under constant wind speed.

2.1. Dynamic Model of Wind Turbine

The drivetrain can be modeled as a two-inertia system in which rotor blades and generator are combined in one axis through a gearbox. Since the moment of inertia of the rotor blade is very high, the influence of the moment of inertia on the gearbox can be neglected [28]. Therefore, the influence of the gearbox is reflected on the generator side, and the wind turbine is expressed as a two-inertia model. Assuming that the shaft is thin and long, a two-inertia system can be modeled as a system with torsion, connected by a spring and a damper. It is assumed that the rotor has inertia J_r and the generator has inertia J_g. They are connected through a torsional spring with spring constant K_{sh} and a torsional damper with damping constant D_{sh}, as illustrated in Figure 1. The aerodynamic torque applied to the drivetrain is denoted by T_a and the generator torque is denoted by T_g. T_{sh} stands for the torsional torque developed in the shaft. ω_r and ω_g are the angular velocities corresponding to rotor and generator, respectively. For other types of drivetrain models, see, e.g., [29–33].

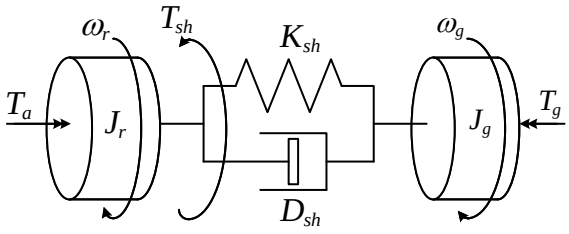


Figure 1. Two-inertia model of the drivetrain.

The dynamics of the drivetrain are derived as [34]

$$\begin{aligned} T_a &= J_r\dot{\omega}_r + T_{sh} \\ T_{sh} &= J_g\dot{\omega}_g + T_g \\ T_{sh} &= Q_s + Q_d = K_{sh}(\theta_r - \theta_g) + D_{sh}(\omega_r - \omega_g). \end{aligned} \tag{1}$$

We define the state vector $x = [\omega_r, \omega_g, Q_s]^\top$ and express the dynamics (1) in the state space as

$$\begin{aligned} \dot{x} &= A_s x + B_s u \\ y &= C_s x, \end{aligned} \tag{2}$$

where $u = [T_a, T_g]^\top$ is the input; y is the system output; and A_s, B_s, C_s are system matrices given by

$$A_s = \begin{bmatrix} -D_{sh}/J_r & D_{sh}/J_r & -1/J_r \\ D_{sh}/J_g & -D_{sh}/J_g & 1/J_g \\ K_{sh} & -K_{sh} & 0 \end{bmatrix}, B_s = \begin{bmatrix} 1/J_r & 0 \\ 0 & -1/J_g \\ 0 & 0 \end{bmatrix}, C_s = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}.$$

The turbine power P_t of the wind turbine and aerodynamic torque T_a applied to the wind turbine are given by

$$\begin{aligned} P_t &= \frac{1}{2}\rho\pi R^2 C_p(\lambda,\beta)V^3 \\ T_a &= \frac{1}{2}\rho\pi R^3 C_q(\lambda,\beta)V^2, \end{aligned} \tag{3}$$

where ρ is the air density, R is the radius of the blade, V is the wind speed, $C_p(\lambda,\beta)$ is the power coefficient, and $C_q(\lambda,\beta)$ is the torque coefficient. $C_p(\lambda,\beta)$ and $C_q(\lambda,\beta)$ depend on the tip-speed-ratio (TSR) λ defined by $\lambda = \omega_r R/V$ and the pitch angle β [31,32,35]; C_p and C_q are related as $C_q = C_p/\lambda$. We take a widely used model of C_p given by

$$C_p(\lambda,\beta) = c_1\left(c_2\frac{1}{\Lambda} - c_3\beta - c_4\beta^{c_5} - c_6\right)e^{-c_7\frac{1}{\Lambda}}, \tag{4}$$

where the parameter $\frac{1}{\Lambda}$ is defined as

$$\frac{1}{\Lambda} = \frac{1}{\lambda + 0.08\beta} - \frac{0.035}{1+\beta^3},$$

and $c_1,\ldots,c_7$ are constants that depend on system parameters [34,36]. Since $C_p(\lambda,\beta)$ is related to the wind-rotor aerodynamic characteristics [37], the numerical values of $c_1,\ldots,c_7$ depend on the wind turbine under consideration. In this paper, the parameters of the T-100 of Argolabe. S.L. Engineering Company are used, where $C_{p,max}$ is 0.4728 and λ is 6 [38]. The $C_p(\lambda,\beta)$ curve is extracted from Matlab/Simulink simulations with zero pitch angle ($\beta = 0^\circ$). Through simulations, the parameters of $c_1,\ldots,c_7$ are chosen as $c_1 = 0.29$, $c_2 = 115$, $c_3 = 0.5$, $c_4 = 0$, $c_5 = 0$, $c_6 = 6$, and $c_7 = 13.1$.

2.2. Discrete-Time Linear Model

Most modern control systems are controlled by digital devices. One of the well-established procedures to develop controllers is based on discretization of the system model. In this subsection, we first linearize the wind turbine system (2) with T_a given by (3) around a point of the rated power operation and then discretize under the assumption that ZOH at the actuator side and simple sampler (SS) at the sensor side are used. It is emphasized that this discrete linear model containing unstable zeros can be used to generate an undetectable cyberattack, which will be discussed in the later part of this paper.

It is observed that the aerodynamic torque T_a given in (3) is a nonlinear function of ω_r and V, and it can be linearized around an operating point $(\bar{\omega}_r, \bar{V})$ (the rated power point) [30,34] as

$$\hat{T}_a = k_{\omega_r}(\bar{\omega}_r,\bar{V})\hat{\omega}_r + k_V(\bar{\omega}_r,\bar{V})\hat{V}, \tag{5}$$

where $\bar{\omega}_r$ and $\bar{V}$ are the values of ω_r and V at the operating point, $\hat{\omega}_r = \omega_r - \bar{\omega}_r$, $\hat{V} = V - \bar{V}$, and $\hat{T}_a = T_a - \bar{T}_a$ ($\bar{T}_a$ is the aerodynamic torque at the operating point). The gains k_{ω_r} and k_V are given by

$$\begin{aligned} k_{\omega_r}(\bar{\omega}_r,\bar{V}) &= \left.\frac{\partial T_a}{\partial \omega_r}\right|_{(\bar{\omega}_r,\bar{V})} = \left.\frac{1}{2}\rho\pi R^4\bar{V}\frac{\partial C_q}{\partial\lambda}\right|_{(\bar{\omega}_r,\bar{V})} \\ k_V(\bar{\omega}_r,\bar{V}) &= \left.\frac{\partial T_a}{\partial V}\right|_{(\bar{\omega}_r,\bar{V})} = \left.\frac{1}{2}\rho\pi R^3\bar{V}\left(2C_q - \lambda\frac{\partial C_q}{\partial\lambda}\right)\right|_{(\bar{\omega}_r,\bar{V})}. \end{aligned}$$

Substituting (5) to the dynamics (2), a linearized state-space model is obtained as

$$\begin{aligned} \dot{\hat{x}} &= \hat{A}_s\hat{x} + \hat{B}_s\hat{u} + \hat{B}_V\hat{V} \\ \hat{y} &= C_s\hat{x}, \end{aligned} \tag{6}$$

where $\hat{x} = [\hat{\omega}_r, \hat{\omega}_g, \hat{Q}_s]$; $\hat{u} = \hat{T}_g$; and the matrices $\hat{A}_s$, $\hat{B}_s$, $\hat{B}_V$, and C_s are given by

$$\hat{A}_s = \begin{bmatrix} (k_{\omega_r} - D_{sh})/J_r & D_{sh}/J_r & -1/J_r \\ D_{sh}/J_g & -D_{sh}/J_g & 1/J_g \\ K_{sh} & -K_{sh} & 0 \end{bmatrix}, \hat{B}_s = \begin{bmatrix} 0 \\ -1/J_g \\ 0 \end{bmatrix}$$
$$\hat{B}_V = \begin{bmatrix} k_V/J_r \\ 0 \\ 0 \end{bmatrix}, \; C_s = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}.$$

From this linear model, the transfer function from $\hat{T}_g$ to $\hat{\omega}_g$ is computed as

$$G(s) = \frac{\hat{\omega}_g(s)}{\hat{T}_g(s)} = -\frac{b_2 s^2 + b_1 s + b_0}{a_3 s^3 + a_2 s^2 + a_1 s + a_0}, \tag{7}$$

where

$$a_3 = J_r J_g, \quad a_2 = D_{sh}(J_r + J_g) - k_{\omega_r}(\bar{\omega}_r, \bar{V}) J_g$$
$$a_1 = K_{sh}(J_r + J_g) - k_{\omega_r}(\bar{\omega}_r, \bar{V}) D_{sh}, \quad a_0 = -k_{\omega_r}(\bar{\omega}_r, \bar{V}) K_{sh}$$
$$b_2 = J_r, \quad b_1 = D_{sh} - k_{\omega_r}(\bar{\omega}_r, \bar{V}), \quad b_0 = K_{sh}.$$

From the linearized model (6), we derive a discrete-time model for the purpose of controller design. Let T_s be the sampling time and suppose that the control input u_k is determined by a digital controller and the actual control input $\hat{u}(t)$ is generated via ZOH so that $\hat{u}(t) = \hat{u}_k$ for $kT_s \leq t < (k+1)T_s$, where k is a non-negative integer. The measured output that is transmitted to the controller is sampled at each sampling time kT_s, we call this sampling device a simple sampler, and this sampled output is denoted by $\hat{y}_k$. Assuming the wind turbine is at steady state under constant wind speed, we have the following discrete-time linear model

$$\begin{aligned} \hat{x}_{k+1} &= \hat{A}_{\mathrm{d}} \hat{x}_k + \hat{B}_{\mathrm{d}} \hat{u}_k \\ \hat{y}_k &= C_{\mathrm{d}} \hat{x}_k, \end{aligned} \tag{8}$$

where $\hat{x}_k = \hat{x}(kT_s)$ is the state vector, $\hat{A}_{\mathrm{d}} = e^{\hat{A}_s T_s}$, $\hat{B}_{\mathrm{d}} = \int_0^{T_s} e^{\hat{A}_s (T_s - \tau)} \hat{B}_s d\tau$, and $C_d = C_s$. It is noted that this model is an exact discretization of the continuous-time model (6).

We use a PI-type digital controller with sampling time T_s whose discrete-time transfer is given by

$$C_{\mathrm{PI}}(z) = K_P + K_I \frac{T_s}{z - 1},$$

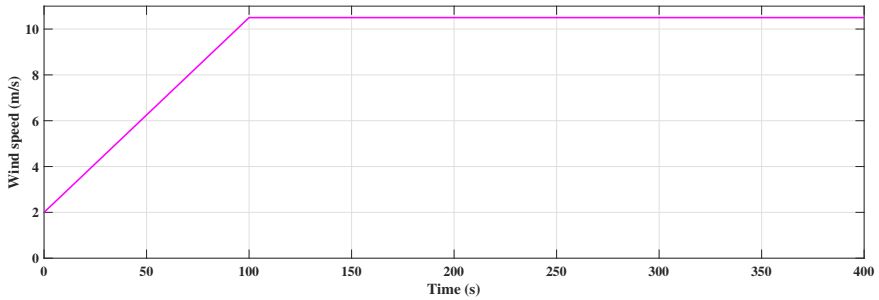
where K_P and K_I are the proportional gain and integral gain, respectively. The discrete control input signal $\hat{u}_k$ is computed from the relation $\hat{u}_k = \mathcal{Z}^{-1}(C_{\mathrm{PI}}(z)(0 - \hat{Y}(z))$ where $\hat{Y}(z)$ is the z-transform of $\hat{y}_k$.

2.3. Wind Turbine Simulation Model and Its Behavior under Normal Condition

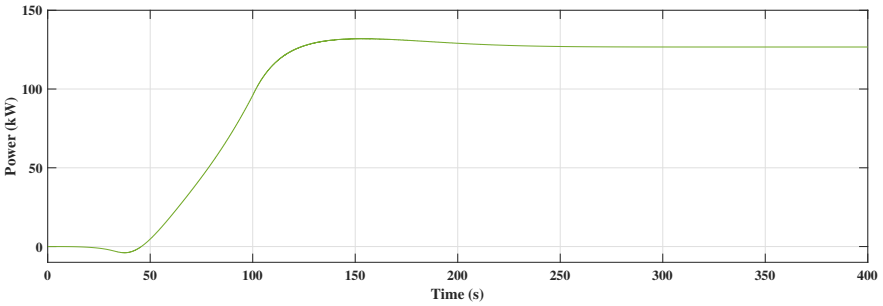
We take a small size wind turbine whose system parameters, summarized in Table 1, are taken from [33] and the data-sheet of the T-100 wind turbine of Argolabe S.L. Engineering Company [38]. It is a horizontal axis wind turbine and is designed for distributed generation and (or) electric self-consumption applications, connected to a power grid. According to the data-sheet, the shaft of the rotor and the generator are connected by a gearbox, but by including the gearbox in the inertia of the generator, it can be modeled as a two-inertia model connected by one shaft with torsion, as shown in Figure 1.

Figure 2 is the result of the turbine behavior simulation obtained using the simulation tool Matlab/Simulink. As shown in Figure 2a, wind speed is simulated with the numerical data described under the scenario that the wind speed changes from 0 to 10.5 m/s and reaches 10.5 m/s at 100 s. Figure 2b shows the generated power calculated using (3), it is observed that the generated power in the turbine changes according to the wind speed (V) and power coefficient (C_p) and that the generated power reaches its maximum after about

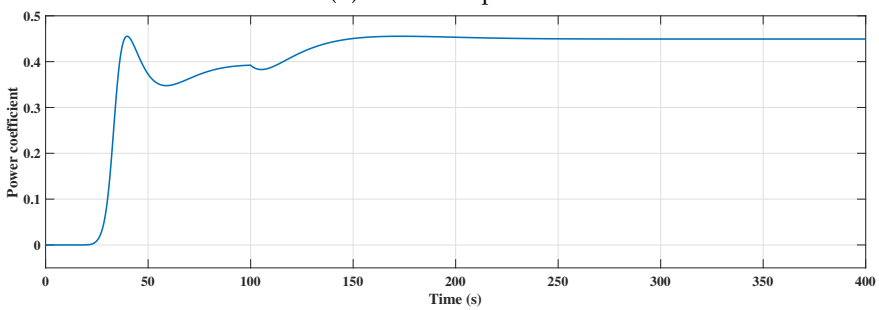
200 s. The maximum power is about 133 kW. Figure 2c shows the response of the power coefficient (C_p), which reaches 0.4724 after about 200 s. The generator angular velocity (ω_g) and rotor angular velocity (ω_r) are plotted in Figure 2d. According to the specifications [38], the rated speed of the rotor is 5.6 rad/s and the gear ratio is 22.2. Using this information, the generator speed ω_g is plotted considering the gear ratio, of which the rated value is 124.32 rad/s. A PI controller is used to control the angular velocity of the generator and the gains are chosen as K_p = 400 and K_I = 600. In Figure 2d, as the wind speed changes—as shown in Figure 2a—it is observed that the generator angular velocity reaches 124.32 rad/s after 200 s so that the rotor angular velocity reaches its rated value.



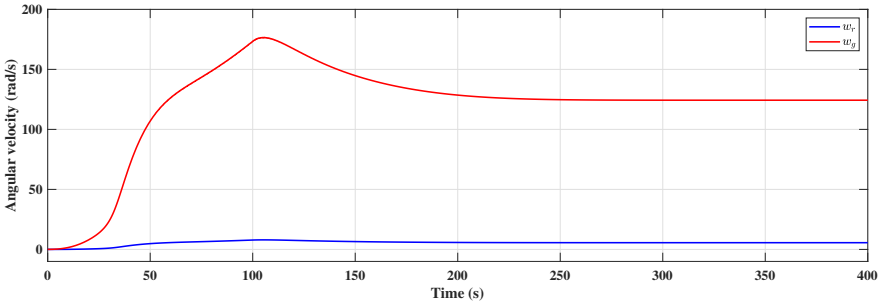
(**a**) Wind speed profile.



(**b**) Generated power.



(**c**) Power coefficient.



(**d**) Angular velocities: generator (red), rotor (blue).

Figure 2. Response of the wind turbine under constant wind speed.

Table 1. Model parameters of a small-sized wind turbine.

J_r	J_g	K_{sh}	R	λ_{opt}	$C_{p,max}$
30,375 kg·m^2	151 kg·m^2	0.31×10^6 N·m/rad	11.25 m	6	47.24%

It is noted that the steady state behavior of this wind turbine is obtained under the condition that no cyberattack has been injected. In what follows, we consider the case where the system is under a ZDA that is obtained from this steady state condition (i.e., the information on the operating point) and show that the presence of the attack cannot be detected for a considerably long time interval.

3. Zero-Dynamics Attack on Wind Turbine

Thanks to the development of communication and computing technology, modern wind turbine systems are generally operated by remote control and monitoring systems such as SCADA systems [39–41]. Operating wind power generators using the SCADA system enables efficient monitoring and control over wide areas such as wind farms [42,43]. An operator of the SCADA system can comprehensively manage the system based on the signals delivered through the network such as rotor and generator speed, wind speed, and generator torque; see, e.g., [39,40] for details. For the reasons discussed above, the network-based monitoring (or controlling) systems bring an advantage in terms of efficient management of the system. Through a communication network, multiple wind turbines installed in a wide area can be managed in one place, which can result in reduced manpower and immediate state monitoring [44,45].

However, there are also problems with network usage, such as vulnerabilities to cyberattack. If a large area is connected through communication lines, the number of paths through which an attacker with a malicious purpose can inject signals into the system may increase [46–48]. In fact, many studies on cyberattacks using these vulnerabilities have been conducted recently [8,49], such as data integrity attack [6], false-data injection attack [50], ZDA [7], etc. Among these cyberattacks, ZDA is one of the sophisticated cyberattacks based on system dynamics [23,24].

Consider a wind turbine system that operates as shown in Figure 3. The turbine receives control input from a remote controller and feeds the system state back to the controller through a network. ZDA becomes possible by occupying the network line between the controller and target system.

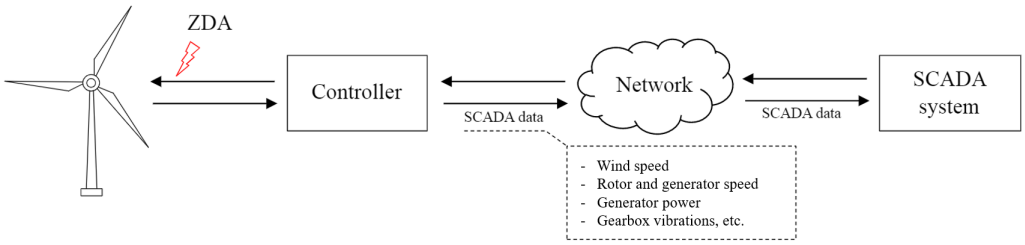


Figure 3. Schematic of remotely monitored and controlled wind turbine systems subject to zero-dynamics attacks. ZDA—zero-dynamics attack; SCADA—supervisory control and data acquisition.

Assume that the attacker who has taken control of the network line knows the model information of the system and can add the attack signal a_k to the controller output, as shown in Figure 4. Then, using the system model, the attacker can generate a sophisticated attack signal that enables the discrete-time output signal to pretend that the system is operating normally but make the internal state actually unbounded [51,52]. The mathematical explanation for the zero-dynamics attack is as follows:

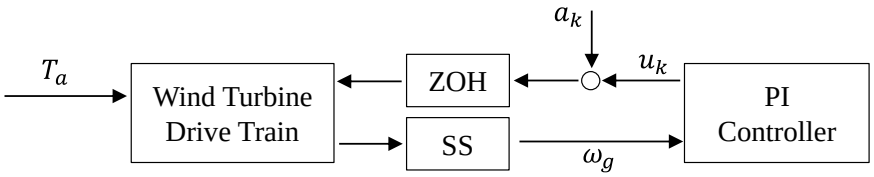


Figure 4. Wind turbine control system under the zero–dynamics attack at the actuator side. ZOH—zero-order hold; SS—simple sampler; PI—Proportional–Integral.

From (8), the dynamics of the wind turbine under ZDA becomes

$$\begin{aligned} \hat{x}_{k+1} &= \hat{A}_{\mathrm{d}}\hat{x}_k + \hat{B}_{\mathrm{d}}(\hat{u}_k + a_k) \\ \hat{y}_k &= C_{\mathrm{d}}\hat{x}_k, \end{aligned} \tag{9}$$

where a_k is the attack signal of ZDA. The attack signal a_k is generated from a dynamic system which is identical to the zero dynamics of the system. We recall that the zero dynamics of the system (9) can be identified by rewriting it in the normal form [53] given by

$$\begin{aligned} \eta_{k+1} &= S_{\mathrm{d}}\eta_k + P_{\mathrm{d}}\xi_k,\ \eta_k \in \mathbb{R}^2 \\ \xi_{k+1} &= \psi_{\mathrm{d}}^{\top}\eta_k + \phi_{\mathrm{d}}\xi_k + g_{\mathrm{d}}(\hat{u}_k + a_k),\ \xi_k \in \mathbb{R} \\ \hat{y}_k &= \xi_k, \end{aligned} \tag{10}$$

where the dynamics of ξ_k explains how the input u_k directly affects the system output ($\hat{y}_{k+1}$ explicitly depends on u_k) and that of η_k describes the internal behavior of the system. The dynamics $\eta_{k+1} = S_{\mathrm{d}}\eta_k$ is called the zero dynamics and the eigenvalues of S_{d} correspond to the zeros of the system (9).

The attack signal a_k of ZDA is generated from a dynamic system given by

$$a_k = -\frac{1}{g_{\mathrm{d}}}\psi_{\mathrm{d}}^{\top} z_k, \qquad z_{k+1} = S_{\mathrm{d}} z_k, \tag{11}$$

where $z_k \in \mathbb{R}^2$ is the state of attack generator. It is noted that the attack is constructed using the system parameters such as S_{d}, ψ_{d}, and g_{d}.

Now, we investigate the behavior of the closed-loop system under ZDA. Firstly, the controller $C_{\mathrm{PI}}(z)$ represented in the state space

$$\begin{aligned} c_{k+1} &= c_k + e_k,\ e_k = -\hat{y}_k \\ \hat{u}_k &= k_I c_k + k_P e_k, \end{aligned}$$

has been designed so that the closed-loop system under no ZDA is stable, as demonstrated in Section 2.3, namely, the matrix $\hat{A}_{\mathrm{CL}}$ shown below is Schur.

$$\hat{A}_{\mathrm{CL}} = \begin{bmatrix} S_{\mathrm{d}} & P_{\mathrm{d}} & 0 \\ \psi_{\mathrm{d}}^{\top} & \phi_{\mathrm{d}} - g_{\mathrm{d}}k_P & g_{\mathrm{d}}k_I \\ 0 & -1 & 1 \end{bmatrix}. \tag{12}$$

When the attack a_k generated by (11) is injected into system (10) (it is equivalent to system (9)), we can derive

$$\begin{bmatrix} \eta_{k+1} \\ \xi_{k+1} \\ c_{k+1} \\ z_{k+1} \end{bmatrix} = \begin{bmatrix} S_{\mathrm{d}} & P_{\mathrm{d}} & 0 & 0 \\ \psi_{\mathrm{d}}^{\top} & \phi_{\mathrm{d}} - g_{\mathrm{d}}k_P & g_{\mathrm{d}}k_I & -\psi_{\mathrm{d}}^{\top} \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & S_{\mathrm{d}} \end{bmatrix} \begin{bmatrix} \eta_k \\ \xi_k \\ c_k \\ z_k \end{bmatrix},$$

from which one has

$$\begin{bmatrix} \eta_{k+1} - z_{k+1} \\ \xi_{k+1} \\ c_{k+1} \end{bmatrix} = \hat{A}_{\mathrm{CL}} \begin{bmatrix} \eta_k - z_k \\ \xi_k \\ c_k \end{bmatrix}.$$

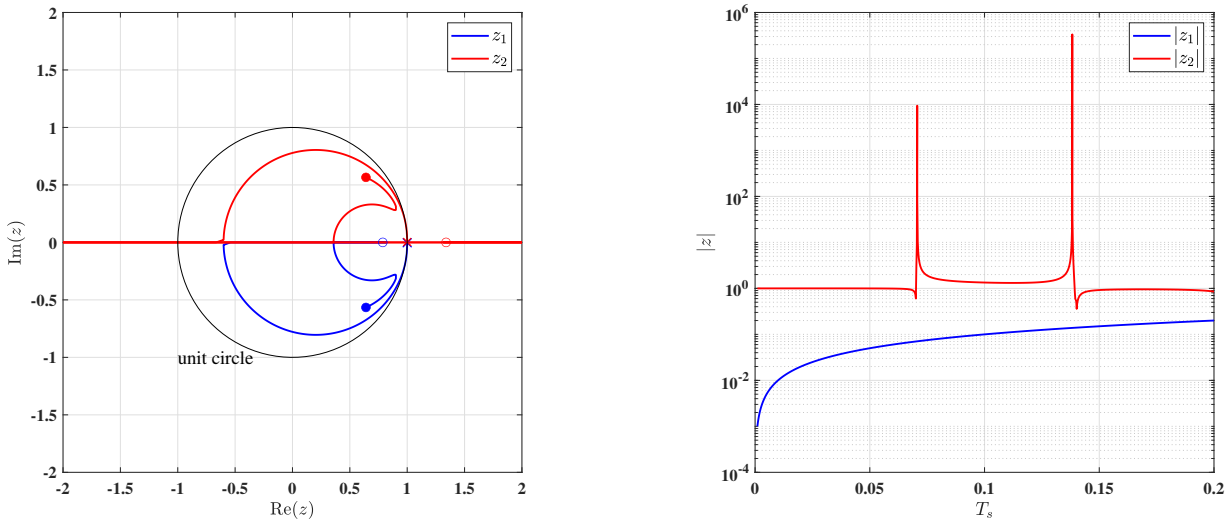
Since $\hat{A}_{\mathrm{CL}}$ given in (12) is Schur, there exist $\kappa > 0$ and λ with $|\lambda| < 1$ such that

$$\left\| \begin{bmatrix} \eta_k - z_k \\ \xi_k \\ c_k \end{bmatrix} \right\| \leq \kappa \lambda^k \left\| \begin{bmatrix} \eta_0 - z_0 \\ \xi_0 \\ c_0 \end{bmatrix} \right\|. \tag{13}$$

This relation implies that under a ZDA, the internal state η_k converges to the state of ZDA, while other states ξ_k and c_k converge to zero.

It is remarkable that the relation (13) holds regardless of the stability of the zero dynamics. Hence, if S_{d} is unstable, then the internal state η_k diverges whenever z_0 depends on an unstable eigenvector of S_{d}, while this behavior cannot be observed by monitoring the signal (ξ_k, c_k).

Unfortunately, the wind turbine system (8) has an unstable zero when the sample time T_s belongs to some region. Figure 5a shows the locus of the zeros with respect to the sampling time from $T_s = 0.001$ s to $T_s = 0.1$ s. When $T_s = 0.001$ s, two zeros are located near 1, as depicted by the crosses. When T_s increases and then becomes 0.08 s, z_2 is located outside the unit circle. The blue and red circles on the real axis in Figure 5a indicate the location of two zeros when $T_s = 0.1$ s. As shown in Figure 5b, if $T_s \in [0.08, 0.13]$ s, at least one zero is located outside the unit circle.



(**a**) (**b**)

Figure 5. (**a**) Locus of discrete-time zeros and (**b**) the magnitude of them with respect to the sampling time T_s.

Suppose that T_s belongs to the region where the wind turbine has an unstable zero. When the attack (11) is injected, the rotor angular velocity ω_r and the (spring) torsional torque Q_s will diverge while the generator angular velocity ω_g and the controller state c_k converge to zero. This can be interpreted so that the attack intentionally moves two components (ω_r and Q_s) of the operating point but leaves ω_g at the normal operating point and deceives the controller as if all components remain unchanged.

Under the situation described in Figure 4, the effect of ZDA on the wind turbine system is presented. Since the system is of nonminimum phase when $T_s = 0.1$ s, the attack signal diverges for an appropriately chosen initial condition as shown in Figure 6, and it is expected that the internal states also diverge. Suppose that the hacker injected a_k through the communication network at $t = 0$. Let $\hat{\omega}_{g,\mathrm{Th}}$ be a threshold that the steady

state value of $\hat{\omega}_g$ should not exceed (the dotted line in Figure 7a and $\hat{\omega}_{g,\mathrm{Th}} = 0.18$ rad/s), in other words, if $|\hat{\omega}_g| > \hat{\omega}_{g,\mathrm{Th}}$, the monitoring system determines that a fault has occurred or an attack has been injected. As can be seen in Figure 7a, the continuous-time output $y(t) = \omega_g(t)$—the generator speed—becomes unbounded, while the discrete-time signal $y_k = \omega_{g,\mathrm{ZOH}}$ that is transmitted to the controller and the SCADA system remain almost unchanged, indicating that the wind turbine still operates normally.

Meanwhile, the attack also affects the generated power and internal state. Figure 7b,c show the responses of the internal states ω_r and Q_s, respectively, and it is observed that ω_r and Q_s become unbounded. In addition, the generated power under ZDA decreases, as shown in Figure 7d.

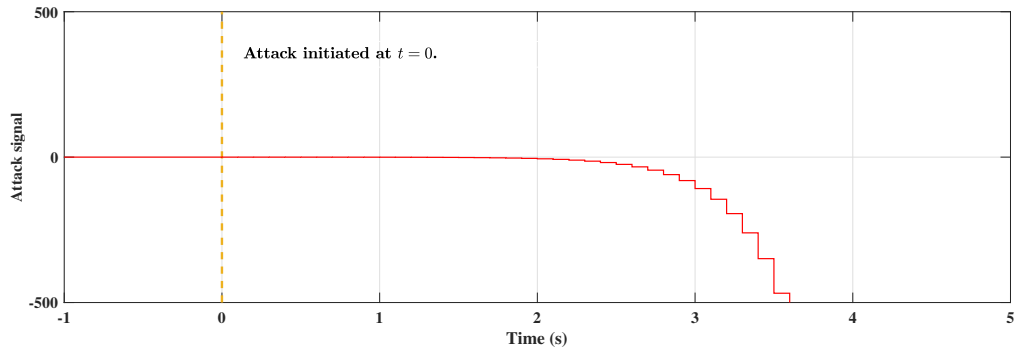
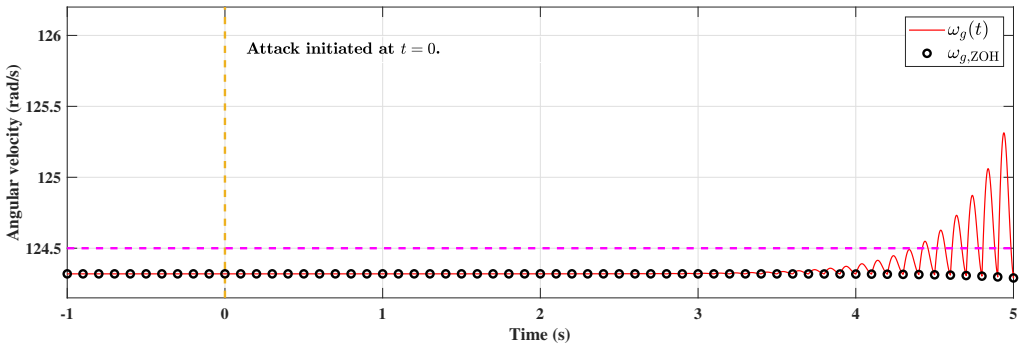
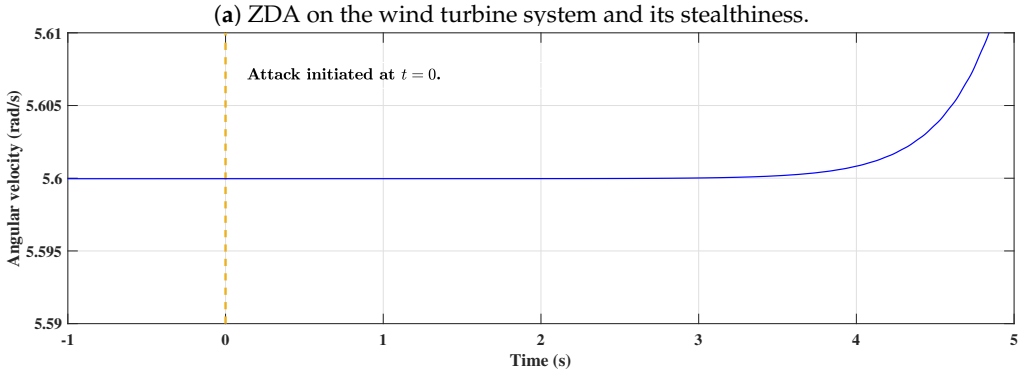


Figure 6. Zero-dynamics attack a_k signal when $T_s = 0.1$ s.

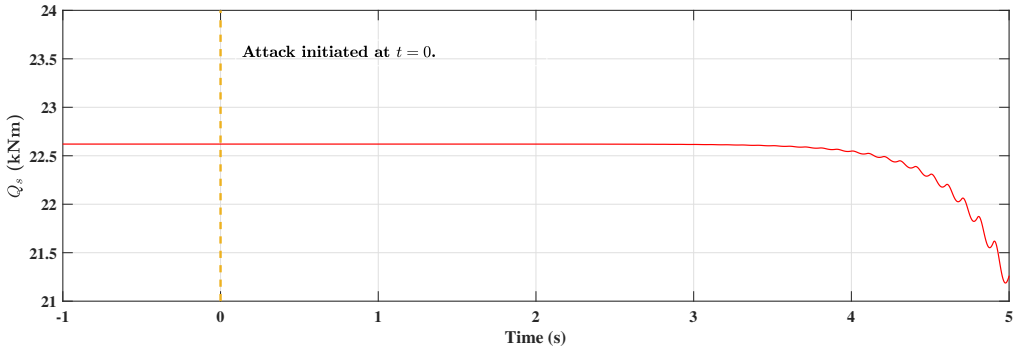


(**a**) ZDA on the wind turbine system and its stealthiness.

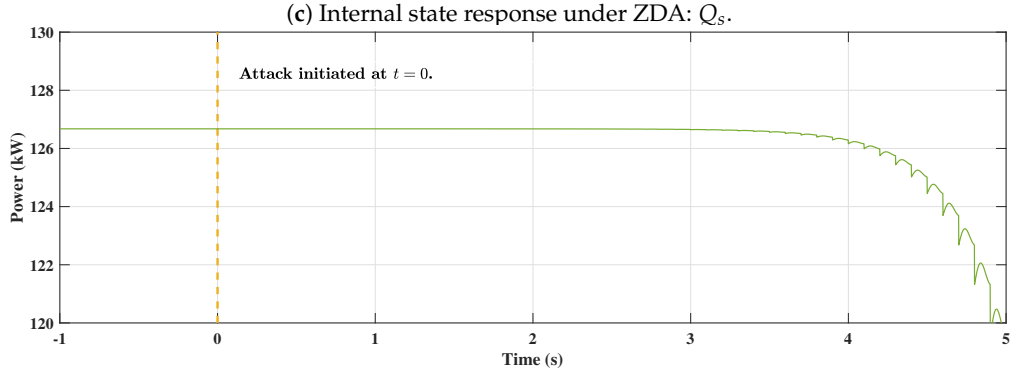


(**b**) Internal state response under ZDA: ω_r.

Figure 7. *Cont.*



(**c**) Internal state response under ZDA: Q_s.



(**d**) Generated power under ZDA.

Figure 7. Responses of the wind turbine under ZDA: with ZOH and SS.

4. Two Countermeasures against Zero-Dynamics Attack

ZDA becomes effective when the discrete-time system has an unstable zero and, as discussed in Section 3, it can happen even if the continuous-time system has stable zero dynamics. Among several countermeasures to ZDA, we introduce two strategies that share the same idea, shifting zeros. These approaches are based on the fact that the zeros of the discrete-time system can be arbitrarily assigned if the ZOH is replaced by a generalized hold (GH) or if a generalized sampler (GS) is used instead of SS [20]. Applications of these ideas to security problems are reported in [23,24], and in this section, we apply these approaches to wind turbine systems.

4.1. Generalized-Hold-Based Strategy

GH has been introduced in [20] and involves a function $h_g(t)$, the so-called hold function that is defined as a piecewise continuous function h_g so that the actual input applied to the system is given by

$$\hat{u}(t) = \sum_{k=-\infty}^{\infty} h_g(t - kT_s)\hat{u}_k.$$

If a GH having a hold function $h_g(t)$ is used instead of ZOH, the sampled-data model of wind turbine system (6) under constant wind speed $\bar{V}$ (so that $\hat{V} = 0$) and ZDA becomes

$$\begin{aligned} \hat{x}_{k+1} &= \hat{A}_\mathrm{d}\hat{x}_k + \hat{B}_g(\hat{u}_k + a_k) \\ \hat{y}_k &= C_\mathrm{d}\hat{x}_k, \end{aligned} \tag{14}$$

where $\hat{A}_\mathrm{d} = e^{\hat{A}_s T_s}$, $\hat{B}_g = \int_0^{T_s} e^{\hat{A}_s(T_s-\tau)}\hat{B}_s h_g(\tau)d\tau$, and $C_\mathrm{d} = C_s$. The discrete-time transfer function from the generator torque $\hat{u}_k (= \hat{T}_g)$ (equivalently from the attack a_k) to generator angular velocity $\hat{y}_k (= \hat{\omega}_g)$, denoted by $G_\mathrm{d}(z)$, is then given by

$$G_\mathrm{d}(z) = C_\mathrm{d}(zI - \hat{A}_\mathrm{d})^{-1}\hat{B}_g. \tag{15}$$

It is emphasized that since $(\hat{A}_s, \hat{B}_s)$ is controllable, one can always find a hold function h_g so that the zeros of $G_\mathrm{d}(z)$ can be placed anywhere in the complex plane [20,23].

Let $z_{d,1}$ and $z_{d,2}$ be the desired zeros located inside the unit circle and k_d be a gain. The problem is to find $\hat{B}_g$ such that the transfer function $G_\mathrm{d}(z)$ has desired zeros and gain, i.e., the following identity holds

$$G_\mathrm{d}(z) = C_\mathrm{d}(zI - \hat{A}_\mathrm{d})^{-1}\hat{B}_g = k_d \frac{(z - z_{d,1})(z - z_{d,2})}{\det(zI - \hat{A}_\mathrm{d})} =: G_\mathrm{d}^*(z).$$

Let $\det(zI - \hat{A}_\mathrm{d}) = z^3 + d_2 z^2 + d_1 z + d_0$. Then, $G_\mathrm{d}^*(z)$ can be realized in the control canonical form [54] given by

$$\begin{aligned} \bar{x}_{k+1} &= A_\mathrm{con}\bar{x}_k + B_\mathrm{con}\bar{u}_k \\ \bar{y}_k &= C_\mathrm{con}\bar{x}_k, \end{aligned} \tag{16}$$

where

$$A_\mathrm{con} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -d_0 & -d_1 & -d_2 \end{bmatrix},\ B_\mathrm{con} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix},\ C_\mathrm{con} = \begin{bmatrix} k_d z_{d,1} z_{d,2} & -k_d(z_{d,1} + z_{d,2}) & k_d \end{bmatrix}.$$

Equating the Markov parameters of the two transfer functions, one has

$$C_\mathrm{d}\hat{A}_\mathrm{d}^k\hat{B}_g = C_\mathrm{con}A_\mathrm{con}^k B_\mathrm{con},\ k = 0, 1, \ldots,$$

from which $\hat{B}_g$ is determined by

$$\hat{B}_g = \begin{bmatrix} C_\mathrm{d} \\ C_\mathrm{d}\hat{A}_\mathrm{d} \\ C_\mathrm{d}\hat{A}_\mathrm{d}^2 \end{bmatrix}^{-1} \begin{bmatrix} C_\mathrm{con} \\ C_\mathrm{con}A_\mathrm{con} \\ C_\mathrm{con}A_\mathrm{con}^2 \end{bmatrix} B_\mathrm{con}, \tag{17}$$

where the invertibility is assured by the observability of $(\hat{A}_\mathrm{d}, C_\mathrm{d})$.

As discussed in [20,23], one candidate of GH is to use a piecewise constant function given by

$$h_g(t) = h_i,\ \frac{(i-1)T_s}{N} \le t < \frac{iT_s}{N}, i = 1, \ldots, N,$$

where h_i are constant gains and N is the number of subintervals. It can be shown that the gains h_i and the vector $\hat{B}_g$ are related as

$$\hat{B}_g = \sum_{l=1}^{N} h_l \int_{\frac{(l-1)T_s}{N}}^{\frac{lT_s}{N}} e^{\hat{A}_s(T_s - \tau)}\hat{B}_s d\tau \tag{18}$$

and this can be rewritten as

$$\hat{B}_g = \begin{bmatrix} A_{\mathrm{d},N}^{N-1}B_{\mathrm{d},N} & \cdots & A_{\mathrm{d},N}B_{\mathrm{d},N} & B_{\mathrm{d},N} \end{bmatrix} h =: \mathcal{C}_{\mathrm{d},N}h,$$

where $h = [h_1, \ldots, h_N]^\top$ and

$$A_{\mathrm{d},N} = e^{\hat{A}_s\frac{T_s}{N}},\ B_{\mathrm{d},N} = \int_0^{\frac{T_s}{N}} e^{\hat{A}_s(\frac{T_s}{N} - \tau)}\hat{B}_s d\tau.$$

The hold gains are then computed as

$$h = C_{d,N}^\dagger \hat{B}_g. \tag{19}$$

For more details on the derivation, see [23].

4.2. Generalized-Sampler-Based Approach

By GS, we mean a device that generates a discrete-time signal $\check{y}_k$ from a continuous-time signal $y(t)$ in a way that N measurements (i.e., generator angular velocity) $y(\frac{1}{N}T_s + (k-1)T_s), y(\frac{2}{N}T_s + (k-1)T_s), \ldots, y(kT_s)$ are taken from the sampling interval $((k-1)T_s, kT_s]$ and a weighted average of them is computed as

$$\check{y}_k = \sum_{i=1}^{N} w_i y\left(\frac{i}{N}T_s + (k-1)T_s\right), \tag{20}$$

where $w_1, \ldots, w_N$ are weights for GS.

Similar to the case of GH, we can rewrite the system (6) under constant wind speed and ZDA as

$$\begin{aligned} \hat{x}_k &= \hat{A}_\mathrm{d}\hat{x}_{k-1} + \hat{B}_\mathrm{d}(\hat{u}_{k-1} + a_{k-1}) \\ \check{y}_k &= \check{C}_\mathrm{d}\hat{x}_{k-1} + \check{D}_\mathrm{d}(\hat{u}_{k-1} + a_{k-1}), \end{aligned} \tag{21}$$

where

$$\hat{A}_\mathrm{d} = e^{\hat{A}_s T_s}, \qquad \hat{B}_\mathrm{d} = \int_0^{T_s} e^{\hat{A}_s(T_s-\tau)}\hat{B}_s d\tau$$
$$\check{C}_\mathrm{d} = \sum_{i=1}^{N} w_i C_\mathrm{d} e^{\hat{A}_s \frac{i}{N}T_s}, \quad \check{D}_\mathrm{d} = \sum_{i=1}^{N} w_i C_\mathrm{d} \int_0^{\frac{i}{N}T_s} e^{\hat{A}_s(\frac{i}{N}T_s-\tau)}\hat{B}_s d\tau.$$

From (21), we can compute the transfer function from $\hat{u}_k$ to $\hat{y}_k$ as

$$G_\mathrm{d}(z) = z^{-1}(\check{C}_\mathrm{d}(zI - \hat{A}_\mathrm{d})^{-1}\hat{B}_\mathrm{d} + \check{D}_\mathrm{d}). \tag{22}$$

Note that $\check{C}_\mathrm{d}$ and $\check{D}_\mathrm{d}$ contain the sampler weights $w_1, \cdots, w_N$ of GS, which are design parameters. If the weights are chosen appropriately, it is expected that the numerator of the transfer function (22) can be chosen as desired. In fact, this is true under mild assumptions [24].

Let $z_{d,1}, z_{d,2}$, and $z_{d,3}$ be the desired zeros whose magnitudes are less than 1. We want to find the weights of GS such that the transfer function $G_\mathrm{d}(z)$ becomes identical to

$$G_\mathrm{d}^*(z) = k_d z^{-1}\frac{(z-z_{d,1})(z-z_{d,2})(z-z_{d,3})}{\det(zI - \hat{A}_\mathrm{d})}, \tag{23}$$

where k_d is a high-frequency gain. To proceed, let c_0, c_1, c_2 be such that $(z-z_{d,1})(z-z_{d,2})(z-z_{d,3}) = z^3 + c_2 z^2 + c_1 z + c_0$. We first find $\check{C}_\mathrm{d}$ and $\check{D}_\mathrm{d}$, then determine the weights w_i. As in the case of GH, we realize (23) in the control canonical form given by

$$\begin{aligned} \bar{x}_k &= A_\mathrm{con}\bar{x}_{k-1} + B_\mathrm{con}\bar{u}_{k-1} \\ \bar{y}_k &= C_\mathrm{con}\bar{x}_{k-1} + D_\mathrm{con}\bar{u}_{k-1}, \end{aligned}$$

where A_con and B_con are identical to those of (16), and

$$C_\mathrm{con} = \begin{bmatrix} k_d(c_0 - d_0) & k_d(c_1 - d_1) & k_d(c_2 - d_2) \end{bmatrix}, \; D_\mathrm{con} = k_d.$$

From the fact that two transfer functions $G_\mathrm{d}(z)$ and $G_\mathrm{d}^*(z)$ are identical if and only if

$$\begin{aligned} \check{D}_\mathrm{d} &= D_\mathrm{con} \\ \check{C}_\mathrm{d}\hat{A}_\mathrm{d}^k\hat{B}_\mathrm{d} &= C_\mathrm{con}A_\mathrm{con}^k B_\mathrm{con}, \; k = 0, 1, \ldots, \end{aligned}$$

we have, from the controllability of $(\hat{A}_\mathrm{d}, \hat{B}_\mathrm{d})$,

$$\check{C}_\mathrm{d} = C_\mathrm{con}\begin{bmatrix} B_\mathrm{con} & A_\mathrm{con}B_\mathrm{con} & A_\mathrm{con}^2 B_\mathrm{con}\end{bmatrix}\begin{bmatrix}\hat{B}_\mathrm{d} & \hat{A}_\mathrm{d}\hat{B}_\mathrm{d} & \hat{A}_\mathrm{d}^2\hat{B}_\mathrm{d}\end{bmatrix}^{-1}$$
$$\check{D}_\mathrm{d} = k_d.$$

With $\check{C}_\mathrm{d}$ and $\check{D}_\mathrm{d}$ obtained above, it follows from the relation between the weights and $(\check{C}_\mathrm{d}, \check{D}_\mathrm{d})$ that

$$\begin{bmatrix}\check{C}_\mathrm{d} & \check{D}_\mathrm{d}\end{bmatrix} = w\begin{bmatrix} C_\mathrm{d}e^{\hat{A}_s\frac{1}{N}T_s} & C_\mathrm{d}\int_0^{\frac{1}{N}T_s} e^{\hat{A}_s(\frac{1}{N}T_s-\tau)}\hat{B}_s d\tau \\ C_\mathrm{d}e^{\hat{A}_s\frac{2}{N}T_s} & C_\mathrm{d}\int_0^{\frac{2}{N}T_s} e^{\hat{A}_s(\frac{2}{N}T_s-\tau)}\hat{B}_s d\tau \\ \vdots & \vdots \\ C_\mathrm{d}e^{\hat{A}_s T_s} & C_\mathrm{d}\int_0^{T_s} e^{\hat{A}_s(T_s-\tau)}\hat{B}_s d\tau \end{bmatrix} =: wM,$$

and the weights are computed as

$$w = \begin{bmatrix}\check{C}_\mathrm{d} & \check{D}_\mathrm{d}\end{bmatrix}M^\dagger, \tag{24}$$

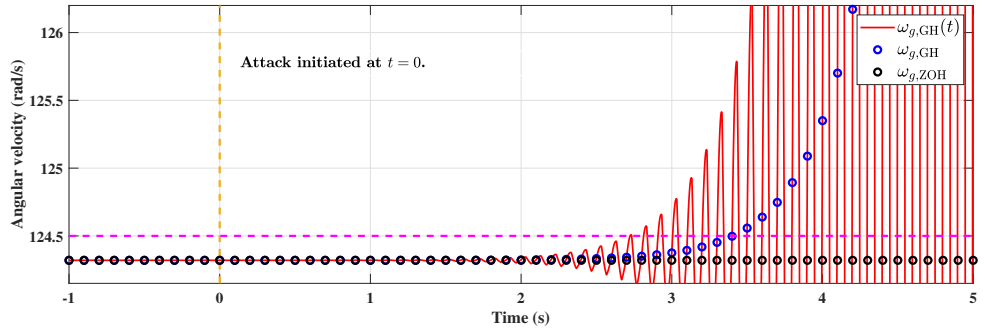
where $M^\dagger$ is the pseudo-inverse of M. For more details, see [24].

5. Evaluation of Countermeasures against ZDA

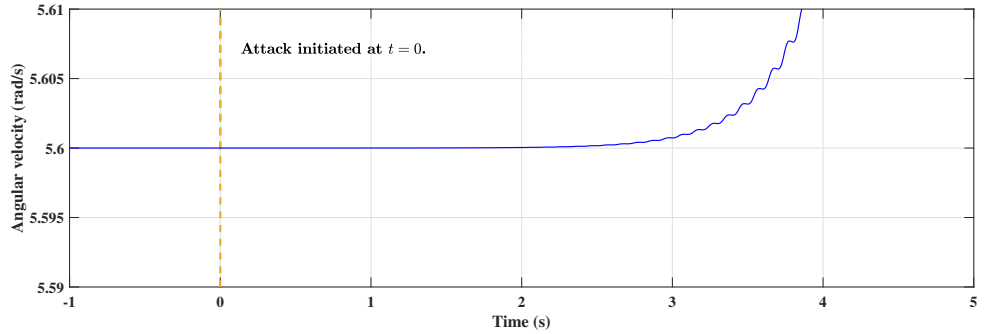
In this section, we apply the theory given in Section 4 and demonstrate that the two countermeasures that can shift the zeros into the stable region effectively reveal the presence of ZDA. Although both approaches work well in ideal situations, they also face challenges arising from practical issues such as nonlinearities and measurement noise. These issues are also discussed through intensive numerical simulations.

Following the procedure described in Section 4, a GH is designed so that the discrete-time system has zeros at $z_{d,1} = 0.1$ and $z_{d,1} = 0.9$. We use a piecewise constant hold function with three subintervals ($N = 3$) and the hold gain is $h = [2.155, -0.577, 1.422]^\top$. The sampling time is given by $T_s = 0.1$ s. Figure 8 shows the behavior of the system under the ZDA (11) that has been designed using the system parameters S_d, g_d, and ψ_d assuming that ZOH and SS are used to interface analog and digital signals. The attack is injected when the system is at a steady state (rated power point). It is seen that the generator angular velocity $\omega_g(t)$ starts oscillating with increasing magnitude and this is captured by the sampled output $\omega_g(kT_s)$ (denoted as $\omega_{g,\mathrm{GH}}$ in the figure) when GH is used, while the sampled output under ZOH remains almost unchanged. It is noted that the signal $\omega_{g,\mathrm{ZOH}}$ also diverges as time goes to infinity but very slowly compared to $\omega_{g,\mathrm{GH}}$, which means that it is practically meaningless to use $\omega_{g,\mathrm{ZOH}}$ as a monitoring signal for the purpose of attack detection. This comes from the nonlinearity of the wind turbine; the diverging attack signal makes the state variables escape the region where the linear approximation is valid.

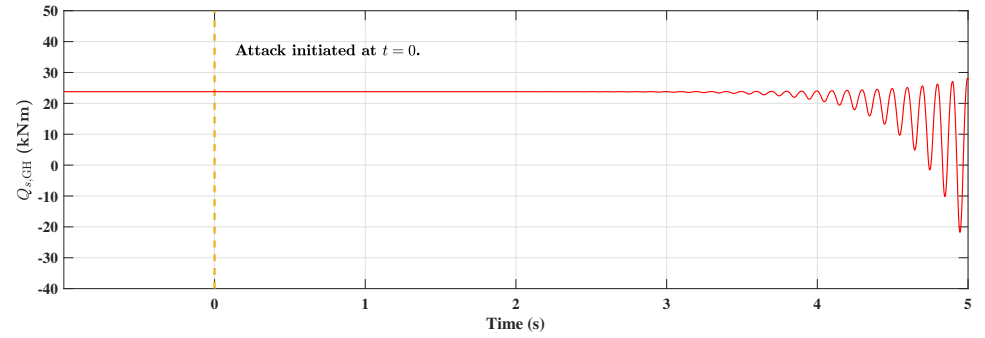
It is well known that even though a GH can shift the zeros to desired locations, it may induce a violent transient between sampling instants [20]. Typically, this can happen when the pattern associated to the GH has a large transition. For example, consider the GH designed above and suppose that the control input generated by the GH using $u_k = \bar{T}_g$, shown in Figure 9a, is applied to the wind turbine. Then, as can be seen in Figure 9b, the sampled output $\omega_{g,\mathrm{GH}}$ seems to converge to a constant, but its continuous-time counterpart oscillates severely, and this can happen even if no attack is injected.



(**a**)

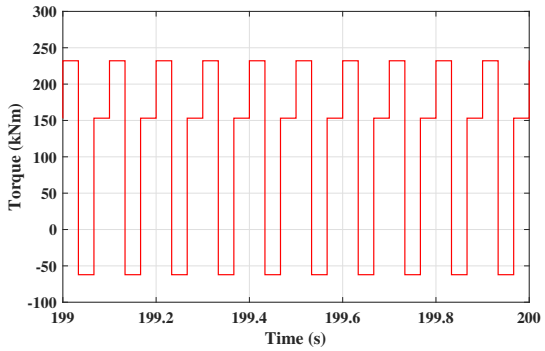


(**b**)

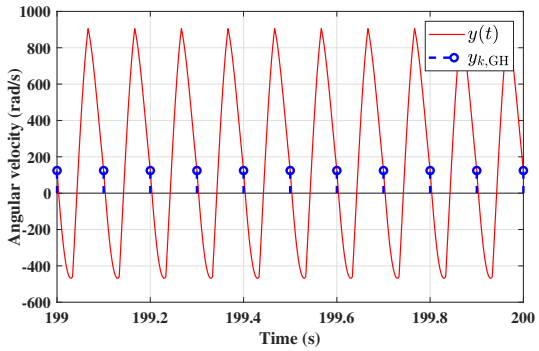


(**c**)

Figure 8. Response of the wind turbine under ZDA, generalized hold (GH) with desired zeros 0.1 and 0.9. (**a**) Response of system output (generator angular velocity), continuous-time signal $\omega_{g,\mathrm{GH}}(t)$ and its sampled signal $\omega_{g,\mathrm{GH}}$. For comparison, $\omega_{g,\mathrm{ZOH}}$ (identical to Figure 7a) is also drawn. (**b**) Response of internal variable, ω_r. (**c**) Response of internal variable, Q_s.



(**a**)



(**b**)

Figure 9. (**a**) Control input generated by a GH; (**b**) generator angular velocity $\omega_g(t)$ and its sampled signal $\omega_{g,\mathrm{GH}}$.

The possibly undesirable intersample behavior can be avoided by using GS instead of SS at the output side and using ZOH at the input side. To demonstrate this, we follow the

design described in Section 4 to obtain a GS with $N = 4$ and $w = [-28.252, 58.5731, -70.906, 41.5846]$ so that the zeros are placed at $z_{d,1} = 0.1$, $z_{d,2} = 0.9$, and $z_{d,3} = 0$. Figure 10 shows that the presence of ZDA can be detected by monitoring the signal $\omega_{g,\mathrm{GS}}$, which is the output of the GS. In the simulation, the same ZDA injected in the case of GH is used. It is emphasized that the behavior of the internal states are the same as the case with ZOH and SS shown in Figure 7, and it is free of violent intersample behavior possibly induced by a GH.

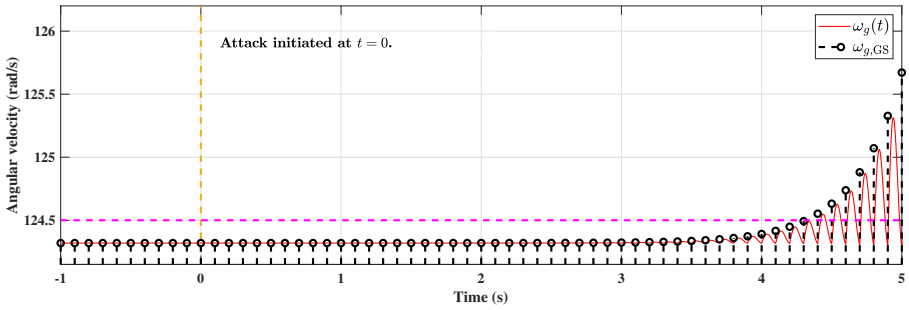
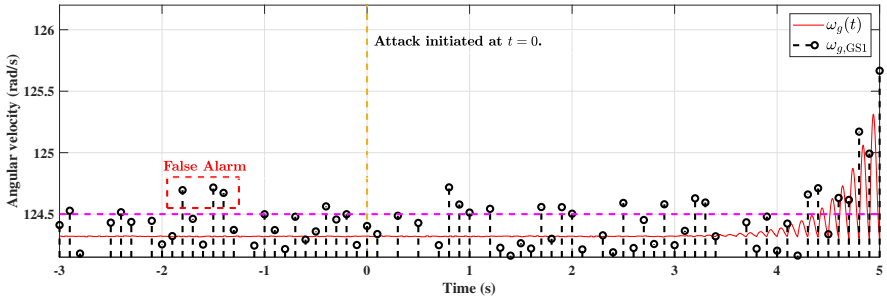
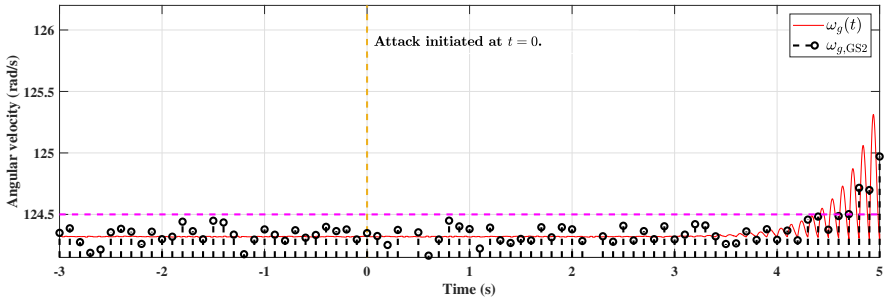


Figure 10. ZDA detection using a generalized sampler (GS).

In practice, the noise of measurements is always present and if the weights of GS are very large, then the noise will be amplified, leading to a false alarm. To demonstrate this, suppose that the measurement $\omega_g(t)$ is contaminated by noise and consider two designs of GS: GS1 with $w = [-28.252, 58.5731, -70.906, 41.5846]$ and $z_{d,1} = 0.1$, $z_{d,2} = 0.9$, $z_{d,3} = 0$; GS2 with $w = [-8.924, 18.983, -22.903, 13.844]$ and $z_{d,1} = 0.1$, $z_{d,2} = 0.7$, $z_{d,3} = 0$. Figure 11 shows the effect of the measurement noise under the same setting of Figure 10. The sampled output of GS $\check{y}_k$ is denoted by $\omega_{g,\mathrm{GS}}$ in the figure. In Figure 11a, some of the sampled outputs of GS $\omega_{g,\mathrm{GS1}}$ exceed the threshold although no attack signal is injected, leading to a false alarm. On the contrary, Figure 11b shows that GS2 with relatively smaller weights is less affected by measurement noise.



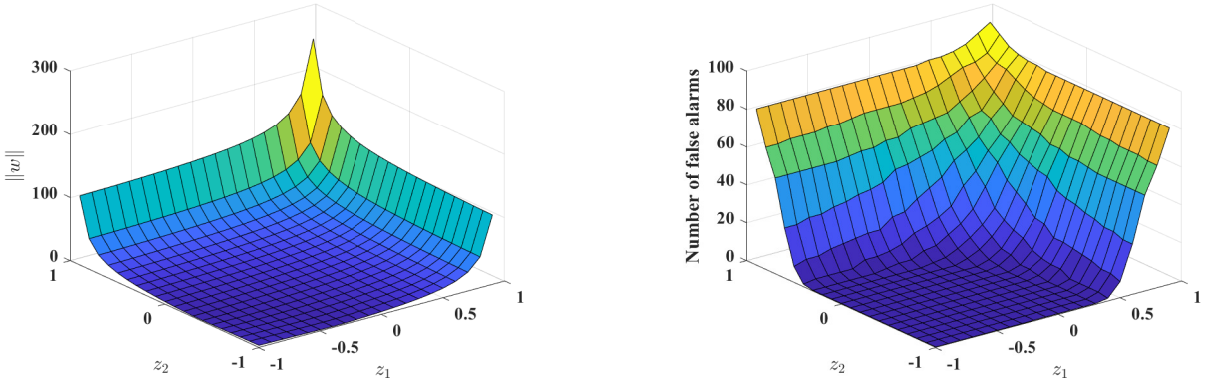
(**a**) False alarm due to measurement noise.



(**b**) False alarm removed with reduced sampler weight.

Figure 11. GS simulation with measurement noise.

Since the sampler weights depend on the location of desired zeros, we numerically investigate how they are related. With N and $z_{d,3}$ fixed as $N = 4$ and $z_{d,3} = 0$, the desired zeros $z_{d,1}, z_{d,2}$ are selected from $(-1, 1) \times (-1, 1)$ and the corresponding sampler weights are determined. The result is shown in Figure 12a. In addition, by doing the simulation with the designed GS, we count the number of false alarms, see Figure 12b. It is observed that the number of false alarms is roughly proportional to the norm of sampler weights, and this explains why GS2 is less sensitive to measurement noise.



(**a**) Norm of sampler weight w.

(**b**) Number of false alarms.

Figure 12. Effect of the location of desired zeros on the size of sampler weight and the number of false alarms.

6. Conclusions

In this paper, we study the security problem on wind turbines that are controlled and monitored through the communication network. It is shown that at the rated power point, the linearized discrete-time model of the wind turbine has an unstable zero for a range of sampling periods, which means that wind turbines that are digitally controlled are vulnerable to zero-dynamics attacks. In order to increase security against ZDA, two countermeasures based on generalized hold and generalized sampler have been proposed with detailed design procedures, and through numerical simulations, it is shown that these approaches make ZDA ineffective. Practical issues such as nonlinearities and measurement noise are discussed in detail.

We are currently working on a robust and optimal design of the proposed strategies, which are challenging research topics. Validation of the proposed approaches using more realistic models or software and simultaneous design of two components are also interesting future research topics.

Author Contributions: Idea development and analysis, D.K. and K.R.; writing—original draft, D.K. and K.R.; supervision, J.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Korea Institute of Energy Technology Evaluation and Planning(KETEP) grant funded by the Korea government (MOTIE) (20204030200010, Graduate Track for Core Technologies of Wind Power System Engineering) and the Research Grant of Kwangwoon University in 2019.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. International Renewable Energy Association. *Future of Wind: Deployment, Investment, Technology, Grid Integration and Socio-Economic Aspects (A Global Energy Transformation Paper)*; International Renewable Energy Agency: Abu Dhabi, United Arab Emirates, 2017.
2. Lee, R.M.; Assante, M.J.; Conway, T. German steel mill cyber attack. *Ind. Control. Syst.* **2014**, *30*, 62.
3. Kesler, B. The vulnerability of nuclear facilities to cyber attack. *Strateg. Insights* **2011**, *10*, 15–25.
4. Alert, I.C. *Cyber-Attack against Ukrainian Critical Infrastructure*; Tech. Rep. ICS Alert (IR-ALERT-H-16-056-01); Cybersecurity Infrastruct. Secur. Agency: Washington, DC, USA, 2016.
5. Cárdenas, A.A.; Amin, S.; Lin, Z.S.; Huang, Y.L.; Huang, C.Y.; Sastry, S. Attacks Against Process Control Systems: Risk Assessment, Detection, and Response. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11), Hong Kong, China, 22–24 March 2011; pp. 355–366.
6. Sridhar, S.; Manimaran, G. Data integrity attacks and their impacts on SCADA control system. In Proceedings of the IEEE PES General Meeting, Providence, RI, USA , 25–29 July 2010; pp. 1–6. [CrossRef]
7. Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K.H. Revealing stealthy attacks in control systems. In Proceedings of the 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 1–5 October 2012; pp. 1806–1813.
8. Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K.H. A secure control framework for resource-limited adversaries. *Automatica* **2015**, *51*, 135—148. [CrossRef]
9. Ding, D.; Han, Q.L.; Ge, X.; Wang, J. Secure state estimation and control of cyber-physical systems: A survey. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *51*, 176–190. [CrossRef]
10. Mahmoud, M.S.; Hamdan, M.M.; Baroudi, U.A. Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges. *Neurocomputing* **2019**, *338*, 101–115. [CrossRef]
11. Giraldo, J.; Urbina, D.; Cardenas, A.; Valente, J.; Faisal, M.; Ruths, J.; Tippenhauer, N.O.; Sandberg, H.; Candell, R. A survey of physics-based attack detection in cyber-physical systems. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 1–36. [CrossRef]
12. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. *Computer* **2002**, *35*, 54–62. [CrossRef]
13. Mallikarjunan, K.N.; Muthupriya, K.; Shalinie, S.M. A survey of distributed denial of service attack. In Proceedings of the 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 7-8 January 2016; pp. 1–6.
14. Agarwal, M.; Purwar, S.; Biswas, S.; Nandi, S. Intrusion detection system for PS-Poll DoS attack in 802.11 networks using real time discrete event system. *IEEE/CAA J. Autom. Sin.* **2016**, *4*, 792–808. [CrossRef]
15. Li, X.; Wang, Q.; Dai, H.N.; Wang, H. A novel friendly jamming scheme in industrial crowdsensing networks against eavesdropping attack. *Sensors* **2018**, *18*, 1938. [CrossRef]
16. Malladi, S.; Alves-Foss, J.; Heckendorn, R.B. *On Preventing Replay Attacks on Security Protocols*; Technical Report; Idaho University Moscow Department of Computer Science: Moscow, Idaho, 2002.
17. Schellenberger, C.; Zhang, P. Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system. In Proceedings of the 2017 IEEE 56th Annual Conference on Decision and Control (CDC), Melbourne, Australia, 12–15 December 2017; pp. 1374–1379. [CrossRef]
18. Park, G.; Shim, H.; Lee, C.; Eun, Y.; Johansson, K.H. When adversary encounters uncertain cyber-physical systems: Robust zero-dynamics attack with disclosure resources. In Proceedings of the 2016 IEEE 55th Conference on Decision and Control (CDC), Las Vegas, NV, USA, 12–14 December 2016; pp. 5085–5090.
19. Jeon, H.; Eun, Y. A Stealthy Sensor Attack for Uncertain Cyber-Physical Systems. *IEEE Internet Things J.* **2019**, *6*, 6345–6352. [CrossRef]
20. Yuz, J.I.; Goodwin, G.C. *Sampled-Data Models for Linear and Nonlinear Systems*; Springer: London, UK, 2014.
21. Hoehn, A.; Zhang, P. Detection of covert attacks and zero dynamics attacks in cyber-physical systems. In Proceedings of the 2016 American Control Conference (ACC), Boston, MA, USA, 6–8 July 2016; pp. 302–307.
22. Naghnaeian, M.; Hirzallah, N.; Voulgaris, P.G. Dual rate control for security in cyber-physical systems. In Proceedings of the 2015 54th IEEE Conference on Decision and Control (CDC), Osaka, Japan, 15–18 December 2015; pp. 1415–1420. [CrossRef]
23. Kim, J.; Back, J.; Park, G.; Lee, C.; Shim, H.; Voulgaris, P.G. Neutralizing zero dynamics attack on sampled-data systems via generalized holds. *Automatica* **2020**, *113*, 108778. [CrossRef]
24. Kim, D.; Ryu, K.; Back, J. Security Enhancement of Sampled-Data Systems: Zero Assignment via Generalized Sampler. In Proceedings of the 21st IFAC World Congress 2020, Berlin, Germany, 12–17 July 2020.
25. Naghnaeian, M.; Hirzallah, N.; Voulgaris, P.G. Security via multirate control in cyber–physical systems. *Syst. Control. Lett.* **2019**, *124*, 12—18. [CrossRef]
26. Mao, Y.; Jafarnejadsani, H.; Zhao, P.; Akyol, E.; Hovakimyan, N. Novel stealthy attack and defense strategies for networked control systems. *IEEE Trans. Autom. Control.* **2020**, *65*, 3847-3862 [CrossRef]
27. Gallo, A.J.; Turan, M.S.; Boem, F.; Parisini, T.; Ferrari-Trecate, G. A distributed cyber-attack detection scheme with application to DC microgrids. *IEEE Trans. Autom. Control.* **2020**, *65*, 3800–3815. [CrossRef]
28. Singh, M.; Santoso, S. *Dynamic Models for Wind Turbines and Wind Power Plants*; Technical Report; National Renewable Energy Laboratory (NREL): Golden, CO, USA, 2011.
29. Lubosny, Z.; Lubosny, Z. *Wind Turbine Operation in Electric Power Systems: Advanced Modeling*; Springer: Berlin/Heidelberg, Germany, 2003.

30. Bianchi, F.D.; De Battista, H.; Mantz, R.J. *Wind Turbine Control Systems: Principles, Modelling and Gain Scheduling Design*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2006.
31. Georg, S.; Schulte, H.; Aschemann, H. Control-oriented modelling of wind turbines using a Takagi-Sugeno model structure. In Proceedings of the 2012 IEEE International Conference on Fuzzy Systems, Brisbane, Australia, 10–15 June 2012; pp. 1–8.
32. Simani, S. Overview of modelling and advanced control strategies for wind turbine systems. *Energies* **2015**, *8*, 13395–13418. [CrossRef]
33. Ansoategui, I.; Zulueta, E.; Fernandez-Gamiz, U.; Lopez-Guede, J.M. Mechatronic Modeling and Frequency Analysis of the Drive Train of a Horizontal Wind Turbine. *Energies* **2019**, *12*, 613. [CrossRef]
34. Novak, P. *On the Modelling and Partial-Load Control of Variable-Speed Wind Turbines*; Technical Report; Chalmers University of Technology, Göteborg, Sweden, August 1995.
35. Kim, K.H.; Van, T.L.; Lee, D.C.; Song, S.H.; Kim, E.H. Maximum output power tracking control in variable-speed wind turbine systems considering rotor inertial power. *IEEE Trans. Ind. Electron.* **2012**, *60*, 3207–3217.
36. Manyonge, A.W.; Ochieng, R.; Onyango, F.; Shichikha, J. Mathematical modelling of wind turbine in a wind energy conversion system: Power coefficient analysis. *Appl. Math. Sci.* **2012**, *6*, 4527–4536.
37. Dai, J.; Hu, Y.; Liu, D.; Wei, J. Modelling and analysis of direct-driven permanent magnet synchronous generator wind turbine based on wind-rotor neural network model. *Proc. Inst. Mech. Eng. Part A J. Power Energy* **2012**, *226*, 62–72. [CrossRef]
38. Available online: https://www.argolabe.es/100kw-windturbine.html (accessed on 28 January 2021).
39. Maldonado-Correa, J.; Martín-Martínez, S.; Artigao, E.; Gómez-Lázaro, E. Using SCADA Data for Wind Turbine Condition Monitoring: A Systematic Literature Review. *Energies* **2020**, *13*, 3132. [CrossRef]
40. Pandit, R.; Infield, D. Gaussian process operational curves for wind turbine condition monitoring. *Energies* **2018**, *11*, 1631. [CrossRef]
41. Yang, W.; Court, R.; Jiang, J. Wind turbine condition monitoring by the approach of SCADA data analysis. *Renew. Energy* **2013**, *53*, 365–376. [CrossRef]
42. Sun, P.; Li, J.; Wang, C.; Lei, X. A generalized model for wind turbine anomaly identification based on SCADA data. *Appl. Energy* **2016**, *168*, 550–567. [CrossRef]
43. Zaher, A.; McArthur, S.; Infield, D.; Patel, Y. Online wind turbine fault detection through automated SCADA data analysis. *Wind. Energy Int. J. Prog. Appl. Wind. Power Convers. Technol.* **2009**, *12*, 574–593. [CrossRef]
44. Qiu, Y.; Feng, Y.; Tavner, P.; Richardson, P.; Erdos, G.; Chen, B. Wind turbine SCADA alarm analysis for improving reliability. *Wind Energy* **2012**, *15*, 951–966.
45. Tautz-Weinert, J.; Watson, S.J. Using SCADA data for wind turbine condition monitoring—A review. *IET Renew. Power Gener.* **2016**, *11*, 382–394. [CrossRef]
46. Smith, R.S. Covert misappropriation of networked control systems: Presenting a feedback structure. *IEEE Control. Syst. Mag.* **2015**, *35*, 82–92.
47. Mo, Y.; Weerakkody, S.; Sinopoli, B. Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control. Syst. Mag.* **2015**, *35*, 93–109.
48. Canaan, B.; Colicchio, B.; Ould Abdeslam, D. Microgrid Cyber-Security: Review and Challenges toward Resilience. *Appl. Sci.* **2020**, *10*, 5649. [CrossRef]
49. Pasqualetti, F.; Dörfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control.* **2013**, *58*, 2715–2729. [CrossRef]
50. Teixeira, A.; Dán, G.; Sandberg, H.; Johansson, K.H. A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator. *IFAC Proc. Vol.* **2011**, *44*, 11271–11277. [CrossRef]
51. Park, G.; Lee, C.; Shim, H.; Eun, Y.; Johansson, K.H. Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zero-dynamics attack. *IEEE Trans. Autom. Control.* **2019**, *64*, 4907–4919. [CrossRef]
52. Teixeira, A.; Pérez, D.; Sandberg, H.; Johansson, K.H. Attack models and scenarios for networked control systems. In Proceedings of the 1st International Conference on High Confidence Networked Systems, Beijing, China, 17–18 April 2012; pp. 55–64.
53. Khalil, H.K. *Nonlinear Systems*, 3rd ed.; Prentice-Hall: Upper Saddle River, NJ, USA, 2002.
54. Chen, C.T. *Linear System Theory and Design*, 4th ed.; Oxford University Press: New York, NY, USA, 2013.