electronics

MDPI

Article

Cyber-Resilient Converter Control System for Doubly Fed Induction Generator-Based Wind Turbine Generators

Nathan Farrar and Mohd. Hasan Ali *

Department of Electrical and Computer Engineering, The Herff College of Engineering, The University of Memphis, Memphis, TN 38152, USA; n.farrar@memphis.edu
* Correspondence: mhali@memphis.edu

Abstract: As wind turbine generator systems become more common in the modern power grid, the question of how to adequately protect them from cyber criminals has become a major theme in the development of new control systems. As such, artificial intelligence (AI) and machine learning (ML) algorithms have become major contributors to preventing, detecting, and mitigating cyber-attacks in the power system. In their current state, wind turbine generator systems are woefully unprepared for a coordinated and sophisticated cyber attack. With the implementation of the internet-of-things (IoT) devices in the power control network, cyber risks have increased exponentially. The literature shows the impact analysis and exploring detection techniques for cyber attacks on the wind turbine generator systems; however, almost no work on the mitigation of the adverse effects of cyber attacks on the wind turbine control systems has been reported. To overcome these limitations, this paper proposes implementing an AI-based converter controller, i.e., a multi-agent deep deterministic policy gradient (DDPG) method that can mitigate any adverse effects that communication delays or bad data could have on a grid-connected doubly fed induction generator (DFIG)-based wind turbine generator or wind farm. The performance of the proposed DDPG controller has been compared with that of a variable proportional–integral (VPI) control-based mitigation method. The proposed technique has been simulated and validated utilizing the MATLAB/Simulink software, version R2023A, to demonstrate the effectiveness of the proposed method. Also, the performance of the proposed DDPG method is better than that of the VPI method in mitigating the adverse impacts of cyber attacks on wind generator systems, which is validated by the plots and the root mean square error table found in the results section.

Keywords: cyber attack; wind turbine generator; artificial intelligence; mitigation; converter

Citation: Farrar, N.; Ali, M.H. Cyber-Resilient Converter Control System for Doubly Fed Induction Generator-Based Wind Turbine Generators. *Electronics* **2024**, *13*, 492. https://doi.org/10.3390/electronics13030492

Academic Editors: Georgios Papadakis, George Kyriakarakos and Christos-Spyridon Karavas

Received: 27 December 2023
Revised: 19 January 2024
Accepted: 22 January 2024
Published: 24 January 2024

1. Introduction

Thanks to the global initiative to reduce the effects of energy production on climate change, distributed energy resources (DER) have become an important contributor to the modern power grid, with wind energy being the preferred DER implemented globally. According to the Pacific Northwest National Laboratory, wind energy represents more than 10 percent of the electricity produced in the United States, making it the largest contribution of renewable power generation in the nation [1]. On 21 November 2023, the Biden–Harris administration announced its approval of the Empire Wind Project, the sixth approval of an off-shore wind energy project under the administration, supporting President Biden's goal of 30 GW of offshore wind energy capacity by the year 2030 [2].

Many wind farms are in very remote locations or offshore and are subject to right-of-way constrictions of local and regional municipalities, and due to their incredible size, finding the right location can be challenging. To optimize the energy produced by wind farms, a detailed analysis of wind power flow through possible site locations must be performed to insure the investment in wind energy yields not only a steady supply of energy, but also reliable profits for investors [3]. To help alleviate these constraints, remote

internet-of-things (IoT) devices are becoming a common solution to monitor, control, and manage wind farm power systems.

There are several different types of wind turbine generators, and depending on the available resources such as location, budget, and municipal regulations, the optimal generator should be implemented. In the last few decades, synchronous generators, such as the permanent magnet synchronous generator, have been used due to their high reliability. However, due to wind speeds being variable, an expensive gear box, torque converter, and speed converter are necessary to maintain the synchronous speed of the generator [4]. Due to these issues, many modern wind farms are implementing induction generators, such as the double-fed induction generator (DFIG), due to their lower costs and variable speeds [5]. Induction generators are variable-speed, so they do not require a sophisticated gearbox to maintain a synchronous speed. However, they do require intelligent electronic devices such as AC/DC converters, voltage source converters inverters (VSC), and a step-up gearbox, and they may also use energy storage systems to remove any fluctuations in the generator frequency and to boost power output when wind speeds are low, as reported in ref. [6]. Because DFIGs allow for the decoupling of real and reactive power through the independent control of torque and rotor excitation currents, they have become a preferable generator for modern wind farms. Figure 1 depicts a grid connected DFIG-based wind turbine generator model with pitch angle control and a rotor-side converter, grid-side converter, DC-link capacitor, turbine blades, rotor shaft, and set-up gearbox.

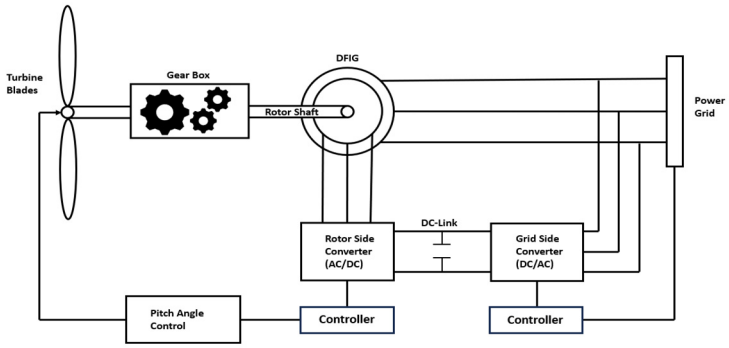


Figure 1. DFIG-based wind turbine generator model.

With the increased implementation of IoT devices in wind farm control schemes, major cybersecurity risks have arisen that, if not rectified quickly, could lead to major losses in revenue for power providers, as well as unstable and unreliable power for consumers. Historically, cyber attacks on wind farms have been isolated to ransomware attacks, which involve hacking into a vendor's wide area network (WAN) and stealing as much data as possible before severing communication lines to control devices and holding the data and devices hostage until a monetary demand is met. On 19 November 2021, a wind farm operated by the Danish wind turbine manufacturer Vestas was attacked by a LockBit ransomware attack that stole sensitive proprietary data and employee personal information [7]. Thanks to the quick response of Vestas's cyber response team, no third-party vendors were affected, and no damage was reported in any wind farms [7]. In March 2022, the wind farm operator Enercon lost control of their satellite communication with approximately 5800 wind turbine generators [7]. The staff were forced to shut down the entire wind farm system, effectively removing 11,000 MW of power from the interconnected power grid. As of 15 March 2022, only 15%—roughly 900 wind turbine generators—had been restored [7]. In this case, no damage was reported to any wind turbine generators.

Again, in March 2022, the wind farm operator Nordex SE was hit with a Conti ransomware attack that forced the entire platform offline [7]. The attack only affected the internal IT infrastructure, and no third-party assets were affected [7]. No wind turbine generator damage was reported as a result of this attack. Lastly, on 11 April 2022, the wind farm operator Deutsche Windtechnik AG was attacked by a ransomware attack and lost

control of 2000 wind turbine generators [7]. The incident forced the responders to switch off the remote data monitoring connections to the wind turbine system, effectively shutting the turbines down for 48 h [7].

To reduce the occurrence and effects of malicious attacks, researchers and engineers must continuously develop advanced control schemes to protect these vital assets to maintain a reliable power supply to consumers and prevent losses of revenue for utility providers. Based on a thorough literature review, very few artificial intelligence (AI)-based control methods have been utilized to both detect and mitigate cyber attacks on wind farms. An event-triggered scheme is proposed in the presence of denial of service (DoS) attacks, which are carried out by a class of periodically detectable jammers [8]. By taking the event-triggered scheme under DoS attacks and deception attacks into consideration, a new model for LFC multiarea power systems is constructed as a switched system. On the basis of the new model, the exponentially mean-square stability of LFC multiarea power systems is obtained by virtue of Lyapunov stability theory. The work [9] proposes a test-bed performance evaluation of attack-resilient control for wind farm supervisory control and data acquisition (SCADA) that detects different cyber attacks on SCADA measurements and provides mitigation using forecast information. In the work of ref. [10], a dynamic model is improved for LFC considering cyber attacks, load disturbance, and the influence of variable wind speeds of a wind farm. A consensus-based distributed control system for modular multilevel converter (MMC) submodules (SMs) was proposed in ref. [11] to prevent bad data attacks. Additionally, a Kalman Filter-based FDIA detection method was introduced. The work of ref. [12] deals with Pearson correlation coefficient data points with an autoencoder/decoder and a time sequence machine learning algorithm approach to find outliers efficiently and to detect false data injection attacks (FDIAs)/bad data injection attacks (BDIAs) and DoS.

Although there are many methods used for monitoring and controlling wind turbine generators and a plethora of methods used to detect cyber attacks on wind farms, the clear lack of mitigation methods other than removing the entire wind farm from the power grid leads to room for improvement in the current control methodology. Specifically, a control method that can not only mitigate data injection attacks to controller set-point values but also manage the wind turbine generators during network attacks is lacking. Therefore, more research in this area is necessary to protect wind farm assets. Based on the National Institute of Standards and Technology (NIST) special publication 800-207, new cyber architectures for access control with respect to wind turbine generators are necessary to prevent cyber attacks on the energy management system [13]. This fact motivates the proposed research, and it introduces an important research question on how a cyber-resilient converter control-based wind farms can be developed.

Based on the above background, this paper proposes a multi-agent deep deterministic policy gradient (DDPG) controller for cyber attack mitigation in a wind farm. There are several reasons and key factors for choosing the DDPG in this work. Firstly, wind farm control often involves making continuous adjustments to the pitch angles of wind turbine blades and other parameters. A DDPG agent is designed for solving problems with continuous action spaces, making it well-suited for such tasks. Other networks such as deep-Q networks (DQN) or artificial neural networks (ANN) are designed for discrete action spaces, and while the data can be discretized, they may be insufficient to capture all the features of the action space. DDPG also uses a deterministic policy, which can lead to more stable training and better convergence in continuous control tasks. In wind farm control, stability is crucial to ensure that the turbines operate efficiently and safely. DQN, on the other hand, uses a stochastic policy and can be less stable in continuous action spaces.

Another key feature of DDPG algorithms is that they incorporate experience replay, which helps in breaking correlations between consecutive experiences, making the learning process more stable. This is important in scenarios where data can be highly correlated, such as wind data. DQN also uses experience replay, but it is more critical in continuous action spaces leading to longer training times and a higher likelihood of convergence challenges.

Also, DDPG employs target networks for both the actor and critic networks. This stabilizes the learning process by making the target values less volatile. This is particularly beneficial for wind farm control, where actions can have delayed and long-term effects on the stability of the system. DQN also uses target networks, but ANNs typically do not.

Another key feature of DDPG is that it utilizes an actor–critic method. This means that it maintains two separate neural networks, one for estimating the value function (critic) and one for estimating the policy (actor). This separation of tasks makes it easier to optimize the policy in complex environments such as wind farms. Wind farm control also requires a balance between exploration and exploitation. DDPG incorporates noise in the action space for exploration, which allows it to explore different control actions systematically. DDPG is known for being more sample-efficient than DQN and in wind farm control, where collecting data can be costly or time-consuming. DDPG typically requires fewer samples to achieve better performances, whereas ANNs, without a reinforcement learning framework, may struggle with the exploration–exploitation balance. Lastly, wind farm control often involves optimizing the controller for long-term rewards, such as maximizing energy production over extended periods of time. A DDPG agent is convenient for this because it considers the cumulative future rewards, while networks such as ANNs may not naturally capture this long-term perspective. DDPGs are also the perfect choice for DERs due to the decentralization of the control system, the adaptability of DDPG algorithms, the scalability of DDPG algorithms, and the highly non-linear nature of DERs and the power system.

In order to see the effectiveness of the proposed DDPG controller, its performance has been compared with that of a variable proportional–integral (VPI) control-based mitigation method. Two types of cyber attacks, DoS and FDIA, have been considered in this work. The proposed technique has been simulated and validated utilizing the MATLAB/Simulink software version R2023a to demonstrate the effectiveness of the proposed method. The contributions of the paper can be summarized as follows:

- A novel approach, i.e., a DDPG controller, is developed to mitigate cyber attacks on DERs.
- The proposed method offers a low-cost approach to maintain wind farm stability during malicious cyber attacks on converter management systems.
- This research analyzes the effects of different types of cyber attacks on the converter control system of a grid-connected DFIG-based wind farm.

The organization of this paper is as follows. Section 2 describes the problem statement. Section 3 describes the considered cyber attack modeling and attack detection method. Section 4 explains the AI agents for cybersecurity and cybersecurity issues with wind turbine generator control systems, including the proposed multi-agent DDPG control mitigation system. Section 5 provides a discussion including the future directions of this work. Section 6 deals with a simulation of the proposed control system compared to the current system. Lastly, a conclusion of the research is provided in Section 7.

2. Problem Statement

As already mentioned, dual-fed induction wind turbine generators require a sophisticated control system utilizing AC/DC converters and DC/AC inverters to manage the speed of the rotor, the wind power extracted, the reactive power generated by the DFIG, and the DC link voltage. By controlling these parameters, the control systems maintain proper currents and voltages through the generator, as well as the output lines of the generator and the grid side of the system. The grid-side and rotor-side converters, known as back-to-back converters in this application, are an essential part of any variable speed generator, as they allow for the electronic control of the rotor, which affects the frequency and power output by the wind turbine generator as well as direct control of the reactive power that will be generated due to the inductive nature of DFIGs [14]. The rotor-side converter, as the name implies, has direct control over the speed of the rotor, which directly affects the electronic torque of the wind turbine generator, as well as the overall active power output

from the DFIG. The grid-side converter controls the DC-link voltage that exists between the two converters and allows for direct control of the reactive power present in the system. Due to these features, the torque and the active and reactive power control is decoupled, allowing for better controllability and power quality delivered to the interconnected power grid [14]. Figure 2 depicts the block diagram for the grid-side converter (GSC), and Figure 3 depicts the block diagram of the rotor-side converter (RSC). Equations (1)–(5) depict the mathematical modeling of the grid side converter current and voltage reference points, as well as the reactive power equation. Equation (6) depicts the modeling for the DC-link voltage. Equations (7)–(11) depict the mathematical model of the rotor side converter current and voltage reference points, as well as the active power equation.

$$v_{ds}^{*} = r_s i_{ds}^{*} - \omega_s \lambda_{qs} + \frac{\lambda_{ds}}{dt} \tag{1}$$

$$v_{qs}^{*} = r_s i_{qs}^{*} - \omega_s \lambda_{ds} + \frac{\lambda_{qs}}{dt} \tag{2}$$

$$i_{ds}^{*} = \frac{v_{qs}^{*} + \omega_s \lambda_{qs} - \frac{\lambda_{ds}}{dt}}{r_s} \tag{3}$$

$$i_{qs}^{*} = \frac{v_{qs}^{*} + \omega_s \lambda_{qs} - \frac{\lambda_{ds}}{dt}}{r_s} \tag{4}$$

$$Q = v_{ds} i_{ds} - v_{qs} i_{qs} + v_{dr} i_{dr} - v_{qr} i_{qr} \tag{5}$$

$$C \frac{du_{dc}}{dt} = d_a i_a + d_b i_b + d_c i_c \tag{6}$$

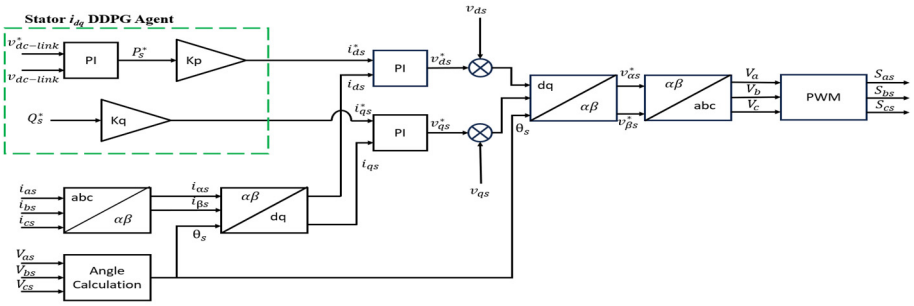


Figure 2. Grid-side converter block diagram.

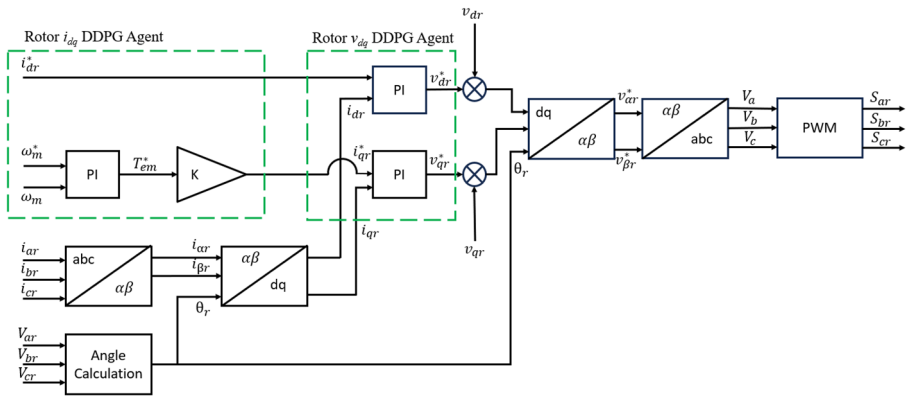


Figure 3. Rotor-side converter block diagram.

In this paper, both converters are voltage source converters (VSC) utilizing insulated gate bipolar transistor (IGBT)/diode-based converters, in which a series of gates and diodes control the flow of electricity, depending on the duty cycle (D) or modulation index. In the

simulation, two voltage-fed pulse width-modulated (PWM) converters are wired to the rotor and stator circuits, which connect the slip ring terminals to the AC supply network electrically [14]. This allows for the direct control of both the magnitude and direction of the power flow between the rotor circuit and the supply side. The grid-side converter is known as an inverter, as it inverts the DC-link voltage to AC voltage.

$$i_{dr}^{*} = \frac{-\omega_s L_{ss} i_{ds}^{*} - R_s i_{qs}^{*} + v_{qs}}{\omega_s L_m} \tag{7}$$

$$i_{qr}^{*} = \frac{R_s i_{ds}^{*} - \omega_s L_{ss} i_{qs}^{*} - v_{ds}}{\omega_s L_m} \tag{8}$$

$$v_{dr}^{*} = r_r i_{dr}^{*} - s\omega_s \lambda_{qr} + \frac{\lambda_{dr}}{dt} \tag{9}$$

$$v_{qs}^{*} = r_r i_{qs}^{*} - \omega_s \lambda_{dr} + \frac{\lambda_{qr}}{dt} \tag{10}$$

$$P = v_{ds} i_{ds} + v_{qs} i_{qs} + v_{dr} i_{dr} + v_{qr} i_{qr} \tag{11}$$

Figure 4 shows a DFIG-based wind farm model including the above-mentioned grid-side converter and rotor-side converter with cyber attack points. As shown in Figure 4, a SCADA system maintains bidirectional communication with the GSC and RSC of the DFIG system. The cyber attackers can enter the SCADA system and change any set points of the GSC and RSC controllers. Also, they can significantly delay the operation of the controllers. Thus, the functionality of the controllers could be hampered, and consequently, the DFIG system and connected power grid.

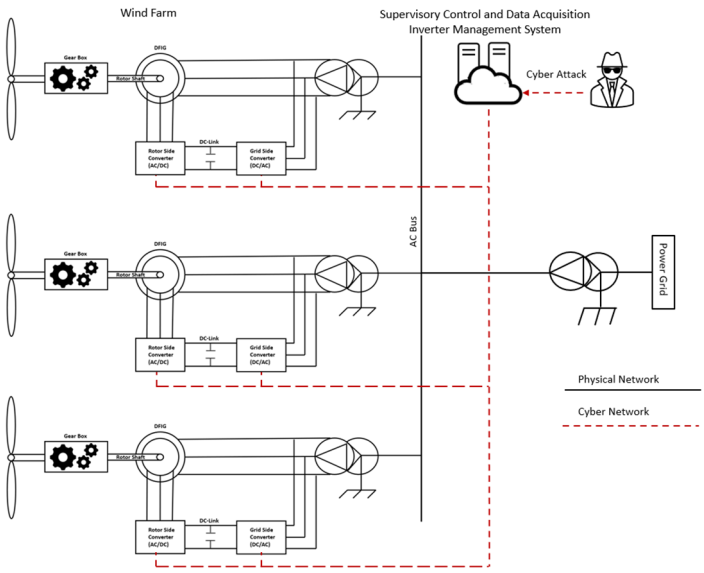


Figure 4. Wind farm model with cyber attack points.

From the literature review, there are two types of attacks that researchers focus on. These attacks are DoS and FDIA/BDIA. A DoS attack describes when a hacker overwhelms the communication lines of the control system for a wind farm, causing complete loss of control in the system and adding significant delay to the automated control processes of the wind farm [15]. A FDIA/BDIA is an attack where the hacker penetrates the control network of a wind farm and maliciously manipulates sensor data or reference set points, causing instability or damage to the wind turbines. When these two attacks are conducted simultaneously, severe damage can be caused to a wind generator or the entire wind farm, which could also have disastrous effects on the interconnected power grid. The other types of cyber attacks that could be implemented to disrupt or disable wind turbine

systems are brute force, man in the middle, spoofing, jamming, crash override, tripping [16], manipulation of data via IoT [17], and zero-dynamics attacks, according to ref. [18]. Any combination of these attacks can have detrimental impacts to the affected wind farm as well as the interconnected power grid. Even though these types of attacks have not been utilized in the past to disrupt wind farms, it is important to take them into consideration when designing a cyber-resilient wind turbine control system. This fact motivates exploring appropriate methods to mitigate the adverse impacts of cyber attacks on DFIG-based wind farms.

3. Cyber Attack Modeling

In this paper, the focus of the research is the mitigation of DoS and FDIA attacks on wind turbine systems. The attacks were implemented utilizing MATLAB function blocks and communication-controlled multi-switches. When the FDIA occurred, the multi-switches changed channels and allowed for false data to be injected into the control blocks for the reference set points of the specific controllers. When the DoS attack occurred, the communication lines experienced delays introduced into the measured values or control signals, which affected the measurement data used to control the PWM signal of the converter control system.

3.1. False Data Injection Attack

To model a false data injection attack in MATLAB, the MATLAB function block was utilized to implement the formulas found in Equations (12) and (13). The formula found in Equation (1) represents a scaling attack in which the attacker manipulates the data measured by a sensor, P_i, and multiplies that value by a scaling factor, $(1 + \gamma_{scale})$ [9]. This will cause the measurements to increase, forcing the energy management control system to respond inappropriately, with the worst-case scenarios causing damage to electronic equipment, damage to mechanical components, or disconnection of the wind farm from the interconnected power grid.

$$P_{scale} = P_i(1 + \gamma_{scale}) \tag{12}$$

The second attack modeled in this paper is a BDIA, in which the communication line of the sensor or controller is blocked, and the attacker injects a malicious measured value or command that will cause a poor response from the control system. In Equation (13), the bad data injection attack is modeled, with $\overline{y}(t)$ being the parameter or control signal being attacked, $y(t)$ being the true signal value, t_0 being the initial sampling time, t_{attack} being the time in which the data is injected, and $\alpha(t)$ being the malicious input by the attacker [19].

$$\overline{y}(t) = \begin{cases} y(t), & t_0 < t_{attack} \\ \alpha(t), & t_0 \geq t_{attack} \end{cases} \tag{13}$$

3.2. Denial of Service Attack

To implement a DoS attack, a hacker gains access to a control or measurement communication line and sends thousands of empty packets to bottleneck and eventually stop communication between devices. When this occurs, the stability of a wind turbine system can become compromised, as the power flow and quality control devices are unable to respond to the dynamic fluctuations of the control parameters of the system. In Equation (14), a periodic jamming DoS attack is modeled, where $n \in \mathbb{N} > 0$ is the period number, $T \in \mathbb{R} > 0$ is the period of the jammer, and T_{off} represents the sleeping time of the jammer, with the lower time bounded by T_{off}^{min} in each jamming signal period, where $T_{off}^{min} \leq T_{off} < T$ [19]. Within one period of T, the interval $[0, T_{off})$ denotes the sleeping interval of the jamming signal, and the interval $[T_{off}, T)$ represents the active interval of the jamming signal. In this represen-

tation, the communication line operates correctly in the interval $[(n-1)T, (n-1)T + T_{off}]$ and is blocked in interval $[(n-1)T + T_{off}, nT]$ [19].

$$\tau_{DOS} = \begin{cases} 0, & t \in \left[(n-1)T,\ (n-1)T + T_{off}\right] \\ 1, & t \in \left[(n-1)T + T_{off},\ nT\right] \end{cases} \quad (14)$$

Remark 1. *As stated in [19], the parameter T_{off} is not necessarily time-invariant; therefore, it is assumed that there exists a uniform real scalar $T_{off}^{min} \in \mathbb{R} > 0$ such that $T_{off}^{min} \leq T_{off} < +\infty$ hold for all $n \in \mathbb{N}_o$ [19].*

3.3. Cyber Attack Detection Method

Although the focus of this paper on cyber attack mitigation methods, an event trigger was utilized to detect the DoS attack. To detect a FDIA, the system utilizes the change in the DC-link voltage to determine if the reference set points for the converters have been manipulated, as both converters are linked electrically through the DC-link and magnetically through the generator. The parameters for the event trigger, the DC-link variation, and the correlation between the DC-link voltage and manipulation of set points for the converters are validated in the simulations. These methods were chosen over other methods, as the computational burden to find the ripple in the DC-link voltage and the time difference in two consecutive samples is far less than for the other methods utilized in the literature review.

4. Materials and Methods

4.1. Deep Deterministic Policy Gradient (DDPG) Approach

As explained in the Introduction Section, the DDPG is an optimal candidate for wind turbine generator control. The DDPG algorithm is a model-free, online, off-policy reinforcement learning method that utilizes an actor–critic reinforcement learning agent that can search for an optimal policy that can maximize the expected cumulative long-term reward [20]. The DDPG algorithm utilizes two neural networks known as actor–critic networks, where the actor, denoted as $\pi(S;\theta)$ with parameters θ, takes an observation, S, and returns the corresponding action that maximizes the long-term reward [20]. The critic, denoted as $Q(S, A; \phi)$ with parameters ϕ, takes an observation, S, and an action, A, and returns the long-term expected value [20]. The DDPG also leverages a target actor and a target critic. The target actor, denoted as $\pi_t(S;\theta_t)$, is used to improve the stability of the optimization by allowing the agent to periodically update the target actor parameters, θ_t, using the latest actor parameter values [20]. The target critic, denoted as $Q_t(S, A; \phi_t)$, is also used to stabilize the optimization, as the agent periodically updates the target critic parameters, ϕ_t, using the latest critic parameter values [20].

The training algorithm, depicted on MathWorks [20], begins by initializing the critic with random parameter values and then initializes the target critic with the same parameter values. This is also done with the actor and target actor parameters, respectively. For each training time step, there are 8 steps that will be completed, which are listed as follows [20]:

i. For the current observation S, select an action A = $\pi(S;\theta) + N$, where N is the stochastic noise.
ii. Execute action A. Observe the reward and next observation S'.
iii. Store the experience (S, A, R, S') in the experience buffer.
iv. Sample a random mini batch of M experiences (S_i, A_i, R_i, S'_i) from the experience buffer.
v. If S'_i is a terminal state, set the value function target y_i to R_i. Otherwise, set it to Equation (15).

$$y_i = R_i + \gamma Q_t\left(S'_i, \pi_t\left(S'_i;\theta_t\right);\phi_t\right) \quad (15)$$

The value function target is the sum of the experience reward, R_i, and the discount future reward. To compute the cumulative reward, the agent first computes the next action by passing the next observation, S'_i, from the sampled experience to the target actor. The agent then finds the cumulative reward by passing the next action to the target critic [20].

vi. Update the critic parameters by minimizing the loss, L, across all sampled experiences, as depicted in the following Equation (16).

$$L = \frac{1}{2M}\sum_{i=1}^{M}(y_i - Q(S_i,\ A_i;\phi))^2 \tag{16}$$

vii. Update the actor parameters using the following sampled policy gradient to maximize the expected discounted reward, as depicted in Equations (17)–(19).

$$\nabla_\theta J \ \approx\ \frac{1}{M}\sum_{i=1}^{M} G_{ai}G_{\pi i} \tag{17}$$

$$G_{ai} = \Delta_A Q(S_i,\ A_i;\phi) \qquad \text{where } A = \pi(S_i;\theta) \tag{18}$$

$$G_{\pi i} = \nabla_\theta \pi(S_i;\theta) \tag{19}$$

viii. Update the target actor and critic parameters depending on the target method.

The target update method has 3 options: smoothing, periodic, and periodic smoothing [20].

Smoothing—Update the target parameters at every time step using the smoothing factor, τ. The equations for updating the target parameters utilizing the smoothing factor are depicted in Equations (20) and (21).

$$\phi_t = \tau\phi + (1-\tau)\phi_t \text{ (for critic parameters)} \tag{20}$$

$$\theta_t = \tau\theta + (1-\tau)\theta_t \text{ (for actor parameters)} \tag{21}$$

Periodic—Update the target parameters periodically without smoothing.

Periodic Smoothing—Update the target parameters periodically with smoothing.

4.2. Proposed DDPG Control Methodology for Attack Mitigation

In this paper, a multi-agent DDPG algorithm is leveraged to predict the stator and rotor current reference values, $\left\{i^*_{ds},\ i^*_{qs},\ i^*_{dr},\ i^*_{qr}\right\}$ for the gride-side and rotor-side converters. These values are then be used to predict the *d-q* $\left\{v^*_{dr},\ v^*_{qr}\right\}$ reference rotor voltages that are then passed to the pulse width modulation (PWM) controller to determine the proper duty cycle for the rotor-side converter. If an FDIA/BDIA is launched against the reference values for the controllers, the effect will be seen on the DC-link voltage, and the DDPG controller will then replace the missing reference values to prevent the system from reacting to the attack. If a DoS attack occurs and communication between the SCADA and the converter system is blocked or jammed, the packet sampling time $t_{received}$ will violate the minimum and maximum allowed sampling times, which are based on the specific network communication structure. The affected communication line will then be disconnected from the system, and the specific DDPG agent will assume control of the affected system until a cyber team can assess and respond accordingly to the situation. In this thesis, the sampling time will be based on the simulation sampling time, which is 50 microseconds per sample.

By integrating these algorithms into a controller that is physically attached to the converters, the PWM signals will be consistently updated in the event of a sophisticated cyber attack conducted against the communication network of a wind turbine generator or wind farm, as there will be no wireless nodes to be attacked in the DDPG network. The

following Figure 5 displays the flow chart of the proposed control algorithm, with Figure 6 depicting the block diagram of the proposed multi-agent DDPG converter controllers. In Figure 5, the 'Y' means the condition was found to be true, so the controller follows this path. If the condition is found to not be true, the controller follows the 'N' path.

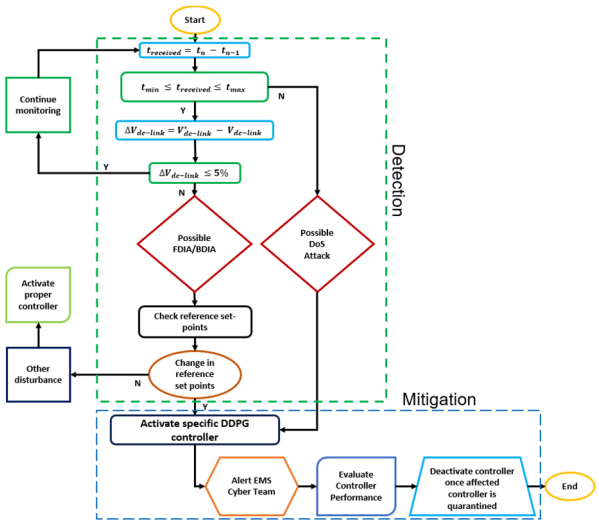


Figure 5. Proposed multi-agent DDPG control network flow chart.

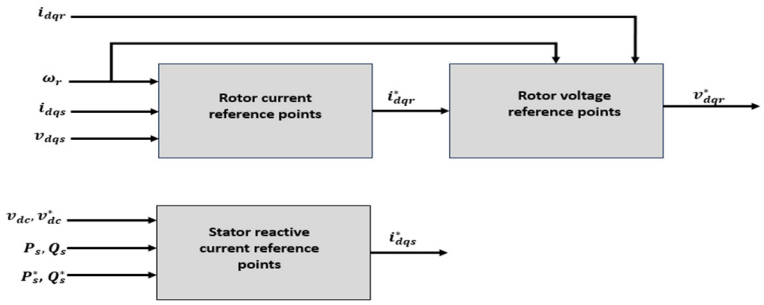


Figure 6. Proposed multi-agent DDPG control network block diagram.

4.2.1. Stator Active and Reactive Power Measurement and Set Points

The direct (d) part of the stator current is directly related to the real power of the stator, and the quadrature (q) part of the stator current is related to the reactive power of the stator [14]. Thus, by utilizing these values, the real and reactive power of the stator can be found mathematically in real time. The data points are created using a small-scale wind farm consisting of six wind turbine DFIGs, and the AI controller is trained during a live simulation. Therefore, the training should closely resemble real world parameters. The set points for the system are determined by the generators utilized in the wind farm and are considered constants under best-case scenarios. In this paper, the stator active power set point is 9 MW, and the reactive power set point is 0 MVAR.

4.2.2. Stator Current Reference Point Sub-System

The stator current is predicted utilizing the active and reactive power measurements of the stator, as well as the measured DC-link voltage and the reference DC-link voltage. The real and reactive power measurements, the DC-link measured voltage, and their respective reference points are used as observations in this network, and the outputs of the network are compared to the conventional system for the reward calculation during live training. In the conventional wind turbine generator control system, a proportional–integral (PI) controller is utilized to adjust the gains to maintain stability in the system. In the following Figure 7, the actor and critic networks for the stator current d-q predictions are depicted.

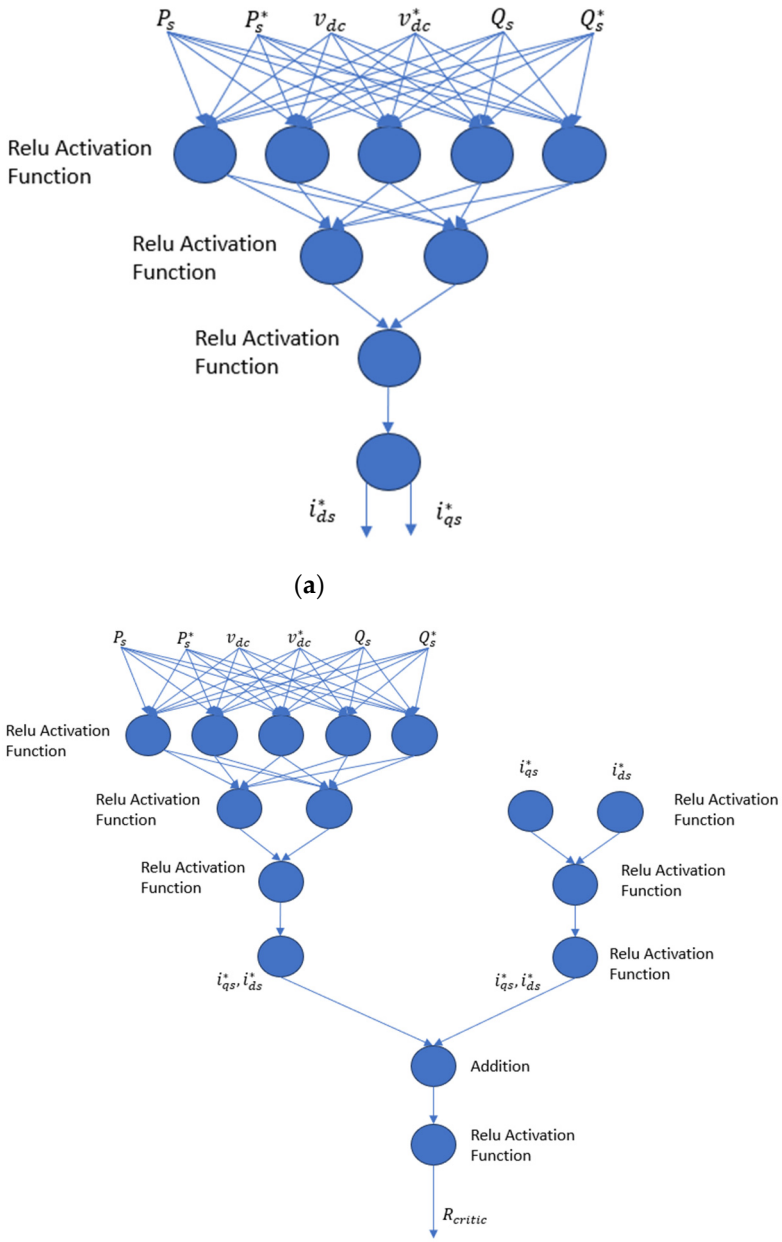


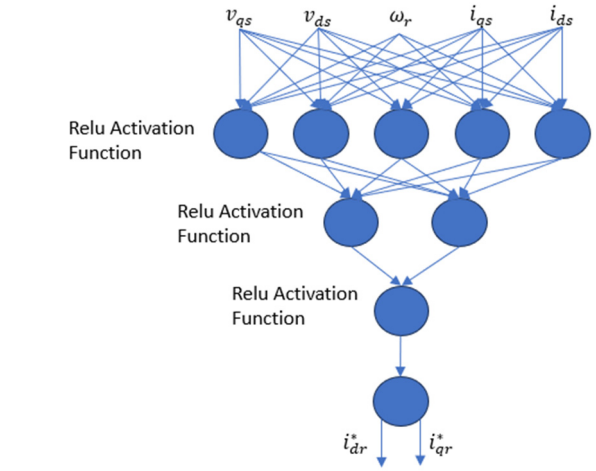
Figure 7. (**a**) DDPG actor network for stator i_{dq} reference points; (**b**) DDPG critic network for stator i_{dq} reference points.

The first fully connected layer of the actor network consists of 20 nodes with the relu activation function. The second fully connected layer of the actor network consists of 10 nodes with the relu activation function. The final fully connected layer of the actor network consists of 6 nodes with the relu activation function, and the final output node outputs the predicted i_{ds} and i_{qs} measurements.

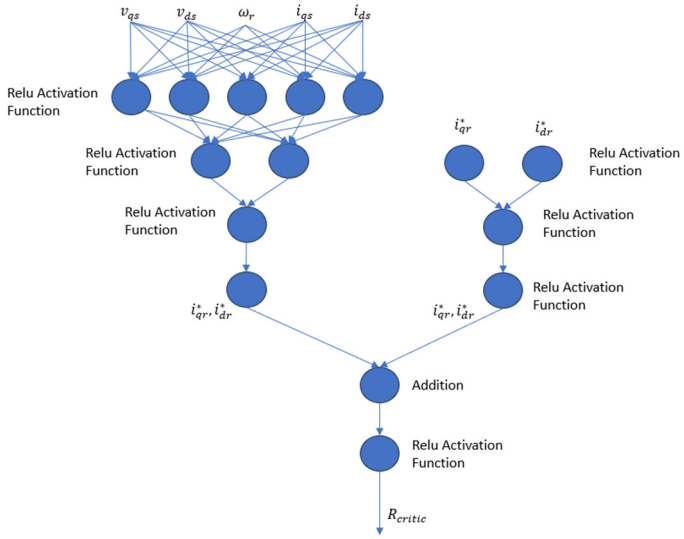
The critic network has the same structure as for the observation side; however, the action side consists of a layer of 10 nodes and then a layer of 6 nodes, both using the relu activation function. The outputs of the observation node and action nodes are then added together in a fully connected node, with the output yielding the predicted reward of the step based on the state–action pair.

4.2.3. Rotor Current Set Point Sub-System

By using the measured stator current d-q values along with the measured stator voltage d-q values, the rotor reference d-q current values can be found. Used along with the rotor speed ω_r as observations, the DDPG agent can quickly and accurately predict the reference set points for the rotor current d-q values. In the conventional system, this process is done by a PI controller, which again will be removed from the system in the event of a cyber attack so that the DDPG agent can replace any missing set-point values and maintain a steady-state of the system until cyber analysts can resolve the breach. In the following Figure 8, the actor and critic networks for the rotor current d-q predictions are depicted.



(**a**)



(**b**)

Figure 8. (**a**) DDPG actor network for rotor i_{dq} reference points; (**b**) DDPG critic network for rotor i_{dq} reference points.

4.2.4. Rotor Voltage Set Point Sub-System

The d-q reference values for the rotor voltage are found by using the rotor current d-q measured values and the rotor current d-q reference values. Also, the rotor speed, ω_r, is utilized as an input in this agent. Typically, a PI controller would have the error of the reference values compared to the measured values as inputs, and then a specified gain would be applied to keep the system stable and output the reference d-q voltage values.

In this thesis, the measured rotor d-q currents, the rotor speed ω_r, and reference rotor d-q current values are used as inputs to the DPPG agent, and the output of the conventional PI controller system is used to determine the reward for the current state/action pair. The DDPG agent was trained during a live simulation so the agent would be better equipped to handle real-world scenarios. When a cyber-attack occurs, the DDPG agent will be utilized to replace the missing set-points, or in the event of a DoS attack, both rotor DDPG agents will control the entire system until a cyber defense team can quarantine the effected unit. The following Figure 9 depicts the actor and critic networks of the rotor voltage set-point DDPG controller.

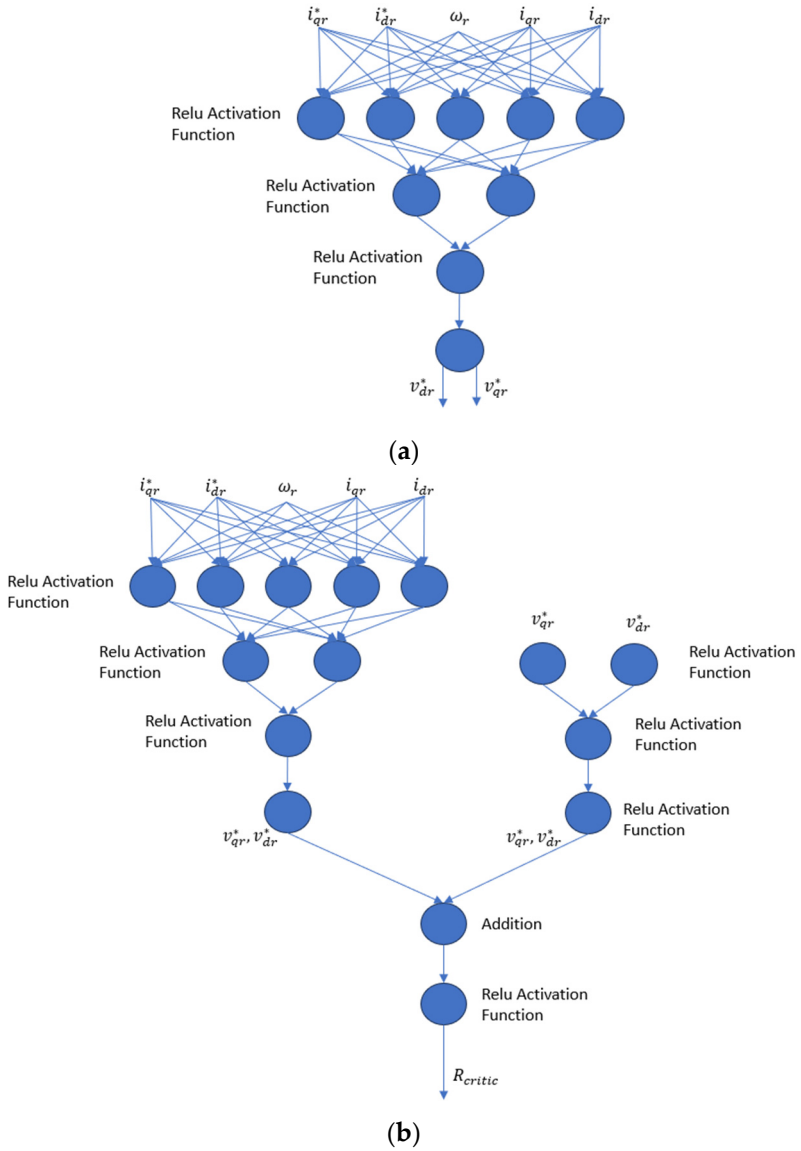


Figure 9. (**a**) DDPG actor network for rotor v_{dq} reference points; (**b**) DDPG critic network for rotor v_{dq} reference points.

4.3. Proposed Variable Proportional–Integral (VPI) Control Methodology

In this paper, the performance of the proposed multi-agent DDPG controller was compared to the performance of the VPI controller during the considered cyber attacks. Therefore, a description of the VPI controller and its structure is described and depicted below.

Stator VPI–idqs: The variable proportional–integral (VPI) controller for the stator idqs ref values utilizes the error in the DC-link voltage to scale the Kp-dc and Ki-dc gains if the dc-link voltage changes by more than 5% of the nominal value. The Kp-dc and Ki-dc

gains are adjusted by multiplying the error by the gain value and then adding this value to the original gain value, creating a variable gain value to mitigate the effects of an FDIA. As seen in the plots and the RMSE performance table in the Results section, the VPI can dampen the effects of an FDIA on the idqs PI controller.

Rotor VPI–vdqs: The VPI controller for the rotor vdqr ref values utilizes the error in the idr and iqr measured values with respect to their ref values. If the dc-link voltage changes by more than 5% of the nominal value, the VPI will scale the gains accordingly. The scaled Kp-rsc and Ki-rsc gains for the rotor VPI controller are found by multiplying the error by the respective gain value and then adding this value to the original gain value for Kp-rsc and subtracting this value from Ki-rsc. As seen from the plots and the RMSE performance table in the Results section, the VPI can dampen the effects of an FDIA on the vdqs PI controller. The mathematical modeling of stator VPI and rotor VPI controllers are provided below. Figures 10 and 11 show the diagrams for the stator VPI and rotor VPI controllers.

$$\text{Stator VPI–idqs}$$
$$e_{vdc}(t) = (V_{dc\_nom} - Vdc)/V_{dc\text{-}nom} \quad (22)$$

$$K_{vp} = K_{p\_dc} + [K_{p\_dc} * e_{vdc}(t)] \quad (23)$$

$$K_{vi} = K_{i\_dc} + [K_{i\_dc} * e_{vdc}(t)] \quad (24)$$

$$\text{Rotor VPI–vdqs}$$
$$[e_{idr}(t); e_{iqr}(t)] = [Idr\_ref - Idr; Iqr\_ref - iqr] \quad (25)$$

$$K_{vp\_rsc} = \tan\left(\frac{\pi}{2} * K_{p\text{-}rsc}\right) + \left[\tan\left(\frac{\pi}{2} * K_{p\text{-}rsc}\right) * e_{idr}(t)\right];\ \tan\left(\frac{\pi}{2} * K_{p\text{-}rsc}\right) + \left[\tan\left(\frac{\pi}{2} * K_{p\text{-}rsc}\right) * e_{iqr}(t)\right] \quad (26)$$

$$K_{vi\_rsc} = \tan\left(\frac{\pi}{2} * K_{i\text{-}rsc}\right) - \left[\tan\left(\frac{\pi}{2} * K_{i\text{-}rsc}\right) * e_{idr}(t)\right];\ \tan\left(\frac{\pi}{2} * K_{i\text{-}rsc}\right) - \left[\tan\left(\frac{\pi}{2} * K_{i\text{-}rsc}\right) * e_{iqr}(t)\right] \quad (27)$$

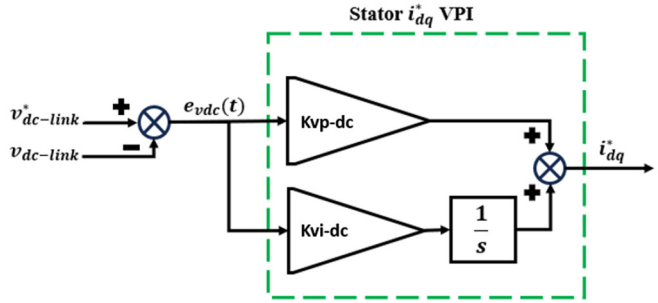


Figure 10. Stator VPI control diagram.

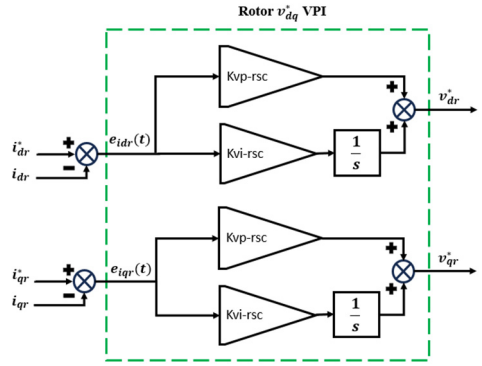


Figure 11. Rotor VPI control diagram.

4.4. Conventional PI Controller

The conventional PI controller takes a specified measured signal and utilizes a feedback loop from its output to determine the error of the output versus the input. The error is

fed through the controller and finds the integral of the error with respect to time as well as the proportional gain. These values are then added together to become the output of the system, which as was stated before, is fed back into the input and subtracted from the measured value. The PI controller can be tuned utilizing several different methods, such as the root locust method to ensure proper stability of the system. However, in this thesis, the PI controller was tuned only for normal operation and not for the mitigation of cyber attacks. The following Figure 12 depicts the conventional PI controller, with k_1 being the tuned proportional gain and $\frac{k_2}{s}$ being the tuned integrated gain.

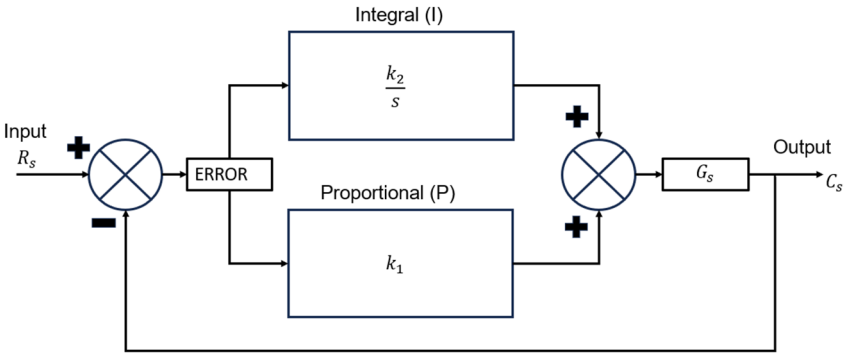


Figure 12. PI controller block diagram.

5. Results

In this section, the effectiveness of the proposed controller is presented to prove the effectiveness of the system as well as validate the approach. The simulation was conducted using the MATLAB/Simulink software. In the simulation, a grid-connected, 9 MW wind farm consisting of six DFIG-based wind turbines was used to train and test the performance of the control system. The following Table 1 presents the parameters for the grid-connected wind farm used in the simulation.

Table 1. Simulation parameters of the grid-connected wind farm.

Parameter	Value
Nominal power—P_{nom}	10 MVA
Line-to-line nominal voltage—$V_{l\text{-}l\ nom}$	575 v_{rms}
Nominal rotor voltage—$V_{r\text{-}nom}$	1975 v_{rms}
Nominal frequency—F_{nom}	60 Hz
Stator resistance—R_s	0.023 p.u.
Stator inductance—L_{ls}	0.18 p.u.
Rotor resistance—R_r	0.016 p.u.
Rotor inductance—L_{lr}	0.16 p.u.
Mutual inductance—L_m	2.9 p.u.
Inertia constant—H	0.685 s
Friction factor—F_μ	0.01 p.u.
Number of pole pairs—$P_\#$	3
RSC PWM frequency—$PWM_{freq\text{-}rsc}$	1620 Hz
GSC PWM frequency—$PWM_{freq\text{-}gsc}$	2700 Hz
DC-link nominal voltage—$V_{dc\text{-}nom}$	1150 v
DC-link capacitor—$C_{dc\text{-}link}$	10 mF
Nominal mechanical power—$P_{mec\text{-}nom}$	9 MW

5.1. Cyber Attack Scenarios

In the simulation, a DoS attack, an FDIA, and a combination of both attacks were implemented on the wind turbine generator control system. In all case studies, if the communication signal violated the time sampling bounds of 50 µs or if the DC-link voltage fluctuated greater than 5% of the nominal voltage, the controller then checked if the specific

set points changed more than 5% of their original values. If this was found to be the case, the specified DDPG agent would be commanded on.

In the first scenario, the PWM signal to the rotor-side converter will be hit with a DoS attack in the form of a jamming attack. The signal to the converter will be extremely delayed, with the jamming signal overwhelming the communication lines of the controllers, effectively disabling them. In the second and third scenarios, the set points for the current and voltage d-q parameters will be adjusted with a scaling attack, with the scaling value being -2, thus inverting the control signal. This will cause an increase or decrease in the set-point values, causing over-voltage or under-voltage conditions. Figures 13 and 14 depict the performance of the conventional PI controllers (not mitigation controllers) under a DoS attack on the rotor-side controller PWM signal and an FDIA attack on the rotor voltage set points. These figures clearly show the need for a mitigation strategy when cyber attacks occur on wind turbine generator control systems.

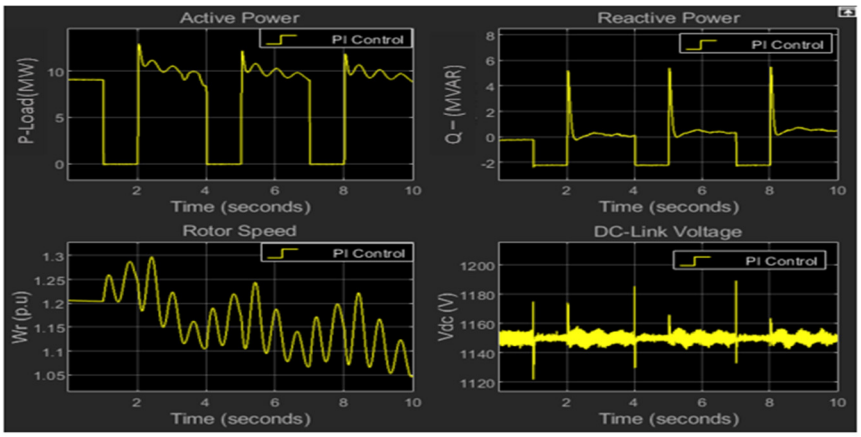


Figure 13. DoS attack on the rotor-side converter PWM signal.

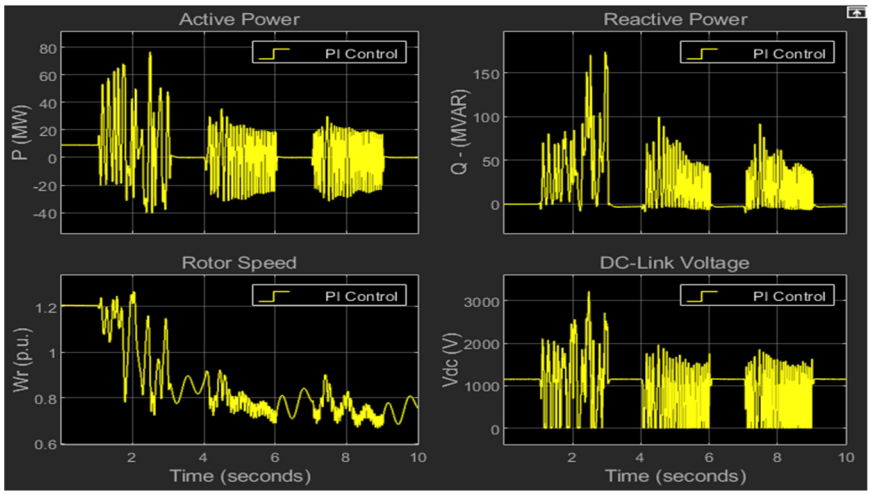


Figure 14. FDIA on the stator current d-q set-points.

5.2. Effectiveness of Proposed Mitigation Method and Performance Comparison

Figures 15 and 16 show the performance of the proposed DDPG control-based attack mitigation method. The active power, reactive power, DC link voltage, and rotor speed are shown in both plots. It is evident that the proposed DDPG method is effective in mitigating the adverse effects of cyber attacks on the DFIG-based wind farm. Also, the performance of the proposed method is better than that of the VPI method. Moreover, both methods are far better compared to the conventional PI controller (not mitigation controller) method.

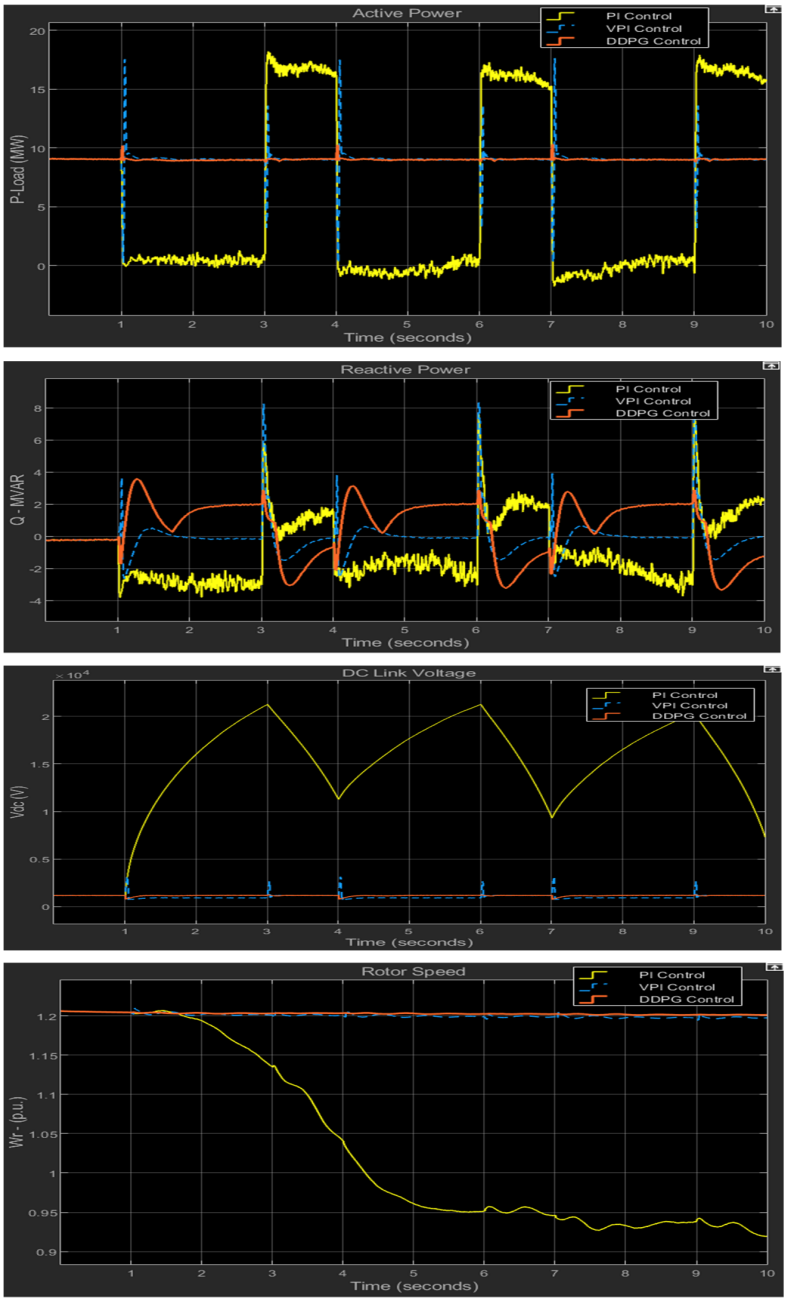


Figure 15. PI, VPI, and DDPG control comparison during FDIA on stator current reference points.

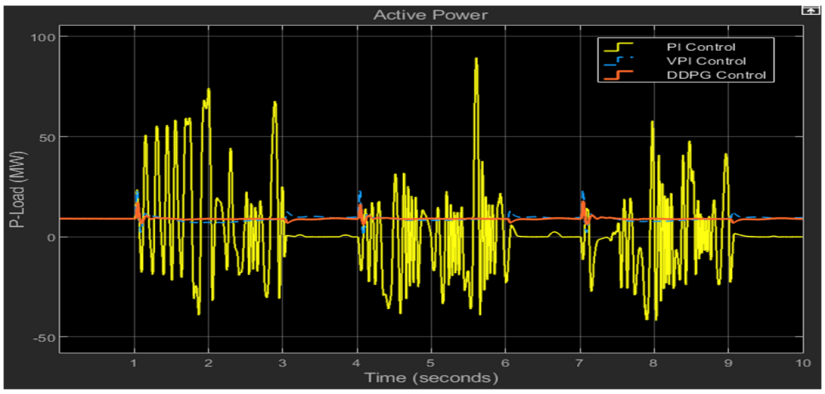


Figure 16. *Cont.*

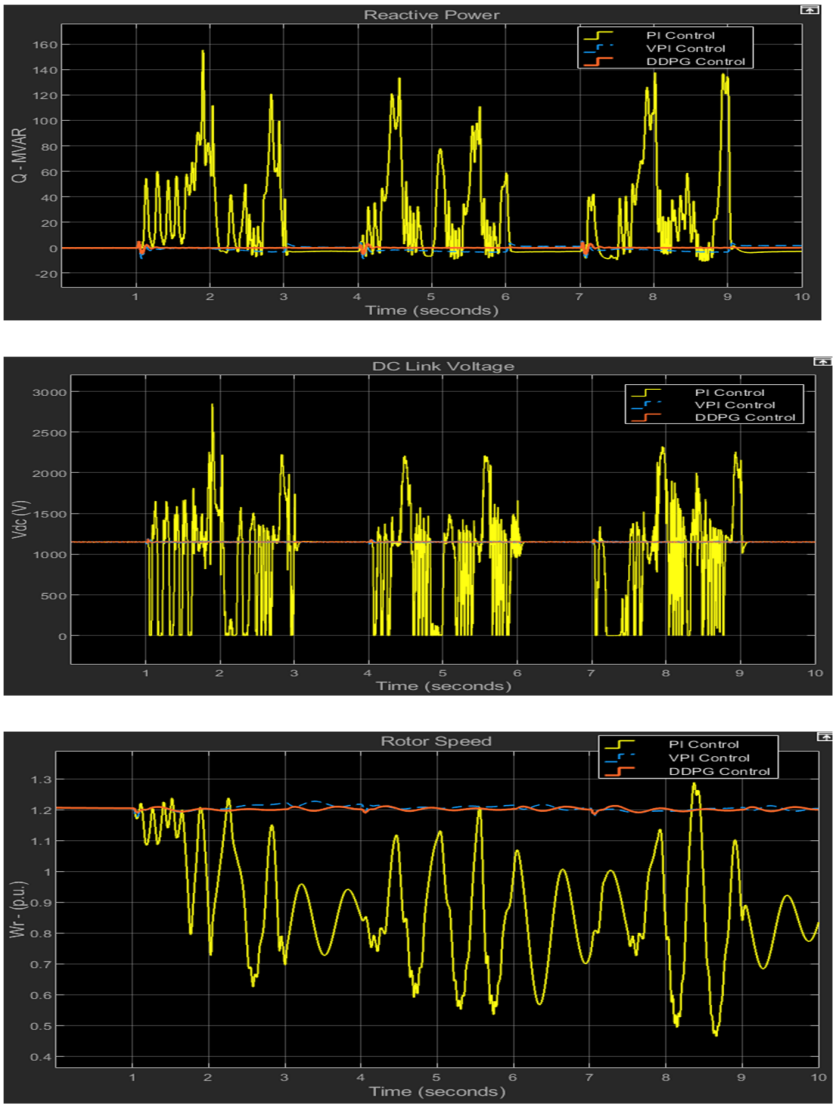


Figure 16. PI, VPI, and DDPG control comparison during FDIA on rotor voltage reference points.

5.3. Root Mean Square Error (RMSE) Performance Validation

In this research, the performance evaluation of the proposed control system was determined by finding the root mean square error (RMSE) of the conventional PI controller, the variable PI controller, and the proposed DDPG controller. The RMSE is a standard metric used in model evaluation, as it is the optimal metric for "normal" errors to determine how the model "fits" the data [21]. In the power system and with respect to wind energy generation, there is an acceptable amount of deviation from the optimal set points that will still allow the system to remain in a steady-state condition. Due to this feature, RMSE is a better option than mean absolute error. To determine the RMSE, the formula depicted in the following Equation (28) was utilized:

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(\hat{y}_i - y_i)^2} \tag{28}$$

where n is the number of observations, y_i is the theoretical value, and $\hat{y}_i$ is the experimental value. In this context, the y_i values are the set points for the specific measured value, and $\hat{y}_i$ is the simulated value obtained by the AI controller. The following Table 2 depicts the RMSE evaluation of the conventional controller, the VPI controller and the DDPG agents.

Table 2. RMSE comparison table.

		Attack Type		Active Power RMSE			Reactive Power RMSE			Rotor Speed RMSE			DC-Link Voltage RMSE		
		DoS	FDIA	PI	VPI	DDPG	PI	VPI	DDPG	PI	VPI	DDPG	PI	VPI	DDPG
Case Study	1	✓	-	6.97	7.07	0.88	1.78	1.87	1.10	0.119	0.120	0.006	2.07	1.89	2.32
Case Study	2	-	✓	8.08	0.94	0.08	2.12	1.08	1.81	0.20	0.004	0.003	14,459	264.62	57.14
Case Study	3	-	✓	18.3	0.75	0.79	29.65	0.80	0.77	0.423	0.005	0.001	582.43	2.23	2.22

From the case studies presented in the table as well as the plots presented in the previous sub-section, the performance of the DDPG agents during a cyber attack is clearly better than its conventional counterpart and the VPI implemented in this study. With more training and fine tuning of the inputs, the DDPG agent could perform even better. Implementing a DDPG agent to predict the stator rotor voltage set points could also help alleviate cyber attacks on the grid-side converter, especially in the presence of a DoS attack.

6. Discussion

This research provides a new approach to distributed energy resource control, with impacts on society beyond a power generation perspective. Emergency services, such as hospitals and police, require power to provide lifesaving services during emergencies. The military also needs reliable energy production to operate military bases globally. This paper offers a solution to prevent cyber attacks from causing chaos in these industries. Basic consumers will have more reliable power, and cyber attacks will impact their lives less than they currently do. Autonomous energy generation has become a practical approach to control power generation, and this research has a positive contribution to the respective field.

In the future, this work could be extended to the following tasks:

- The stator voltage controller can be replaced by a DDPG agent, allowing for the PWM signal to be replaced for the grid-side converter during a cyber-attack, like what was presented for the rotor-side control system.
- The method can be utilized for other DERs, such as ocean/wave energy production.
- The effects of a battery energy storage system on the DC-link circuit could be investigated to determine if better stability can be achieved.
- Exploring new AI detection and mitigation techniques based on the works presented in this paper could be explored.

7. Conclusions

This work researched the effects of different types of cyber attacks on the control system of a grid-connected DFIG-based wind farm. A multi-agent DDPG AI controller was designed and leveraged to mitigate the adverse effects of cyber attacks on the energy management system of a wind turbine generator. The performance of the proposed DDPG controller was compared with that of a VPI control-based mitigation method. The proposed technique was simulated and validated utilizing the MATLAB/Simulink software. This paper can be concluded as follows:

- The proposed DDPG method can effectively mitigate the adverse effects of cyber attacks, regardless of which set point is manipulated or whether the PWM signal to the rotor-side converter is blocked.
- The performance of the proposed DDPG method is better than that of the VPI method, as shown in the plots and the RMSE table presented in the results section.
- This research offers a novel approach to mitigating cyber attacks on DERs by offering a low-cost approach to maintaining wind farm stability during a malicious cyber-attack on the converter management system.

Author Contributions: Conceptualization, N.F. and M.H.A.; methodology, N.F.; software, N.F.; validation, N.F. and M.H.A.; formal analysis, N.F.; investigation, N.F.; resources, M.H.A.; data curation, N.F.; writing—original draft preparation, N.F.; writing—review and editing, M.H.A.; visualization, N.F.; supervision, M.H.A.; project administration, M.H.A.; funding acquisition, M.H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors are pleased to acknowledge the funding support from the Electrical and Computer Engineering department at the University of Memphis, USA to complete this work.

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

Abbreviations

AI	Artificial intelligence
ANN	Artificial neural network
BDIA	Bad data injection attack
CDM	Continuous diagnostics and mitigation
DT	Decision tree
DDPG	Deep deterministic policy gradient
DoS	Denial of service
DER	Distributed energy resource
DFIG	Double-fed induction generator
FDIA	False data injection attack
IGBT	Insulated-gate bipolar transistor
LAN	Local area network
MitM	Man in the middle
MaDIoT	Manipulation of data via IoT
NOAA	National Oceanic and Atmospheric Administration
PID	Proportional, integral, and derivative
PMSG	Permanent magnet synchronous generator
PIFPI	PI/fractional-order fuzzy/PI
PAC	Pitch angle controller
PLC	Programable logic controller
PWM	Pulse width modulated
RMSE	Root mean square error
SCADA	Supervisory control and data acquisition
SVM	Support vector machine
VSC	Voltage source converter
WAMPAC	Wide area monitoring, protection, and control
YAC	Yaw angle controller

References

1. Mahon, A. Wind Energy. Available online: https://www.pnnl.gov/wind-energy (accessed on 5 January 2024).
2. U.S. Department of the Interior. Biden-Harris Administration Approves Sixth Offshore Wind Project. Available online: https://www.doi.gov/pressreleases/biden-harris-administration-approves-sixth-offshore-wind-project (accessed on 5 January 2024).
3. Abdelmassih, G.; Al-Numay, M.; El Aroudi, A. Map optimization fuzzy logic framework in wind turbine site selection with application to the USA wind farms. *Energies* **2021**, *14*, 6127. [CrossRef]
4. Chang-Chien, L.-R.; Sun, C.-C.; Yeh, Y.-J. Modeling of wind farm participation in AGC. *IEEE Trans. Power Syst.* **2013**, *29*, 1204–1211. [CrossRef]
5. Adouni, A.; Chariag, D.; Diallo, D.; Hamed, M.B.; Sbita, L. FDI based on artificial neural network for low-voltage-ride-through in DFIG-based wind turbine. *ISA Trans.* **2016**, *64*, 353–364. [CrossRef] [PubMed]
6. Al-Deen, K.A.N.; Hussain, H.A. Review of dc offshore wind farm topologies. In Proceedings of the 2021 IEEE Energy Conversion Congress and Exposition (ECCE), Vancouver, BC, Canada, 10–14 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 53–60.
7. Stupp, C. European Wind-Energy Sector Hit in Wave of Hacks. *The Wall Street Journal*, 25 April 2022. Available online: https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000 (accessed on 1 November 2022).

8. Liu, J.; Gu, Y.; Zha, L.; Liu, Y.; Cao, J. Event-Triggered $H\infty$ Load Frequency Control for Multiarea Power Systems Under Hybrid Cyber Attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1665–1678. [CrossRef]
9. Singh; Kumar, V.; Sharma, R.; Govindarasu, M. Testbed-based performance evaluation of attack resilient control for wind farm scada system. In Proceedings of the 2020 IEEE Power & Energy Society General Meeting (PESGM), Montreal, QC, Canada, 2–6 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–5.
10. Yang, K.; Li, J.; Zhang, G.; Xing, Y.; Bamisile, O.; Huang, Q. A Cooperative Control Strategy against Cyber-attacks for Power System with High Penetration Wind Farm. In Proceedings of the 2022 4th Asia Energy and Electrical Engineering Symposium (AEEES), Chengdu, China, 25–28 March 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 321–327.
11. Burgos-Mellado, C.; Donoso, F.; Dragičević, T.; Cardenas-Dobson, R.; Wheeler, P.; Clare, J.; Watson, A. Cyber-attacks in modular multilevel converters. *IEEE Trans. Power Electron.* **2022**, *37*, 8488–8501. [CrossRef]
12. Sadi, H.M.A.; Zhao, D.; Hong, T.; Ali, M.H. Time Sequence Machine Learning-Based Data Intrusion Detection for Smart Voltage Source Converter-Enabled Power Grid. *IEEE Syst. J.* **2023**, *17*, 2477–2488. [CrossRef]
13. Scott Rose Oliver Borchert Stu Mitchell Sean Connelly. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (accessed on 7 August 2023).
14. Mehdipour, C.; Hajizadeh, A.; Mehdipour, I. Dynamic modeling and control of DFIG-based wind turbines under balanced network conditions. *Int. J. Electr. Power Energy Syst.* **2016**, *83*, 560–569. [CrossRef]
15. Chen, B.; Yim, S.I.; Kim, H.; Kondabathini, A.; Nuqui, R. Cybersecurity of wide area monitoring, protection, and control systems for hvdc applications. *IEEE Trans. Power Syst.* **2020**, *36*, 592–602. [CrossRef]
16. De Carvalho, R.S.; Saleem, D. Recommended functionalities for improving cybersecurity of distributed energy resources. In Proceedings of the 2019 Resilience Week (RWS), San Antonio, TX, USA, 4–7 November 2019; IEEE: Piscataway, NJ, USA, 2019; Volume 1.
17. Shekari, T.; Cardenas, A.A.; Beyah, R. {MaDIoT} 2.0: Modern {High-Wattage}{IoT} botnet attacks and defenses. In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), Boston, MA, USA, 10–12 August 2022; pp. 3539–3556.
18. Wang, Z.; Zhang, H.; Cao, X.; Liu, E.; Li, H.; Zhang, J. Modeling and Detection Scheme for Zero-Dynamics Attack on Wind Power System. *IEEE Trans. Smart Grid* **2024**, *15*, 934–943. [CrossRef]
19. Fallahnejad, M.; Kazemy, A.; Shafiee, M. Event-triggered H∞ stabilization of networked cascade control systems under periodic DoS attack: A switching approach. *Int. J. Electr. Power Energy Syst.* **2023**, *153*, 109278. [CrossRef]
20. RlDDPGAgent. MathWorks. Available online: https://www.mathworks.com/help/reinforcement-learning/ug/ddpg-agents.html (accessed on 21 September 2023).
21. Hodson, T.O. Root-Mean-Square Error (RMSE) or Mean Absolute Error (MAE): When to Use Them or Not. Geoscientific Model Development. Available online: https://gmd.copernicus.org/articles/15/5481/2022/ (accessed on 18 August 2023).