Smart Grids and Sustainable Energy (2024) 9:17
https://doi.org/10.1007/s40866-024-00201-9

ORIGINAL PAPER

A New Nonlinear Virtual Inertia Approach to Mitigate Destructive Effects of Cyber Attacks on Active Power and Rotor Speed Profiles of Wind Turbine DFIG Sustainable Energy Production

Hossein Mahvash[1] · Seyed Abbas Taher[1] · Josep M. Guerrero[2,3,4]

Received: 16 November 2023 / Accepted: 24 February 2024

Abstract
As the popularity of applying doubly fed induction generators (DFIGs) in wind and marine current turbine generators of sustainable energy production, the requirement to the deep survey on cyber attacks and mitigation techniques against them is undeniable. Cyber attacks as the resultant of internet of things (IoT) in cyber physical systems threaten control signals and measurement data in the control process of converters in power electronic strategy. In this regard, the active power reference and measurement data in addition with the rotor speed parameters are vulnerable to be manipulated by cyber attacks due to the existence of communications, internet connections and the other probable access for attackers to influence in the control process. In this paper, a novel nonlinear virtual inertia control (VIC) is suggested to effectively mitigate the destructive effects of the important cyber attacks including false data injection attack (FDIA), denial of service (DoS) and hijack attack (HjA), happening with the active power and rotor speed profiles of DFIGs in an AC microgrid (ACMG). Moreover, a detection approach is proposed for the cyber conditions in the rotor side converter (RSC) of DFIG. Various simulation results are obtained via MATLAB software to verify the new method, precisely.

Keywords Doubly Fed Induction Generator (DFIG) · Denial of Service (DoS) · False Data Injection Attack (FDIA) · Hijack Attack (HjA) · Virtual Inertia Control (VIC) · Sustainable Energy Production

Introduction

Internet of things (IoT) by propagation of electronic devices and internet facilities via communications is one of the main reasons for attackers to send malwares to control signals derived via control loops and also, measurement data in cyber physical microgrids (MGs) [1, 2]. In the other words, cyber attacks could affect on sensors and actuators [3]. The destructive effects cause by cyber attacks directly threaten cyber security, meanwhile the mitigation methods must be proposed to solve this problem, effectively. In MGs as the cyber physical systems (CPSs), improving cyber security is indispensable. As the important kinds of attacks, false data injection attacks (FDIAs) [4] are the prevalent cyber attacks which influence in MGs by injecting false data including constant values, periodic and noisy values to healthy data. The other important attack which would be able to cause malicious effects is known as denial of service (DoS) [5], by disconnecting the service of the attacked signal or data and enforcing problems on availability. In the other kind of attacks similar to FDIA, different false data are completely replaced by the healthy data [6] which cause the corruption of confidentiality. It must to be mentioned cyber attack and cyber security investigation are mainly considered in the secondary level of hierarchical control in MGs [7, 8].

Various researches are carried out about cyber attack subjects in wind power generation [9–26]. However, the relative literatures specialized in the field of cyber attack detection and mitigation in wind power plants in the view point of

✉ Seyed Abbas Taher
sataher@kashanu.ac.ir

1 Department of Electrical Engineering, University of Kashan, Kashan, Iran

2 Center for Research On Microgrids (CROM), Department of Electronic Engineering, Technical University of Catalonia, 08019 Barcelona, Spain

3 ICREA, Pg. Lluis Companys 23, 08010 Barcelona, Spain

4 CROM, AAU Energy, Aalborg University, 9220 Aalborg East, Denmark

Published online: 06 March 2024

power studies and power management system are limited [18–26].

In Refs. [9, 10], the main goals are on the reliability assessment and evaluation incorporating the wind farm cyber security. In these articles, the kind of important attacks such as FDIA and/or DoS are not discussed; hence, the reliability indices are considered. The article [11] is merely devoted to the control strategy of wind turbine (WT) considering the time delay attacks by flooding the communication link between the rotor speed sensor and the relative controller. The suggested control method is based on the adaptive observer using the one mass mechanical model. The wind speed regime is chosen in the range of [4.5 6.5] m/s which could not support the higher speeds to validate the performance of the method, well. Generalities discussions of cyber attacks for the cyber physical model of WTs without expressing the kinds of attacks, is the main issue in [12]. This is done by focusing on the supervisory control and data acquisition (SCADA) system model for monitoring the wind farm. The authors of Ref. [15] proposed an anomaly detection mechanism for FDIA according to the combination of physics and machine learning approaches for WT. The principles of this method are based applying observation, preprocessing, feature engineering, physics-based model and also, iForest model. Limited results without monitoring the important parameters including power, frequency and voltage are shown in this article. Ref. [14] just presented an analysis about cyber attacks in wind energy based power system. In this regard, the FDIA is considered without noticing the kind of generators in the wind farm. Also, the obtained results are limited. The research study in [15] is about the issue of cyber attacks against wind farm sensor systems. An observer based on the adaptive control is defined; hence, the adequate results are not shown to complete this research. A virtualized cyber physical wind energy site for studying the impact of cyber security and resiliency, is the objective of [16]. In this regard, the WT generators are simulated by a single wind generator in the original ACTIVSg2000 model. The kinds of attacks are as manipulation of control, DoS and adversary performance of wind site reconnaissance. The experimental results are obtained via the tables for the cost–benefit analysis and cyber hardening technology impact on the load and remote chains. Finally, in the point of view of SCADA system in wind farm, an analysis on cyber security regard to the market research and computer crime is carried out in [17].

Based on Ref. [18], the robust method using the linear matrix inequality (LMI) is presented to mitigate the destructive effects of FDIA for the doubly fed induction generators (DFIGs) in the wind park composed of 266 generators. The attacks are categorized into two groups including the internal and external cyber attacks. The static subsynchronous damping controller (SSDC) is applied for the both inner and outer attacks. Moreover, to recognize the cyber conditions, the residues definition is used and thresholds are defined as the detection scheme. More than one hundred WT generators are considered in [19] to investigate a remedial action against the FDI and DoS attacks by solving the LMI conditions. Hence, the recognition tool is based on using the observers in combination with the fuzzy control. The results are obtained via EMPT software and a co-simulation platform. Another work [20] for WT DFIGs in a 400 MW wind park, is devoted to the kinds of FDIAs and HjAs. To suppress the cyber effects, the conventional droop control is expressed. Moreover, for the detection scheme of the attacks, the firewall approach is suggested. The results for validation are just shown for the frequency and rotor speed profiles in MATLAB/Simulink. Badihi, et al., proposed an adaptive control approach according to the fuzzy reference model in order to reduce the FDIA effects on the active power profile in a wind farm without noticing the kind of generators. Moreover, the detection scheme in this article is realized by in line monitoring and firewall [21]. The impact of manipulating parameters in the offshore wind farm comprised the squirrel cage induction generators is the research objective of [22]. In this test system, the array of WT generators is connected to the grid via two connection links. First link is connected by the AC subsea export cable and the other one is formed via the DC subsea cable, AC/DC and DC/AC converters. The pertinent results are demonstrated for the active/reactive power, rotor speed, pitch angle and DC link voltage profiles. Resilient load frequency control for the islanded ACMG which is built by the single DGs such as solar cell, WT, fixed capacitor and diesel generator is suggested against the DoS attack [23]. According to this method, the robust H_∞ based on the variable Lyapunov analysis is presented. Furthermore, the detecting approach is done by applying the piecewise observer and linearizing the state space model. In the experimental work related to the FDIA in an ACMG composed of WT, solar cell, battery and super capacitor [24], the mitigation scheme is realized by minimizing the cost function of the active power for all the distributed generators (DGs) in the MG. Meanwhile, the estimator error is used as the weighted matrix for the hidden layers of the neural network to diagnose the FDIA conditions. In the research presented by the authors of [25], a detection approach for the wind farm connected to the grid against the FDIA is discussed. The detecting process is based on the margin setting algorithm (MSA). The validation setup is constructed in MATLAB considering a wind farm with the rated power of 24 kW and the experimental data sets are also collected to complete the verification process. In [26], the identification of FDIA considering the impact of wind generation is carried out. The proposed algorithm is based on calculating the variance index in addition to a fuzzy c-means clustering scheme. Simulations are done in the IEEE 34-bus system

with 18 MW wind farm, without noticing the kind of WT generators. In the references addressed in this paragraph, the majority of research studies have concentrated on the just FDIA or FDIA and DoS attacks, except than Ref. [20] which considered FDIA and HjA. Meanwhile, in Refs. [20] and [25], the detection methods are suggested; hence, in [22], there is not any solution for detection or mitigation of cyber attacks. In our study, three kinds of attacks including FDIA, HjA and DoS are paid attention and the new detection and nonlinear mitigation methods are expressed.

Widespread application of DFIGs [27] in wind power plants due to its high controllability is a good reason for investigating cyber attacks effects and remedial actions in sustainable energy production based on applying DFIGs. In this regard and because of research gaps in cyber security enhancement in DFIGs, we have motivated to concentrate on the cyber attacks problems in this kind of generator in the viewpoint of power studies and to suggest an effective solution while the targets of attacks are on the active power and rotor speed profiles. Following this goal, a solution is based on applying the virtual inertia concept considering the two mass mechanical model to mitigate the destructive effects of various important cyber attacks. Hence, because of appearing the nonlinear behavior which would be caused during the cyber conditions in the generator parameters, the proposed virtual inertia control (VIC) is improved by the nonlinear backstepping control scheme in the rotor side converter (RSC). This paper aims to contribute the following items:

1) Proposing an advantageous detection scheme by applying the ISE criterion.
2) Broadening a nonlinear backstepping based on VIC.
3) Ability to develop the proposed method for the other kinds of ACMGs such as inverter-based MGs, type 4 wind turbine generators MG and hybrid MGs.

The organization of this paper is as follows: Section 2 is devoted to the principles of the proposed method. The verification based on the obtained results via MATLAB/Simulink software is done in Section 3 and finally, the conclusions from this research are collected in Section 4.

Mitigation of Cyber Attacks Using Nonlinear Virtual Inertia Control

FDIA, DoS and HjA Mathematical Models

In the first step and before presenting the principles of the proposed method, the useful mathematical model of various cyber attacks applied in MGs are introduced, here [28–30]:

$$\begin{aligned} &FDIA: x^{att} = x + \alpha\Delta \\ &DoS: x^{att} = (1-\alpha)x \\ &HjA: x^{att} = (1-\alpha)x + \alpha\Delta \end{aligned} \tag{1}$$

In which, x^{att}, x, α are the attacked signal/data, healthy signal/data attack and the flag to identify the initiation of attacks. By α=1, the attack is launched and α=0 means there is not attacks. HjA is a combination of FDIA and denial of service (DoS) attack which has similarities to FDIA and DoS in the modeling. However, realization of FDIA seems to be simpler than HjA. Equation (1) expresses the important cyber attacks harm the integrity, availability and also, confidentiality of the target signals.

Introduction to Backstepping Control

One of the powerful nonlinear control methods so called backstepping is introduced in 1990 to design stable controls for a class of nonlinear dynamic systems. This method is recursive to stabilize the origin of the system using a strict feedback form. Therefore, backstepping approach determines how to stabilize the subsystems modeled by the states and in the presence of changes in variables. Moreover, backstepping control links the Lyapunov based stability benchmark with the feedback controller thus, the guarantee of global asymptotic stability is reached. This method is flexible to realize for a two dimension linear system to a three dimension jerk chaotic system [31]. Suppose the nonlinear system described by Eq. (2):

$$\dot{e} = e^4 + \sin(e) + \eta \;\; \dot{\eta} = u \tag{2}$$

where, e and η are the states and u is a backstepping control to be designed. Let's call η the virtual control. To find the stabilizing control law, a choice is:

$$\eta = -e^4 - \sin(e) - ke \;\; k \succ 0 \tag{3}$$

Substituting (2) in (1):

$$\dot{e} = ke \tag{4}$$

Then, the Lyapunov function is selected by

$$v = {}^{1}/_{2}\, e^2 \tag{5}$$

To prove the stability, the derivative of v must be globally negative definite on R^2. According to Eq. (6) the stability is reached.

$$\dot{v} = e\,\dot{e} = -ke^2 \prec 0 \tag{6}$$

Virtual Inertia Strategy

In recent years, applying VIC method is broadened in MGs [32–34]. The concept of VIC is utilized in low inertia

systems such as MGs to improve the inertia level. Moreover, this method is a supplementary control to release or absorb kinetic energy of rotary elements by changing frequency. As an important result, VIC can improve the frequency stability and transient response characteristic of DFIGs. In [32], the VIC for the DFIG is suggested by:

$$P^*_{stotal} = P^*_s + k_p(f^*_{sys} - f_{sys}) - k_d \dot{f}_s \tag{7}$$

Here, P^*_{stotal}, P^*_s, f^*_{sys}, f_{sys}, k_p and k_d are respectively the total stator reference active power, the stator reference active power derived via the conventional control loop, the reference system frequency, the system frequency and the fixed gains. The technique for VIC approach in [33] is based on Eq. (8):

$$P^* = P_{MPP} + P_{vir} \;\; P_{vir} = -k_1\Delta\omega - k_2 \dot{\Delta\omega} \tag{8}$$

In which, P^*, P_{MPP}, P_{vir} and $\Delta\omega$ are the total reference active power, the reference active power extracted via the conventional maximum power point tracking (MPPT) operation, the virtual active power and the difference between the reference and actual angular speed. k_1 and k_2 are the gains to be designed. The pertinent technique in the Laplace domain is expressed by [34]:

$$\Delta P_{vir} = \frac{k}{1+sT} s\Delta f \tag{9}$$

In the above equation, k and T denote the gain and the time constant. To mitigate the effects of cyber attacks on the frequency stability for islanded ACMG, a VIC scheme is proposed in [35] according to (10) in the Laplace domain:

$$\Delta P = \frac{1}{1+sT}\Delta f(ks + k_1) \tag{10}$$

Here, ΔP and Δf are the virtual active power and the deviation of the frequency. However, this research work is limited to investigate the contribution of VIC via the obtained results. In [36], the proposed VIC is implemented by:

$$P^*_{vir} = \frac{ks}{1+sT}(V^* - V) \tag{11}$$

V^* and V are the reference and measured voltage. It is worth mentioning that in the low inertia power systems such as MGs, the relation between active power-voltage could be considerable. It could be a reason that is why in (11) the relation between the voltage and active power is used for the VIC scheme.

Detection Approach

To activate the VIC approach in the active power control loop, first the cyber conditions caused by the attackers must be recognized, precisely. To do this task, the combined integral square error (ISE) of the active power and rotor speed as Eq. (12) is proposed.

$$\begin{aligned} SE &= \int_0^t [k_1(\omega^*_r - \omega_r)^2 + k_2(P^*_s - P_s)^2]\, dt \qquad k_1, k_2 \succ 0 \\ \Delta ISE(t+\tau) &= k_3 |ISE(t+\tau) - ISE(t)| \quad k_3 \succ 0 \end{aligned} \tag{12}$$

Here, ω^*_r is the reference rotor speed extracted via the lookup table to reach the MPPT mode. τ is the time constant for calculating the value of ΔISE in the short time intervals for the accuracy of the detecting method. Thus, this parameter is set to 0.000001 in the simulation process. Choosing a too low value of this time interval would be a proper guarantee for the accurate execution of the detection scheme. Moreover, if failing in some samples of the detection signals be probably happened, it would not cause malfunction of the discrete detection procedure. If the values of ΔISE are out of the defined thresholds (healthy band), the cyber conditions are diagnosed. In Fig. 1, the profile of this benchmark considering the cyber attacks on the reference active power (P^*_s), measured active power (P_s) and rotor speed (ω_r) during t = 1.5 s to 3 s in the test system is depicted as the samples. As can be seen the suitability of the proposed detection index is verified.

Why Proposing the Nonlinear Method?

To control active/reactive power of DFIG, RSC control loops must be carefully designed. The conventional control method is based on applying the PI controllers according to the stator voltage or flux orientation vector control [37]. Thus, designing two internal control loops of the rotor current components in the d and q axes is necessary. If the stator voltage orientation (SVO) is used, then the external control loop in the d axis is designed to control the active power. Hence, the other outer control loop in the q axis is specialized for the reactive power control. Instead, according to the stator flux orientation (SFO) approach, these duties are vice versa for the external control loops. Here, the problem for power control of DFIG is analytically considered via the following equations in per unit form [37]:

$$\begin{aligned} &P_s = Re(V_{sdq} I^*_{sdq}) = V_{sd} I_{sd} + V_{sq} I_{sq} \\ &V_{sdq} = V_{sd} + jV_{sq} \quad I_{sdq} = I_{sd} + jI_{sq} \\ &SVO \Rightarrow P_s = |V_s| I_{sd} \Rightarrow P_{s-inject} = -|V_s| I_{sd}, \quad |V_s| = 1 \quad p.u. \end{aligned} \tag{13}$$

$$SVO \Rightarrow V_{sq} = 0 \Rightarrow \psi_{sd} \approx 0 \Rightarrow I_{sd} = -\frac{L_m}{L_s} I_{rd}, \frac{L_m}{L_s} \approx 1 p.u. \Rightarrow P_{s-inject} \approx I_{rd} \tag{14}$$

Here, P, V, I, R, L and ψ are respectively the active power, voltage, current, resistance, inductance and

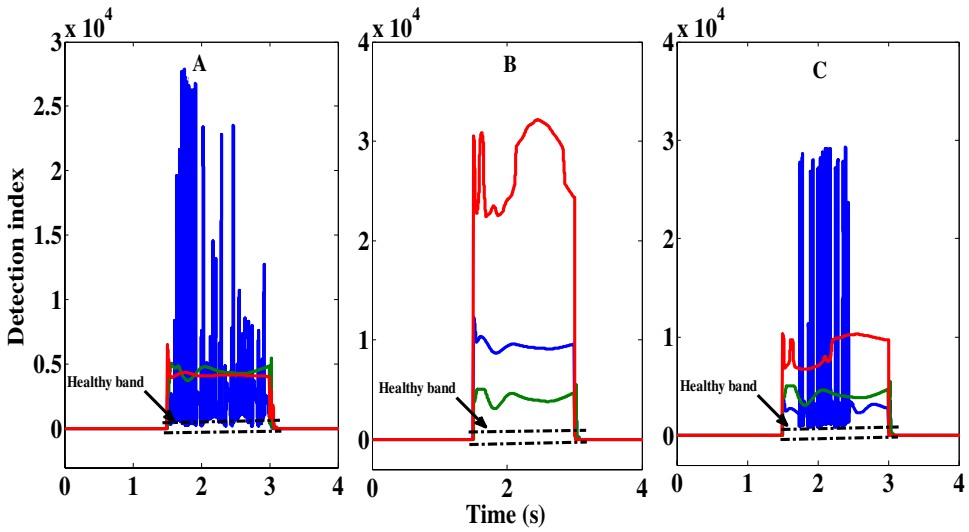

Fig. 1 Profile of the proposed detection index considering cyber attacks; (Blue: Attack on the reference active power, Green: Attack on the measured active power, Red: Attack on the rotor speed), Attack duration = [1.5 3] s, A: FDIA, B: HjA, C: DoS, $k_1 = 100$, $k_2 = 1$ and $k_3 = 1e8$

electromagnetic flux. The subscript of s, r, d and q denote, stator, rotor, d axis and q axis component. Equation (14) clearly expresses that the injected active by the DFIG is directly related to the rotor current. Hence, the rotor current components in the both axes have a direct relation with the rotor voltage components based on the next question in Laplace domain:

$$\begin{aligned} &V_{rd}(s) = R_r{}'I_{rd}(s) + \frac{L_r{}'}{\omega_b}SI_{rd}(s) - \omega_2 L_r{}'I_{rq}(s) + E_{rd}(s) \\ &V_{rq}(s) = R_r{}'I_{rq}(s) + \frac{L_r{}'}{\omega_b}SI_{rq}(s) + \omega_2 L_r{}'I_{rd}(s) + E_{rd}(s) \\ &R_r{}' \approx R_r + R_s, L_r{}' \approx L_r - L_m, \omega_2 = \omega_s - \omega_r, E_{rd}(s) \approx \\ &SV_{sd} = S|V_s|, E_{rq}(s) \approx SV_{sq} = 0 \end{aligned} \tag{15}$$

where, E_{rd} and E_{rq} are the disturbances which would be negligible in the steady state mode and $\omega_2 L_r{}'I_{rd}$ and $\omega_2 L_r{}'I_{rq}$ are the cross coupling terms with the low values which would be compensated by the feed forward terms. Accordingly, the transfer function of the inner control loops as $TF_d(s) = \frac{V_{rd}(s)}{I_{rd}(s)}$ and $TF_q(s) = \frac{V_{rd}(s)}{I_{rd}(s)}$ are similarly equal to $\frac{1}{\frac{L'_r}{\omega_b}s + R'_r}$ for the both axes. by manipulating the measurement active power, reference active power or rotor speed via cyber attacks, unpredictable changes would directly be effective on the rotor current components and consequently, on the rotor voltage reference components which are sent to the pulse width modulation (PWM) commands of the RSC. For example by injecting a periodic sinusoidal FDIA to the active power value, the additional term of $\frac{K\omega}{s^2+\omega^2}$ is appeared on the active power profile during the cyber attack which directly affects the rotor current components and consequently the rotor reference voltage components. Thus, the nonlinear behavior during the attacks would be expected. The samples of the irregular and nonlinear behaviors caused by various attacks are shown in Fig. 2.

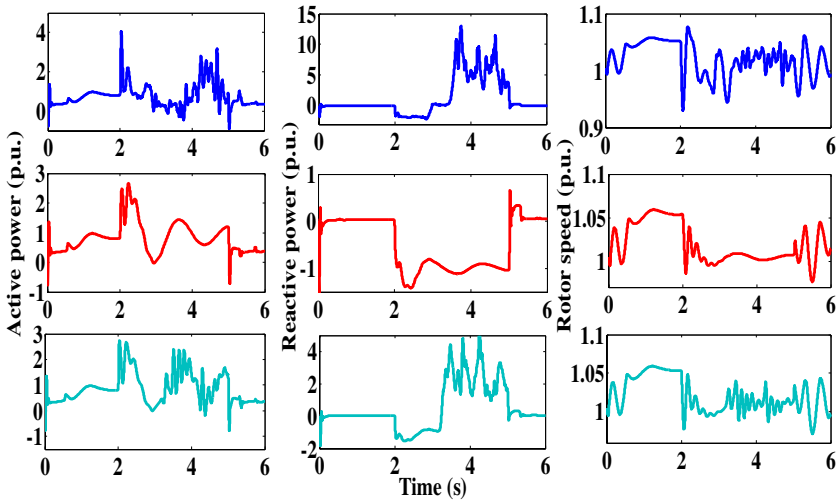

Fig. 2 Samples of nonlinear behavior caused by the FDIA (blue), DoS (red), HjA (green) in the WT DFIG for t = [2 5] s

Realization of the Proposed Method in the RSC

It is inferred in the general form of the VIC, the additional term of the reference active power is as a function of the frequency or angular frequency. This compensatory term is helpful in the cyber conditions, where the power and also, the energy level of the plant are disturbed by the cyber attacks. Therefore, by designing a suitable VIC scheme, certainly the malicious effects of attacks would be alleviated. In [35], applying the VIC for the impact assessment and mitigation of time delay in the measurement systems as the cyber attacks is proposed. However, the obtained results are shown, incompletely without the sufficient discussions.

In nonlinear backstepping approach for DFIG, the appropriate error signals must be chosen [38]. For realizing the backstepping VIC to effectively suppress the destructive effects of various cyber attacks, happening with P_s^*, P_s and ω_r, first the suitable error signal by Eq. (16) must be defined.

$$e_\omega = \omega_r^* - \omega_r \tag{16}$$

After defining the error signal, the Lyapunov candidate function is chosen to $v_f = {}^1/_2\, e_f^2$, therefore:

$$\dot{v} = e_\omega \dot{e_\omega} \equiv -k_\omega e_\omega^2 \;\; k_\omega > 0 \Rightarrow \dot{e_\omega} = -k_\omega e_\omega < 0 \tag{17}$$

Considering (4) as the main rule of backstepping control and using (16), results in (18).

$$\dot{\omega_r^*} - \dot{\omega_r} = -k_\omega(\omega_r^* - \omega_r) \Rightarrow \dot{\omega_r} + k_\omega \omega_r = \dot{\omega_r^*} + k_\omega \omega_r^* \tag{18}$$

In the normal operating conditions, the electrical parameters such as the rotor speed follow their references, therefore Eq. (18) is logical. Calculating the rotor speed via (18) is expressed in (19).

$$\omega_r = \frac{f_\omega(\omega_r^*) - \dot{\omega_r}}{k_\omega} \; f_\omega\left(\omega_r^*\right) = \dot{\omega_r^*} + k_\omega \omega_r^* \tag{19}$$

The mechanical model relates the mechanical and the electrical torques. By applying soft turbine shafts between turbine and generator, the two mass model has higher accuracy in comparison with the one mass model. The two mass model is realized by Eq. (20) [37].

$$\begin{aligned} 2H_g \, \dot{\omega_r} &= -T_e + D_{tg}(\omega_t - \omega_r) + k_{seq}\theta_{sh} \\ 2H_t \, \dot{\omega_t} &= T_m - D_{tg}(\omega_t - \omega_r) - k_{seq}\theta_{sh} \\ \dot{\theta_{sh}} &= \omega_b(\omega_t - \omega_r) \end{aligned} \tag{20}$$

H_g, H_t, T_e, T_m, ω_t, ω_b, D_{tg} and k_{seq} are respectively the generator and turbine inertia constant, the generator and turbine torque, the turbine speed, the base angular speed, the equivalent torsial damping and the torsial spring constant. Based on (20), Eq. (21) is established.

$$2H_g \, \dot{\omega_r} = -T_e + T_m - 2H_t \, \dot{\omega_t} \quad \Delta T = T_m - T_e \tag{21}$$

The relation between the mechanical and electrical speed considering the two mass model is extracted by (22):

$$\omega_t = \frac{\dot{\theta_{sh}}}{\omega_b} + \omega_r \tag{22}$$

Substituting (22) in (21):

$$\begin{aligned} \dot{\omega_r} &= \frac{\Delta T - \frac{2H_t \ddot{\theta}_{sh}}{\omega_b}}{2H} \\ H &= H_g + H_t \\ \Delta T &= T_m - T_e \end{aligned} \tag{23}$$

Now, we use the extracted $\dot{\omega}_r$ via the two mass model to the backstepping equation in (19).

$$\omega_r = \frac{2Hf_\omega(\omega_r^*) - \Delta T + \frac{2H_t \ddot{\theta}_{sh}}{\omega_b}}{2Hk_\omega} \tag{24}$$

Finally, the proposed higher order backstepping VIC is realized by applying (24) in (25).

$$P_{svir}^* = k_p e_\omega + k_d \, \dot{e_\omega} + k_{d1} \, \ddot{e_\omega} = k_p \omega_r^* - k_p \omega_r - k_d \, \dot{\omega_r} - k_{d1} \, \ddot{\omega_r} \tag{25}$$

Simulation Results

The Test Platform

The simulation platform for our study is including the three WT DFIGs connected via the transmission lines of 7 km from the 690 V bus to the 20 kV bus, ending to the weak grid as the sustainable energy production. The transformer of 690 V: 20 kV is provided to adjust the voltage level. More details are available in our previous work [37]. Single line diagram of the test system is depicted in Fig. 3. The final block diagram to realize the proposed method during the cyber conditions in the RSC is shown in Fig. 4. The following results are shown in the two case studies, without applying VIC in the blue dotted curves and with applying VIC based on the proposed detection and mitigation approaches in the red solid curves. The attacks are considered for all the DFIGs in the test system.

Scenario 1: Evaluation of the Proposed Method in the MPPT Mode

MPPT mode is as a suitable benchmark to evaluate the performance of DFIG. By the mean wind speed of about 12 m/s, the MPPT could be reached. Hence, a variable wind speed

profile of 12 m/s with about 25% turbulence, shown in Fig. 5 is applied in the simulation process.

Forcing a periodic FDIA including $\sin(40\pi t)$ during 8 s, launching at t = 2 s on P_s in the RSC is our first contingency. In Figs. 6 and 7, the DFIG active power and network frequency profile are depicted. From the both figures, it is inferred the improvement of the active power and frequency profiles while using the nonlinear VIC in the active power control loop of the RSC during the cyber occurrence.

The next attack as the DoS is considered for the rotor speed profile in the time interval of [4 8] s which the relative results are demonstrated via Figs. 8 and 9. As can be observed in Fig. 8, the severe oscillations up to 2.5 pu are suppressed in the red curve. Simultaneously, the significant

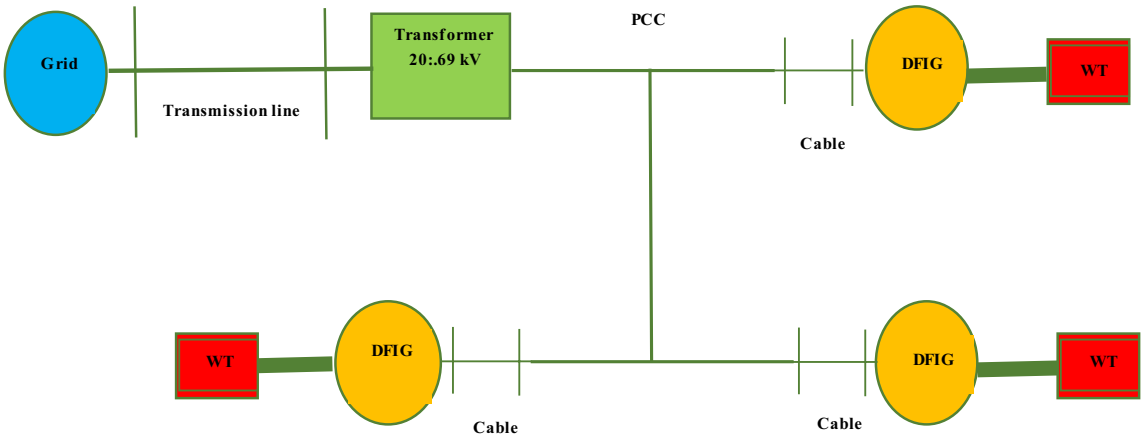

Fig. 3 Single line diagram of the sustainable energy production test system

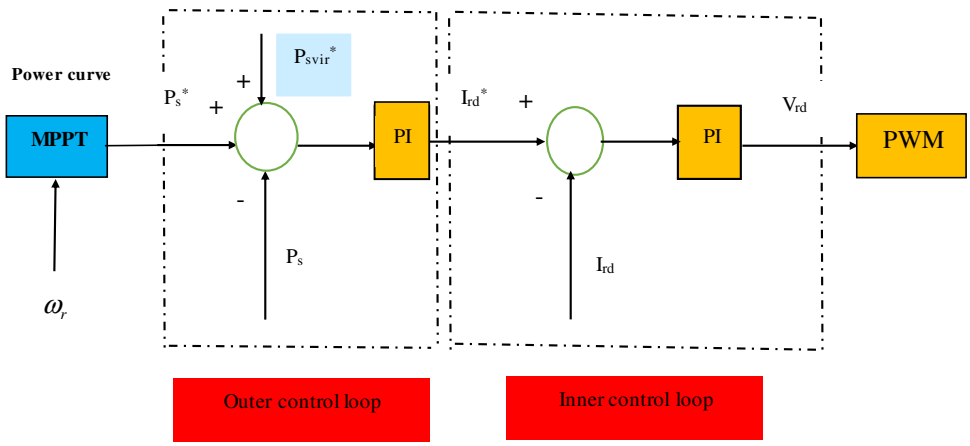

Fig. 4 Block diagram of the RSC control loops in the *d* axis considering the proposed VIC method

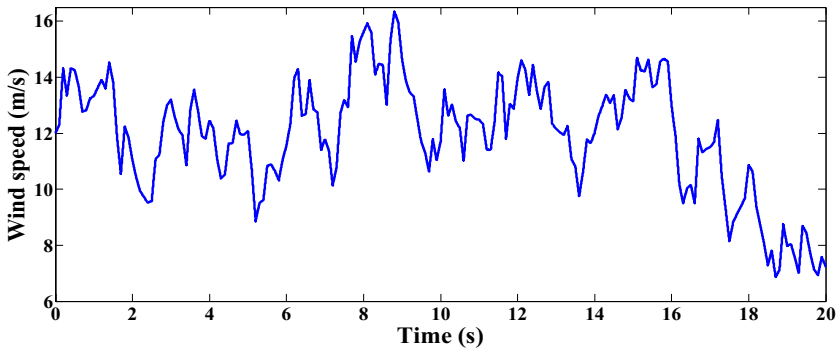

Fig. 5 Applied wind speed profile in the simulation process

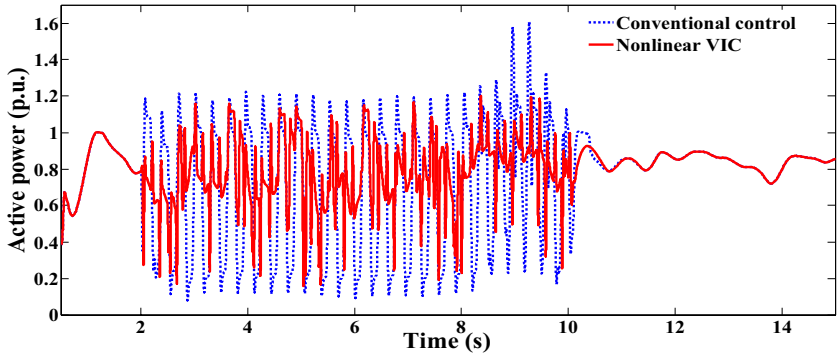

Fig. 6 DFIG active power profile considering the FDIA on the active power

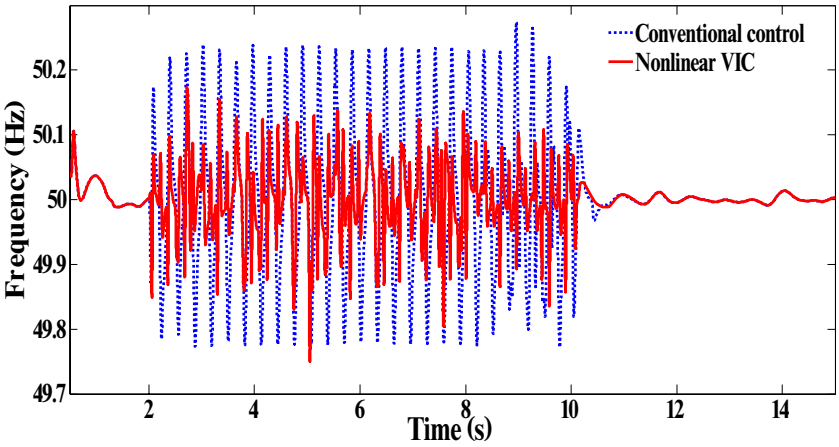

Fig. 7 Network frequency profile considering the FDIA on the active power

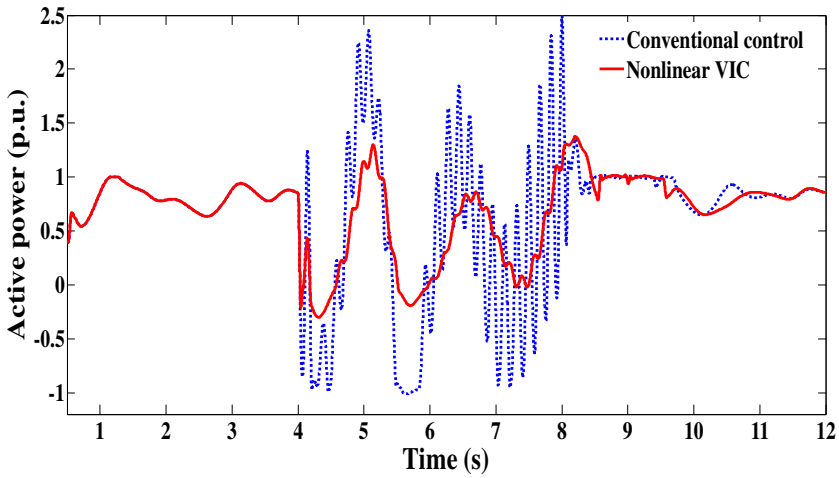

Fig. 8 DFIG active power profile considering the DoS on the rotor speed

improvement in the frequency profile during the DoS attack is confirmed according to Fig. 9.

In the next case, a hybrid HjA composed of a noisy HjA enforced on the reference active power, starting at the fifth s which is lasted until the ninth s. Meanwhile, the other HjA is the constant value of 0.3 pu on the rotor speed profile in the time domain of 3 to 12 s. The results for the active power and frequency profiles are illustrated in Figs. 10 and 11. Smoothing the DFIG active power and network frequency profiles by happening the HjAs as the superiority of the performance of the nonlinear control method is obvious in these figures which means the VIC would be an appropriate

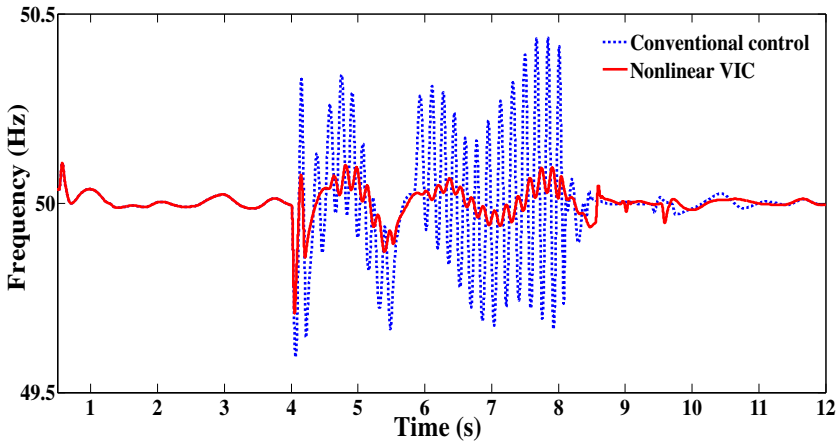

Fig. 9 Network frequency profile considering the DoS on the rotor speed

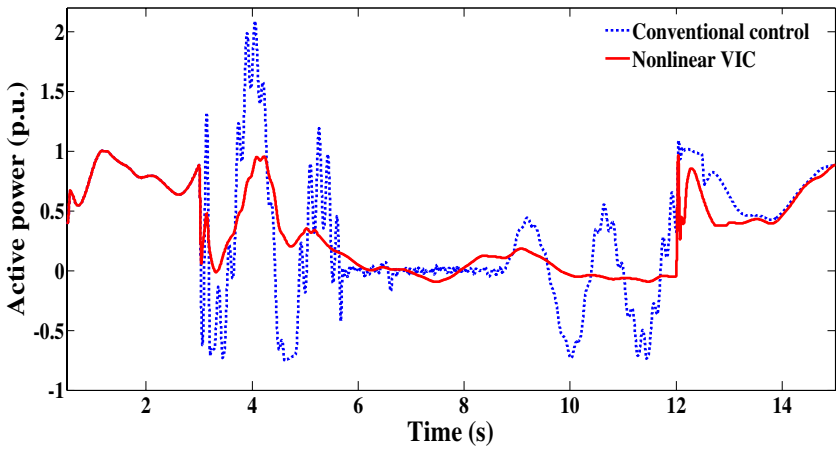

Fig. 10 DFIG active power profile considering the hybrid HjA on the reference active power and the rotor speed

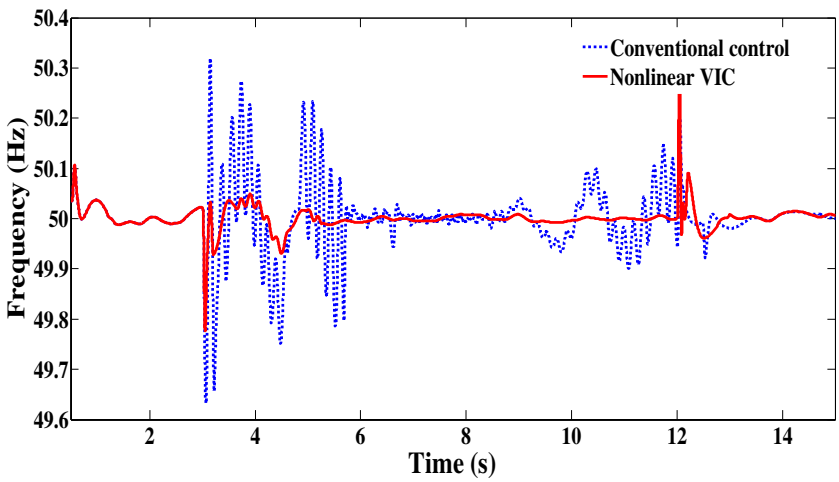

Fig. 11 Network frequency profile considering the hybrid HjA on the reference active power and the rotor speed

remedial action to enhance the cyber security of the test ACMG.

Scenario 2: Considering Uncertainties

Considering uncertainties is the suitable benchmark to evaluate the proposed method. In this regard, the first contingency is carried out by 50% reduction in the grid short circuit capacity (SCC) which means weakening the grid, significantly. A cascade cyber scenario including the DoS from t = 6 to 12 s and a fixed FDIA of -0.8 pu on P_s^* in the time domain of [12 14] s is considered. The relative obtained results are shown in Figs. 12 and 13. The pulsations of the active power profile bounded in the domain of [0 1.6] pu as

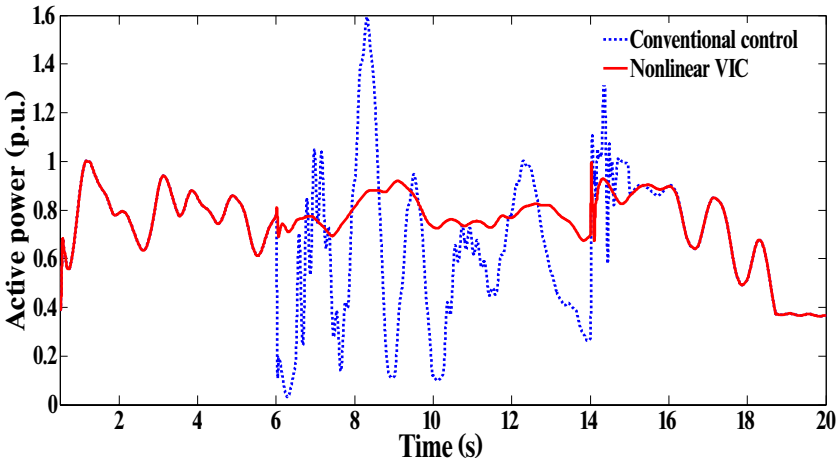

Fig. 12 DFIG active power profile considering the cascade DoS and FDIA on the reference active power and reducing the grid SCC

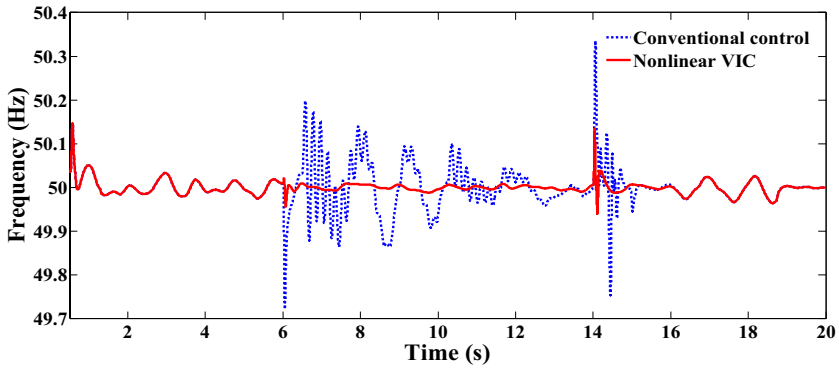

Fig. 13 Network frequency profile considering the cascade DoS and FDIA on the reference active power and reducing the grid SCC

the destructive effects of the attacks are highly damped out by activating the suggested VIC in the control loop which is shown in Fig. 12. Moreover, in the presence of the DoS and FDIA, the oscillations of frequency profile between 49.7 Hz to 50.35 Hz are remarkably suppressed, to reach a fairly flat profile according to Fig. 13.

Now, the X/R ratio of the grid is reduced to 2 as the other uncertainty in the grid parameters and a FDIA equal

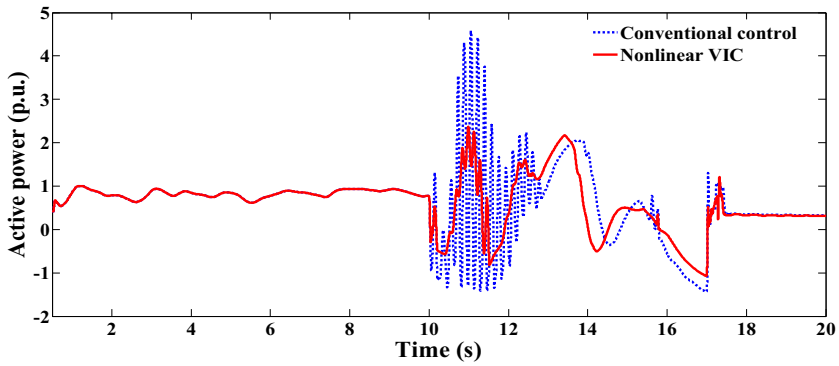

Fig. 14 DFIG active power profile considering the FDIA on the rotor speed and reducing the grid X/R ratio

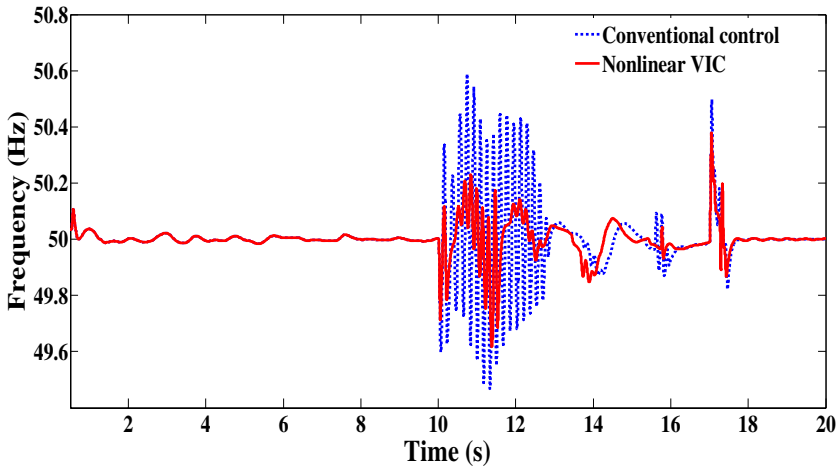

Fig. 15 Network frequency profile considering the FDIA on the rotor speed and reducing the grid X/R ratio

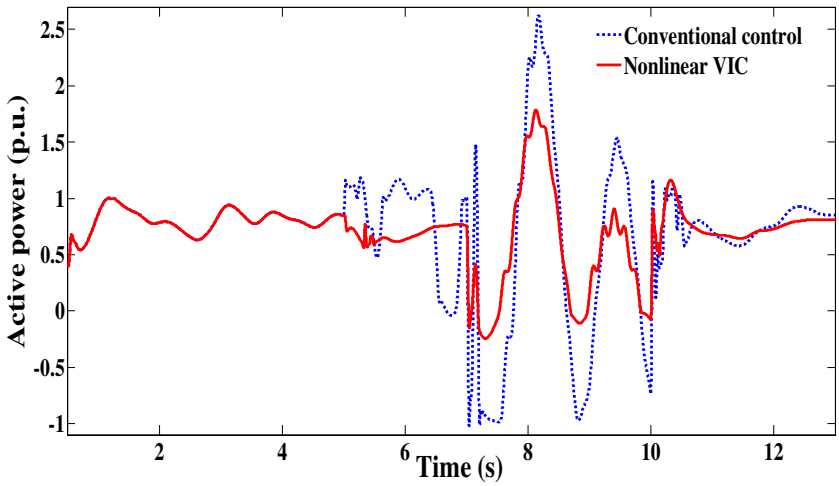

Fig. 16 DFIG active power profile considering the HjA on the active power and the DoS on the rotor speed and increasing the stator and rotor parameters

to $2\sin(2\pi t)$ as the pu value is forced to the rotor speed, launching at t = 10 s, ending after 7 s. Similar to the previous figures, the results are drawn via Figs. 14 and 15. As shown in Fig. 14, the oscillations of DFIG active power during the cyber conditions are varied from -1.3 pu to 4.5 pu by applying the conventional control without activating the

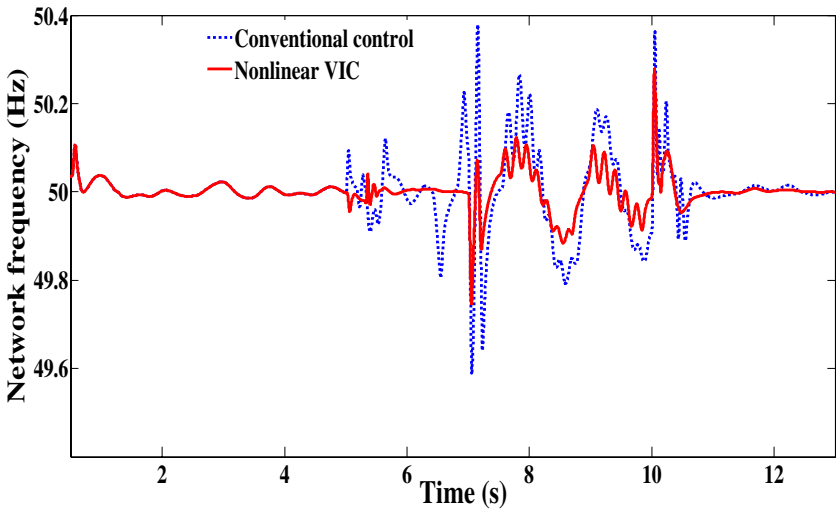

Fig. 17 Network frequency profile considering the HjA on the active power and the DoS on the rotor speed and increasing the stator and rotor parameters

VIC. These variations are severely mitigated by using the nonlinear VIC. Moreover, the frequency profile in Fig. 15 is improved as well in the red curve. Finally, a combined cyber attack composed of the DoS on ω_r during t = 7 to 10 s and the sinusoidal HjA of $0.65\sin(10\pi t)$ on P_s for 3 s, launching at the 5th s is the last case study. In this regard, the stator and rotor resistances and inductances are increased as 30%. The results are presented via Figs. 16 and 17. As can be seen from Fig. 16, the unacceptable oscillations caused by these attacks are reduced on the active power profile when performing the VIC scheme. Also, about 1 pu reduction in the upper and lower pulsations is visible. Due to the direct relation of DFIG active power and the stator frequency, by enhancing the active power control loop via the nonlinear VIC during the cyber conditions, the frequency profile is improved as well which is verified in Fig. 17.

Conclusion

This paper has investigated the application of the nonlinear virtual inertia approach in the active power control loops of the DFIGs in an AC sustainable energy production under cyber attacks. The attacks are including FDIA, HjA and DoS which caused the destructive effects on the DFIG parameters such as the active power and frequency profiles. In this regard and by proposing a detection scheme based on the combined ISE, the proposed higher order backstepping VIC method is activated during the cyber conditions. By realizing the new control scheme, it is shown the remarkable performance of the method during the various contingencies. The verification in the weak grid connected operation mode via MATLAB/Simulink software is precisely carried out. The scenarios are including various single and multi-cyber attacks; hence, the uncertainties in the grid and generator parameters are considered to evaluate the performance of the nonlinear VIC. It must to be noticed that this method would be broadened for the other test MGs such as hybrid MGs including DFIGs and full converter synchronous generators with wind and marine current turbines.

Author Contribution Hossein Mahvash: Writing-original draft, MATLAB simulation, investigation, methodology.

Seyed Abbas Taher: Supervision, consideration, verification, writing correction.

Joseph M Guererro: Consideration, advisor.

Funding The authors declare that they have no known competing financial interests and funding or personal relationships that could have appeared to influence and also participate the work reported in this paper.

Data Availability The data that has been used is confidential which are collected in our previous work [24].

Declarations Any possible declaration about ethics approval, consent to participate and publication are not relevant to the content of our submission and are not applicable.

Conflict of Interest The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

References

1. Carlini EM, Giannuzzi GM, Mercogliano P, Schiano P, Vaccaro A, Villacci D (2016) A decentralized and proactive architecture based on the cyber physical system paradigm for smart transmission grids modelling, monitoring and control. Technol Econ Smart Grids Sustain Energy 1(1):1–15. https://doi.org/10.1007/s40866-016-0006-1
2. Jha AK, Appasani B, Ghazali AN (2022) A comprehensive framework for the assessment of synchrophasor communication networks from the perspective of situational awareness in a smart grid cyber physicals System. Technol Econ Smart Grids Sustain Energy 7(20):1–18. https://doi.org/10.1007/s40866-022-00146-x
3. An L, Yang GH (2018) Improved adaptive resilient control against sensor and actuator attacks. Inform Sci 423:145–156
4. Liu Ch, He W, Deng R, Tian YCh, Du W (2023) "False-data-injection-enabled network parameter modification in power systems: Attack and detection. IEEE Trans Ind Inf 19(1):177–188
5. Ganguly P, Nasipuri M, Duta S (2018) A novel approach for detecting and mitigating the energy theft issues in the smart metering infrastructure. Technol Econ Smart Grids Sustain Energy 3:13.https://doi.org/10.1007/s40866-018-0053-x
6. Sahoo S, Chih-Hsien Peng J, Mishra S, Dragicevic T (2020) Distributed screening of hijacking attacks in DC microgrid. IEEE Trans, Power Electron 35(7):7574–7582
7. Shen H, Liu UA, Shi K, Park JH, Wang J (2023) Event-based distributed secondary control for AC islanded microgrid with semi-Markov switched topology under cyber-attacks. IEEE Syst J 17(2):2927–2938. https://doi.org/10.1109/JSYST.2022.3204754
8. Khalili J, MahdianDehkordi N, Hamzeh M (2022) Distributed event-triggered secondary frequency control of islanded AC microgrids under cyber attacks with input time delay. Int J Electr Power Energy Syst 143:108506
9. Zhang Y, Xiang Y, Wang L (2017) Power system reliability assessment incorporating cyber attacks against wind farm energy management systems. IEEE Trans Smart Grid 8(5):2343–2357
10. Wu H, Liu J, Liu J, Cui M, Liu X, Gao H (2019) Power grid reliability evaluation considering wind farm cyber security and ramping events. Appl Sci 9:3003 (1-18)
11. Zhao Sh, Xia J, Deng R, Cheng P, Yang Q (2023) Adaptive observer-based resilient control strategy for wind turbines against time-delay attacks on rotor speed sensor measurement. IEEE Trans Sustainable Energy 14(3):1807–1821
12. Zabetian-Hosseini A, Mehrizi-Sani A (2018) Cyberattack to cyber-physical- model of wind farm SCADA. In: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society. IEEE, Washington, DC. https://doi.org/10.1109/IECON.2018.8591200
13. Alotibi F, Tipper D (2022) Physics-informed cyber-attack detection in wind farms. In: GLOBECOM 2022 - 2022 IEEE Global Communications Conference. IEEE. https://doi.org/10.1109/GLOBECOM48099.2022.10000944
14. Datta A, Ashiqur Rahman M (2017) Cyber threat analysis framework for wind energy based power system. In: CPS '17: Proceedings of the 2017 Workshop on Cyber-Physical Systems

Security and Privacy, November 2017, pp 81–92. https://doi.org/10.1145/3140241.3140247
15. Elisa Ambarita E, Kuncara I, Widyotriatmo A, Karlsen A, Scibilia F, Hasan A (2023) On cyber-attacks against wind farms. In: IECON 2023-49th Annual Conference of the IEEE Industrial Electronics Society. IEEE, Singapore. https://doi.org/10.1109/IECON51785.2023.1031211
16. Mccarty M, Johnson J, Richardson B, Rieger C, Cooley R, Gentle J, Rothwell B, Phillips T, Novak B, Culler M, Wright B (2023) Cybersecurity resilience demonstration for wind energy sites in co-simulation environment. IEEE Access 11:15297 (1-17)
17. Sabev E, Trifonov R, Pavlova G, Rainova K (2021) Cybersecurity analysis of wind farm SCADA systems. In: 2021 International Conference on Information Technologies (InfoTech). IEEE, Varna. https://doi.org/10.1109/InfoTech52438.2021.9548589
18. Ghafouri M, Karaagac U, Ameli A, Yan J, Assi C (2021) A cyber attack mitigation scheme for series compensated DFIG-based wind parks. IEEE Trans. Smart Grid 12(6):5221–5232
19. Amini A, Ghafouri M, Mohammadi A, Konstantinos Plataniotis K (2022) Secure sampled-data observer-based control for wind turbine oscillation under cyber attacks. IEEE Trans Smart Grid 13(4):3188–3202
20. Ansari M, Ghafouri M, Ameli A (2022) Cyber-security vulnerabilities of the active power control scheme in large-scale wind-integrated power systems. In: 2022 IEEE Electrical Power and Energy Conference (EPEC). IEEE, Victoria. https://doi.org/10.1109/EPEC56903.2022.10000140
21. Badihi H, Jadidi S, Yu Z, Zhang Y, Lu N (2022) Smart cyber-attack-diagnosis and mitigation in a wind farm network operator. IEEE Trans Ind Inform 19(9):9468–9478. https://doi.org/10.1109/TII.2022.3228686
22. Kulev N, Torres FS (2022) Simulation of the impact of parameter manipulations due to cyber-attacks and severe electrical faults on offshore wind farms. Ocean Eng 260:111936
23. Hu S, Ge X, Chen X, Yue D (2023) Resilient load frequency control of islanded AC microgrids under concurrent false data injection and denial-of-service attacks. IEEE Trans Smart Grid 14(1):690–700
24. Naderi E, Asrari A (2023) Experimental validation of a remedial action via hardware-in-the-loop system against cyber attacks targeting a lab-scale PV/wind microgrid. IEEE Trans Smart Grid 4(5):4060–4072
25. Wang Y, Amin M, Fu J, Moussa HB (2017) A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids. IEEE Access 5:26022–26033
26. Mohammadpourfard M, Sami A, Weng Y (2018) Identification of false data injection attacks with considering the impact of wind generation and topology reconfigurations. IEEE Trans Sustain Energy 9(3):1349–1364
27 Ackermann T (2005) Wind power in power systems. Wiley
28. Solat A, Gharehpetian GB, SalayNaderi M, Anvari-Moghaddam A (2024) On the control of microgrids against cyber-attacks: A review of methods and applications. Appl Energy 353:122037
29. Mustafa A, Poudel B, Bidram A, Modares H (2020) Detection and mitigation of data manipulation attacks in AC microgrids. IEEE Trans Smart Grid 11(3):2588–2603
30. Abhinav Sh, Modares H, Lewis FL, Ferrese F, Davoudi A (2018) Synchrony in networked microgrids under attacks. IEEE Trans, Smart Grid 9(6):6731–6741
31. Vaidyanathan S, Azar AT (2020) An introduction to backstepping control. In: 2020 IEEE PES/IAS PowerAfrica. IEEE, Nairobi. https://doi.org/10.1109/PowerAfrica49420.2020.9219790
32. Zhang J, Li F, Chen T, Cao Y, Wang D, Gao X (2022) Virtual inertia control parameter regulator of doubly fed induction generator based on direct heuristic dynamic programming. Energy Rep 8:259–266
33. Liu B, Zhao J, Huang Q, Milano F, Zhang Y, Hu W (2021) Nonlinear virtual inertia control of WTGs for enhancing primary frequency response and suppressing drivetrain torsional oscillations. IEEE Trans Power Systems 36(5):4102–4113
34. Oshnoei S, Aghamohammadi MR, Oshnoei S, Sahoo S, Fathollahi A, Khooban MH (2023) A novel virtual inertia control strategy for frequency regulation of islanded microgrid using two-layer multiple model predictive control. Appl Energy 343:121233
35. Aluko AO, Carpanen RP, Dorreli DG, Ojo E (2020) "Impact assessment and mitigation of cyber attacks on frequency stability of isolated microgrids using virtual inertia control," IEEE PES/IAS power Africa
36. Chlea M (2017) Cyber security enhancement against cyber-attacks on microgrid controllers. PhD Thesis McGill University Canada
37. Mahvash H, Taher SA, Rahimi M (2017) A new approach for power quality improvement of DFIG based wind farms connected to weak utility grid. Ain Sham Eng J 8(3):415–430
38. Patel R, Hafiz F, Swain A, Ukil A (2021) Nonlinear rotor side converter control of DFIG based wind energy system. Electr Power Syst Res 198:107358