A User-centric Approach toward Resilient Frequency-regulating Wind Generators

MOHAMMADREZA ARANI and DEEPA KUNDUR, University of Toronto

Smart microgrids are rapidly being developed and deployed, even as concerns over their cyber-physical security are increasing. The high penetration of these power electronic-interfaced energy resources has resulted in weaker power grids and an increase in cyberattack surface. The implementation of frequency regulation in these new resources—particularly in wind generators—is on the rise. This article investigates how malicious controllable loads can threaten the integrity of frequency-regulating wind generators. Adopting a user-centric approach and benefiting from small-signal analyses, the article shows for the first time how these wind generators can be the target of attackers. Effective methods to enhance system resilience are sought by mitigating the attack risk in the extended end-users, wind generators. The article models and explores how proper tuning and design of the physical system can improve cyber-physical security. The work also extends the user-centric method to the physical layer of smart grids. Detailed time-domain simulations verify the results of the analyses.

CCS Concepts: • **Security and privacy → Malware and its mitigation**;

Additional Key Words and Phrases: Microgrid, weak grid, cyber-physical security, user-centric security, wind generator, frequency regulation, virtual inertia, droop, resiliency

ACM Reference format:
Mohammadreza Arani and Deepa Kundur. 2020. A User-centric Approach toward Resilient Frequency-regulating Wind Generators. *ACM Trans. Cyber-Phys. Syst.* 4, 3, Article 36 (May 2020), 23 pages.
https://doi.org/10.1145/3389682

NOMENCLATURE

A	State Matrix	T_g	Wind generator electromagnetic torque
AGC	Automatic Generation Control	T_{sample}	Sampling Time
B	Input Matrix	${v_{dc}}^2$	Square of wind generator dc-link voltage
C	Output Matrix	${V_{ref}}^2$	Square of reference value for dc-link voltage

This work is supported by the National Science and Engineering Research Council, under award PDF - 502484 - 2017.
Authors' addresses: M. Arani, Ryerson University, Toronto, Ontario, Canada; email: marani@ryerson.ca; D. Kundur, University of Toronto, Toronto, Ontario, Canada; email: dkundur@ece.utoronto.ca.

2378-962X/2020/05-ART36 $15.00
https://doi.org/10.1145/3389682

com	Subscript denotes communication subsystem	v_w	Wind speed
D	Thermal generator damping	*w*	Subscript denotes wind power plant subsystem
DER	Distributed Energy Resources	*wco*	Subscript denotes wind side converter and the generator subsystem
DG	Distributed Generation	*wrg*	Subscript denotes frequency-regulating subsystem
D_i	Feedthrough Matrix	*x*	state
D_v	Active Damping gain	ZOH	Zero-Order Hold
E(s)	Communication error	β	Pitch angle
ESS	Energy Storage System	θ	Shaft angle
$i_{aq\text{-}ref}$	Reference value for the wind generator q-axis current	λ	Mode (pole or eigen-value)
i_q	Wind generator q-axis current	ξ	Damping factor
K_a	Attack gain	ϕ_{adi}	Internal states of active damping subsystem
LP	Load Point	ϕ_{agc}	AGC state
M_{diesel}	Thermal generator inertia	ϕ_{atti}	Internal states of the Attack Method block
mg	Subscript denotes whole microgrid subsystem	ϕ_{dly}	Communication delay state
ml	Subscript denotes malicious load subsystem	ϕ_{ffi}	Internal states of the frequency regulation method (virtual inertia/droop) used in the Frequency regulation subsystem
M_v	Virtual inertia gain	ϕ_{flli}	Internal states of the PLL used in the Frequency regulation subsystem
P_{ad}	Active damping power reference	ϕ_{gov}	Governor state
P_{att}	Active power consumed by malicious load	ϕ_{ireg}	Wind side converter current regulating state
P_{conv}	Grid side converter active power	ϕ_{rot}	Thermal generator rotating mass state
P_g	Wind side converter active power	ϕ_{tur}	Thermal turbine state
P_L	Microgrid load	ϕ_{vreg}	Grid side converter dc-link voltage regulating state
PLL	Phase Locked Loop	ϕ_{zohi}	ZOH internal state
P_{reg}	Frequency regulation power reference	ω_{att}	Attack Method natural frequency
$\hat{}P_w$	The output of the wind power plant	ω_g	Wind generator rotating speed
$\hat{}p_w$	Received wind power plant output signal from the communication system	ω_m	Microgrid frequency
ROCOF	Rate of change of frequency	ω_t	Wind turbine rotating speed
tg	Subscript denotes thermal generator subsystem		

1 INTRODUCTION

Smart grids have come a long way in recent years, with academic discussions on the subject leading to standards that have been widely adopted by industry. The standard IEC 61850, which was initially developed to standardize substation automation, has particularly gained the attention of microgrid researchers. Initial studies were mainly focused on proposing dynamic communication-based protection methods responding to the challenges of these grids [1, 3]. The second edition of the standard evolved to broaden its scope from substations alone to the entire utility [4]. This signfiicant extension proposed a standardized platform for microgrid communication that has attracted even greater attention. Not only were new, more robust distributed protection methods introduced [5, 6], but novel control schemes were also enabled. Some of the early researchers in this field were Ali et al. [7] and Cintuglu et al. [8], who employed IEC 61850-based communication for secondary and tertiary frequency regulation and [9] benefited from the standard to support smart volt/var regulation.

Despite the benefits that automation brings to power systems, new and significant challenges have also emerged that must be addressed. Of these challenges, cyber-physical security is such a priority that researchers have begun to investigate the various aspects of this new threat [10, 11]. Initial efforts were mainly focused on attacks on transmission systems, with traditional thermal synchronous generators impacting transient stability [12, 16].

Other aspects of power systems have also gained research attention. Li et al. [17] warned of "*selfish*" behavior of renewable energy resources, and Qi et al. [18] discussed the risks of unauthorized access to distributed energy resources. Liang et al. [19] similarly emphasized the importance of investigating False Data Injection Attacks in distribution systems and on the consumer side. It should be no surprise, then, that new trends in cyber-physical security of power systems have emerged with such vigor.

In addition to articles such as Reference [20], which explored Denial of Service and Timed Delay Switch attacks on power system frequency regulation, malicious utilization of controllable loads was investigated almost simultaneously by several different research teams. Brown and Demarco [21] discussed how emulated inertia could be misused by an attacker to destabilize the power grid. However, despite its merits, the system neglects all system limits and nonlinearities, and loads as large as 3 pu are needed for the relay to trip. Ultimately, the paper [21] focused on controllable loads and did not examine emulated inertia in-depth. Amini et al. [22, 23] addressed some of the gaps in Reference [21], demonstrating that a smaller load could be employed to destabilize the power system and proposing a method for allocating the attack. However, this work also suffers from over-simplification and ignores turbine and governor dynamics and all system nonlinearities. More comprehensive modeling of the power system was covered in Reference [24], although the attack effort in terms of load was also unaddressed. Note that while these contributions focused on malicious controllable loads, the scope of the work relates to transmission systems dominated by traditional synchronous generators.

The research efforts of Zhang et al. [25] are among only a few resources that address the cyber vulnerabilities of wind generators. However, in their study, the authors looked mainly at power system reliability (in contrast to stability) and attack impacts that typically lead to wind generator disconnection, while ignoring the primary frequency regulation implementation in wind generators. More specifically, Zhang and colleagues [25] focused on the cyber vulnerabilities of wind generators that allow an attacker to send false commands to disconnect the generator from the main grid. The authors also discussed how attacking a wind turbine control feature is often more feasible than accessing its associated control center. It should be noted that the physical

vulnerabilities of the wind generator (i.e., its soft shaft) and the use of a controllable load to destabilize wind generation is absent in their work.

In the present article, we propose that microgrid cyber-physical security requires extra scrutiny, given the unique characteristics that make attacking them and achieving impacts more attainable. While the deployment and use of microgrids is considered one approach to improve overall grid resiliency, we assert that microgrids with a high penetration of power-electronic interfaced energy resources can often suffer from a lack of sufficient inertia, thus diminishing resiliency. Further, many of these distributed energy resources may be owned by non-utility entities or be more easily accessible both physically and electronically via communication networks. Hence, such systems exhibit greater fragility in terms of physical stability and an increased attack surface, making them prime targets of attack. Cyber-physical security approaches thus play a vital role in the secure, stable, and safe operation of microgrids.

Unfortunately, typical network-oriented security methods are incapable of addressing all these issues alone, as they are information-centric. They exclude the attack impact on the stability of physical system, which must be accounted for to effectively address cyber-physical system resilience. For example, a malicious insider that is the legitimate reciever of data cannot always be detected easily and effectively by typical network-oriented methods [26]. By extending the user-centric approaches, this article defines the physical components as the end-user to provide a novel perspective to address the gap in the limited studies on the cyber-physical security of microgrids.

Chlela et al. [27] investigated the impact of denial of service attacks on microgrid secondary frequency regulation by employing an expanded attack time, an oversimplified grid, and a high reliance on battery energy storage despite the presence of a diesel generator. In contrast, the researchers in Reference [28] adopted a practical approach, proposing a new and more resilient network communication architecture for microgrids. Their research focused on presenting the network architecture and proposed a relevant infrastructure and testbed for future studies.

While previous efforts were mainly network-centric (such as References [29, 31]), we, in the present study, adopt a user-centric approach by focusing on a vital end-user of the communication network: the frequency-regulating wind generator. Distributed Energy Resources (DERs), which include wind generators, are often owned by private parties, not the utility that operates the grid. In this sense, they are the users of the physical power system that provides energy to the loads and other users, and they economically benefit from this transaction. Moreover, these DERs are essentially end-users of the associated (cyber) communication network system. From a cyber-physical perspective, two systems—the power system and the communication system—coexist and cooperate. In this way, even a generation plant or an energy storage device owned by the utility is an end-user, from the perspective of the communication network system.

User-centric approaches have recently gained attention in smart grid cybersecurity discussions; however, they are largely related to privacy concerns of smart meters. For example, Reference [32] tries to enhance the privacy by changing the sampling period, Reference [33] by using wavelet transform, and Reference [34] by aggregation of data. However, these references and others, including References [35, 36], are primarily focused on electrical loads. One exception is Reference [37], which discusses the necessity of user-centric methods for distributed energy resources. Like Reference [37], we pursue a "*security by design*" approach for the end-user, but instead of focusing solely on a cyber perspective, we extend the concept to cyber-physical aspects more appropriate for the smart grid. We investigate the vulnerabilities that wind-based frequency regulation can expose the system to in the presence of malicious controllable loads.

In this article, user-centric approaches for smart grids are employed to remove the vulnerabilities that end-users in the physical layer (power system) can introduce to the cyber-physical system (smart grid) and that can be exploited in a cyber attack. The article seeks an approach to

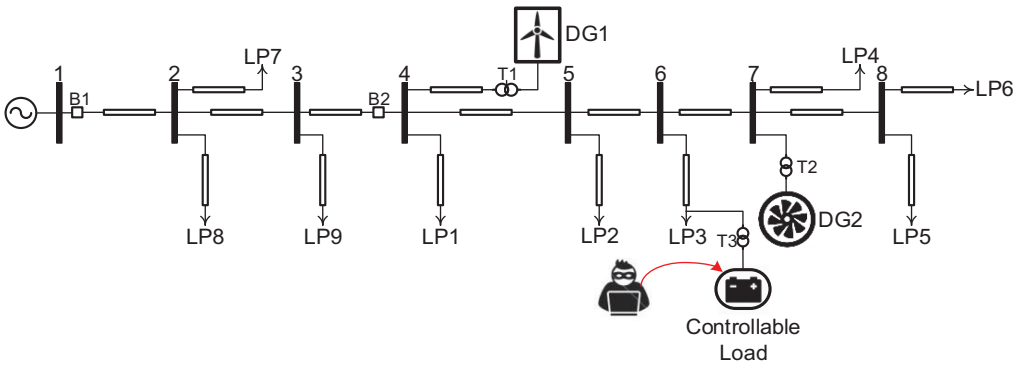

Fig. 1. Physical system under study.

further enhance microgrid resiliency through proper design. This work complements necessary approaches to improve communication network design and focuses on reducing physical risk in frequency-regulating wind generators as an end-user of the cyber system. We assert, in this article, that a practical approach to studying the cyber-physical security of microgrids should simultaneously consider its salient aspects, which consist of its weak grid nature, the existence of a high penetration of renewable energy resources, and the presence of distributed resources more easily exploitable than in transmission systems, in addition to their associated interactions.

The systematic approach provided in this article benefits from small signal modeling to provide additional insight. The model is then enhanced and evolved to account for important system nonlinearities. The improved model can be used not only to observe the vulnerabilities of the system, but to design and improve its inherent resiliency by enhancing the cyber-physical security of end-users of the system. Time-domain simulations are employed to demonstrate the accuracy of the model. Overall, the three main contributions of this article are:

(1) Proposing an effective model for investigating the attacks on primary frequency regulation.
(2) Identifying cyber-physical vulnerabilities of frequency-regulating wind generators.
(3) Exploring user-centric resiliency as a design factor for primary frequency regulation tuning.

The remainder of this article is organized as follows: The next section is devoted to small-signal modeling and analysis of frequency-regulating wind generators and their attacks. Section 3 discusses the proposed design approaches to enhance resilience, while Section 4 focuses on enhancing the model to provide deeper insight to the problem and its solution. Time-domain simulation results are presented in the subsequent section, and in the final section, conclusions are drawn.

2 MODELING AND ANALYSIS

While the deployment of renewable energy-based microgrids is increasing rapidly, the major market share belongs to thermal generation-based microgrids. This trend will likely not change significantly in the near future [38], which underscores the importance of analyzing the resiliency of thermal generation-based microgrids. Moreover, such studies can be generalized to other weak grids that suffer from lack of sufficient inertia. In the present article, we refer to a system as "weak" if it suffers from either high impedances or low inertia, as such systems have problems maintaining their required voltage and frequency levels [39].

The system shown in Figure 1 (based on a real system in Ontario, Canada) is employed in this article and represents a typical medium-voltage rural distribution system. The US Department

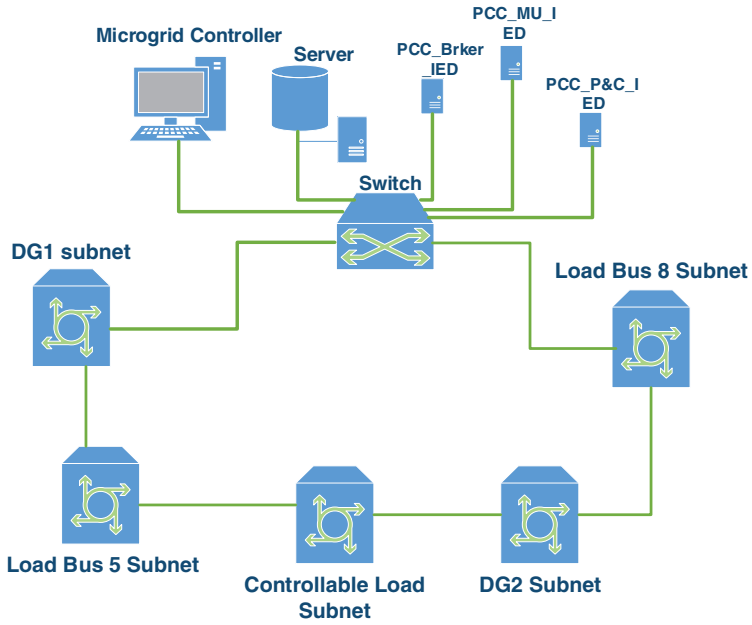

Fig. 2. Communication network architecture for the microgrid under study.

of Energy (DOE) defines a microgrid as "*a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island-mode.*" Commercial microgrids are described as microgrids with less than 10 MW load [40]. Accordingly, the segment after the circuit breaker B2 can operate in the islanded mode and constitutes a microgrid with an overall load of 3.77 MW/1.24 MVAr and two Distributed Generation (DG) units. The DG units used in a microgrid are in line with the CIGRE working group's description of microgrid generation [41].

A DG1 is a variable speed wind turbine connected to a 2.5 MVA PMSG with a full-scale converter, while a DG2 is a 2.5 MVA synchronous generator with droop and excitation controls. Here, droop represents a load-sharing speed-regulating mechanism that drops the generator speed as the load increases [39] and enables active power and frequency regulation. Excitation involves controlling the generator field voltage responsible for voltage and reactive power regulation [39]. A malicious controllable load is connected to Bus 3, which is a battery storage device connected to the grid via a converter. In reality, it can represent other energy storage types, such as an electric vehicle parking lot.

Figure 2 shows the communication network architecture for the microgrid. It is based on the IEC 61850 protocol. Each subnet consists of several switches connected to Intelligent Electronic Devices (IEDs). These IEDs receive signals from the sensors and send commands to actuators. A detailed explanation of the microgrid communication network architecture and protocol can be found in Reference [7].

2.1 Modeling

For systematic and comprehensive study, we will use the model shown in Figure 3. Each block is represented by state-space equations. For example, the wind generator side converter

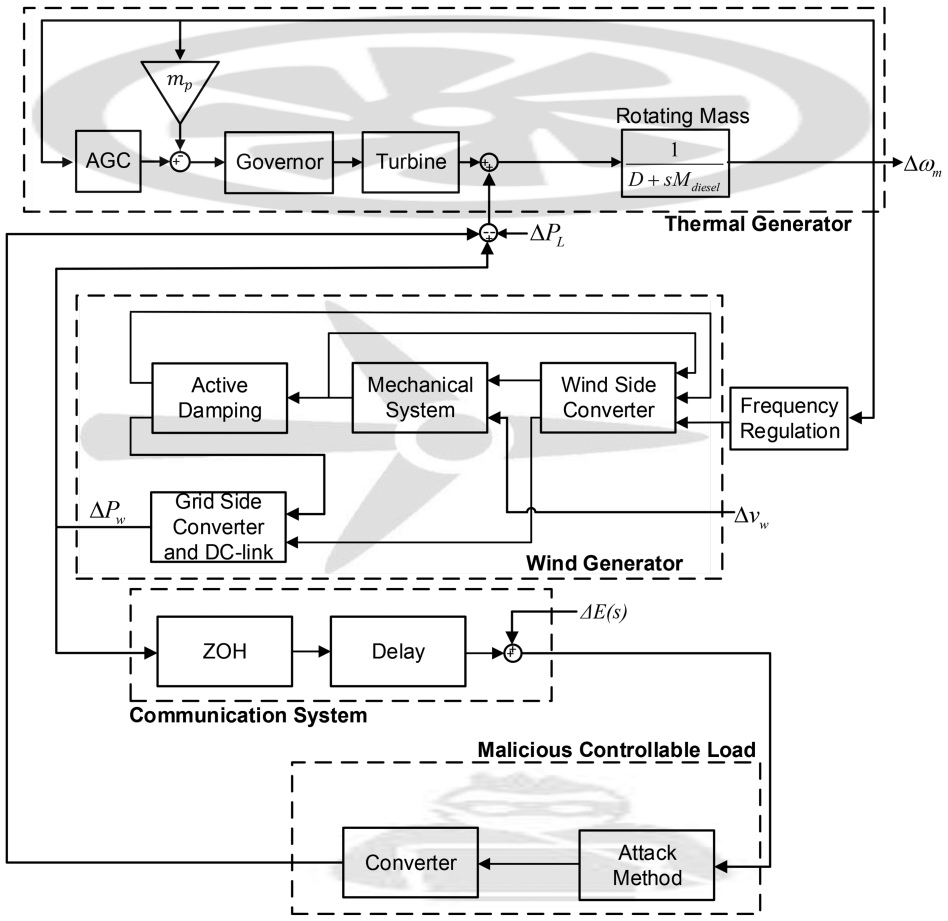

Fig. 3. Block diagram of microgrid frequency regulation.

controller is modeled by Equations (1)–(3), while Equations (4)–(5) represent the mechanical system. Additionally, x_{wco} refers to the states of the converter, while ω_g, P_{reg}, P_{ad}, and $i_{aq\text{-}ref}$ are the inputs and denote the rotating speed of the generator, the desired power for frequency regulation, the active damping reference power, and the active damping reference current corresponding to the q-axis, respectively. A more detailed discussion of methods for implementing primary frequency regulation in wind generation can be found in References [48, 49].

The outputs of the block are P_g, the converter active power, and T_g, the generator torque. These outputs play the role of input for the Grid Side Converter and DC-link, and the Mechanical System blocks, respectively, while x_{mec} represents the mechanical system states. The inputs are T_g, v_w, wind speed, β, and pitch angle. For this study, the pitch angle is assumed to be consistently zero. The output of the block is ω_g, which is an input for both the Wind Side Converter and the Active Damping blocks. The work in Reference [42] provides further details on Grid Side and Wind Side Converter control strategies. The prefix Δ denotes small signal modeling, and A, B, and C are matrices used for describing the state-space equations.

$$\Delta\dot{x}_{wco} = A_{wco}\Delta x_{wco} + B_{1wco}\Delta\omega_g + B_{2wco}\Delta P_{reg} + B_{3wco}\Delta P_{ad} + B_{4wco}\Delta i_{aq-ref} \quad (1)$$

$$\Delta T_g = C_{3wco}\Delta x_{wco} \tag{2}$$

$$\Delta P_g = C_{4wco}\Delta x_{wco} + D_{4wco}\Delta\omega_g \tag{3}$$

$$\Delta\dot{x}_{mec} = A_{mec}\Delta x_{mec} + B_{3mec}\Delta T_g + B_{4mec}\Delta v_w + B_{6mec}\Delta\beta \tag{4}$$

$$\Delta\omega_g = C_{1mec}\Delta x_{mec} \tag{5}$$

The blocks within each dashed box are subsequently merged to construct more comprehensive models. The thermal generator, x_{tg}, wind generator, x_{wind}, frequency regulation, x_{wrg}, communication system, x_{com}, and malicious controllable load, x_{ml}, models are formulated as Equations (5)–(14). Variable x denotes the states and ω_m refers to the microgrid frequency. *E(s)* is the error introduced by the communication system. The malicious controllable loads will be explained in more detail, but the details of other blocks are omitted due to space limitations; the reader is referred to Reference [39] for details on the thermal generator and to References [43, 44] for more information on the wind generator.

$$\Delta\dot{x}_{tg} = A_{tg}\Delta x_{tg} + B_{tg}\left(\Delta P_L - \Delta P_w + \Delta P_{att}\right) \tag{6}$$

$$\Delta\omega_m = C_{tg}\Delta x_{tg} \tag{7}$$

$$\Delta\dot{x}_{wind} = A_w\Delta x_{wind} + B_{2w}\Delta P_{reg} + B_{5w}\Delta v_w + B_{8w}\Delta V_{ref}^2 \tag{8}$$

$$\Delta P_w = C_{9w}\Delta x_{wind} \tag{9}$$

$$\Delta v_{dc}^2 = C_{10w}\Delta x_{wind} \tag{10}$$

$$\Delta\dot{x}_{com} = A_{com}\Delta x_{com} + B_{1com}\Delta P_w \tag{11}$$

$$\Delta\hat{P}_w = C_{com}\Delta x_{com} + D_{2com}E(s) \tag{12}$$

$$\Delta\dot{x}_{wrg} = A_{wrg}\Delta x_{wrg} + B_{wrg}\Delta\omega_m \tag{13}$$

$$\Delta P_{reg} = C_{wrg}\Delta x_{wrg} \tag{14}$$

$$\Delta\dot{x}_{ml} = A_{ml}\Delta x_{ml} + B_{1ml}\Delta\hat{P}_w + B_{2ml}\Delta\omega_m \tag{15}$$

$$\Delta P_{att} = C_{ml}\Delta x_{ml} \tag{16}$$

The microgrid model is derived by combining Equations (6)–(16) to give the state-space description of Equation (17), which contains 27 states related to the entire microgrid. The associated state-space matrix is shown in Equation (18), where the matrix zeros are not scalar but 2-D matrices with zero elements.

$$\Delta\dot{x}_{mg} = A_{mg}\Delta x_{mg} + B_{1mg}\Delta v_w + B_{2mg}\Delta P_L \tag{17}$$

$$A_{mg} = \begin{bmatrix} A_{tg} & 0 & -B_{tg}C_{9w} & 0 & B_{tg}C_{ml} \\ B_{wrg}C_{tg} & A_{wrg} & 0 & 0 & 0 \\ 0 & B_{2w}C_{wrg} & A_w & 0 & 0 \\ 0 & 0 & B_{1com}C_{9w} & A_{com} & 0 \\ B_{2ml}C_{tg} & 0 & 0 & B_{1ml}C_{com} & A_{ml} \end{bmatrix} \tag{18}$$

$$x_{mg} = [x_i]^T = \Big[\varphi_{agc}\ \varphi_{gov}\ \varphi_{tur}\ \varphi_{rot}\ \varphi_{fll1}\ \varphi_{fll2}\ \varphi_{ff1}\ \varphi_{ff2}\ \varphi_{ad1}\ \varphi_{ad2}\ \varphi_{ad3}\ \varphi_{ad4}\ \varphi_{ad5}\ \varphi_{ireg}\ i_q\ \omega_g\ \theta\ \omega_t\ \varphi_{vreg}\ P_{conv}\ v_{dc}^2\ \varphi_{zoh1}\ \varphi_{zoh2}\ \varphi_{dly}\ \varphi_{att1}\ \varphi_{att2}\ P_{att} \Big]^T \tag{19}$$

2.2 Attack Model

It is assumed that the attacker obtains information from frequency-regulating units and uses the controllable load to destabilize the microgrid. Our attack model is as follows: The attacker has access to critical information from wind-based frequency-regulating units. References such as [25] have explained how protocols like IEC 61850-7 and IEC 61400-25 may be exploited to achieve this. The attacker has agency over a controllable load. Internet-based access to the load is discussed in several references, such as [22] and [45]. Moreover, Reference [18] has mentioned direct control over smart inverters in distribution systems as a plausible scenario. An attack is deemed successful if the resulting impact leads to relay tripping and subsequent system reduction (load/generator disconnection).

The last point needs greater elaboration. A successful attack leads to relay-tripping and consequent disconnection of some generation and/or load. Different types of relays protect the grid frequency. A well-known class, also implicitly used in Reference [22], aims to prevent under- (and over-) frequency by requiring frequency deviation to stay below a threshold for a predetermined time to trip [46]. An attack of an oscillatory nature, however, results in oscillatory power system frequency within thresholds.

As such, another type of important relay is responsive to the Rate Of Change Of Frequency (ROCOF). In case of very fast frequency changes, this relay will trip, even though the frequency is in the allowable range. In transmission systems, a threshold of 0.1–1.2 Hz/s is typically adopted for this relay [47]. However, in grids with high penetration of inverter-interfaced distributed generation, this constraint is more relaxed [46]. In the present study, and without loss of generality, a threshold of 3 Hz/s is used; however, the main findings are still applicable to grids with more sensitive relays. The attacker control will be discussed in more detail in the next sections.

2.3 Attack Impacts

By introducing wind-based frequency regulation, the dominant modes of the system migrate to the left half-plane and the power system becomes more stable [48, 49]. Although it appears on initial observation that the stability margin of the power system has increased and consequently system resiliency has also increased, we assert that this is not a complete picture. Type-4 wind generators, which are direct-drive permanent magnet synchronous generators, have the second largest share of the wind market. These wind generators are connected to the grid through a full-rated back-to-back (AC/DC/AC) converter. Type-4 generators have *soft shafts*. The torsional stiffness of the shaft describes the relation between the transmitted torque and the angular twist of two ends of the shaft [39]. The softer the shaft, the larger the angular twist can be. In contrast, masses connected to a stiff shaft always rotate together as one. Arani and Mohamed [43] have shown that implementing frequency regulation, whether via virtual inertia or droop, can stimulate the natural resonance frequency of the mechanical drive-train of the generator and lead to instability.

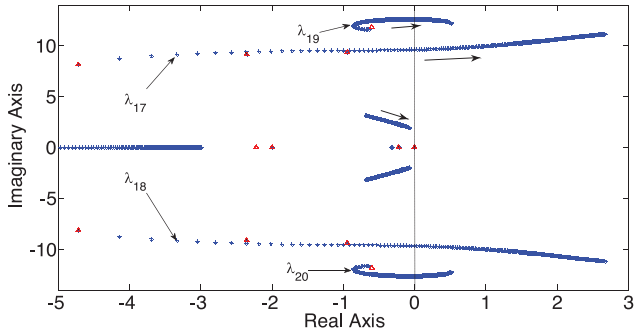

Fig. 4. Dominant modes of microgrid frequency when K_a is increasing. The blue stars represent the system poles, and the red triangles are the zeros impacting microgrid frequency behavior. The vertical black dashed line divides the plane into stable (left) and unstable (right) regions.

This section investigates whether this weakness can be exploited through malicious controllable loads to destabilize the power system.

Frequency-regulating wind generators respond to changes in power system frequency and consequently any load disturbance. Therefore, one strategy would be for an attacker to expose the power system to load changes that stimulate the wind generator mechanical resonance. As mentioned, type-4 wind generators suffer from a soft shaft, but maximum power tracking usually provides sufficient damping for generator stability [42]. However, we hypothesize that sufficiently large feedback may stimulate the generator mechanical resonance.

To effectively close such a positive feedback loop, an attacker would need some information from the generator. Although the generator's rotating speed is the most directly useful signal for the attacker, a more accessible one is the active power output of the wind generator, P_w. This signal is typically sampled and transmitted over a communication system for different purposes [28]; hence, an attacker can eavesdrop on the transmitted signal, $\hat{P}_w$, to facilitate resonance. Such an effective resonance attack is shown in Equation (20), which represents a bandpass filter centered on the resonance frequency of a wind generator mechanical system. This attack strategy is represented and modeled by the *Attack Method* block in Figure 3, while the *Converter* block represents the malicious load converter and its energy storage dynamics.

$$\Delta P_{att-ref} = \frac{K_a s}{s^2 + 2\zeta\omega_{att} s + {\omega_{att}}^2} \Delta\hat{P}_w \tag{20}$$

The impact of the attack on the microgrid is illustrated in Figure 4. As shown in the figure, the dominant poles are depicted when attack gain, K_a, is increased from zero. The real component (horizontal) of the poles quantifies the damping, and their imaginary component (vertical) relates to the frequency of oscillation of the dynamics. As such, for a system to be stable, it requires all the poles to have negative real parts. Thus, the left half-plane represents the stable region for poles, while the right half-plane is unstable.

A more in-depth explanation is given in Chapter 12 of Reference [39]. Two sets of modes move to the right half-plane and make the system unstable. Participation factor analyses determine which states provide the greatest contribution to these unstable modes [38]. The most unstable ones, λ_{17}-λ_{18}, are, almost equally, influenced by the thermal generator speed (power system frequency), the frequency regulation block, the rotating speed and shaft angle of the wind generator, the sampling dynamic, the attack method, and the malicious load converter dynamic. The other unstable

Table 1. Participation Factor of the Most Influential States on the Most Unstable Modes of the Microgrid

States	Description	λ_{17}-λ_{18}	λ_{19}-λ_{20}
x_4	Thermal generator rotating speed	0.2832	0.0642
x_7	Virtual inertia	0.1208	0.0319
x_8	Virtual inertia	0.1583	0.0475
x_{16}	Wind generator rotating speed	0.1441	0.5460
x_{17}	Wind generator shaft angle	0.1681	0.5613
x_{22}	ZOH	0.1743	0.0496
x_{25}	Attack method	0.1431	0.0400
x_{26}	Attack method	0.2111	0.0671
x_{27}	Malicious load converter	0.1797	0.0473

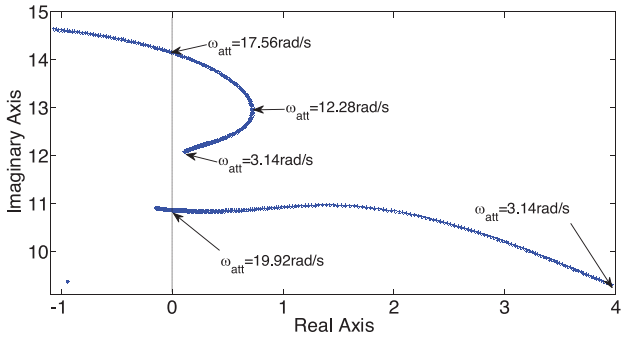

Fig. 5. Dominant modes of the microgrid when the attack frequency is changing. The vertical black dashed line divides the plane into stable (left) and unstable (right) regions.

modes, λ_{19}- λ_{20}, are under the influence of the wind generator rotating speed and shaft angle. These participation factors are listed in Table 1.

Interestingly, in the absence of frequency regulation in the wind generator, increasing K_a does not make the system unstable, even though the dominant modes of the microgrid are closer to the right half-plane due to lack of wind frequency regulation. Thus, we can conclude that the interaction of the malicious load and frequency-regulating wind generator makes the system unstable. It is worth mentioning that, to the best of the authors' knowledge, this article represents the first time in the literature that the vulnerability of frequency-regulating wind generators to such attacks from malicious load has been discussed. This observation can also help us to distinguish this kind of attack from other incidents in the power system. The unstable modes λ_{19}- λ_{20} will result in distinguishable, non-decaying oscillations that are not present or damp out relatively fast in other possible incidents in the microgrid.

Another interesting observation is related to the different frequencies of the mechanical system and malicious controllable loads. Obviously, the modes are not exactly the same. The success of the attack despite the difference in these modes suggests that the attacker does not need the exact resonance frequency of the wind generator. This fact is shown more clearly in Figure 5, where the impact of changing the frequency of attack is depicted. The poles related to the attack reach their most unstable location when the attack frequency is almost equal to the resonance frequency of the wind generator. For a relatively large range around this frequency, the system remains unstable.

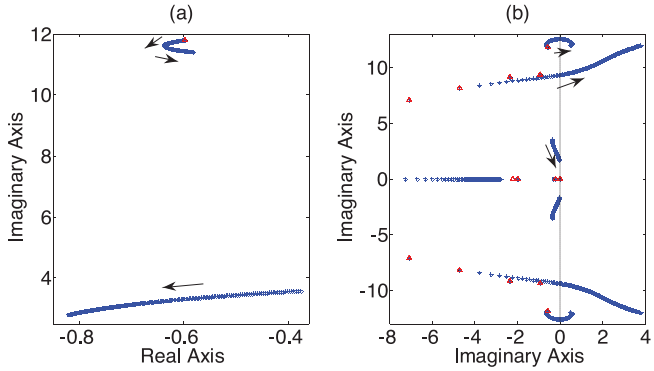

Fig. 6. Impact of increasing the virtual inertia gain from zero when (a) there is no attack or (b) the wind generator is under attack. The vertical black dashed line divides the plane into stable (left) and unstable (right) regions.

In other words, the most effective attack is expected to occur when the central frequency of the attack is close to the natural resonance frequency of the wind generator. We observe, however, that even a reasonable estimate of the natural resonance frequency is sufficient for an attacker to destabilize the system.

A relevant question here is: How can the resonance frequency of the wind generator be estimated? As addressed in Reference [42], the conventional wind generator is well-damped because of maximum power tracking, but a frequency-regulating wind generator behaves differently. Figure 6(a) illustrates the modes of a microgrid without any attack when the virtual inertia gain, M_v, is increasing. Obviously, the modes related to the wind generator mechanical system become dominant after some point. This dominancy means that the microgrid frequency can be used to estimate the natural resonance of the wind generator.

The high contribution of wind generators to frequency regulation not only reveals their natural resonance frequency but also makes the system more vulnerable to attacks. This fact is better clarified in Figure 6(b), where the change in virtual inertia gain is the same as for the case shown in Figure 6(a), but now the attack is present. By increasing the virtual inertia gain, the modes related to the thermal generator start to move toward the right-hand side. For the range of virtual inertia considered, these modes get closer to—but never reach—the unstable region.

Meanwhile, the modes related to the attacker and the wind generator mechanical system move into the right half-plane, making the system unstable. This movement suggests that virtual inertia, which is expected to increase resiliency by reducing the microgrid's degree of weakness, may in fact make the system more vulnerable to attacks. We deduce, then, that a natural tension exists in terms of optimizing system resilience. Even though a high contribution of wind generators to frequency increases vulnerability to attack (suggesting that the wind generator's contribution should be limited for improved cyber-physical attack resilience), restricting wind generation maintains system weakness (hence, decreasing physical grid resilience). We propose solutions to address this dilemma in more detail in the next section.

The above-mentioned attack method makes use of an eavesdropped signal from the communication system, where time delay is an indispensable reality. Hence, to be effective, the attack needs to be sustainable against different delays. Figure 7 sheds light on this issue. As shown, the delay varies from 1 ms to 500 ms at different sampling times. The upper band reflects the maximum delay allowed for MMS signals in the IEC 61850 standard [50]. Although some of the unstable modes begin moving toward the left half-plane, the system remains unstable at all times.

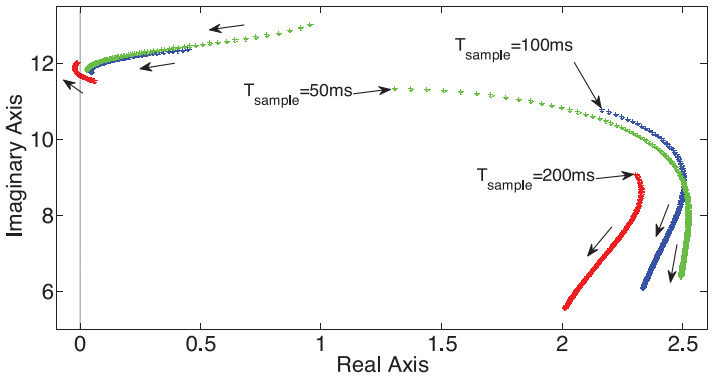

Fig. 7. Impact of communication system delay on the attacked microgrid behavior in different sample times. T_{delay} changes from 1 ms to 500 ms. The vertical black dashed line divides the plane into stable (left) and unstable (right) regions.

Participation factor analyses reveal another interesting aspect of this behavior. The modes that move toward the left-hand side are related more to the mechanical resonance of the wind generator, while other modes are under greater influence of the microgrid frequency and virtual inertia. In other words, the thermal generator and its frequency regulation dynamic are under attack. The wind generator output power has a frequency regulation term. The delayed feedback of this frequency regulation, regardless of wind natural resonance, can destabilize the system. In short, we observe that the attack can work effectively, despite the presence of communication delays on critical attack data.

The success of the attack, despite the considerably large delays, also shows that the command delaying methods successfully tested in other applications in power systems (e.g., References [26, 51]) are ineffective in this case. It should be noted that the maximum possible delay that can be used in this case is limited in comparison to load shedding under study in References [26, 51]. Also noteworthy is that Automatic Generation Control (AGC), responsible for secondary frequency regulation, has no significant influence on the attack. This should be no surprise, as AGC is tuned to have slower dynamics than primary frequency regulation [39].

3 SOLUTIONS

Given the effectiveness of the proposed attack, this section addresses an appropriate solution. A naive approach restricts the frequency regulation of the wind generator, maintaining a weak microgrid. This means that although the microgrid is immune to a particular type of cyber-physical attack, it is vulnerable to natural physical disturbances. However, using encryption to ensure data confidentiality and to avoid eavesdropping is insufficient. Consider the case in which the attacker owns or controls the load representing the legitimate destination for the data. In such a situation, the attacker is a real network participant and insider. This means that no cryptographic security measure added to the communication network will be effective, and that a user-centric method, focused on the physical components of the end-users of the communication network, is necessary. In such an approach, the vulnerability exploited by the attacker at the end-user, in the physical (power) system, will be detected and mitigated. While this section demonstrates the vulnerability of frequency-regulating wind generators that can be exploited to target the generator and entire microgrid, the next section is devoted to finding a user-centric solution.

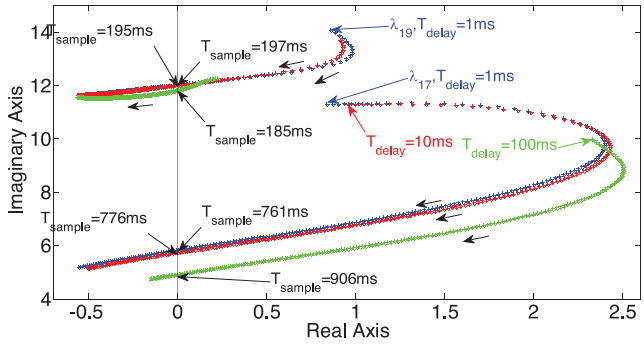

Fig. 8. Dominant modes of the attacked microgrid when the sampling time changes from 1 ms to 1 s. The vertical black dashed line divides the plane into stable (left) and unstable (right) regions.

Table 2. Participation Factor of the Most Influential States on the Most Unstable Modes of the Microgrid

States	Description	λ_{17}-λ_{18}	λ_{19}-λ_{20}
x_3	Thermal generator turbine	0.1016	0.0011
x_4	Thermal generator rotating mass	0.2947	0.0135
x_7	Virtual inertia	0.1791	0.0080
x_{16}	Wind generator shaft angle	0.0021	0.4282
x_{17}	Wind generator rotating speed	0.0250	0.4918
x_{22}	ZOH	0.2890	0.0099
x_{23}	ZOH	0.2632	0.0098
x_{25}	Attack method	0.2754	0.0076
x_{26}	Attack method	0.1062	0.0116
x_{27}	Malicious load converter	0.1218	0.0073

3.1 Sample Time

Figure 7 demonstrates that the attack is relatively robust against delays even at different sample rates, but its behavior is significantly impacted by a change in sample time, T_{sample}. A similar observation was successfully employed to improve the privacy of smart meter data [32]; however, the work is largely related to data confidentiality and not the operational stability of the grid, which has distinct requirements. One question, then, is: Can the sample rate be exploited for cyber-physical attack mitigation? This question is particularly important, because in many cyber-physical studies of the smart grid, the sampling rate impact is totally ignored. Figure 8 illustrates the dominant microgrid modes as T_{sample} changes and can be used to develop an answer.

In short, the answer to the above question is "yes," and Figure 8 provides greater context for this response. As is evident, there are two sets of unstable modes. One set reaches the stable zone for a much smaller sample time of 200 ms. Participation factor analyses, presented in Table 2, reveal that these modes, λ_{19}-λ_{20}, are more strongly affiliated with the mechanical system of the wind generator. From the Nyquist Theorem, this sample rate corresponds to a bandwidth of 2.5 Hz, which is close to the natural resonance frequency of the wind generator. Hence, by increasing the sample rate, the sampled wind output active power cannot reflect the behavior of the mechanical system of the wind generator. Therefore, the attacker is limited in terms of attack effectiveness.

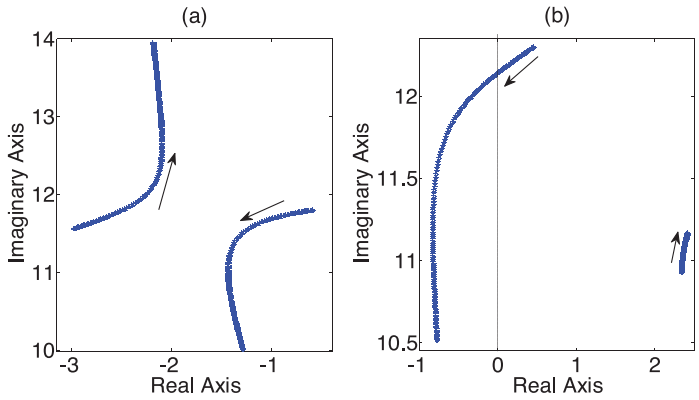

Fig. 9. Impact of increasing the active damping gain from zero on the dominant poles of (a) the wind generator and (b) the whole microgrid. The vertical black dashed line divides the plane into stable (left) and unstable (right) regions.

However, the microgrid is still unstable at this sampling rate, and a sampling time of nearly 0.9 s is needed to make the system immune against attack. Table 2 shows the participation factor for λ_{17}-λ_{18} when they are marginally stable. Obviously, the wind generator's mechanical system, x_{16}-x_{17}, has no significant impact. The difference is clear when comparing Tables 1 and 2. Instead of the wind generator dynamic, the impact of the thermal generator turbine has increased. In other words, the attacker impacts the thermal generator frequency regulation. The sampling time that makes the system stable is larger than 0.76 s, which corresponds to a bandwidth of 0.65 Hz. Again, this bandwidth is close to the modes of the thermal generator, verifying the participation factor analyses.

The sampling rate can be used for removing risks of an attack on a frequency-regulating unit, but this approach has its own disadvantages. Here, a sample rate of one sample per second guarantees safe operation, but suggests that only a very slow communication rate between components is allowed. In other words, using a lower sampling rate is a simple and cost-effective method for attack mitigation, but applies only to slow time-scale applications where lower data resolution is needed. Since this is not applicable to situations exhibiting fast system dynamics that require high granularity information, a more robust solution is required. These fast dynamics also prevent effective utilization of methods such as faster-than-real-time, simulation-based command authentication, which has been successfully used for cases such as state-estimation in traditional power systems [52].

3.2 Active Damping

For a broad set of scenarios, one possible approach can involve employing active damping, a well-known solution based on the feedback of the wind generator speed that is passed through a band-pass filter centered on the mechanical resonance frequency of the wind generator. However, conventional wind generators that do not contribute to system frequency regulation do not need active damping, as previously mentioned. Figure 9(a) depicts the dominant poles of the wind generator when the active damping gain increases from zero. Obviously, even with no active damping, the mechanical modes are stable. However, adding active damping increases the margin for stability. It also demonstrates that incorporating active damping at specific points can result in no significant benefits, as the modes move almost vertically.

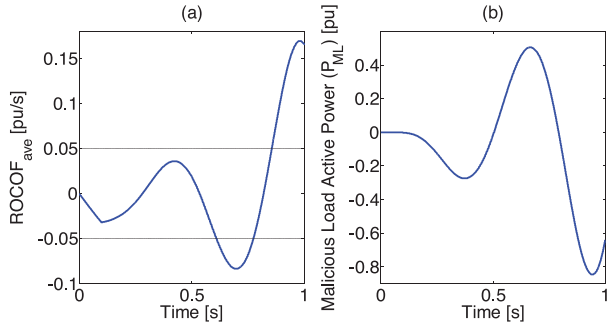

Fig. 10. Time response of the small signal model.

The dominant modes of the microgrid are illustrated in Figure 9(b). A closer look at the figure reveals that only modes related to the mechanical resonance move to the left half-plane, even more effectively than when the sample rate is modified. The other modes, as we discussed previously, are related to the thermal generator dynamics. One question that arises concerns whether there is any benefit to implementing active damping when it cannot comprehensively solve the problem.

4 NUMERICAL FRAMEWORK

While small signal analyses provide some invaluable insights, their numerical results are not precise in a broader context. In addition to well-known nonlinearities of grids, one of the most important challenges is addressing the nonlinearity of attacks. It is reasonable to assume that attackers prefer to exploit controllable loads aggressively to maximize impact. In this situation, the attacker would remain in the nonlinear region. Figure 10 further illustrates this concept by showing the attacker output power and microgrid ROCOF from small signal analyses. As shown in the figure, the malicious load builds up gradually and does not start from maximum power. In addition, as there is no limit placed on load magnitude, the model is free to go as high as it desires, which is unrealistic. In a more practical scenario, the output of the malicious load is limited and the attacker uses a high gain to inject maximum power aggressively from the start. As a result, the output of the malicious load resembles a pulse load.

The model is shown in Figure 3. As previously discussed, it can be simply modified to reflect this important fact. A limiter block is added between the Attack Method and Converter blocks in the Malicious Controllable Load part. The model is no longer a linear small signal description (thus rendering eigen-value analyses impossible), but instead a more accurate representation of microgrid frequency regulation. Moreover, it is simpler than performing a time-domain simulation of the entire system and benefits from lower computational complexity. To the best of the authors' knowledge, this more realistic modeling of attacks on primary frequency regulation is novel and a meaningful contribution of this article.

Figure 11 shows the minimum necessary attack power. The most effective attack occurs when ω_{att} is tuned close to the natural resonance frequency of a wind generator, obtainable from the power system frequency. It is in line with the observation of Figure 5, where the modes related to the mechanical system of the wind generator are at their extreme right positions. However, as can be seen, the exact necessary rating of the malicious load is also determined. Obviously, a small load is sufficient for most of the cases and does not need 0.4 or 0.8 pu, as shown in Figure 10. This finding is also significant, because it demonstrates how a load as small as 0.05 pu (5% of the wind generator rating) is sufficient to execute a successful attack against a generator, eventually impacting the entire microgrid. Such a small rated load is much more likely to be controlled or

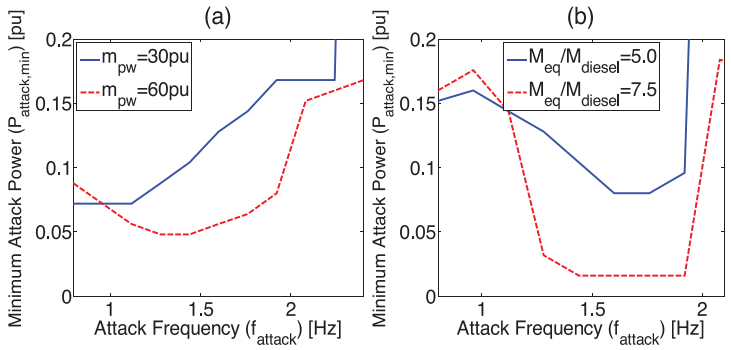

Fig. 11. Impact of frequency attack on the minimum needed attack power, when (a) droop, (b) virtual inertia-based frequency regulation is implemented in a wind generator.

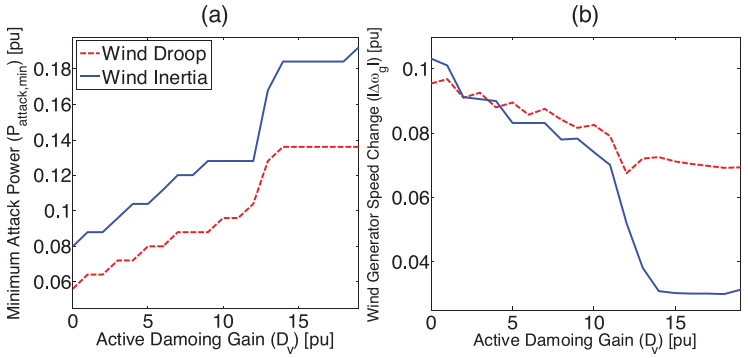

Fig. 12. Impact of active damping (a) the minimum needed attack power, (b) the maximum change in the wind generator rotating speed, for a successful attack.

even owned by a third-party attacker, hence making the attack more feasible and of higher risk. This fact also demonstrates why the proposed model is such a significant contribution. It provides much more realistic modeling and shows how imminent the danger of the discussed attack is. The proposed model reveals that a load eight times smaller than what the present small signal models estimate can destabilize the microgrid.

Our new model allows a richer analysis of the impact of active damping on system resiliency. This is illustrated in Figure 12, where increasing the damping gain, D_v, increases the minimum required power for a successful attack. As expected, it achieves this resiliency by damping the mechanical resonance of the wind generator. This damping can be observed more clearly in Figure 12(b), where the wind generator rotating speed changes have diminished by increasing D_v. As Figure 9(b) depicts, the active damping only forces the wind generator modes to the left half-plane. As a result, the wind generator stops resonating with the attacker. This result is also clear in Figure 12(b) Consequently, the attacker needs more resources to have the same impact on the microgrid, as illustrated in Figure 12(a). Again, the small signal modeling, limited by its inability to consider the limited resources of the attacker, cannot judge the effectiveness of the proposed solution accurately. The proposed modeling can provide a much more realistic picture.

This new framework enables us to more comprehensively answer the question posed in the last section on the possible benefits of active damping. As discussed in Figure 9, the active damping method does not reduce attack risk completely, but it can mitigate its impact and increase the

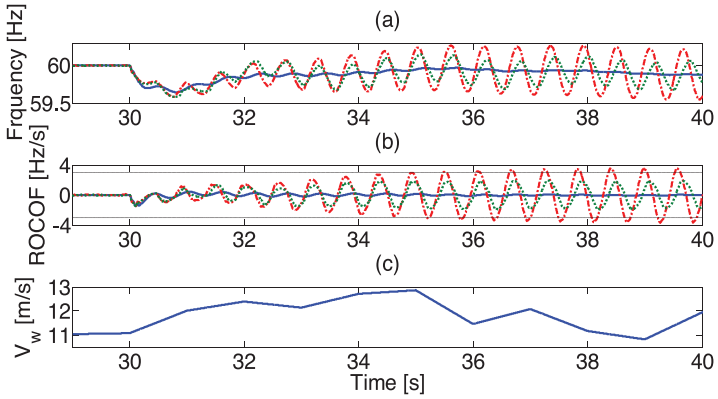

Fig. 13. (a) Microgrid Frequency, (b) Rate of change of Frequency, and (c) wind speed. The blue solid, dashed red and dotted green lines represent no attack, attack on the wind generator in absence of active damping, and attack in the presence of active damping (D_v=20), respectively.

system resiliency of the grid, as mentioned in relation to Figure 12. When applying active damping, an operator has less concern regarding the exploitation of small controllable loads. A proper tuning of active damping can be sufficient to prevent a successful attack, as the attacker also has access to finite limited sources of power and energy. Active damping is more reliable than decreasing the sampling rate or limiting the contribution of the wind generator to frequency regulation, as it does not adversely impact the frequency regulation and microgrid performance in general.

In addition, active damping is also user-centric, as we defined previously, as it removes the physical vulnerabilities of the end-user (i.e., the wind generator). In other words, even if the network-oriented security method is circumvented by the attacker, there are no serious vulnerabilities in the physical end-user to be exploited by the attacker. Furthermore, under a no-attack condition, the power system and wind generator are completely stable and no active damping is necessary. Therefore, a designer who is unaware of the cyber risks of the microgrid has no reason to implement active damping. We assert that resiliency must be taken into account as a necessary design factor, regardless of whether the contribution of the wind generator to the power system or its active damping will be tuned.

5 TIME DOMAIN SIMULATIONS

Detailed nonlinear time-domain simulations, using the microgrid system shown in Figure 1, are employed here to verify the results of the previous sections and investigate the nonlinear dynamics of the microgrid system. Typical distribution system lines, with a low X/R ratio (X/R = 2), are modeled as lumped R-L, and loads are modeled by parallel R-L circuits. The system parameters are given in the Appendix. A real wind speed pattern [53], shown in Figure 13(c), is used here, and an intentional islanding event at t = 30 s is introduced as the system disturbance.

There are two kinds of islanding: intentional and unintentional. The former is permitted by IEEE 1547, but the latter is prohibited [46]. Anti-islanding protection is used to prevent unintentional islanding. This article is focused solely on intentional islanding, and in such scenarios, anti-islanding protection is disabled. No relay tripping in an intentional islanding event is desired. MATLAB/Simulink is employed for the simulation studies.

One of the most important parameters observed in many cases is the Rate Of Change Of frequency (ROCOF). This type of relay does not deal with the exact derivative of the frequency. In this

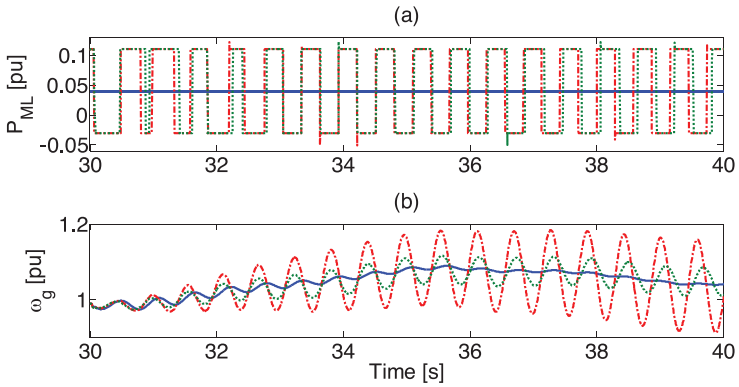

Fig. 14. (a) Malicious controllable loud output power, (b) wind generator rotating speed. The blue solid, dashed red and dotted green lines represent no attack, attack on the wind generator in absence of active damping, and attack in the presence of active damping (D_v=20), respectively.

section, as recommended by standards [47], a moving average window of 100 ms is used. However, we emphasize that no relay is tripped.

Scrutiny of Figures 13(a) and (b) makes it clear why we focus on ROCOF over frequency. While the attack does not result in any passing of the under- and over-frequency relay thresholds, the rate of frequency change surpasses the threshold approximately 5 s after islanding. The threshold, ±3 Hz/s, is depicted in Figure 13(b) by two horizontal dashed lines. When there is no attack (represented by the blue curve), the ROCOF never exceeds its limits and always remains small enough to avoid any relay tripping. In other words, the microgrid continues its operation safely in the absence of an attack. However, the attack changes the operational situation, as demonstrated by the red dashed curves in Figure 13. Fortunately, active damping can significantly mitigate the attack impact. The green dashed curve in Figure 13(b), depicting the microgrid ROCOF, never reaches ±2 Hz/s and stays safely away from the tripping threshold.

A closer look at Figures 13(a) and (b) also determines that frequency of oscillation in both the non-attack case and attack cases is different. As explained in Section 2.3, this difference is because of the attack, which pushes the modes of the wind generator mechanical system to the unstable region. These modes are so stable in non-attack scenarios that they cannot be easily discerned in these scenarios. This oscillation frequency can be used to distinguish this specific attack from other scenarios.

Active damping does not prevent oscillation completely but does deter the wind generator mechanical system (the end-user) from resonating during attack, as described in previous sections. This effect is observed in Figure 14(b), where the oscillation amplitude has decreased considerably from 0.123 pu to less than 0.04 pu. This is also consistent with the findings of the last section and our numerical framework depicted in Figure 12(b). In other words, the attacker is still present in the cyber-physical system, but the user-centric method has prevented the exploiting of the end-user (i.e., the wind generator) to destabilize the whole microgrid. This effective method is one of the main contributions of this article.

The malicious load power is shown in Figure 14(a). As can be seen, its output is limited to the rating of the converter. The oscillation amplitude is almost 0.07 pu, which is close to the results of the previous section. This figure also verifies the results of Figure 9, where active damping cannot make the system completely stable, as the malicious load continues to inject destabilizing power. However, limited nonlinear malicious load behavior was modeled more accurately in Section 4.

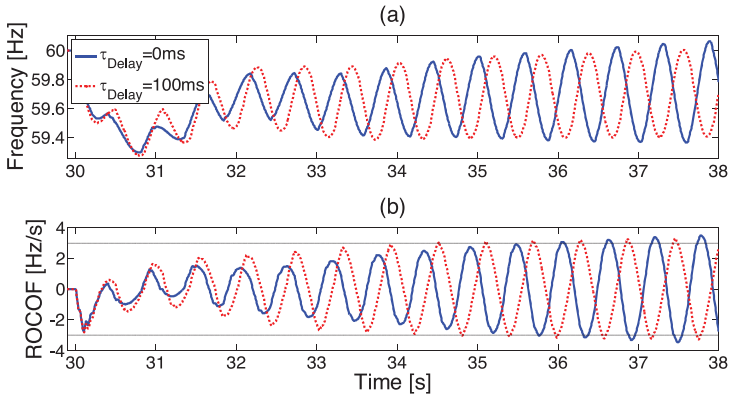

Fig. 15. (a) Microgrid Frequency and (b) Rate Of Change Of Frequency. The blue solid and dotted red lines represent zero delay and a 100 ms delay, respectively. No active damping is implemented in these cases.

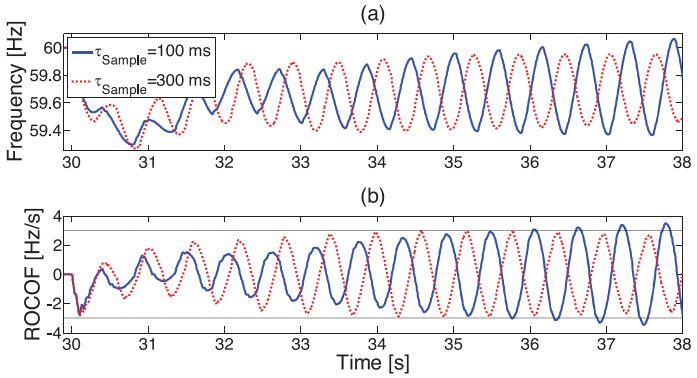

Fig. 16. (a) Microgrid Frequency and (b) Rate Of Change Of Frequency. The blue solid and dotted red lines represent 100 ms and 300 ms sampling times, respectively. No active damping is implemented in these cases.

As discussed with regard to Figure 12(a), much greater resources and effort are required by the attacker to be successful. Otherwise, the attack can make the power system frequency oscillatory, but not sufficiently large to trip a relay. This unsuccessful attempt is demonstrated with green dotted curves in Figures 13 and 14.

Time-domain simulation can also be used to verify the discussions surrounding the communication delay and sampling time impacts. The discussions in Sections 2 and 3, in contrast to the numerical framework analyses presented in Section 4, are based on assumptions of the linear behavior of the attacker and unlimited output power. Although this assumption is not accurate in the real system examined in this section, their prediction is not far from reality. Figure 15 depicts the power system frequency and ROCOF with different communication delay times when there is an attack on the frequency-regulating wind generator and no active damping is implemented. As discussed in Section 2, a delay as high as 100 ms does not neutralize the impact of the attack. In fact, a closer look at Figure 15(b) shows that the system with delay passes the threshold even sooner. In other words, the attack shows robustness against communication delays, which is daunting news for power system operators.

Figure 16 represents the power system frequency and ROCOF when different sampling times are employed. As predicted in Section 3, a sampling time of less than 200 ms results in system

instability and relay tripping. However, with a sampling time of 300 ms, the ROCOF never surpasses the threshold, although it is still oscillating. This behavior can be understood based on the discussion is Section 3. Specifically, with a sampling time of 300 ms, the poles related to the wind generator mechanical system are stable, whereas the modes affiliated with the thermal generator are still in the unstable region. As a result, the frequency is still oscillating, but because the wind generator has stopped resonating during the attack, the attack is not sufficient to result in relay tripping.

6 CONCLUSIONS

The penetration of wind generators is rapidly increasing and utilities have started to implement frequency regulation in these generators to compensate for power system weaknesses. This article investigated an attack that leveraged malicious controllable loads against primary frequency-regulating wind generators. It was shown that: (1) frequency-regulating wind generators with soft shafts are vulnerable to these types of attacks; (2) limiting the contribution of wind generators to frequency regulation, decreasing the sampling rate used for communication, and/or implementing active damping can increase power system resiliency; and (3) the high nonlinearity of cyberattacks necessitates modifying small-signal modeling to provide a more detailed and accurate depiction of the power system under attack. It was also discussed that among the three proposed solutions, active damping shows the most promise, as it does not impact other aspects of microgrid performance. In a more general sense, these analyses demonstrate how critical it is to consider user-centric cyber resiliency as a factor in designing and tuning what is usually thought to be a solely physical system. In particular, the frequency regulation of weak grids should be designed based not only on traditional factors, but also on the resiliency and unprotected (vulnerable) resources of the grid. The process of tuning the active damping of frequency-regulating wind generators should necessarily consider the cyber-physical vulnerabilities of the system. Future work will involve enhancing the simulation platform used in these studies through the integration of communication and/or power system hardware components.

APPENDIX

A. Loads:

LP1: 47 kW+j15.61 kVAr, LP2: 2565 kW+j843.06 kVAr, LP3: 289.75 kW+j95.24 kVAr, LP4: 152 kW+j49.96 kVAr, LP5: 517.8 kW+j170.18 kVAr, LP6: 194.8 kW+j64.01 kVAr.

B. Energy Storage:

1.1 KV, 125 KWh.

C. Generators:

DG1: 2 MVA PMSG, $H_G = 0.53$, $H_T = 4.27$, $K_s = 1.6$, $D_G = D_T = 0$, $Pp = 32$, with 2 MW wind turbine [41], $\tau_c = 0.1$ s. DG2: 2.5 MVA synchronous generator, AVR parameters: $K_{A=}400$, $T_{A=}0.02$, non-reheat thermal turbine [38]: $T_{CH=}450$ ms, $T_{G=}0.08$ s.

REFERENCES

[1] H. J. Laaksonen. 2010. Protection principles for future microgrids. *IEEE Trans. Power Electron.* 25, 12 (2010), 2910–2918.
[2] T. S. Ustun, C. Ozansoy, and A. Zayegh. 2012. Modeling of a centralized microgrid protection system and distributed energy resources according to IEC 61850-7-420. *IEEE Trans. Power Syst.* 27, 3 (2012), 1560–1567.
[3] H. Laaksonen, D. Ishchenko, and A. Oudalov. 2014. Adaptive protection and microgrid control design for Hailuoto Island. *IEEE Trans. Smart Grid* 5, 3 (2014), 1486–1493.
[4] Communication networks and systems for power utility automation Part 7-420: Basic communication structure distributed energy resources logical nodes, IEC 61850-7-420, *Ed.1.0*, 2009.

[5] A. Hussain and H.-M. Kim. 2016. A hybrid framework for adaptive protection of microgrids based on IEC 61850. *Int. J. Smart Home* 10, 5 (2016), 285–296.
[6] M. H. Cintuglu, T. Ma, and O. A. Mohammed. 2017. Protection of autonomous microgrids using agent-based distributed communication. *IEEE Trans. Power Deliv.* 32, 1 (2017), 351–360.
[7] I. Ali and S. Hussain. Communication design for energy management automation in microgrid. *IEEE Trans. Smart Grid, to be Published.*
[8] M. H. Cintuglu, T. Youssef, and O. A. Mohammed. Development and application of a real-time testbed for multiagent system interoperability: A case study on hierarchical microgrid control. *IEEE Trans. Smart Grid, to be Published.*
[9] M. Manbachi et al. 2016. Real-time co-simulation platform for smart grid volt-VAR optimization using IEC 61850. *IEEE Trans. Industr. Inf.* 12, 4 (2016) 1392–1402.
[10] J. Hull, H. Khurana, T. Markham, and K. Staggs. 2012. Staying in control: Cybersecurity and the modern electric grid. *IEEE Power Energy Mag.* 10, 1 (2012), 41–48.
[11] X. Shi, Y. Li, Y. Cao, and Y. Tan. 2015. Cyber-physical electrical energy systems: challenges and issues. *CSEE J. Power Energy Syst.* 1, 2 (2015), 36–42.
[12] J. Hu, H. R. Pota, and S. Guo. 2014. Taxonomy of attacks for agent-based smart grids. *IEEE Trans. Parallel Distrib. Syst.* 25, 7 (2014), 1886–1895.
[13] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry. 2014. A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control. *IEEE Trans. Smart Grid* 5, 6 (2014), 2687–2700.
[14] A. Farraj, E. Hammad, and D. Kundur. 2016. A cyber-enabled stabilizing control scheme for resilient smart grid systems. *IEEE Trans. Smart Grid* 7, 4 (2016), 1856–1865.
[15] A. Farraj, E. Hammad, and D. Kundur. 2018. A cyber-physical control framework for transient stability in smart grids. *IEEE Trans. Smart Grid* 9, 2 (2018), 1205–1215.
[16] F. Pasqualetti, F. Dorfler, and F. Bullo. 2015. Control-theoretic methods for cyberphysical security: geometric principles for optimal cross-layer resilient control systems. *IEEE Control Syst.* 35, 1 (2015), 110–127.
[17] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu. 2012. Securing smart grid: Cyber attacks, countermeasures, and challenges. *IEEE Commun. Mag.* 50, 8 (2012), 38–45.
[18] J. Qi, A. Hahn, X. Lu, J. Wang, and C. C. Liu. 2016. Cybersecurity for distributed energy resources and smart inverters. *IET Cyber-Phys. Syst.: Theor. Applic.* 1, 1 (2016), 28–39.
[19] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong. 2017. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* 8, 4 (2017), 1630–1638.
[20] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei, and B. Carbunar. 2017. Resilient design of networked control systems under time delay switch attacks, application in smart grid. *IEEE Access* 5, 15901–15912.
[21] H. E. Brown and C. L. DeMarco. Risk of cyber-physical attack via load with emulated inertia control. *IEEE Trans. Smart Grid, to be Published.*
[22] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad. Dynamic load altering attacks against power system stability: Attack models and protection schemes. *IEEE Trans. Smart Grid, to be Published.*
[23] S. Amini, F. Pasqualetti, M. Abbaszadeh, and H. Mohsenian-Rad. Hierarchical location identification of destabilizing faults and attacks in power systems: A frequency-domain approach. *IEEE Trans. Smart Grid, to be Published.*
[24] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng. Resonance attacks on load frequency control of smart grids. *IEEE Trans. Smart Grid, to be Published.*
[25] Y. Zhang, Y. Xiang, and L. Wang. 2017. Power system reliability assessment incorporating cyber attacks against wind farm energy management systems. *IEEE Trans. Smart Grid* 8, 5 (2017), 2343–2357.
[26] D. Mashima, P. Gunathilaka, and B. Chen. 2019. Artificial command delaying for secure substation remote control: Design and implementation. *IEEE Trans. Smart Grid* 10, 1 (2019), 471–482.
[27] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf. Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks. *IEEE Trans. Smart Grid, to be published.*
[28] D. Jin et al. 2017. Toward a cyber resilient and secure microgrid using software-defined networking. *IEEE Trans. Smart Grid* 8, 5 (2017), 2494–2504.
[29] John Henry Castellanos et al. 2017. Legacy-compliant data authentication for industrial control system traffic. In *Proceedings of the International Conference on Applied Cryptography and Network Security*. Springer, Cham, 2017.
[30] Y. Kim, V. Kolesnikov, and M. Thottan. 2018. Resilient end-to-end message protection for cyber-physical system communications. *IEEE Trans. Smart Grid* 9, 4 (2018), 2478–2487.
[31] P. Gope and B. Sikdar. An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication. *IEEE Trans. Smart Grid, To be published.*
[32] G. Eibl and D. Engel. 2015. Influence of data granularity on smart meter privacy. *IEEE Trans. Smart Grid* 6, 2 (2015), 930–939.

[33] D. Engel and G. Eibl. 2017. Wavelet-based multiresolution smart meter privacy. *IEEE Trans. Smart Grid* 8, 4 (2017), 1710–1721.
[34] F. Knirsch, G. Eibl, and D. Engel. 2018. Error-resilient masking approaches for privacy preserving data aggregation. *IEEE Trans. Smart Grid* 9, 4 (2018), 3351–3361.
[35] H. Simo Fhom, N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, and A. Monti. 2010. A user-centric privacy manager for future energy systems. In *Proceedings of the International Conference on Power System Technology*. 1–7.
[36] C. Neureiter, G. Eibl, A. Veichtlbauer, and D. Engel. 2013. Towards a framework for engineering smart-grid-specific privacy requirements. In *Proceedings of the 39th Conference of the IEEE Industrial Electronics Society*. 4803–4808.
[37] A. Veichtlbauer, O. Langthaler, D. Engel, C. Kasberger, F. Pröstl Andrén, and T. Strasser. 2016. Towards applied security-by-design for DER units. In *Proceedings of the IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA'16)*. 1–4.
[38] Navigant Research. 2017. Market Data: Combined Heat and Power in Microgrids.
[39] P. C. Kundur. 1994. *Power System Stability and Control*. McGraw-Hill, New York, Toronto.
[40] D. T. Ton and M. A. Smith. 2012. The U.S. Department of Energy's microgrid initiative. *Electric. J.* 25, 8 (2012), 84–89.
[41] C. Marnay et al. 2015. Microgrid evolution roadmap. In *Proceedings of the International Symposium on Smart Electric Distribution Systems and Technologies (EDST'15)*. 139–144.
[42] Fakhari Moghaddam Arani, Mohammadreza. 2017. *Effective Utilization of Distributed and Renewable Energy Resources to Stabilize and Enhance Smart Power Grids Performance*. PhD Dissertation, University of Alberta, Edmonton, Canada.
[43] M. F. M. Arani and Y. A. R. I. Mohamed. 2017. Analysis and damping of mechanical resonance of wind power generators contributing to frequency regulation. *IEEE Trans. Power Syst.* 32, 4 (2017), 3195–3204.
[44] M. F. M. Arani and Y. Mohamed. 2016. Analysis and mitigation of undesirable impacts of implementing frequency support controllers in wind power generation. *IEEE Trans. Energy Conv.* 31, 1 (2016), 174–186.
[45] A. H. Mohsenian-Rad and A. Leon-Garcia. 2011. Distributed internet-based load altering attacks against smart power grids. *IEEE Trans. Smart Grid* 2, 4 (2011), 667–674.
[46] IEEE. 2017. IEEE Approved Draft Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, IEEE P1547/D7.3.
[47] W. Freitas, Wilsun Xu, C. M. Affonso, and Zhenyu Huang. 2005. Comparative analysis between ROCOF and vector surge relays for distributed generation applications. *IEEE Trans. Power Deliv.* 20, 2 (2005), 1315–1324.
[48] M. F. M. Arani and E. F. El-Saadany. 2013. Implementing virtual inertia in DFIG-based wind power generation. *IEEE Trans. Power Syst.* 28, 2 (2013), 1373–1384.
[49] M. Arani, Y. Mohamed. 2015. Analysis and impacts of implementing droop control in DFIGs on microgrid/weak-grid stability. *IEEE Trans. Power Syst.* 30, 1 (2015), 385–396.
[50] Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines, IEC 61850, 2013.
[51] D. Mashima, B. Chen, T. Zhou, R. Rajendran, and B. Sikdar. 2018. Securing substations through command authentication using on-the-fly simulation of power system dynamics. In *Proceedings of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm'18)*. 1–7.
[52] S. Meliopoulos, G. Cokkinides, R. Fan, L. Sun, and B. Cui. 2016. Command authentication via faster than real time simulation. In *Proceedings of the IEEE Power and Energy Society General Meeting (PESGM'16)*. 1–5.
[53] Database of wind characteristics located at DTU, Denmark. Retrieved from: http://www.winddata.com.

Received December 2018; revised January 2020; accepted March 2020