IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 17 October 2023, accepted 6 November 2023, date of publication 8 November 2023,
date of current version 14 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3331314

RESEARCH ARTICLE

Preventing Stealthy Attacks on Power Electronics Dominated Grids

STEPHANIE HARSHBARGER[1], MOHSEN HOSSEINZADEHTAHER[2], (Member, IEEE), ALIREZA ZARE[2], (Graduate Student Member, IEEE), AMIN Y. FARD[2], (Student Member, IEEE), MOHAMMAD B. SHADMAND[2], (Senior Member, IEEE), AND GEORGE AMARIUCAI[1]

[1]Department of Computer Science, Kansas State University, Manhattan, KS 66506, USA
[2]Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, IL 60607, USA

Corresponding author: George Amariucai (amariucai@ksu.edu)

This publication was made possible by NPRP12S-0226-190158 from the Qatar National Research Fund (QNRF is a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors. The publication of this article was financed with support from the Kansas State University Open Access Publishing Fund.

ABSTRACT Stealthy zero-dynamics attacks are a subset of false data injection attacks (FDIAs) that are especially dangerous, as they are designed to be undetectable by any intrusion detection mechanisms. This paper shows that stealthy attacks can be more destructive on power electronic dominated grids (PEDGs) than traditional power systems, by taking advantage of the low inertia property of PEDGs. The low inertia of these power grids causes the system to be prone to frequency instability when disturbances occur, meaning that an attacker can cause more harm to a system in a shorter amount of time. Another advantage to the attacker is an increased amount of telecommunication devices in PEDGs which provides the attacker with a larger attack surface. It is thus critical that we strive to design PEDGs in such a manner that we minimize their susceptibility to stealthy attacks. We provide a small signal model for a PEDG system, along with the the state space representation of the low-inertia part of the system, and we show that even without the state-space model of the whole system, a stealthy zero-dynamics attack can be constructed and can be successful on a PEDG. Results are also provided to show that strategically choosing model parameters in the design phase of the system can prevent the existence of stealthy zero-dynamics attacks.

INDEX TERMS Cyber-intrusion, stealthy attacks, microgrids, zero-dynamics attack.

I. INTRODUCTION

A. POWER ELECTRONIC DOMINATED GRIDS

Traditional power systems are being reformatted by the high penetration of renewable energy resources. An ever-increasing penetration of renewable energy resources will increase the global deployment of energy storage systems as well [1], [2], [3]. Unlike traditional systems, which relied mostly on synchronous generators, in the new power electronic dominated grids (PEDGs) power electronics based power generation will play an important role [4], [5]. A challenging impact of this new energy paradigm is related to the total system inertia which is known as the total stored energy in the synchronous machines in a PEDG and allows them to rotate continuously. This means that a high inertia system is less prone to deviate from its point of operation and will more likely return to an equilibrium point in response to major and minor disturbances which is also referred to as stability in the literature [6], [7], [8]. Moreover, the stability of a PEDG could be classified into voltage, angle, and frequency stability which requires the system to maintain these characteristics within a certain margin so that the system could be considered stable [9]. Furthermore, another factor to consider while encountering a PEDG is its short circuit ratio which is an indicator of its reliability and grid strength and represents the risks associated with high penetration of renewable energy resources. Since a small short circuit ratio is one of the characteristics of a PEDG, the system will become unstable much faster and this means that an attack on a PEDG will have a much greater impact compared to a

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

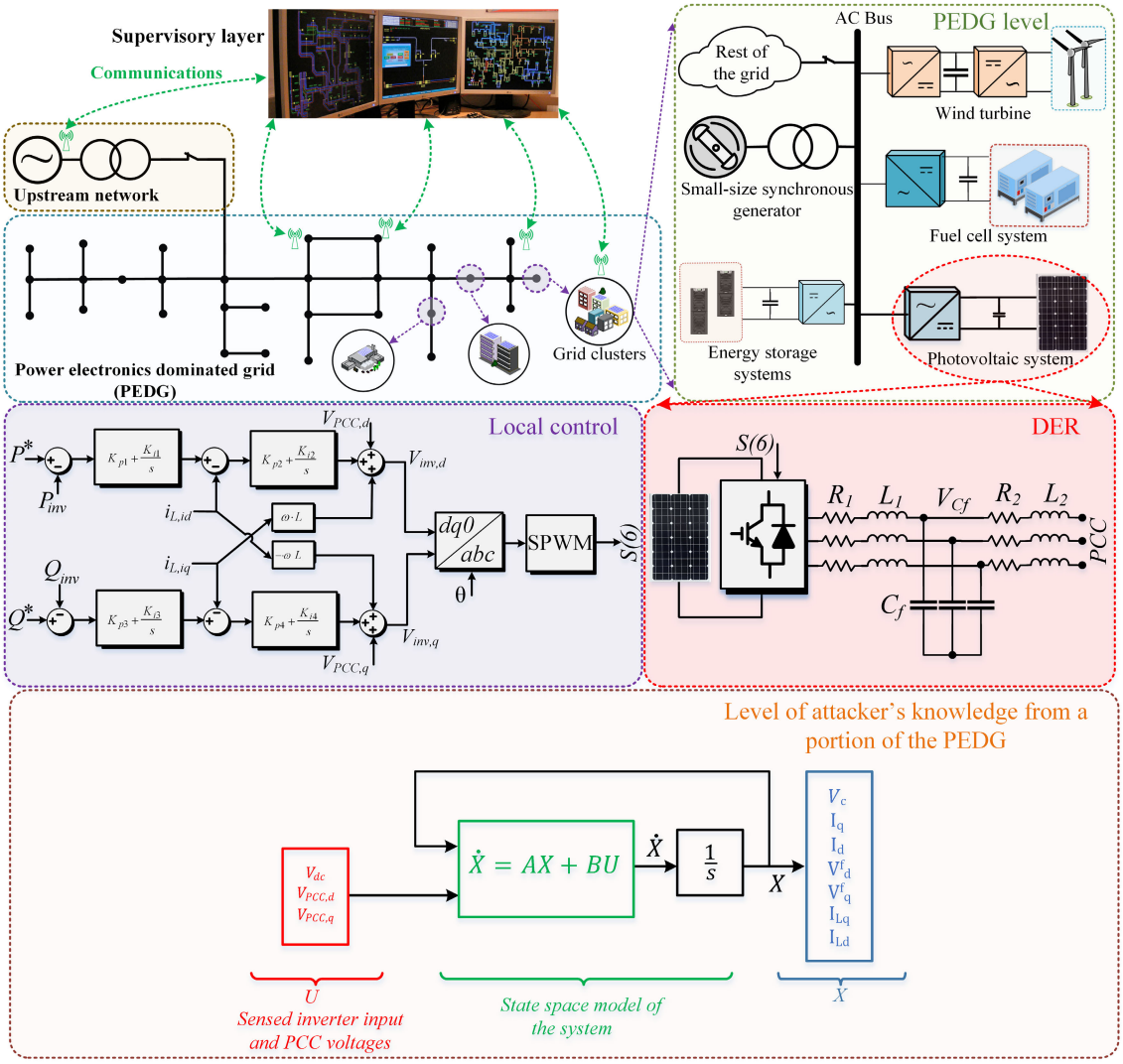


FIGURE 1. A generic overview of the power electronics dominated grid, showing grid clusters with high penetration of renewable resources, and how each renewable source is connected to the PCC via inverters. The local inverter control diagram is also presented. The bottom part represents an equivalent state-space model of a sample cluster, to which the attacker has access.

non-PEDG system [10]. In this article we consider frequency stability as the main focus to present the effectiveness of the proposed method. According to the mentioned challenges in the new energy paradigm, PEDGs should be equipped with numerous advanced measuring infrastructures and intelligent devices such as smart meters and inverters which are able to enhance the grid observability and controllability. These devices are highly dependent on telecommunication infrastructures which unfortunately causes the power grid to be more vulnerable to cyber-physical attacks. Therefore, system stability and the availability of electrical energy may experience numerous challenges due to the potential security gaps [11].

B. STEALTHY ATTACKS

False data injection attacks (FDIAs) are some of the most studied types of cyber attacks on power systems. FDIAs have the potential to cause damage to hardware and even cause blackouts [12]. A stealthy zero-dynamics attack is one of the most serious types of FDIA, in which the attacker targets the control signal of a system, in such a way that the attack has no influence on the system measurements, while causing some of the system states to diverge [13]. Stealthy attacks are feasible in many real control systems, and are made possible by either inadequate communication security [14], or software vulnerabilities that allow attackers to gain access to the system's control boards [15].

Intrusion detection systems are generally deployed to detect anomalies in measurements [16], [17], [18], can be made redundant, and can be located in multiple places within the power system, making them less susceptible to be compromised by attackers. Zero-dynamics attacks are a type of stealthy attacks, designed with the explicit purpose of causing system instability while not influencing the measurements in any way. As such – at least in theory – any type of intrusion detection mechanism is theoretically rendered completely useless.

Even for theoretically-secure systems, [19] demonstrates how zero-dynamics attacks may unexpectedly appear as a result of discretization and robust controllers, and proposes simple defenses by using generalized holds and samplers (see also [20], [21]). These prevention methods have been investigated in very specific power systems applications in [22], [23], and [24]. Interestingly, [25] shows that zero-dynamics attacks are possible even when the control signals are encrypted with a fully-homomorphic encryption scheme, such as LWE. An interesting line of defense against zero-dynamics attacks is the use of plant-side auxiliary systems (systems that are not susceptible to such attacks, and consume the exact same input as the plant), as introduced in [26].

The impacts on stealthy attacks of imperfect system information were investigated in [27]. Other ways of generating stealthy attacks in the absence of a system-wide state-space model were proposed in [28], where a system model is learned using a Chen-Fliess series, in [29], where a stealthy attack is generated by a robust controller, and in [30], which uses reinforcement learning.

Zero-dynamics attacks against multi-agent systems have been investigated in [31] and [32]. In this context, optimal sensor placement was investigated as a countermeasure in [33].

Despite their theoretical efficiency, several practical aspects of stealthy zero-dynamics attacks impose a set of limitations on their capabilities. First, the control signals that the attacker has to inject are themselves diverging, giving the attacker only a limited time for causing significant disruption of the system states, before physical system limitations cause the effects of the attack to saturate. Second, zero-dynamics attacks are extremely sensitive to imperfections in the system model [27], [34], and even small deviations from the real parameters may render the attack detectable. Third, even when the attacker has perfect system information, as the states move away from the operating point, the state space model is no longer an accurate description of the system, thus the attack will become detectable. The zero-dynamics attack is therefore a race against time, aimed at causing sufficient disruption before being detected or reaching saturation. For this reason, slowing down the attacker-caused state divergence, or speeding up the attack's detectability, can make a significant difference to the attack outcome.

Due to the above limitations, in a realistic power system running under normal conditions, it is nearly impossible for a zero-dynamic attack to remain entirely stealthy. The attacker hopes that they can make the attack stealthy for long enough to cause damage to the system, and the system operator hopes that the anomaly detector will catch the imperfections in a stealthy attack before damage is done. Previous work shows that this turns into a race of creating an attack that can beat the current anomaly detectors [35], [36], [37], [38] and creating anomaly detectors that can detect these attacks [39], [40], [41], [42] before they are able to damage the system.

The consequences of stealthy attacks on power systems can range from small service disruptions to the damaging of very expensive hardware. Even when the power grid is well protected by switches, stealthy attacks can be employed to trigger these switches in a coordinated manner, with the potential of causing significant instability, as shown in [43] and [44].

Overall, stealthy attacks remain extremely dangerous, but can often be thwarted by smart system design and by an increased number of measurements. Previous work has shown the impact of stealthy attacks on various power systems models [34], [45]. In this paper, we make the following contributions.

1) We show that even though we have access to the state space model for only a small part of the PEDG – the one modelling the cluster of PV arrays interfaced with power electronics – and even though this state space model depends on parameters from the rest of the PEDG, like synchronous generators and loads, we can still calculate a successful stealthy zero-dynamics attack by using the steady state values of these parameters.
2) We show that such a stealthy attack applied to the inverters can causes the entire power grid to collapse
3) We then demonstrate how to design a PEDG in order to make this system immune to this class of FDIAs.

We study a simple system, the state space model of which is derived in Appendix A. The attack model is presented in Section III, and is followed by the results provided in Section IV. A discussion of attack prevention and detection is presented in Section V, and a conclusion and future work are provided in Section VI.

II. SYSTEM DESCRIPTION

Fig. 1 depicts the overall structure of a PEDG which consists of various grid clusters along with an aggregated state-space model of its subsystem. Each grid cluster contains a small synchronous generator (SG) and multiple renewable energy resources which are interfaced to the common AC bus via inverters. To maintain the stable and resilient operation of the entire PEDG a supervisory control layer is required to monitor the behavior of the entire PEDG and provide the necessary commands through the communication links. As represented in the PEDG level, in each grid cluster, multiple renewable energy resources exist and contribute to supplying the local load as well as supporting the grid's voltage and frequency by providing the required active and reactive power. As depicted by the DER level in Fig. 1, the renewable energy resources are connected to inverters and interfaced to the point of common coupling (PCC) via an LCL filter. To ensure the correct injection of active (P) and reactive (Q) powers, a double-loop PI-based controller is utilized as the primary control layer of the grid following inverter which compares the measured P and Q with their reference values provided by the supervisory layer and the

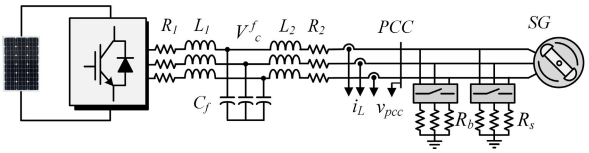


FIGURE 2. The sample cluster of PEDG under study illustrating the interaction between renewable energy resources and synchronous generator (SG).

difference is passed through the PI compensators to correct any existing errors as presented by the local control section of Fig. 1. Finally, a mathematical model of a sample cluster in a PEDG consisting of a grid following and synchronous generator is provided in Fig. 1 to represent the attacker's knowledge of the existing PEDG.

To further study the interaction of renewable energy resources and the SG in a cluster of PEDG, a sample cluster as depicted in Fig. 2 is considered. The system consists of a three-phase grid-following inverter and an SG. The SG provides and maintains proper grid voltage and frequency by utilizing its excitation and governor control systems, while the grid following inverter supplies the additional real and reactive power introduced by non-critical loads via its independent P, Q control system to ensure the stability of the network in the presence of any disturbances. As presented in Fig. 2, the inverter is connected to the PCC via a non-ideal LCL filter where L_1 and R_1 are the inverter side inductor and its equivalent series resistance (ESR), C_f present the filter capacitor, and L_2 and R_2 are the grid side inductor and ESR. Initially, the inverter supports the base load of R_b with the value of 7000 W while the SG continues to support the grid's voltage and frequency. At $t = 10s$ a step load of 4000 W is introduced to the system as represented by R_s in the diagram. As the step load is introduced to the system the supervisory layer observes the frequency behavior and assigns the new P and Q set points for the primary controller of the inverter which is processed through a double-loop PI-based controller to generate the desired current reference and switching sequence accordingly to derive the inverter's bridge. To further analyze the operation of the overall network along with the interaction between SG and inverter, a state space representation of the inverter is derived according to the dynamic model of individual components of the grid, as shown in Appendix A. Next, a MATLAB Simulink model is developed to verify the accuracy of the state space model and compare the observed outcomes with original circuit results as presented in Fig. 1. The simulation results of our cluster of PEDG under normal operating conditions are presented in Fig. 3. Specifically, Fig. 3a represents the values of system states in the d-q frame before and after the step load is introduced. Fig. 3b provides the states that are observable and can be monitored by an intrusion-detection system. The frequency behavior of the cluster is presented in Fig. 3c, where the frequency is at its nominal value of 60 Hz. However, a step load of 4 kW is introduced to the system which results in the deviation of frequency from its nominal value. To mitigate this deviation, the supervisory layer increased the active power set point of the inverter as depicted in Fig. 3d enabling the inverter to contribute to frequency restoration and enhancing the frequency stability of the cluster. The increase in the power set point of the inverter also impacts its output current to increase accordingly as presented in Fig. 3e while the SG ensures that the PCC voltage stays at its nominal value which is illustrated by Fig. 3f.

Since complex power systems like the one in Fig. 1 require communication infrastructure, the overall network will become more susceptible to cyber-attacks. But to mount a successful zero-dynamics stealthy attack, the attacker requires perfect knowledge of the entire system – in practice, this is unlikely to occur. However, it is very possible that the attacker gains access to, or accurately estimates, the model of a portion of the system. The attacker uses this information to create a stealthy attack that could deteriorate the performance of the entire system. As illustrated in Fig. 1, the PEDG consists of various grid clusters. Each of these clusters is equipped with numerous DERs and various loads. Each cluster has the capability to go islanded. To prove the severity of stealthy attacks, it is assumed that the attacker has access to the state-space model of *only one of the DERs*. The level of knowledge of the attacker is depicted in Fig. 1. The attacker has access to the information at the point of common coupling of the DER and uses this data to validate the leaked model while using the validated model to create a stealthy attack that could be applied to the control variables of the three-phase inverter. This consideration helps to include the most plausible attacks on the power system. The results of this article prove that even with limited information on the grid, a stealthy attack could be designed in such a way that the frequency/voltage stability of the entire system collapses.

The state space model is constructed by writing ordinary differential equations (ODEs) and linearizing them about the operating points. By defining a global reference frame and a transformation matrix, all system dynamic equations are given in the defined reference frame and combined in a single state space representation model, which is given by

$$\frac{d}{dt}(\hat{x}) = A\hat{x} + B\hat{u}, \tag{1}$$

$$\hat{y} = C\hat{x}, \tag{2}$$

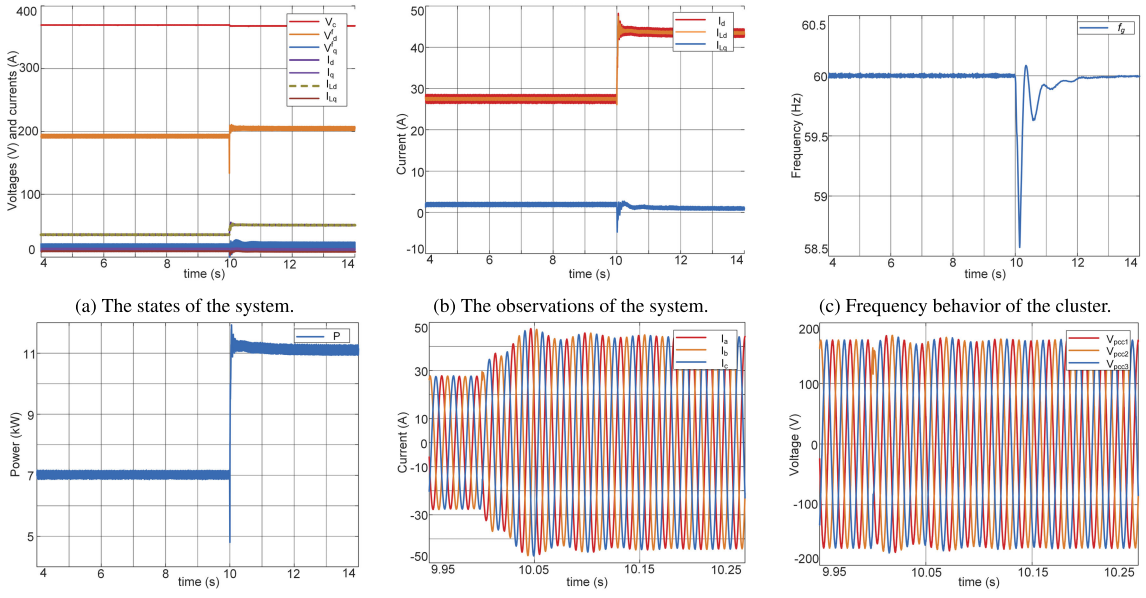
where $\hat{x}$, and $\hat{u}$ are respectively the system state variables and control signal, A is the system matrix, B is the input matrix, and C is the output matrix defined by

$$C = \begin{bmatrix} 0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,1 \end{bmatrix}. \tag{3}$$

The state variables are defined by

$$\hat{x} = \begin{bmatrix} v_c\ i_q\ i_d\ v_q^f\ v_d^f\ i_{Lq}\ i_{Ld} \end{bmatrix}^T, \tag{4}$$

where v_c is the DC-line voltage of the inverter, i_q and i_d are the q and d components of inverter-side current, v_q^f and v_d^f



(a) The states of the system. (b) The observations of the system. (c) Frequency behavior of the cluster.

(d) Inverter's active power profile. (e) Inverter's current behavior. (f) PCC voltage behavior.

FIGURE 3. Simulation results for normal operation of the PEDG cluster and the impact of a step change in loading on system's characteristics.

TABLE 1. Description of some commonly used symbols and notations.

Symbol	Description
x_k, u_k, y_k	System state, input and output at time k.
v_k, w_k	System and measurement noises at time k.
A, B, C	System, input and output matrices.
F	Stealthy attack matrix.
a_k	Attack signal at time k, computed as $a_k = Fz_k$, where $z_k = (A + BF)z_{k-1}$.
V_{pcc}	Voltage at the point of common coupling (PCC).
v_c	DC-line voltage of the inverter
i_d, i_q	The d and q components of the inverter-side current.
v_d^f, v_q^f	The d and q components of the filter's capacitor voltage.
i_{Ld}, i_{Lq}	The d and q components of the grid-side current at the point of common coupling.
v_{dc}	The inverter input voltage.
v_d^g, v_q^g	The filter capacitor voltage transferred to the d-q frame.
ω	Angular frequency of the SG.
ϕ	The angle difference between the global d-q frame and states d-q components.
R_1, R_2	Equivalent series resistance (ESR) of inverter and grid side inductors.
L_1, L_2	Inverter and grid side inductor values.
C_1, C_f	C_1 is the DC-link capacitor and C_f is the filter capacitor values.

are the q and d components of the filter's capacitor voltage, and i_{Lq} and i_{Ld} are the q and d components of the grid-side current at the point of common coupling. For convenience, the symbols and notation most used in this paper are listed in Table 1.

The control signal is defined by

$$\hat{u} = \left[v_{dc}\ v_q^g\ v_d^g\right]^T, \tag{5}$$

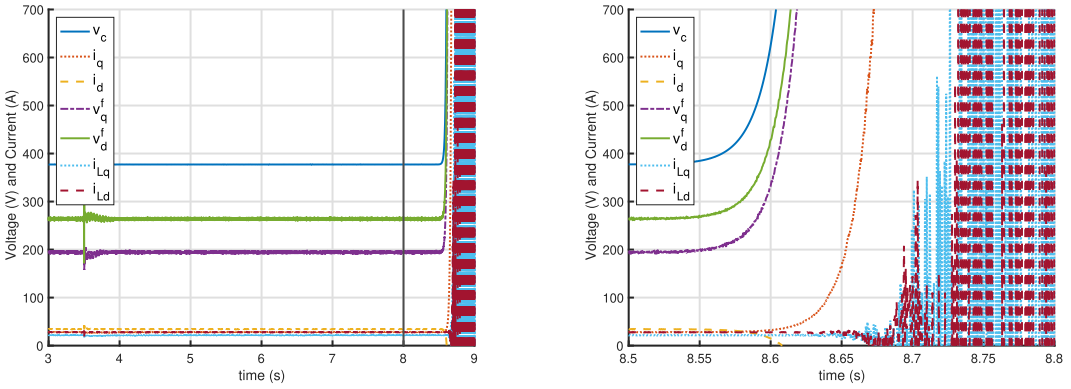
where v_{dc} is the inverter input voltage, while v_d^g and v_q^g represent the filter capacitor voltage transferred to the d-q frame.

A detailed derivation of A and B can be found in Appendix A. This state space representation is then converted from continuous to discrete time using a sampling time of $10\mu s$, as the attacker model uses a discrete time model. Simulation results of the system running under normal operating conditions are shown in Fig. 3.

The novelty of applying a stealthy attack to this PEDG is the fact that the state space model only represents a subset of the whole system. Additionally, the state space model of the inverters requires input from the the rest of the grid, shown in Fig. 1. In our framework, the interaction between the state-space model and the rest of the grid is captured by the input vector u_k of (6), as well as by some of the state space model parameters (see Appendix A for more detail). However, in order to calculate a stealthy attack, we need a time-invariant state space representation. We solve this problem by considering a fixed state-space model, computed using the steady state values of the variable parameters, derived from the circuit simulation – a sub-optimal approach, but one that results in a successful attack nevertheless.

III. ATTACKER MODEL

With larger numbers of smart meters and inverters in smart grids, we see a greater dependence on telecommunication infrastructures. Smart grids incorporate many additional sensors, as well as controllers at different layers of the system, and thus require communication between these sensors and controllers. The large number of communication channels opens the door for numerous types of cyber attacks. Here, we will show the impact that a stealthy attack can have on a PEDG. The attacker model described in [13] is implemented in our simulations.



(a) The states of the system with an attack starting at 8s.

(b) The states of the system under attack–a zoomed-in graph of Fig. 4a showing the divergence of the states.

FIGURE 4. System states with an attack starting at 8s, denoted by the black vertical line. Note that the states being attacked diverge significantly around 8.55s.

Formally, our attacker model can be described by the following three definitions.

a: INTRUSION-DETECTION SYSTEM:

A system that has access to the attacked system's outputs (measurements), and raises an alarm whenever these outputs reflect a behavior inconsistent with the expected system functionality.

b: ATTACKER'S ALLOWANCES:

The attacker (1) has complete knowledge of the state-space model of the inverter, and (2) can add arbitrary signals to the attacked system's input (control signal), in real-time.

c: ATTACKER'S GOAL:

The attacker is successful if they cause a subset of the components of the system's state to diverge from their nominal values, by more than a certain threshold, before any alarms can be raised by the intrusion-detection system.

We use a discrete time state space model to represent the inverter of a PEDG. The states and observations at time k are given by

$$x_k = Ax_{k-1} + Bu_{k-1} + v_{k-1}, \tag{6}$$

$$y_k = Cx_k + w_k, \tag{7}$$

where x_k, u_k, and y_k are the states, control signal, and observations of the system at time k, while v_k and w_k are the system and measurement noises, respectively, assumed to be i.i.d. zero-mean white Gaussian. As defined above, the attacker knows the system matrices A, B, and C, and at each time step k, they can add an arbitrary amount to the control signal u_k. Equation (8) shows the states at time $k+1$ with the attack signal a_k being injected into the control signal:

$$x_{k+1} = Ax_k + B(u_k + a_k) + v_k. \tag{8}$$

This attack vector a_k is chosen such that the observations of the system do not change, while the states of the system diverge. For the attack to be stealthy, a_k is chosen such that

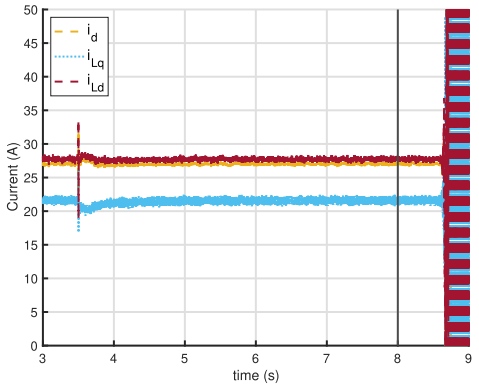
$$a_k = Fz_k, \tag{9}$$

where, F needs to be chosen such that $(A + BF)V^* \subseteq V^*$, where V^* is the maximal output-nulling invariant subspace [13]. The algorithm for calculating V^* is described in [46], and one way to obtain F is provided in Appendix B. Finally, z_k is defined by a recursive equation, $z_k = (A + BF)z_{k-1}$, where z_0 is chosen to be the eigenvector corresponding to the largest eigenvalue of $A + BF$ (the Perron eigenvector). This means that z_k is in the kernel of C, for any value of k. From (6) and (9), we can see that if the attack is made in the kernel of C, then there will be no impact in the output of the system. For a stealthy attack to be possible, the system must be of non minimum phase, which is equivalent to having an unstable eigenvalue of $A + BF$ – otherwise it would be impossible to make the system unstable [47]. This happens to be the case with the PEDG system that we will be simulating in Section IV, where the largest eigenvalue of $A+BF$ is 1.0007.

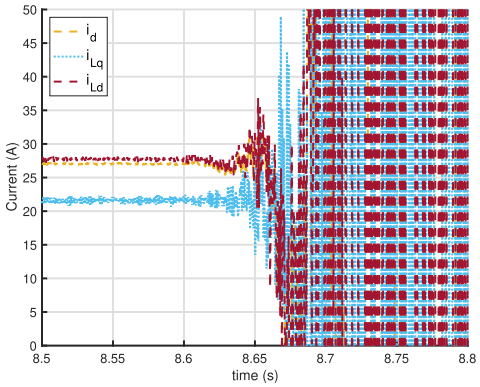
IV. RESULTS AND DISCUSSION

Stealthy attacks can be very threatening for power system stability–especially when the system inertia is comparatively low [48], [49], [50]. Potential disturbances on a PEDG can jeopardize the system's supply-demand balance easily and can negatively impact the system stability. This condition could be even more critical if a stealthy attack occurs in various grid access points. A successful stealthy attack can be easily designed by utilizing an approximated state-space model of a system. Here, a stealthy attack is implemented on a cluster of a PEDG, and the control signals are modified by employing attack disturbance signals into the system controller. It is important to mention that the attacker has designed the attack model according to the approximated state space model of the system.

Fig. 4 shows the states of the system with an attack starting at $t = 8s$. We can see that the states of the system diverge significantly about 0.55s after the attack begins. Fig. 5 shows only the observations of the system, during the same attack. The observations start to diverge shortly after 8.6s. This means that the attacker has about 0.05 to 0.1s to cause the system to collapse before the attack is



(a) The observations of the system with an attack starting at 8s.



(b) The observations of the system under attack – a zoomed-in version of Fig. 5a showing that the attack becomes observable around 8.65s.

FIGURE 5. System observations with an attack starting at 8s, denoted by the black vertical line. Note that observations begin to diverge about 0.1s after the states begin to diverge.

detectable. The attacker is aided by the low inertia property of a PEDG, as the states diverge rapidly and 0.65s is all the attacker needs to cause irreversible damage to the system. As depicted in Figs. 4 and 5, the stealthy attack begins at $t = 8$s. However, the other states of the integrated system stay unaffected for a duration of 0.65s. This could cause cascading failures across a grid with high penetration of distributed resources. By the time the local controller or the supervisory layer and their designated observers detect these stealthy activities, prior to any proper reaction, the physical system is already experiencing the consequences. For instance, the injected active and reactive powers are affected since DC-link voltage, V_c, and i_q (see Fig. 4b) start to diverge prior to $t = 8.65$s. This yields unexpected changes in injected active and reactive power into the system. According to the standards for grid integration of DERs, i.e., IEEE 1547, the frequency of the system and the PCC voltage of the DER must remain within pre-defined boundaries, otherwise, the DER must go islanded. As illustrated in Figs. 4 and 5, the system's active and reactive powers start to change due to the changes in the dq components of DC-link voltage and q component of the current. Since these changes are stealthy in the other states before the supervisory layer can observe them, the existing relays are going to be activated, which means that the DER will be isolated from the rest of the system. In this case, the supervisory layer will not have sufficient time to adjust the references for the nearby DERs and the overall balance between the active power consumption and generation will be lost, which yields cascading failures such as low-frequency oscillations between different grid clusters or even large-scale blackouts [51].

V. STEALTHY ATTACK PREVENTION

Considering recent advances in semiconductor characteristics, the switching frequency capability of inverters has increased significantly, which ensures the proper AC voltage at the inverter's terminal. However, the grid still receives a significant number of harmonics, drastically affecting the power quality. To address this hurdle, an appropriate filter is

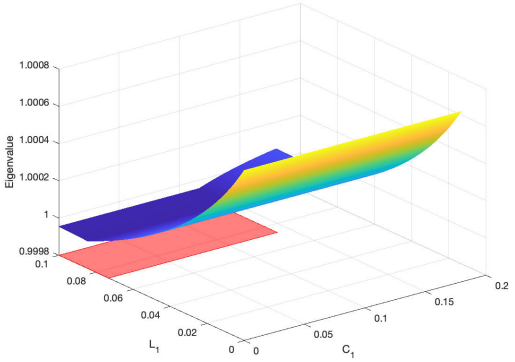
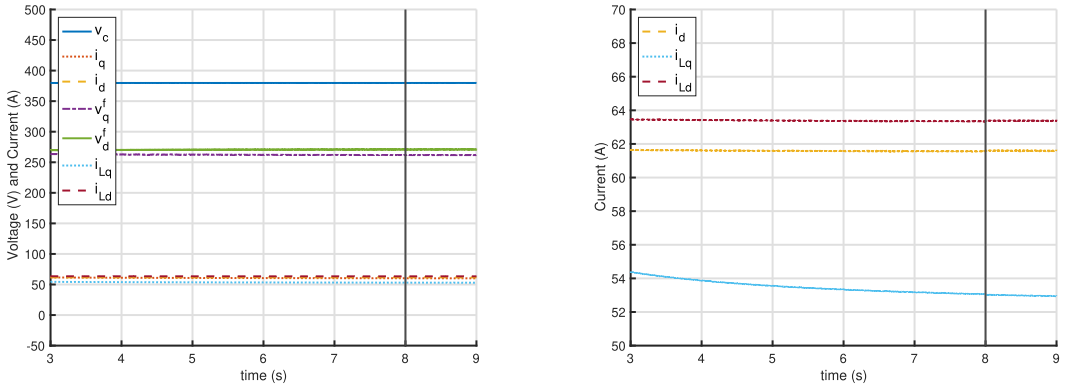


FIGURE 6. The main eigenvalue of $A + BF$ with varying values for C_1 and L_1. A stealthy attack is impossible for $C_1 \in [0.000018, 0.139818]F$ and $L_1 \in [0.0732, 0.1]H$, shown by the red rectangle.

required to diminish the impacts of the injected harmonics. As represented in Fig. 1, an LCL filter is considered to achieve this objective. It is essential to understand the impact that each parameter has on the state space representation, as well as the impact on the overall system operation. This may introduce limitations in the design stage of the filter and the resulting state space model of the system when determining the optimal parameter values that provide the desired system operation as well as values that prevent a stealthy attack. Since the LCL values appear in the matrix A of the state space model, each value introduces a unique impact on the voltage drop on the inductors and the circulating reactive power created by the capacitor branch [52]. A specific range of values for the system parameters may be considered to reduce the impact of the stealthy attacks while also considering design limitations. This provides an acceptable range for the LCL filter values to improve resiliency against such disturbances as represented in Fig. 6.

The impact of zero-dynamics stealthy attacks on PEDGs can be catastrophic, as shown in Section IV. However, zero-dynamics stealthy attacks have many limitations–including that the state space model must be of non minimum phase, meaning there must be an unstable eigenvalue of $A + BF$. This is because the attack is made in the direction of the main



(a) The states of the system with an attack starting at 8s.

(b) The observations of the system with an attack starting at 8s.

FIGURE 7. The states and observations of the system with an attack starting at 8s, denoted by the black vertical line. Note that the states do not diverge, as some of the system parameters were slightly modified in order to make the system minimum phase.

eigenvector of $A + BF$, and without an unstable eigenvalue the system will not diverge when it is attacked. Protecting a PEDG from such attacks may include making stealthy attacks impossible, making the attack detectable, or minimizing the impact that the attack can have on the system.

In this paper, we show that zero-dynamics stealthy attacks can be prevented in the system design phase by making small changes to the parameters of the system in order to push all of the eigenvalues of $A + BF$ inside of the unit circle. In order to calculate the values of parameters that prevent a zero-dynamics attack from being possible, we consider a range of possible values for the constant parameters, found in Table 2, in the state space model. In this paper, we simplify the problem by modifying two parameters at a time. We consider changing the DC link capacitor and the inverter side inductor, C_1 and L_1, in order to prevent a stealthy attack. We consider $C_1 \in [0.000018, 0.18]$F and $L_1 \in [0.0001, 0.1]$H, where the desired values of C_1 and L_1 are 0.0018F and 0.001H, respectively. From Fig. 6, we can see that keeping $C_1 \in [0.000018, 0.18]$F and $L_1 \in [0.0732, 0.1]$H renders all eigenvalues of $A + BF$ inside the unit circle. We choose $C_1 = 0.0018$F and $L_1 = 0.0732$H, as these are the closest to their actual values.

Fig. 7 shows the states and observations of the system under attack with the modified values of C_1 and L_1 chosen above. We can see that the attack is unsuccessful, as there is no change in the states of the system. This means that simply choosing alternative values for parameters in the design phase of a system can completely eliminate the possibility of a stealthy attack. Additionally, Fig. 8 shows that the frequency as well as V_{pcc} remains within acceptable bounds after an attack begins. Thus, it should be considered to design systems to be of minimum phase in the future. Although the modified L_1 and C_1 mitigate the impact of the stealthy attack in the theoretical aspect of inverter design, compared to their typical values in a real-life system, the manufacturing cost of such components is considerable and the dynamics of the system may be altered.

VI. CONCLUSION

The security of our critical infrastructure is of utmost importance. A successful attack on a power system can cause physical damage to the system or in a worst case scenario a blackout. As PEDGs increase in popularity, various attack scenarios must be studied in detail to mitigate the chances of a successful attack. We provide a three inverter PEDG, as well as the state space representation for the inverter of this PEDG. Additionally, we show that even though the state space model requires input from the rest of the system, using the steady state values of these inputs for the calculation of the attack is sufficient for the attacker to collapse the system. We show that preventing a stealthy attack is possible when small changes are made to the system parameters in the design phase. With the low inertia property of a PEDG, as well as the increasing number of telecommunication channels, a PEDG is the perfect system for an attacker to mount a stealthy attack. The impact of a stealthy attacks can be catastrophic, and as PEDGs are increasing in popularity, we believe that preventative measures should be considered in the design phase of a PEDG.

APPENDIX A STATE-SPACE MODEL

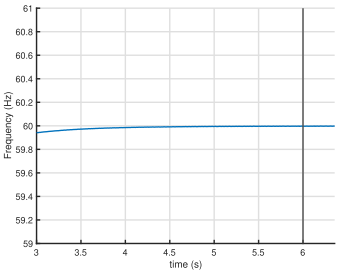
The state-space model of a system including a synchronous generator, the network connecting the SG to the inverters, and an aggregated model of multiple inverters are generated. The state variables are transferred to the d-q frame with respect to a global d-q frame. State-space matrices A, B, and C are driven from the dynamic equations of the SG and aggregated inverter model.

The system matrix is given by

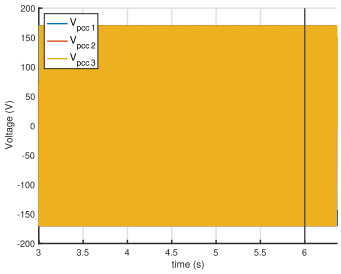
$$A = \begin{bmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ A_{21} & A_{22} & A_{23} & A_{24} \\ A_{31} & A_{32} & A_{33} & A_{34} \\ A_{41} & A_{42} & A_{43} & A_{44} \end{bmatrix},$$

where $A_{11}, \ldots, A_{44}$ are defined as follows:

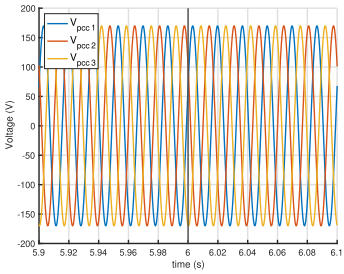
$$A_{11} = \frac{-1}{C_1 R_s}, \quad A_{12} = \begin{bmatrix} \frac{-\sqrt{3} m \cos\phi}{2C_1} & \frac{-\sqrt{3} m \sin\phi}{2C_1} \end{bmatrix},$$



(a) The frequency of the system with an attack starting at 6s.



(b) The point of common coupling voltage of the system with an attack starting at 6s.



(c) A zoomed-in representation of Fig. 8b.

FIGURE 8. The frequency and point of common coupling voltage of the system with an attack starting at 6s, denoted by the black vertical line. Note that these parameters remain withing acceptable bounds, as some of the system parameters were slightly modified in order to make the system minimum phase.

$$A_{13} = \begin{bmatrix} 0 & 0 \end{bmatrix}, A_{14} = \begin{bmatrix} 0 & 0 \end{bmatrix},$$

$$A_{21} = \begin{bmatrix} \frac{\sqrt{3}m\cos(\phi)}{3L_1} & \frac{\sqrt{3}m\sin(\phi)}{3L_1} \end{bmatrix}^T,$$

$$A_{22} = \begin{bmatrix} \frac{-3R_1 - R_f}{3L_1} & -\omega \\ \omega & \frac{-3R_1 - R_f}{3L_1} \end{bmatrix},$$

$$A_{23} = \begin{bmatrix} \frac{-1}{2L_1} & \frac{\sqrt{3}}{6L_1} \\ \frac{-\sqrt{3}}{6L_1} & \frac{-1}{2L_1} \end{bmatrix}, \quad A_{24} = \begin{bmatrix} \frac{R_f}{3L_1} & 0 \\ 0 & \frac{R_f}{3L_1} \end{bmatrix},$$

$$A_{31} = \begin{bmatrix} 0 & 0 \end{bmatrix}^T, \quad A_{32} = \begin{bmatrix} \frac{1}{2C_f} & \frac{\sqrt{3}}{6C_f} \\ \frac{-\sqrt{3}}{6C_f} & \frac{1}{2C_f} \end{bmatrix},$$

$$A_{33} = \begin{bmatrix} 0 & -\omega \\ \omega & 0 \end{bmatrix},$$

$$A_{34} = \begin{bmatrix} \frac{-1}{2C_f} & \frac{-\sqrt{3}}{6C_f} \\ \frac{\sqrt{3}}{6C_f} & \frac{-1}{2C_f} \end{bmatrix}, \quad A_{41} = \begin{bmatrix} 0 & 0 \end{bmatrix}^T,$$

$$A_{42} = \begin{bmatrix} \frac{R_f}{3L_2} & 0 \\ 0 & \frac{R_f}{3L_2} \end{bmatrix}, \quad A_{43} = \begin{bmatrix} \frac{1}{2L_2} & \frac{-\sqrt{3}}{6L_2} \\ \frac{\sqrt{3}}{6L_2} & \frac{1}{2L_2} \end{bmatrix},$$

$$A_{44} = \begin{bmatrix} \frac{-3R_2 - R_f}{3L_2} & -\omega \\ \omega & \frac{-3R_2 - R_f}{3L_2} \end{bmatrix}.$$

The input matrix B is given by

$$B = \begin{bmatrix} B_{11} & B_{12} & B_{14} & B_{15} & B_{16} & B_{17} \end{bmatrix}^T.$$

where, B_{11}, B_{12}, B_{13}, B_{14}, B_{15}, B_{16}, and B_{17} are defined as follows:

$$B_{11} = \begin{bmatrix} \frac{1}{C_1 R_s} & 0 & 0 \end{bmatrix}, \quad B_{12} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix},$$
$$B_{13} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}, \quad B_{14} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix},$$

TABLE 2. Values for the constants in the state space representation.

R_s	0.1 Ω	m	0.849 pu
C_1	$1800e^{-6}$ F	ϕ	1.37 rad
L_1	$1e^{-3}$ H	ω	120π rad/s
R_1	0.15 Ω	R_2	0.8 Ω
L_2	$0.5e^{-3}$ H	C_f	$30e^{-6}$ F

$$B_{15} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}, \quad B_{16} = \begin{bmatrix} 0 & \frac{-1}{L_2} & 0 \end{bmatrix},$$
$$B_{17} = \begin{bmatrix} 0 & 0 & \frac{-1}{L_2} \end{bmatrix}.$$

Values for the constants are provided in Table 2.

APPENDIX B CALCULATION OF *F*

Since matrix D is 0 in our case, we replace the solution in [46] as shown below. We need a value of F_2 that satisfies

$$\begin{bmatrix} V & B \end{bmatrix} \begin{bmatrix} F_1 \\ F_2 \end{bmatrix} V = AV. \tag{10}$$

Note that we shall also find a value of F_1, but this value is not relevant for our purposes. From this, we can easily obtain

$$\begin{bmatrix} V & B \end{bmatrix}^+ \begin{bmatrix} V & B \end{bmatrix} \begin{bmatrix} F_1 \\ F_2 \end{bmatrix} VV^+ = \begin{bmatrix} V & B \end{bmatrix}^+ AVV^+, \tag{11}$$

where $\begin{bmatrix} V & B \end{bmatrix}^+$ and V^+ represent the Moore-Penrose pseudo-inverses of matrices $\begin{bmatrix} V & B \end{bmatrix}$ and V, respectively.

If we choose $\begin{bmatrix} F_1 \\ F_2 \end{bmatrix}$ to be the right-hand side of (11), that is,

$$\begin{bmatrix} F_1 \\ F_2 \end{bmatrix} = \begin{bmatrix} V & B \end{bmatrix}^+ AVV^+, \tag{12}$$

then using one of the properties of the pseudo-inverse, that states that for a general matrix M we have $M^+MM^+ = M^+$, we see that this choice of $\begin{bmatrix} F_1 \\ F_2 \end{bmatrix}$ satisfies (11). Now substituting the same in the left-hand side of (10), and using the property that for a general matrix M we have that $MM^+M = M$, we get

$$\begin{bmatrix} VB \end{bmatrix} \begin{bmatrix} F_1 \\ F_2 \end{bmatrix} V = \begin{bmatrix} V & B \end{bmatrix} \begin{bmatrix} V & B \end{bmatrix}^+ AV, \tag{13}$$

the right-hand side of which is equal to AV (meaning that our choice of $\begin{bmatrix} F_1 \\ F_2 \end{bmatrix}$ satisfies (10)) whenever $\begin{bmatrix} VB \end{bmatrix}$ has linearly independent rows. What remains is to simply set $F = -F_2$.

REFERENCES

[1] B. K. Bose, "Global energy scenario and impact of power electronics in 21st century," *IEEE Trans. Ind. Electron.*, vol. 60, no. 7, pp. 2638–2651, Jul. 2013.

[2] F. Blaabjerg and K. Ma, "Future on power electronics for wind turbine systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 1, no. 3, pp. 139–152, Sep. 2013.

[3] O. Ellabban, H. Abu-Rub, and F. Blaabjerg, "Renewable energy resources: Current status, future prospects and their enabling technology," *Renew. Sustain. Energy Rev.*, vol. 39, pp. 748–764, Nov. 2014.

[4] Q. Peng, Q. Jiang, Y. Yang, T. Liu, H. Wang, and F. Blaabjerg, "On the stability of power electronics-dominated systems: Challenges and potential solutions," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7657–7670, Nov. 2019.

[5] F. Blaabjerg, Y. Yang, D. Yang, and X. Wang, "Distributed power-generation systems and protection," *Proc. IEEE*, vol. 105, no. 7, pp. 1311–1331, Jul. 2017.

[6] P. Denholm, T. Mai, R. W. Kenyon, B. Kroposki, and M. O'Malley, "Inertia and the power grid: A guide without the spin," Nat. Renew. Energy Lab. (NREL), Golden, CO, USA, Tech. Rep. NREL/TP-6A20-73856, 2020.

[7] K. S. Ratnam, K. Palanisamy, and G. Yang, "Future low-inertia power systems: Requirements, issues, and solutions–A review," *Renew. Sustain. Energy Rev.*, vol. 124, May 2020, Art. no. 109773.

[8] F. Milano, F. Dorfler, G. Hug, D. J. Hill, and G. Verbic, "Foundations and challenges of low-inertia systems," in *Proc. Power Syst. Comput. Conf. (PSCC)*, Jun. 2018, pp. 1–25.

[9] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal, "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *IEEE Trans. Power Syst.*, vol. 19, no. 3, pp. 1387–1401, Aug. 2004.

[10] A. J. Wood, B. F. Wollenberg, and G. B. Sheblé, *Power Generation, Operation, and Control*. Hoboken, NJ, USA: Wiley, 2013.

[11] T. Baumeister, "Literature review on smart grid cyber security," Collaborative Softw. Develop. Lab., Univ. Hawaii, Honolulu, HI, USA, Tech. Rep., 2010.

[12] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[13] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1806–1813.

[14] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*. Amsterdam, The Netherlands: Elsevier, 2010.

[15] A. Keliris and M. Maniatakos, "ICSREF: A framework for automated reverse engineering of industrial control systems binaries," 2018, *arXiv:1812.03478*.

[16] Q. Li, F. Li, J. Zhang, J. Ye, W. Song, and A. Mantooth, "Data-driven cyberattack detection for photovoltaic (PV) systems through analyzing micro-PMU data," in *Proc. IEEE Energy Convers. Congr. Exposit. (ECCE)*, Oct. 2020, pp. 431–436.

[17] K. G. Lore, D. M. Shila, and L. Ren, "Detecting data integrity attacks on correlated solar farms using multi-layer data driven algorithm," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, May 2018, pp. 1–9.

[18] A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R. G. Dutta, Y. Jin, and C. Konstantinou, "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581–595, Oct. 2020.

[19] H. Shim, J. Back, Y. Eun, G. Park, and J. Kim, "Zero-dynamics attack, variations, and countermeasures," in *Security and Resilience of Control Systems: Theory and Applications*. Cham, Switzerland: Springer, 2022, pp. 31–61.

[20] J. Kim, J. Back, G. Park, C. Lee, H. Shim, and P. G. Voulgaris, "Neutralizing zero dynamics attack on sampled-data systems via generalized holds," *Automatica*, vol. 113, Mar. 2020, Art. no. 108778.

[21] D. Kim, K. Ryu, J. H. Kim, and J. Back, "Zero assignment via generalized sampler: A countermeasure against zero-dynamics attack," *IEEE Access*, vol. 9, pp. 109932–109942, 2021.

[22] D. Kim, K. Ryu, and J. Back, "Zero-dynamics attack on wind turbines and countermeasures using generalized hold and generalized sampler," *Appl. Sci.*, vol. 11, no. 3, p. 1257, Jan. 2021.

[23] B. Kim, K. Ryu, and J. Back, "A generalized hold based countermeasure against zero-dynamics attack with application to DC–DC converter," *IEEE Access*, vol. 10, pp. 44923–44933, 2022.

[24] J. A. Farber and D. G. Cole, "Nonlinear zero-dynamics attacks targeting nuclear power plants," in *Proc. Dyn. Syst. Control Conf.*, vol. 84270. New York, NY, USA: American Society of Mechanical Engineers, 2020, Art. no. V001T04A004.

[25] J. Lee, J. Kim, and H. Shim, "Zero-dynamics attack on homomorphically encrypted control system," in *Proc. 20th Int. Conf. Control, Autom. Syst. (ICCAS)*, 2020, pp. 385–390.

[26] A. Baniamerian, K. Khorasani, and N. Meskin, "Monitoring and detection of malicious adversarial zero dynamics attacks in cyber-physical systems," in *Proc. IEEE Conf. Control Technol. Appl. (CCTA)*, Aug. 2020, pp. 726–731.

[27] S. Harshbarger, "The impact of zero-dynamics stealthy attacks on control systems: Stealthy attack success probability and attack prevention," Ph.D. dissertation, Dept. Comput. Sci., Kansas State Univ., Manhattan, KS, USA 2022.

[28] W. S. Gray, L. A. Duffaut Espinosa, and M. A. Haq, "Universal zero dynamics attacks using only input-output data," in *Proc. Amer. Control Conf. (ACC)*, Jun. 2022, pp. 4985–4991.

[29] G. Park, C. Lee, H. Shim, Y. Eun, and K. H. Johansson, "Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zero-dynamics attack," *IEEE Trans. Autom. Control*, vol. 64, no. 12, pp. 4907–4919, Dec. 2019.

[30] B. Paudel and G. Amariucai, "Reinforcement learning approach to generate zero-dynamics attacks on control systems without state space models," in *Proc. 28th Eur. Symp. Res. Comput. Secur. (ESORICS)*, 2023.

[31] Y. Wang, J. Gao, Z. Zuo, Q. Han, and W. Zhang, "Periodic zero-dynamics attacks for discrete-time second-order multi-agent systems," *Int. J. Robust Nonlinear Control*, vol. 32, no. 9, pp. 5619–5636, 2022.

[32] Y. Mao, E. Akyol, and Z. Zhang, "A novel defense strategy against zero-dynamics attacks in multi-agent systems," in *Proc. IEEE 58th Conf. Decis. Control (CDC)*, Dec. 2019, pp. 3563–3568.

[33] J. Chen, J. Wei, W. Chen, H. Sandberg, K. H. Johansson, and J. Chen, "Geometrical characterization of sensor placement for cone-invariant and multi-agent systems against undetectable zero-dynamics attacks," *SIAM J. Control Optim.*, vol. 60, no. 2, pp. 890–916, Apr. 2022.

[34] S. Harshbarger, M. Hosseinzadehtaher, B. Natarajan, E. Vasserman, M. Shadmand, and G. Amariucai, "(A little) ignorance is bliss: The effect of imperfect model information on stealthy attacks in power grids," in *Proc. IEEE Kansas Power Energy Conf. (KPEC)*, Jul. 2020, pp. 1–6.

[35] M. Esmalifalak, Z. Han, and L. Song, "Effect of stealthy bad data injection on network congestion in market based power system," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2012, pp. 2468–2472.

[36] Y. Liu, W. Xue, S. He, and L. Cheng, "Stealthy false data injection attacks against extended Kalman filter detection in power grids," in *Proc. 8th Int. Conf. Inf., Cybern., Comput. Social Syst. (ICCSS)*, Dec. 2021, pp. 459–464.

[37] J. Tian, B. Wang, Z. Wang, K. Cao, J. Li, and M. Ozay, "Joint adversarial example and false data injection attacks for state estimation in power systems," *IEEE Trans. Cybern.*, vol. 52, no. 12, pp. 13699–13713, Dec. 2022.

[38] C. Liu, H. Liang, and T. Chen, "Network parameter coordinated false data injection attacks against power system AC state estimation," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1626–1639, Mar. 2021.

[39] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 214–219.

[40] D. I. Urbina, J. A. Giraldo, A. A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg, "Limiting the impact of stealthy attacks on industrial control systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 1092–1105.

[41] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[42] S. D. Roy and S. Debbarma, "A novel OC-SVM based ensemble learning framework for attack detection in AGC loop of power systems," *Electric Power Syst. Res.*, vol. 202, Jan. 2022, Art. no. 107625.
[43] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1183–1195, May 2014.
[44] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.
[45] D. Choeum and D.-H. Choi, "OLTC-induced false data injection attack on volt/VAR optimization in distribution systems," *IEEE Access*, vol. 7, pp. 34508–34520, 2019.
[46] B. D. O. Anderson, "Output-nulling invariant and controllability subspaces," *IFAC Proc. Volumes*, vol. 8, no. 1, pp. 337–345, Aug. 1975.
[47] X. Hu, A. Lindquist, J. Mari, and J. Sand, "Geometric control theory," Lecture Notes, Optim. Syst. Theory Roy. Inst. Technol., Stockholm Sweden, Tech. Rep. SE-100, vol. 44, 2012, pp. 31–51.
[48] W. Qiu, K. Sun, W. Yao, S. You, H. Yin, X. Ma, and Y. Liu, "Time-frequency based cyber security defense of wide-area control system for fast frequency reserve," *Int. J. Electr. Power Energy Syst.*, vol. 132, Nov. 2021, Art. no. 107151.
[49] S. D. Roy and S. Debbarma, "Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2023–2031, Jun. 2020.
[50] F. Akbarian, A. Ramezani, M. Hamidi-Beheshti, and V. Haghighat, "Advanced algorithm to detect stealthy cyber attacks on automatic generation control in smart grid," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 4, pp. 351–358, Dec. 2020.
[51] G. Patsakis, D. Rajan, I. Aravena, J. Rios, and S. Oren, "Optimal black start allocation for power system restoration," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6766–6776, Nov. 2018.
[52] D. Solatialkaran, K. G. Khajeh, and F. Zare, "A novel filter design method for grid-tied inverters," *IEEE Trans. Power Electron.*, vol. 36, no. 5, pp. 5473–5485, May 2021.

STEPHANIE HARSHBARGER received the B.S. degree in computer science and mathematics from the University of Nebraska at Kearney, Kearney, Nebraska, in 2018, and the Ph.D. degree in computer science from Kansas State University, Manhattan, Kansas, in 2022.

MOHSEN HOSSEINZADEHTAHER (Member, IEEE) received the M.Sc. degree in electrical engineering from the Amirkabir University of Technology, Tehran, Iran, in 2014. He is currently pursuing the Ph.D. degree with the Electrical and Computer Engineering Department, University of Illinois at Chicago, USA.

ALIREZA ZARE (Graduate Student Member, IEEE) received the B.Sc. degree in electrical engineering with a focus on power engineering from Shiraz University, Shiraz, Iran, in 2017, and the M.S. degree from Washington State University, Vancouver, WA, USA in 2020. He is currently pursuing the Ph.D. degree with the Electrical and Computer Engineering Department, University of Illinois Chicago.

AMIN Y. FARD (Student Member, IEEE) received the B.Sc. degree in electrical power engineering from Azarbaijan Shahid Madani University, Tabriz, Iran, in 2011, the M.Sc. degree (Hons.) in electrical power engineering from the University of Tabriz, Tabriz, in 2014, and the Ph.D. degree from Kansas State University, in 2020. He is currently pursuing the Ph.D. degree with the Electrical and Computer Engineering Department, University of Illinois at Chicago, USA. His research interests include renewable energy systems, such as photovoltaic systems and wind turbines, power electronics, distributed generation, and power quality.

MOHAMMAD B. SHADMAND (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 2015. From 2017 to 2020, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS, USA. Since 2020, he has been an Assistant Professor with the University of Illinois at Chicago, IL, USA. He was awarded Michelle Munson Serban Simu Keystone Research Scholar, Kansas State University, in 2017. He was awarded the 2019 IEEE Myron Zucker Faculty-Student Research Grant. He has awarded multiple best paper awards at different IEEE conferences. He is the General Co-Chair of 50th Annual Conference of the IEEE Industrial Electronics Society (IECON 2024), Chicago, IL. He serves as Associate Editor for IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON INDUSTRY APPLICATION, and *IET Renewable Power Generation*.

GEORGE AMARIUCAI received the B.S. and M.S. degrees from the Politechnic University of Bucharest, in 2003 and 2004, respectively, and the Ph.D. degree from Louisiana State University, in 2009. Between 2009 and 2017, he was an Adjunct Assistant Professor and then an Adjunct Associate Professor with the Department of Electrical and Computer Engineering, Iowa State University. He joined Kansas State University, in 2017, where he is currently an Associate Professor, and the Director of the PITS Laboratory.