IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

IEEE POWER & ENERGY SOCIETY SECTION

Received December 26, 2020, accepted January 10, 2021, date of publication January 28, 2021, date of current version February 4, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3055229

Cyber-Physical Anomaly Detection in Microgrids Using Time-Frequency Logic Formalism

OMAR ALI BEG[1], (Member, IEEE), LUAN VIET NGUYEN[2], (Member, IEEE), TAYLOR T. JOHNSON[3], (Member, IEEE), AND ALI DAVOUDI[4], (Senior Member, IEEE)

[1]The University of Texas Permian Basin, Odessa, TX 79762, USA
[2]University of Dayton, Dayton, OH 45469, USA
[3]Vanderbilt University, Nashville, TN 37240, USA
[4]The University of Texas at Arlington, Arlington, TX 76019, USA

Corresponding author: Ali Davoudi (davoudi@uta.edu)

This work was supported by the Office of Naval Research under Grant N00014-18-1-2184.

ABSTRACT Modern cyber-physical microgrids rely on the information exchanged among power electronics devices (i.e., converters or inverters with local embedded controllers) making them vulnerable to cyber manipulations. The physical devices themselves are susceptible to potential faults and failures. Effects of these cyber and physical anomalies can propagate throughout the entire microgrid due to information exchanged and the inherent low inertia of the distribution network. This work employs the parametric time-frequency logic (PTFL) framework to detect such cyber-physical anomalies. PTFL is a formalism to analyze the time-frequency content of the observable quantities of interest (such as current, voltage, or frequency) of power electronics devices in comparison with the predefined time-frequency properties. PTFL formalism is presented to detect the anomalies such as false data-injection attacks, denial-of-service attacks, and faults on a cluster of four DC microgrids and an inverter-populated IEEE 34-bus feeder system in a controller/hardware-in-the-loop environment.

INDEX TERMS Distributed control, formal methods, microgrid, parametric time-frequency logic.

I. INTRODUCTION

MICROGRIDS employing distributed control are scalable and reliable alternatives to the traditional counterparts with centralized controllers that had posed a single point-of-failure and required high communication bandwidth [1], [2]. Microgrids with distributed control have evolved into cyber-physical systems (CPS) due to the adoption of complex embedded controllers and communication network, and can be prone to cyber-physical anomalies [3]. An *anomaly* is defined here as an unexpected behavior of a microgrid due to a fault, failure, or cyber attack [4]. The *behavior* of a microgrid is defined by its output voltage and current. The distributed control framework is vulnerable to cyber attacks due to its dependence on local sensing of the observable quantities (e.g., current, voltage, or frequency), the presence of a communication network for data exchange, and the absence of a centralized structure with a global situational awareness to evaluate the prevailing adversarial cyber picture [5]. The physical devices (power electronic converters/inverters, distributed energy sources, sensors, transmission lines, etc) are also susceptible to potential faults and failures, referred to here as the physical anomalies. The distorting effects of these cyber or physical anomalies can rapidly propagate throughout the entire microgrid due to the cyber interconnection and the inherent low inertia of the power distribution network in a microgrid [6].

Recent anomaly detection approaches [7]–[16] are largely based on state estimation techniques. Most techniques are designed for legacy power systems, with centralized control architectures, and could have certain drawbacks; e.g., require detailed modeling, need the structural knowledge of the power systems, merely indicate the presence or absence of an anomaly, or miss quantitative information about after-effects. A summation detector in [16] detects a cyber attack based on current and historical data. Detection techniques based on temporal logic provide a more comprehensive picture about an anomaly by quantifying its effects in both time and space with respect to predefined bounds. They can quantify the effects of an anomaly instead of providing a mere binary detection output. Existing techniques,

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

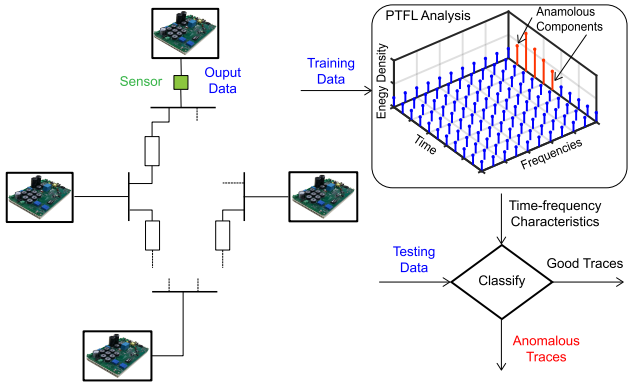

FIGURE 1. Parametric time-frequency logic (PTFL) employed in a context of a microgrid. Microgrid's output waveforms are used as the training data to extract the time-frequency information of anomalous traces via PTFL analysis based on continuous wavelet transform, which will later be used to classify traces in testing data.

e.g., [17], [18], focus on detecting abnormal signal behaviors in the time domain while undesirable behaviors such as unexpected oscillations, abrupt transients, and spurious noise could be difficult to detect without frequency information. Moreover, a carefully-designed anomalous signal could go undetected by such techniques if it does not violate predefined bounds.

To capitalize on the time-frequency information for cyber-physical anomaly detection, this work adopts the *parametric time-frequency logic* (PTFL) formalism [19] in the context of power electronics-intensive microgrids, as shown in Fig. 1. It takes two types of data sets as inputs: the *training* set composed of the anomalous traces, and the *testing* set composed of both the anomalous and the good traces. These data sets are obtained from the output waveforms, referred to as *traces*, of the microgrid, shown as the output data in Fig. 1. This PTFL framework extracts the anomalous time-frequency content from the training data, and subsequently uses them to detect the anomalous traces present in the testing data. One of the advantages of the considered PTFL technique is that it does not require the modeling knowledge of the microgrid. Instead, the anomalous traces of the microgrid are essentially required for anomaly detection. These traces are readily available through measurements of output current and voltage waveforms. Important time-frequency information, from such traces, is extracted through continuous wavelet transform. This class of temporal logic stands apart from its counterparts (e.g., signal temporal logic [5]) in following ways:

- A given trace could be analyzed in both time and frequency domains to detect not only the cyber and physical anomalies but also the unwanted noise in the microgrid output.
- This technique successfully detects an anomalous trace, irrespective of its magnitude, even if it doesn't violate predefined bounds.
- Temporal constraints for a given testing data can be specified to determine the exact time duration for which an anomaly occurs.

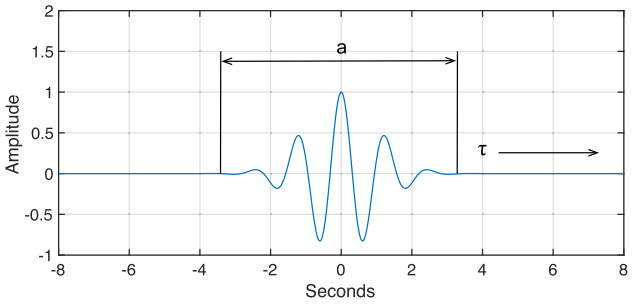

FIGURE 2. Morlet (morl) wavelet is shown with the scaling parameter a and the shifting parameter τ. CWT involves the convolution of complex-conjugate of daughter wavelets, resulting from variation of a, with $s(t)$.

The remainder of this article is organized as follows: Signal analysis of the output traces using continuous wavelet transform is reviewed in Section II. In Section III, an overview of the PTFL is provided in the context of microgrids. Anomaly detection using PTFL is discussed in Section IV. In Section V, various cyber-physical anomalies are detected for DC and AC microgrids in a controller/hardware-in-the-loop (CHIL) environment. Section VI concludes the article.

II. TRACE ANALYSIS USING CONTINUOUS WAVELET TRANSFORM

The *continuous wavelet transform* (CWT) is used to sift through the time-frequency content from the microgrid *traces* (output waveforms). Formally, the real-valued voltage and current measurements over time (i.e., $i(t)$ and $v(t)$ for all $t \in \mathbb{R}_{\geq 0}$, where $\mathbb{R}_{\geq 0}$ represents the set of all positive real numbers) are considered as *traces* that define the microgrid *behavior*. The time-frequency information of microgrid traces is obtained by computing the *time-frequency energy density* of the CWT coefficients. We first review the concept of CWT, and provide examples of DC-DC converter and DC-AC inverter to illustrate how CWT of a given trace (such as the output voltage) provides important time-frequency information which can be used to detect an anomaly.

A. CONTINUOUS WAVELET TRANSFORM

CWT [15] involves convolution of the trace $s(t)$ and daughter wavelets created out of a zero-mean mother wavelet, $\psi(t)$, where

$$\int_{-\infty}^{+\infty} \psi(t)\, dt = 0. \tag{1}$$

This work considers the Morlet (morl) wavelet [20], shown in Fig. 2, as the mother wavelet. The corresponding daughter wavelets, $\psi_{a,\tau}(t)$, are given by

$$\psi_{a,\tau}(t) = \frac{1}{\sqrt{|a|}} \psi\left(\frac{t-\tau}{a}\right), \tag{2}$$

where a is the scaling parameter, and τ is the shifting parameter along the time axis. A smaller a corresponds to a

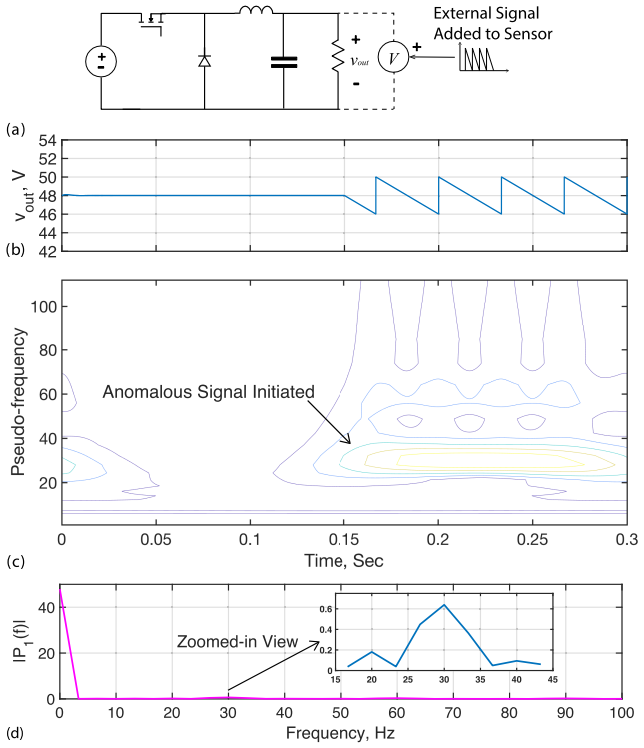

FIGURE 3. A DC-DC buck converter is affected by an anomalous sawtooth trace: (a) Distorting the voltage sensor of a buck converter; (b) Output voltage waveform; (c) CWT using morl wavelet; and (d) Single-sided amplitude spectrum using FFT.

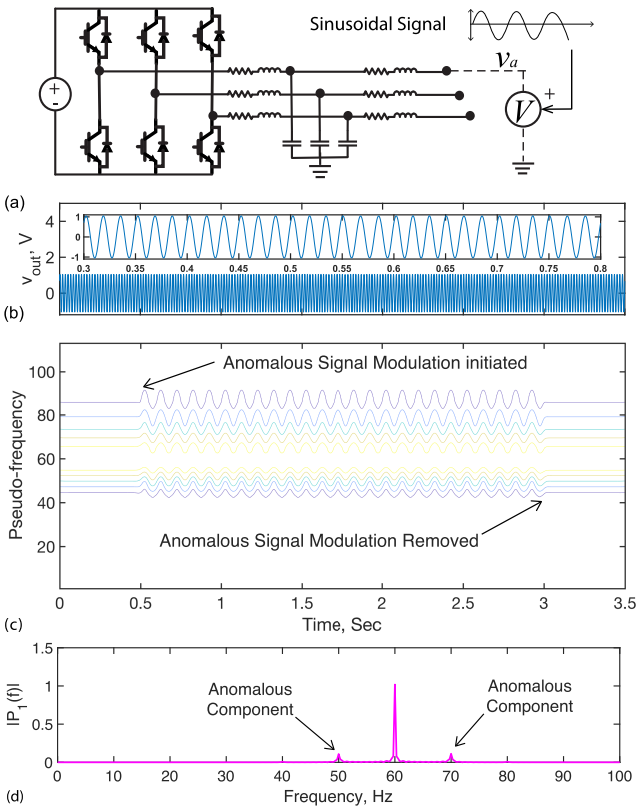

FIGURE 4. An inverter is affected by an anomalous sinusoidal trace modulated from $t = 0.5\ s$ to $t = 3\ s$: (a) Inverter circuit; (b) Voltage waveform; (c) CWT using the morl wavelet; and (d) Single-sided amplitude spectrum using FFT.

compressed daughter wavelet and a larger a results in a *stretched* one. The change in a for the mother wavelet produces a daughter wavelet with a particular pseudo-frequency in the frequency domain.

The CWT of the trace $s(t)$ is obtained by the convolution of $s(t)$ with the complex-conjugate of the daughter wavelet function in (2),

$$W_{f(a,\tau)} = \int_{-\infty}^{+\infty} s(t)\psi^*_{a,\tau}(t)\,dt, \tag{3}$$

The *time-frequency energy density* of these CWT coefficients, given by

$$P_{Wf} = |W_{f(a,\tau)}|^2, \tag{4}$$

will be used in PTFL-based anomaly detection framework, discussed later in Section III.

The concepts to obtain the time-frequency energy density for PTFL are elaborated using examples of a DC-DC buck converter and a DC-AC inverter, the building blocks of DC and AC microgrids, respectively.

B. INSTANTIATION FOR A DC-DC CONVERTER

A 30 Hz sawtooh trace is assumed to distort the output voltage sensor of a buck converter (Fig. 3(a)) at $t = 0.15\ s$. This anomalous output voltage trace, shown in Fig. 3(b), is used to generate the CWT coefficients for various pseudo-frequencies, as shown in Fig. 3(c). The color coding indicates the magnitude of the CWT coefficients varying between the dark blue color (that corresponds to a lesser magnitude) to yellow color (that corresponds to a larger magnitude) for a given pseudo-frequency. The pseudo-frequencies around $30Hz$ produce larger CWT coefficients indicating anomalous data in that range. Using this information, one can identify the presence of an anomalous trace in Fig. 3(c) at $t = 0.15\ s$ onward. Although this difference is quite visible in Fig. 3(b), this would not be the case for lesser magnitudes of anomalous traces. The fast Fourier transform (FFT) of this trace results in its corresponding frequency components (i.e., DC component and 30 Hz) as depicted by the single-sided amplitude spectrum in Fig. 3(d).

C. INSTANTIATION FOR A DC-AC INVERTER

The output voltage for the phase 'a' of a 60 Hz inverter (Fig. 4(a)), is shown in Fig. 4(b). An anomalous sinusoidal trace with 10 Hz frequency is initiated at $t = 0.5\ s$ and removed at $t = 3\ s$. The zoomed-in view of the output voltage in Fig. 4(b) demonstrates that this anomalous trace is undetectable in time domain. However, CWT clearly exhibits this anomaly, initialized at $t = 0.5\ s$ and removed at $t = 3\ s$, as shown in Fig. 4(c). The pseudo-frequencies around 50 Hz and 70 Hz (the frequencies of the anomalous data) produce the larger CWT coefficients. Moreover, one can also observe the variations in the CWT coefficients that start from

$t = 0.5\ s$ until $t = 3\ s$. This picture is further clarified by a single-sided amplitude spectrum of the trace that generates the corresponding frequency components (60 Hz being the base and 50 and 70 Hz as the anomalous frequencies) as shown in Fig. 4(d).

III. PARAMETRIC TIME-FREQUENCY LOGIC

Time-frequency logic (TFL) formulas constitute *predicates* defined over traces [19]. A predicate is formally written in form of constraints over the frequency of $s(t)$, e.g., $f \leq 60\ Hz$. The temporal operators, namely, *always* and *eventually* denoted by $\mathcal{G}$ and $\mathcal{F}$, respectively, define the temporal part in a TFL formula. The temporal operator *always* requires the given TFL formula to be true for the entire trace, whereas the temporal operator *eventually* requires that the TFL formula holds true only for some valuation in the trace. Each temporal operator is evaluated for the given temporal constraints, e.g., $[0, \tau]\ \forall\ \tau \in \mathbb{R}_{\geq 0}$, shown as a subscript. For example, a TFL formula can be stated in plain words as *the frequency of the output voltage should always remain less than or equal to* 70 Hz *in the temporal range* [0, 3.5] , and formally expressed as

$$\phi_f = \mathcal{G}_{[0,3.5]}(f \leq 70). \tag{5}$$

The TFL formula in (5) holds true for the inverter trace in Fig. 4. Instead of frequency, the TFL formula could contain the time-frequency energy density of CWT coefficients given by (4) and known as the *spectral trace*. This work employs such a spectral trace, denoted by $\zeta(f, t)$, e.g.,

$$\phi_\zeta = \mathcal{G}_{[0,3.5]}\big(\zeta(f, t) \geq 1\big). \tag{6}$$

The TFL formula in (5) employs numeric values for both temporal and threshold constraints. Instead, PTFL employs two types of *symbolic parameters* in the TFL formulas, i.e.,

1. Temporal parameters: These correspond to the intervals bounding the temporal operators, e.g., $\mathcal{G}_{[0,20]}$ in (5) is replaced with $\mathcal{G}_{[\tau_1,\tau_2]}$. Generally, the set of temporal parameters in a PFTL formula are given by
$$T = \{\tau_1, \tau_2, \tau_3, \ldots, \tau_{\rho_t}\}, \tag{7}$$
where ρ_t is the total number of temporal parameters.
2. Threshold parameters: These correspond to the constraints in the TFL predicates, e.g., $\zeta(f, t) \geq 1$ in (6) is replaced with $\zeta(f, t) \geq \theta$. Generally, the set of threshold parameters in PTFL formula are given by
$$\Theta = \{\theta_1, \theta_2, \theta_3, \ldots, \theta_{\rho_n}\}, \tag{8}$$
where ρ_n is the total number of threshold parameters.

The corresponding PTFL formula for (6) is written as

$$\phi_\zeta = \mathcal{G}_{[\tau_1,\tau_2]}\big(\zeta(f, t) \geq \theta\big). \tag{9}$$

Alternatively, a PTFL formula can be transformed to a TFL formula by assigning appropriate numeric values to all $\tau \in T$ and $\theta \in \Theta$. This work detects cyber-physical anomalies in microgrids by adopting the *parameter synthesis* approach, elaborated in Section IV, for a given PTFL formula.

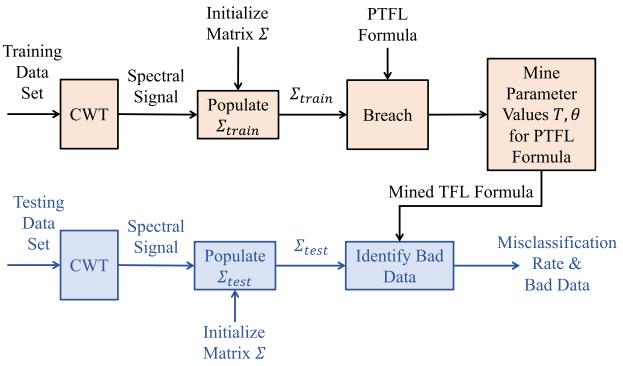

FIGURE 5. The PTFL-based technique [19] can identify the anomalous signal through parameter synthesis. It takes the training and the testing data sets as input, computes the corresponding parameter values using Breach tool [21] for a given PTFL formula, and mines those values to identify a corresponding TFL formula that can classify the test data as either good or anomalous.

IV. PTFL-BASED ANOMALY DETECTION

This technique involves *parameter synthesis* [22] for the PTFL formulas, i.e., it computes the numeric values for the parameters T and Θ, and stores those values to find a TFL formula [19], as shown in Fig. 5. The data classification can then be performed using the stored TFL formula to segregate the good data and the bad data, where the data not satisfying the TFL formula is identified as the bad data, as shown in the lower part of Fig. 5. The details are provided in the following sections.

A. PARAMETER SYNTHESIS

Parameter synthesis requires two sets of time-series data, namely, the *training data* and the *testing data*. The training data contains the anomalous traces only. The testing data contains both the anomalous traces and the good traces (without anomaly). CWT of both data sets results in spectral traces to form two matrices, Σ_{train} and Σ_{test}, computed using (4) corresponding to the training and testing data sets, respectively.

This approach requires the corresponding PTFL formula to compute the parameter values in (7) and (8). Consider the following PTFL formula based on the CWT of a trace

$$\Phi = \bigwedge_{i=1}^{m} \mathcal{F}_{[\tau_1,\tau_2]}\big(\zeta_i(f, t) \geq \theta_i\big) \forall f_1, f_2, \ldots, f_m, \tag{10}$$

where $\zeta_i(f, t)$ is a given spectral trace [19]. It states that *the energy densities of the trace* $\zeta_i(f, t)$ *over a frequency range for a given number of frequencies, m, are eventually more than a threshold value* θ_i. The structure of this formula is similar to (9), except that it is evaluated over a range of frequencies. The *parameter synthesis* approach finds τ_1, τ_2, and θ_i.

During a training process, since the PTFL formula Φ captures time-frequency behaviors of traces and the spectral traces in Σ_{train}, a time-frequency parameter synthesis built on the Breach toolbox [21] automatically searches for the *temporal* and *threshold* parameter values within predefined ranges. The corresponding TFL formula, Φ', satisfied by all

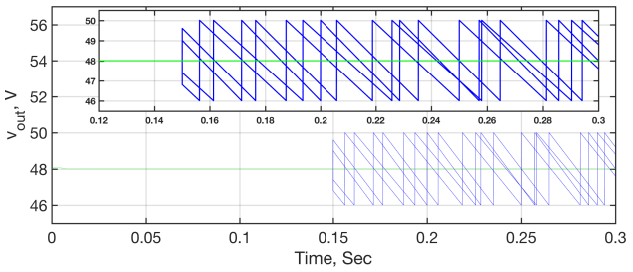

FIGURE 6. Out of total 20 testing traces, the proposed technique has successfully identified 5 anomalous traces (shown in blue color) for the Buck converter voltage through parameter synthesis, with zero misclassification rate.

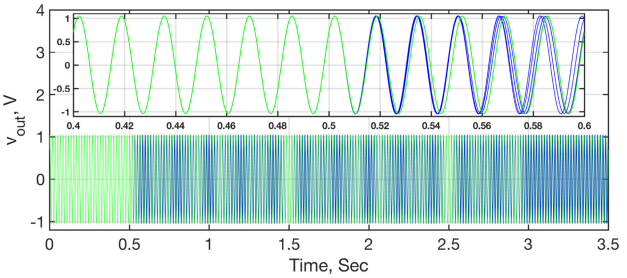

FIGURE 7. Out of total 20 testing traces, the proposed technique has successfully identified 5 anomalous traces (shown in blue color) for the inverter voltage through parameter synthesis with zero misclassification rate.

spectral traces of the training set, is obtained by substituting those mined values into the PTFL formula (10).

Given the spectral traces in Σ_{test}, our approach checks the satisfaction of Φ' w.r.t to those traces and then classifies them as either good or anomalous. It also provides the *misclassification rate* of the anomalous data. A lower rate indicates more success in detecting the anomalous data.

B. IMPLEMENTATION ON POWER ELECTRONICS DEVICES

This technique is evaluated for the buck converter and the inverter examples elaborated in Section III. The training data is composed of 20 anomalous traces under false data-injection attack (FDIA) with frequency randomly varying between 30 to 35 Hz, while the testing data has five anomalous traces and 15 good traces. The frequency of FDIA to generate the anomalous traces is randomly varied, firstly, to see if anomalous traces could be identified irrespective of the frequency variations and, secondly, for better visualization of anomalous data. As depicted in Fig. 6, the proposed technique successfully classifies anomalous traces from the testing data using the PTFL formula in (10). The testing data set is plotted with the anomalous traces shown in blue and the good traces shown in green. The misclassification rate was found to be zero indicating perfect identification of anomalous traces. Some of the parameters corresponding to (10) computed by PTFL technique are, $m = 3, \tau_1 = 0, \tau_2 = 0.22\ s$, and $\theta_3 = 0.99$ for $f_3 = 27.98\ Hz$ to result in

$$\phi_{\zeta_3} = \mathcal{F}_{[0,0.22]}\big(\zeta_3(f,t) \geq 0.99\big), \tag{11}$$

for $f_3 = 27.98\ Hz$. The parameterized formula in (11) in conjunction with other such formulas for f_1 and f_2 is then evaluated for the testing data to classify the good and bad traces as shown in Fig. 6.

This technique is also applied to the inverter example in Section III. The training data is generated such that the original trace is modulated with the anomalous trace having a randomly-varying phase for each iteration. The random phase variation is induced, firstly, to verify that the proposed technique successfully detects the frequency variations irrespective of the phase and, secondly, for better visualization of plotted data in time domain. The training data set is composed of 20 anomalous traces, and the testing data set is composed of five anomalous traces and 15 good traces (without the addition of an anomaly). Examples of the parameters corresponding to (10) computed by the PTFL technique are, $m = 6, \tau_1 = 0, \tau_2 = 8.68\ ms$, and $\theta_2 = 5.996$ for $f_2 = 74.61\ Hz$. This parameterized PTFL formula is then evaluated for the testing data to classify the good and bad traces. As shown in Fig. 7, the proposed technique using the PTFL formula in (10) successfully classifies anomalous traces from the testing data, with a zero misclassification rate.

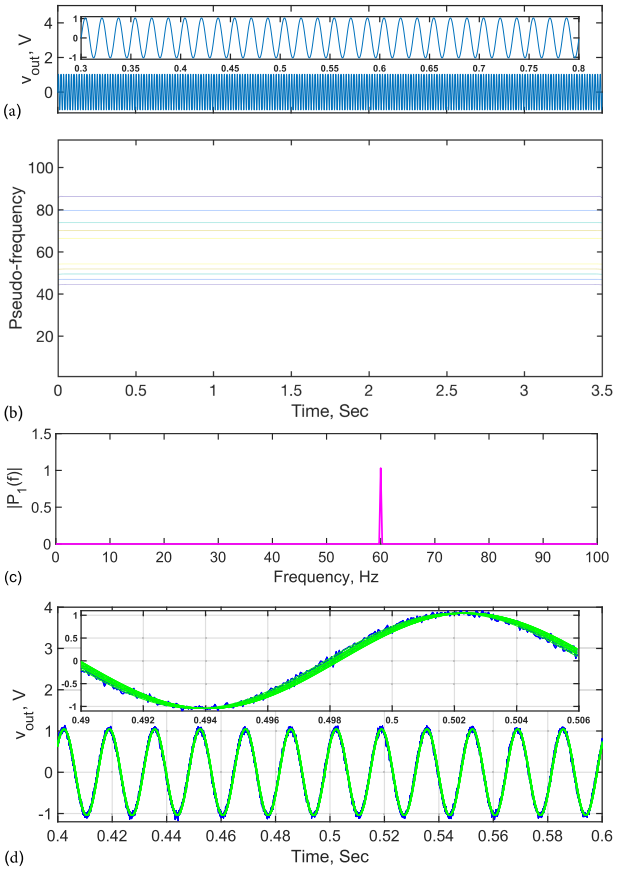

FIGURE 8. A single inverter is affected due to an anomalous noisy trace with a white Gaussian noise: (a) Voltage waveform; (b) CWT using morl wavelet; (c) Single-sided amplitude spectrum using FFT; (d) The proposed technique has successfully identified the 5 anomalous traces with noise (shown in blue color) for the inverter voltage through parameter synthesis while 15 good traces are identified that did not contain noise content (shown in blue color) with a zero misclassification rate.

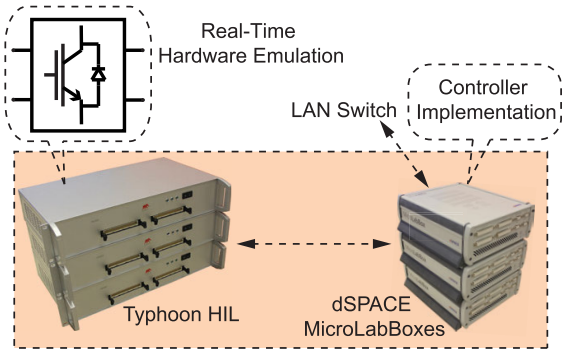

FIGURE 9. Physical components are emulated in Typhoon HIL, control schemes are implemented in dSAPCE MLBXs, and communication among MLBXs is facilitated through an Ethernet switch.

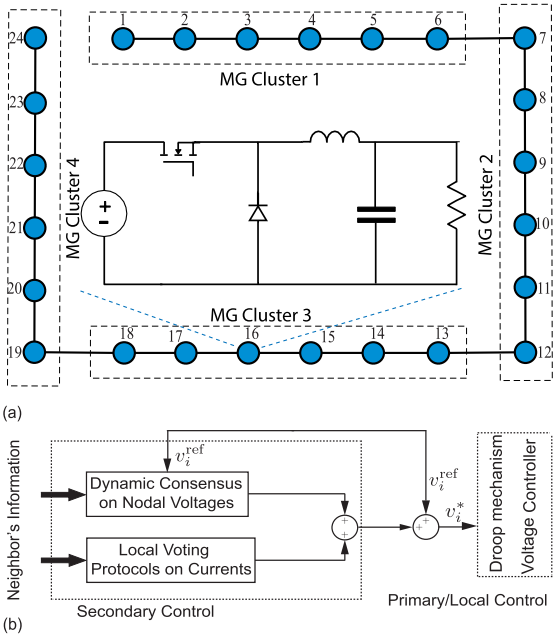

FIGURE 10. Four clusters of dc microgrids employing distributed cooperative control: a) Each cluster has six buck converters; b) Each converter uses its neighbor information for voltage regulation and load sharing.

C. DETECTION OF ANOMALOUS SIGNALS WITH NOISE

Since noise tends to affect the frequency content and, hence, the time-frequency characteristics of the original trace, this technique can effectively classify the noisy traces due to the integration of CWT. Consider the inverter example with a white Gaussian noise added to the voltage of phase A, as shown in Fig. 8(a). The training data set has 20 anomalous traces, and the testing data is composed of five anomalous and 15 good traces (without noise). CWT and FFT analysis for the output voltage are provided in Fig. 8(b) and (c), respectively. Although the noise intensity is small enough, the parameter synthesis technique successfully classifies five anomalous traces (with noise), highlighted with blue color in Fig. 8(d), with a zero misclassification rate.

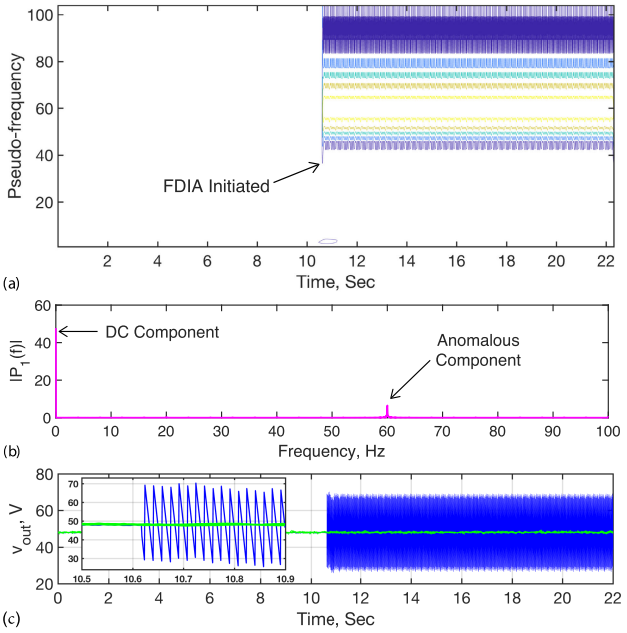

FIGURE 11. All converters are affected by unconstrained FDIA: (a) CWT using morl wavelet; (b) Single-sided amplitude spectrum using FFT; (c) The proposed technique has successfully identified six anomalous traces (shown in blue color) for the DC microgrid through parameter synthesis with zero misclassification rate.

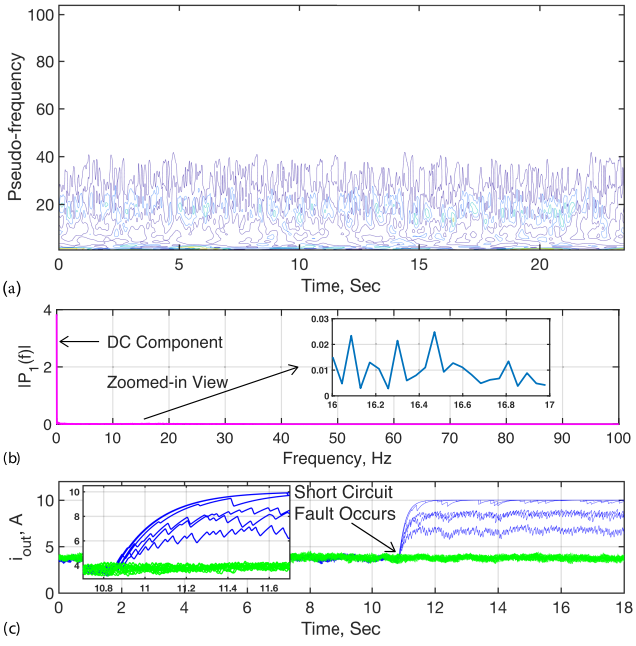

FIGURE 12. Short-circuit fault is emulated in the third converter of the third microgrid: (a) CWT using morl wavelet; (b) Single-sided amplitude spectrum using FFT; (c) Out of total 24 testing traces, the proposed technique has successfully identified six anomalous traces (shown in blue color) for the DC microgrid through parameter synthesis with zero misclassification rate.

V. CONTROLLER/Hardware-IN-THE-LOOP EVALUATION

The PTFL-based anomaly detection technique is evaluated in a controller/hardware-in-the-loop (CHIL) environment shown in Fig. 9, wherein Typhoon HIL 604 systems

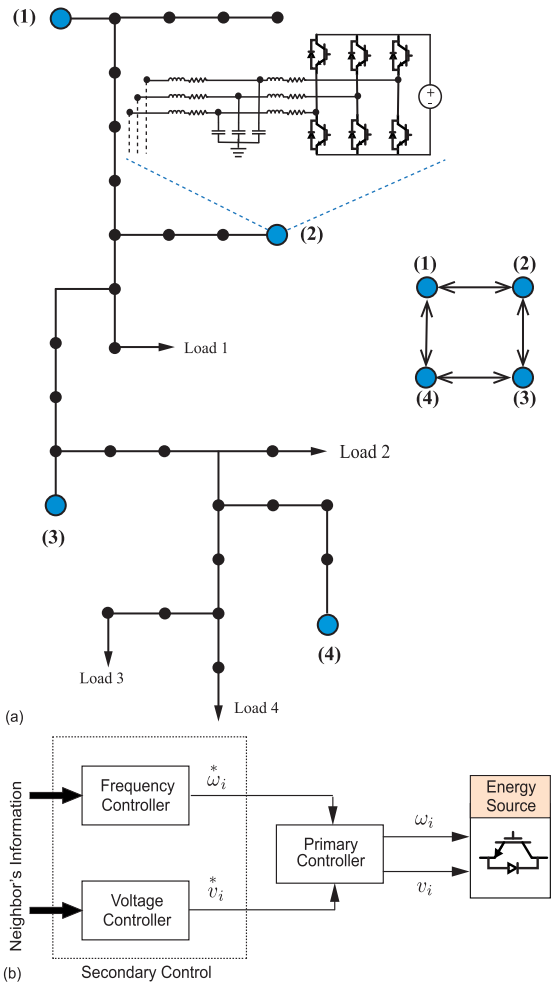

FIGURE 13. IEEE 34-bus feeder augmented with four inverters employing distributed cooperative control: a) distribution network with the communication topology among inverters; b) distributed cooperative control to regulate inverter voltage and frequency using its neighbor data.

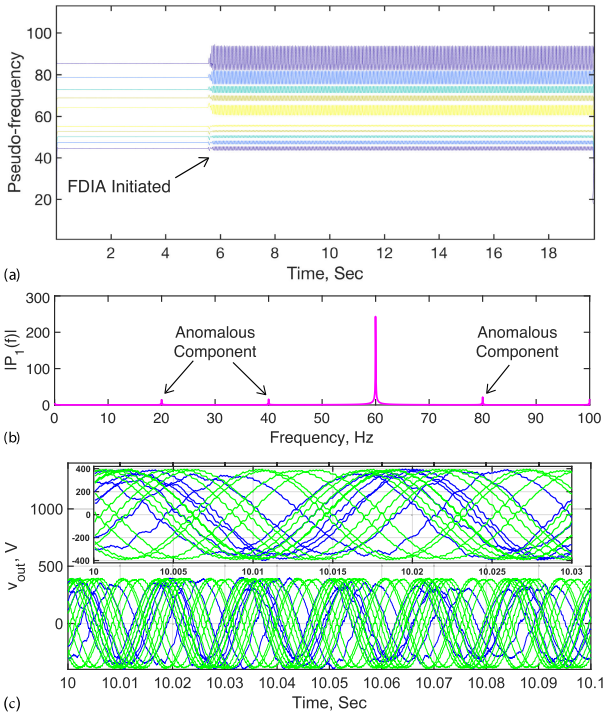

FIGURE 14. Inverter 1 is effected due to an FDIA targeting the controller with 20 *Hz* sawtooth trace: (a) CWT using morl wavelet; (b) Single-sided amplitude spectrum using FFT; (c) Out of total 20 testing traces, the proposed technique has successfully identified six anomalous traces (shown in blue color) through parameter synthesis with zero misclassification rate.

emulate physical components, dSPACE DS1202 Microlab Boxes (MLBXs) implement control schemes, and an Ethernet switch communicates among MLBXs. This work considers the distributed cooperative control paradigm for both DC and AC microgrids, wherein a converter (inverter) in DC (AC) microgrid is considered as an agent that exchanges information with its neighbors over a sparse communication graph. Interested readers can refer to [23] and [24] to see the general discussion about cooperative control of DC and AC microgrids, respectively. The misclassification rate is zero in all the following case studies signifying that PTFL technique is 100 % successful in classifying the anomalous signals.

A. CLUSTER OF DC MICROGRIDS

Four DC microgrid clusters, with distributed cooperative control, shown in Fig. 9, are emulated in the CHIL setup of Fig. 10. Each cluster contains six DC-DC Buck converters emulated in a single Typhoon HIL604 device with their corresponding cooperative controllers in a separate dSPACE MLBX.

1) FDIA

The output voltages are contaminated with a false data trace (a sawtooth voltage with 60 *Hz*). A training data set is generated that contains 24 anomalous traces. The testing data contains six anomalous traces and 18 good traces. Both data sets are subjected to the proposed technique to obtain the results shown in Fig. 11. Only CWT and FFT analysis results for the output voltage of converter 1 are shown in Fig. 11(a) and Fig. 11(b), respectively. The color coding in Fig. 11(a) indicates the magnitude of the CWT coefficients varying between the dark blue color (indicating a lesser magnitude) to yellow color (indicating a larger magnitude) for a given pseudo-frequency. The pseudo-frequencies around 60 *Hz* produce larger CWT coefficients indicating that the trace contains the anomalous data in that range. It is also evident that the anomalous trace is injected at about 10.2 *s*, as shown in Fig. 11(a). This anomalous frequency component (60 *Hz*) is also depicted in Fig. 11(b). The six anomalous traces (shown in blue), out of total 24 traces, are successfully detected within the testing data with zero misclassification rate, and the good traces are shown in green color in Fig. 11(c).

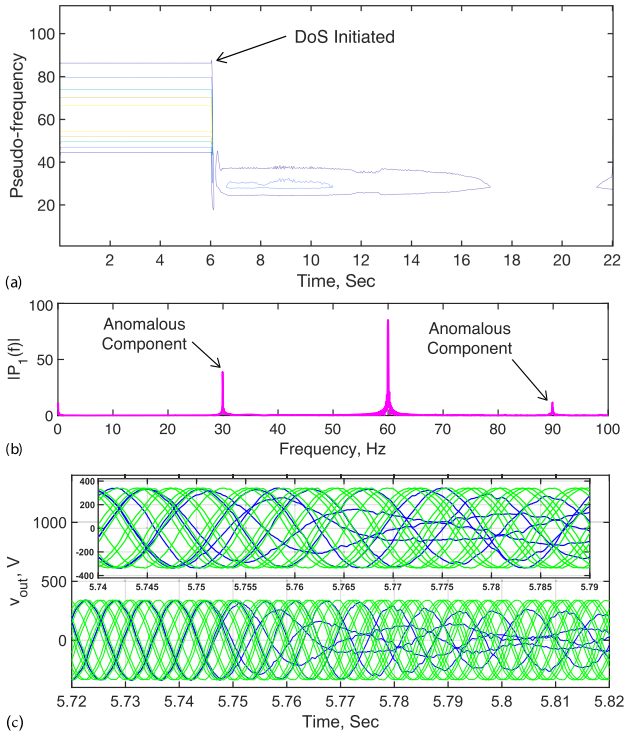

FIGURE 15. Incoming communication links of inverter 4 are subjected to a DoS attack: (a) CWT using morl wavelet; (b) Single-sided amplitude spectrum using FFT; (c) Out of total 20 testing traces, six anomalous traces (shown in blue color) are identified with zero misclassification rate.

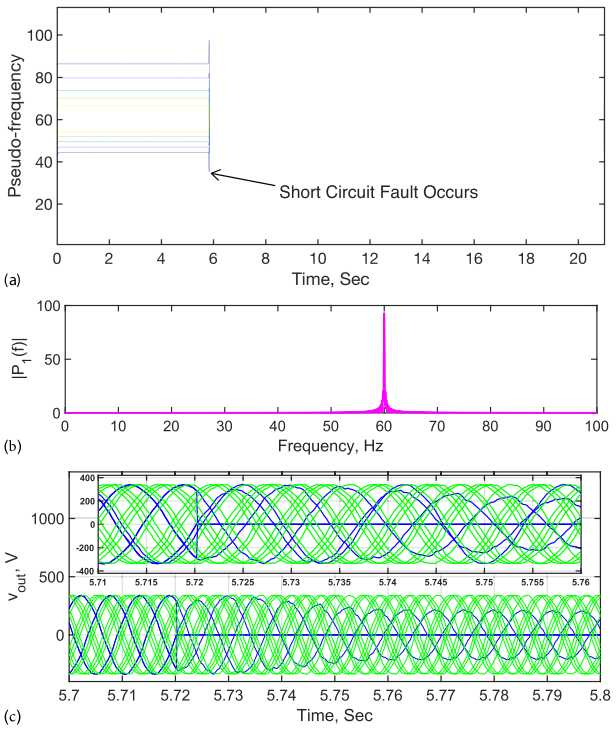

FIGURE 16. A 3 phase-to-ground fault is emulated in inverter 2: (a) CWT using morl wavelet; (b) Single-sided amplitude spectrum using FFT; (c) Out of total 20 testing traces, the proposed technique has successfully identified six anomalous traces (shown in blue color) for the IEEE 34-bus feeder through parameter synthesis with zero misclassification rate.

2) SHORT-CIRCUIT FAULT

The second study considers a short circuit fault emulated in the third converter of the third DC microgrid. The output currents of corresponding converters are considered to extract the required time-frequency information. The training data contains 24 anomalous traces, and the testing data contains six anomalous and 18 good traces. CWT and FFT analyses for the output current under normal working conditions (i.e., without fault) are provided in Fig. 12(a) and (b), respectively. During initial analysis based on CWT and FFT, it was observed that frequency components around 16 *Hz* exist in good traces as depicted in Fig. 12(b), which are non-existent in the anomalous trace. This distinguishing characteristic is employed to classify the good and anomalous traces for a given testing data set under the short-circuit scenario. Both the data sets are subjected to the proposed technique to obtain the results shown in Fig. 12. This technique has successfully detected six anomalous traces (shown in blue) out of total 24 traces, where the good traces are shown by the green color in Fig. 12(c).

B. INVERTER-AUGMENTED IEEE 34-BUS SYSTEM

An IEEE 34-bus feeder system augmented with four inverters, shown in Fig. 13, is emulated in the CHIL setup of Fig. 9. Four inverters employ distributed cooperative controllers that exchange information over the communication graph shown in Fig. 13. For PTFL analysis, the output voltages of the corresponding inverters are considered to extract the required time-frequency information in all the subsequent case studies. Moreover, the training data set contains 20 anomalous traces, and the testing data set contains six anomalous and 14 good traces.

1) FDIA

A 20 *Hz* sawtooth FDIA voltage targets the controller of inverter 1 in the AC microgrid of Fig. 13(a). CWT and FFT analysis for the output voltage of inverter 1 are provided in Fig. 14(a) and (b), respectively. The pseudo-frequencies around 20 *Hz*, 40 *Hz*, 60 *Hz* (the mains frequency), and 80 *Hz* produce larger CWT coefficients. Larger CWT coefficients around the pseudo-frequencies of 20 *Hz*, 40 *Hz* and 80 *Hz* indicate that the trace contains the anomalous data in that range. Moreover, the time-frequency information also indicates that the anomalous trace is injected at about 5.8 *s*, as shown in Fig. 11(a). The anomalous frequency as well as its harmonics are depicted in Fig. 14(b). The PTFL-based technique has successfully detected six anomalous traces (shown in blue) out of total 20 traces. Good traces are shown in green color in Fig. 14(c).

2) DoS ATTACK

In this context, denial-of-Service (DoS) attack involves paralyzing few or all the communication links of the communication network. Under this scenario, the incoming communication to inverter 4 is targeted. CWT and FFT analysis for

the output voltage of the inverter 4 are provided in Fig. 15(a) and (b), respectively. The time-frequency information indicates that DoS attack is initiated at about 6 *s*, and severely effects the 60 *Hz* main frequency, as shown in Fig. 11(a). After about 6 *s*, the pseudo-frequencies around 30 *Hz* produce the larger CWT coefficients. The PTFL-based technique has successfully detected six anomalous traces (shown in blue) out of total 20 traces, with the good traces shown in green in Fig. 15(c).

3) 3 PHASE-TO-GROUND FAULT

This type of fault is emulated in inverter 2. CWT and FFT analysis for the output voltage of inverter 2 are provided in Fig. 16(a) and (b), respectively. The time-frequency information in Fig. 16(a) indicates that the anomaly occurred around 6 *s* that severely effected the main 60 *Hz* frequency. Six anomalous traces (shown in blue), out of the total 20 traces, are properly identified, as shown in Fig. 16(c).

VI. CONCLUSION

A comprehensive cyber-physical anomaly detection framework, based on the PTFL formalism, is presented in the context of DC and AC microgrids to detect FDIA and DoS attacks and physical faults. This approach has an edge over the other temporal logic-based techniques in that it extracts the time-frequency information from a given training data set to successfully detect the anomalous traces within another data set. It is also independent of the threshold levels and can successfully detect the anomalous traces containing noise. The proposed technique is verified for DC and AC microgrids in a CHIL environment. For future work, one could extend this detection technique to include classification of various cyber-physical anomalies. This would require amending an intelligent mechanism that can classify anomalies based on their respective signatures or characteristics. This would be useful, e.g., to distinguish among simultaneous anomalies with various time durations.

ACKNOWLEDGMENT

The technical content has been approved for public release under DCN# 43-7427-20.

REFERENCES

[1] X. Dou, P. Xu, Q. Hu, W. Sheng, X. Quan, Z. Wu, and B. Xu, "A distributed voltage control strategy for multi-microgrid active distribution networks considering economy and response speed," *IEEE Access*, vol. 6, pp. 31259–31268, 2018.

[2] H. E. Z. Farag and E. F. El-Saadany, "A novel cooperative protocol for distributed voltage control in active distribution systems," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1645–1656, May 2013.

[3] W. Liu, Q. Gong, H. Han, Z. Wang, and L. Wang, "Reliability modeling and evaluation of active cyber physical distribution system," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 7096–7108, Nov. 2018.

[4] R. Moghaddass and J. Wang, "A hierarchical framework for smart grid anomaly detection using large-scale smart meter data," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5820–5830, Nov. 2018.

[5] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in DC microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585–3595, Jul. 2019.

[6] S. Abhinav, I. D. Schizas, F. L. Lewis, and A. Davoudi, "Distributed noise-resilient networked synchrony of active distribution systems," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 836–846, Mar. 2018.

[7] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[8] G. Anagnostou, F. Boem, S. Kuenzel, B. C. Pal, and T. Parisini, "Observer-based anomaly detection of synchronous generators for power systems monitoring," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 4228–4237, Jul. 2018.

[9] L. Cai, N. F. Thornhill, S. Kuenzel, and B. C. Pal, "Real-time detection of power system disturbances based on k -Nearest neighbor analysis," *IEEE Access*, vol. 5, pp. 5631–5639, 2017.

[10] L. Cai, N. F. Thornhill, S. Kuenzel, and B. C. Pal, "Wide-area monitoring of power systems using principal component analysis and k-nearest neighbor analysis," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4913–4923, Sep. 2018.

[11] M. Jamei, A. Scaglione, C. Roberts, E. Stewart, S. Peisert, C. McParland, and A. McEachern, "Anomaly detection using optimally placed μPMU sensors in distribution grids," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 3611–3623, Jul. 2018.

[12] Y. Zhao, A. Goldsmith, and H. Vincent Poor, "Minimum sparsity of unobservable power network attacks," *IEEE Trans. Autom. Control*, vol. 62, no. 7, pp. 3354–3368, Jul. 2017.

[13] S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, and A. Joshi, "Joint-transformation-based detection of false data injection attacks in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 1, pp. 89–97, Jan. 2018.

[14] H. Wang, J. Ruan, G. Wang, B. Zhou, Y. Liu, X. Fu, and J. Peng, "Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4766–4778, Nov. 2018.

[15] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 3271–3280, Jul. 2018.

[16] D. Ye and T.-Y. Zhang, "Summation detector for false data-injection attack in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 50, no. 6, pp. 2338–2345, Jun. 2020.

[17] E. Bartocci, L. Bortolussi, and G. Sanguinetti, "Data-driven statistical learning of temporal logic properties," in *Proc. Int. Conf. Formal Model. Anal. Timed Syst.* Cham, Switzerland: Springer, 2014, pp. 23–37.

[18] G. Bombara, C.-I. Vasile, F. Penedo, H. Yasuoka, and C. Belta, "A decision tree approach to data classification using signal temporal logic," in *Proc. 19th Int. Conf. Hybrid Syst., Comput. Control*, Apr. 2016, pp. 1–10.

[19] L. V. Nguyen, J. Kapinski, X. Jin, J. V. Deshmukh, K. Butts, and T. T. Johnson, "Abnormal data classification using time-frequency temporal logic," in *Proc. 20th Int. Conf. Hybrid Systems: Comput. Control*, Pittsburgh, PA, USA, Apr. 2017, pp. 237–242.

[20] S. S. Osofsky, "Calculation of transient sinusoidal signal amplitudes using the Morlet wavelet," *IEEE Trans. Signal Process.*, vol. 47, no. 12, pp. 3426–3428, Dec. 1999.

[21] A. Donzé, "Breach, a toolbox for verification and parameter synthesis of hybrid systems," in *Proc. 22nd Int. Conf. Comput. Aided Verification*, 2010, pp. 167–170.

[22] A. Cimatti, A. Griggio, S. Mover, and S. Tonetta, "Parameter synthesis with IC3," in *Proc. Formal Methods Comput.-Aided Design*, Portland, OR, USA, Oct. 2013, pp. 165–168.

[23] V. Nasirian, S. Moayedi, A. Davoudi, and F. L. Lewis, "Distributed cooperative control of DC microgrids," *IEEE Trans. Power Electron.*, vol. 30, no. 4, pp. 2288–2303, Apr. 2015.

[24] A. Bidram, F. L. Lewis, and A. Davoudi, "Distributed control systems for small-scale power networks: Using multiagent cooperative control theory," *IEEE Control Syst. Mag.*, vol. 34, no. 6, pp. 56–77, Dec. 2014.

OMAR ALI BEG (Member, IEEE) received the Ph.D. degree in electrical engineering from The University of Texas at Arlington, TX, USA, in 2017. He was a recipient of the U.S. Air Force Research Laboratory Summer Research Fellowship, in 2015. He was also a recipient of the Rising STARs (Science and Technology Acquisition and Retention) grant by the UT System. He is currently an Assistant Professor with the Department of Electrical Engineering, College of Engineering, The University of Texas Permian Basin, TX, USA. His research interests include formal verification and cyber-attack detection in cyber-physical power systems using formal methods.

LUAN VIET NGUYEN (Member, IEEE) received the B.E. and M.Sc. degrees from The Catholic University of America, in May 2012 and December 2012, respectively. During his Ph.D., he was a member of the Verivital Lab, The University of Texas at Arlington. He was a Postdoctoral Research Associate with the PRECISE Center, University of Pennsylvania, and also with the Department of Electrical Engineering, University of Notre Dame. He is currently an Assistant Professor with the Department of Computer Science, University of Dayton, OH, USA. His current research interests include cyber-physical systems, hybrid systems, formal methods, temporal logic, and control theory. He is particularly interested in research-related requirement mining, formal verification, reachability analysis, and model-based design of cyber-physical systems to improve safety and security. His contributions in those areas have been made public through more than two dozen peer-reviewed articles, and state-of-the-art software with practical applications in various domains such as power and energy systems, medical devices, automotive, aerospace, and robotics.

TAYLOR T. JOHNSON (Member, IEEE) received the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Illinois at Urbana–Champaign, Urbana, IL, USA, in 2010 and 2013, respectively. He is currently an Assistant Professor of electrical engineering and computer science with Vanderbilt University, Nashville, TN, USA. His research interests include developing algorithmic techniques and software tools to improve the reliability of cyber-physical systems.

Dr. Johnson received the National Science Foundation Computer and Information Science and Engineering Research Initiation Initiative Award, in 2015, and the Air Force Office of Scientific Research Young Investigator Program Award, in 2016 and 2018.

ALI DAVOUDI (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Illinois Urbana–Champaign, IL, USA, in 2010. He is currently a Professor with the Electrical Engineering Department, The University of Texas at Arlington, Arlington, TX, USA. He has received The Best Paper Award from the 2015 IEEE International Symposium on Resilient Control Systems, the 2014-2015 Best Paper Award from the IEEE TRANSACTIONS ON ENERGY CONVERSION, the 2016 Prize Paper Award from the IEEE Power and Energy Society, the 2017 IEEE Richard M. Bass Outstanding Young Power Electronics Engineer Award, the 2017-2018 Best Paper Award from the IEEE TRANSACTIONS ON ENERGY CONVERSION, and the 2019-2020 Faculty Fellow of Janet and Mike Greene Endowed Professorship. He is an Associate Editor of the IEEE TRANSACTIONS ON POWER ELECTRONICS, and an Editor of the IEEE TRANSACTIONS ON ENERGY CONVERSION and the IEEE POWER ENGINEERING LETTERS.