IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

IEEE POWER & ENERGY SOCIETY SECTION

Received December 9, 2020, accepted January 10, 2021, date of publication January 13, 2021, date of current version January 28, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3051300

Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack

MOSLEM DEHGHANI[1], MOHAMMAD GHIASI[1], TAHER NIKNAM[1], (Member, IEEE), ABDOLLAH KAVOUSI-FARD[1], (Member, IEEE), ELHAM TAJIK[2], SANJEEVIKUMAR PADMANABAN[3], (Senior Member, IEEE), AND HAMDULAH ALIEV[4]

[1]Department of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz 71557-13876, Iran
[2]School of Electrical and Computer Engineering, University of Oklahoma, Norman, OK 73019, USA
[3]Department of Energy Technology, Aalborg University, 6700 Esbjerg, Denmark
[4]Faculty of Energy, Tajik Technical University, Dushanbe 734042, Tajikistan

Corresponding authors: Hamdulah Aliev (hhuali334@gmail.com) and Taher Niknam (niknam@sutech.ac.ir)

ABSTRACT Since Smart-Islands (SIs) with advanced cyber-infrastructure are incredibly vulnerable to cyber-attacks, increasing attention needs to be applied to their cyber-security. False data injection attacks (FDIAs) by manipulating measurements may cause wrong state estimation (SE) solutions or interfere with the central control system performance. There is a possibility that conventional attack detection methods do not detect many cyber-attacks; hence, system operation can interfere. Research works are more focused on detecting cyber-attacks that target DC-SE; however, due to more widely uses of AC SIs, investigation on cyber-attack detection in AC systems is more crucial. In these regards, a new mechanism to detect injection of any false data in AC-SE based on signal processing technique is proposed in this paper. Malicious data injection in the state vectors may cause deviation of their temporal and spatial data correlations from their ordinary operation. The suggested detection method is based on analyzing temporally consecutive system states via wavelet singular entropy (WSE). In this method, to adjust singular value matrices and wavelet transforms' detailed coefficients, switching surface based on sliding mode controller are decomposed; then, by applying the stochastic process, expected entropy values are calculated. Indices are characterized based on the WSE in switching level of current and voltage for cyber-attack detection. The proposed detection method is applied to different case studies to detect cyber-attacks with various types of false data injection, such as amplitude, and vector deviation signals. The simulation results confirm the high-performance capability of the proposed FDIA detection method. This detection method's significant characteristic is its ability in fast detection (10 ms from the attack initiation); besides, this technique can achieve an accuracy rate of over 96.5%.

INDEX TERMS Cyber-attack detection, wavelet transform, wavelet singular entropy, smart-island, false data injection attack, AC state.

NOMENCLATURES

$\mathbf{J}$	Jacobian matrix
$\hat{\mathbf{x}}$	Estimated state vector
$\mathbf{z}$	Measurement vector
$\mathbf{T_r}$	Threshold
$\mathbf{z_a}$	Injected manipulated data
$\hat{\mathbf{x}}_\mathbf{a}$	Defective estimated state
$\boldsymbol{\varepsilon}$	Measurement noise
$\mathbf{T_a}$	Time period
$\mathbf{J^s}$	Sub matrix of the Jacobian matrix
$\mathbf{J_{ji,:}}$	ji-th row of the Jacobian matrix
$\boldsymbol{\tau}$	Non-negative constant
$\mathbf{x_i}$	State of system
$\mathbf{W_i}$	Constant bias in the manipulated states
$\boldsymbol{\beta_i}$	Constant coefficient
$\boldsymbol{\vartheta}$ (t)	Scaling function
$\boldsymbol{\alpha_k}$	Nonzero singular values
$\mathbf{Q}$	Diagonal matrix
$\mathbf{P_k}$	Probability
$\mathbf{h(0)}$	Utility's information about the smart island grid
$\mathbf{z_t}$	Real-time measurements

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

$\mathbf{u}$	Controller's input signal
$\mathbf{V_{INV}}$	Inverter output voltage (V)
$\mathbf{V_{dc}}$	The voltage of the uninterruptible power supply (V)
$\mathbf{V_o}$	Capacitor voltage (V)
$\mathbf{I_L}$	Inductive current (A)
$\mathbf{I_c}$	The output current of the capacitor (A)
$\mathbf{I_o}$	The output current of the filter (A)
$\mathbf{C_f}$	The capacitor of the filter (μF)
$\mathbf{L_f}$	Inductive of the filter (mH)
$\mathbf{S_V}$	Switching surface of voltage
$\mathbf{x}$	Smart island voltage (V)
$\mathbf{x_{base}}$	The base voltage of Smart Island (V)
$\mathbf{S_I}$	Switching surface of the current
$\mathbf{y}$	Smart island current (A)
$\mathbf{y_{base}}$	The measured base current of smart island loads (A)
$\mathbf{E}$	An edge that links 2 nodes
$\mathbf{x_j}$	Load node
$\mathbf{x_k}$	Adjacent node
$\mathbf{Z_{jn}}$	Exchanged data between two consequent nodes
$\mathbf{L}$	Laplacian matrix
$\mathbf{deg(m_j)}$	Degree of j^{th} node
$\mathbf{M}$	Total number of the system's agents
$\boldsymbol{\mu}$	Positive parameter
$\mathbf{c}$	Constant parameter

LIST OF ABBREVIATION

SIs	Smart Islands
SE	State estimation
WSE	Wavelet singular entropy
MG	Micro-Grid
SI	Smart Island
DG	Distributed generation
RESs	Renewable energy resources
SCADA	Supervisory Control and Data Acquisition
AESs	All-electric ships
FDIA	False data injection attack
DSE	Dynamic state estimation
RCKF	Robust Cubature Kalman Filter
CKF	Cubature Kalman Filter
DNN	Deep neural network
WT	Wavelet transform
SVD	Singular Value Decomposition
BDD	Bad data detection
RTUs	Remote Terminal Units
LASSO	least absolute shrinkage and selection operator
UPS	Uninterruptible Power Supply
Pos	Positive
Neg	Negative
CRR	Correct Reject Rate
HR	Hit Rate
FAR	False Alarm Rate
MR	Miss Rate
TP	True positive
TN	True negative
FP	False-positive
FN	False-negative
DSP	Digital signal processing
FPGA	Field-programmable gate array

I. INTRODUCTION

To deliver electricity to remote areas with isolated communication, transmitting electricity is not economically efficient or having technical complications, supplying power in a stand-alone mode microgrid (MG) is a reasonable solution. In the Smart Island (SI) configuration, voltage and frequency control, as well as cyber-attack and fault detection and protection, are performed by distributed generation (DG) units [1], [2]. SI can solve integrate renewable energy resources (RESs), modern controllable electric loads, and storage devices into an islanded MG [3], [4]. Operating of these units in the AC paradigm is a practical choice to improve its efficiency. Compared to the centralized communication scheme, to avoid a single point of failure, applying distributed controllers' approach is a technical way to enhance MGs' robustness and stability [5], [6]. The distributed control method requires transmitting a lesser amount of data and less traffic in communication links than the integrated communication approach [7]. Cooperative secondary controllers in MGs have been applied for purposes such as regulation of average voltage, proportional load-sharing, and energy balancing [8], [9]. High-level functions such as unit commitment and global optimization algorithms can be performed in conventional central approach with supervisory control and data acquisition (SCADA) that offers an efficient integration of crucial subsystems [10]–[13]. While there is full access to system data, centralized control functions such as optimal control are used to attain objectives like greenhouse gas emission reduction for all-electric ships (AESs) and dynamic power management under security contingencies [14], [15]. However, centralized control schemes can be subject to single-point failure that may be attacked in physical and/or cyber forms [16]. Due to the absence of reliable encryption in communication protocols and lack of firewalls because of latency concerns, the SCADA communication networks are exposed to cyber-attacks [17]. As MGs employ control systems with existing commercial computing platforms that have been subjected to cyber-attacks and many of them are far from land and require lengthy connection links, to avoid these threats, they require serious attention [18].

A. BACKGROUND

Generally, the primary purpose of developing the protection and security in a large-scale network is to improve the performance of the individual sensors of the system. In theory, employing an authentication process to sensor networks can be the central revocation of any compromised node; but it would be challenging to implement due to the computation and storage constraints [19]. Existing studies in this subject are mostly focused on the secure control theories based on state estimation methods, developed

techniques to detect an abnormality and networking security of cyber elements [20], [21]. In this way, a detailed analysis of cyber-attack detection methods in power grids has been presented in reference [22]. The most significant challenge among cyber-attacks that destroys state estimation is false data injection attack (FDIA) [23]. Unlike other cyber-attacks (distributed rejection of service and clogging attacks), FDIA can avoid the current detection methods that are residual-based insufficient data [10]. Hence, obtaining advanced detection mechanism is necessary to prevent multiple FDIA occurrences, that involve serious risks to the grid [24]. A great deal of research effort is often concentrated on examining possible ways to build FDIA. These works mainly focus on power systems that contain DC state estimation under various situations because of the system's straightforward investigative models [23]. For example, one frequently identified power system cyber-attack scenario is that the opposition does not have enough configuration data of the network, and thus, a partial set of variables can be manipulated [25]. Conventional detection methods are not adequate in preventing FDIA; therefore, the system is at risk of malicious data injection. In recent years, FDIA targeting AC state estimation has been a subject of research interest and to construct such cyber-attacks, analytical studies are performed. FDIA construction methods in AC state estimation system where there is partial or complete knowledge of the system have been presented in [26]. There are many techniques with satisfactory performance such as statistical methods [23], [27], Kalman filter [28], [29], network theory [30], state forecasting [21], sparse optimization [31], machine learning [32] and time series simulation [33] applied for FDIA in DC state estimation. However, as the FDIA detection methods in DC state estimation do not detect AC FDIA, there is a lack of research on the AC form paper [26]. The AC FDIA detection scheme proposed in [28] was developed on the Kullback-Leibler distance from the compromised system states' probability distribution from the nominal operating conditions. The robustness of the suggested scheme in typical power system incidents such as a change in load distribution is undetermined. In new attack methods, the manipulated system states still comply with Kirchhoff's circuit laws to pretend to be typical changes in operating condition that make it harder to be detected [26]. To detect AC FDIA, a state estimation scheme based on information network is proposed in [31]. Assuming an AC FDIA attack with complete information of power network, the transmission line parameters are vigorously changed in reference [34] and the AC FDIA detection is performed.

For having dynamic state estimation (DSE) of generator units under cyber-attacks, A robust Cubature Kalman Filter (RCKF) method has been presented in reference [35]. At which the first stage, two different models of cyber-attacks including FDIA and denial of service attacks (DSA) were simulated and besides that presented into DSE of the generator with mixing the attack vectors by the measurement information; and second, under having cyber-attacks with various degrees of sophistication, the RCKF method and the CKF method were adopted to the DSE; finally, the performance of these presented methods have been compared and analyzed. In reference [36] also other forms of FDIA detection techniques for AC-SE were presented. In this method, when the state vectors manipulated malicious datum, their temporal and spatial data solidarities might stray from those in common operational situations. The presented approach could capture these inconsistencies by assessing temporally sequential estimated system states by utilizing wavelet transform (WT) and deep neural network (DNN) algorithms.

B. MOTIVATION AND MAIN CONTRIBUTION

In this paper, considering recent AC-FDIA patterns, a novel FDIA detection technique is developed. To detect attacks, unlike previous FDIA detection methods which just implement the spatial data features in the state during a single time interval, the proposed technique is based on wavelet singular entropy (WSE) that uses WT data correlation that is introduced in successive system states.

This proposed technique combines both benefits of singular value decomposition (SVD) [37], Haar wavelet transforms [38] and spectrum entropy [39] to obtain the system state elements in a period. This WSE technique shows decent performance in cyber-attack detection in AC-SIs. Current and voltage signals are gained at the relay point, then via sliding mode controller scheme; the switching surface (error signals based on the base signal) is calculated. Afterwards, it is analyzed using Haar WT to retrieve the detailed coefficients. Next, to estimate the singular value from the comprehensive coefficient matrix, the SVD technique is applied and finally to detect cyber-attack, WSE of the signals are computed. WSE technique goal is to obtain the system state elements in a time interval and define a threshold that can distinguish between the normal power system operation incidents and AC-FDIA. The key contributions of this paper are itemized as:

- This study is one of the pioneering researches works for applying WSE in FIDA detection.
- The presented technique goal is FDIA detection in AC state estimation of the latest attack models by partial power grid data [26].
- The WSE detection method is assessed with a recently proposed FDIA pattern on SI test cases, and satisfactory performance with acceptable precision and false alarm rate is demonstrated in the simulation results.
- To assess the performance of the presented technique, a parameter sensitivity analysis is presented.

C. PAPER STRUCTURE

The reminder of this research is arranged as follows. Section II introduces the SE methods and their sensitivity to FDIA. The proposed FDIA detection mechanism and WSE are explained in Section III. Section IV illustrates the simulation results on the examined SI with different case studies. Finally, this research article is concluded in Section V.

II. CONCEPTS OF FALSE DATA INJECTION ATTACKS AND SE METHOD

Firstly, in the current section, a brief introduction of the state estimation way via the utilities and the integrated bad data detection (BDD) technique is given. After that, a typical model of effective AC FDIA is described.

A. ATTACK STATEMENT

Conventionally, the state estimation procedure's precision through BDD methods is validated via computing the L-norm of measurement remnant [40].

$$\left\| z - J\hat{x} \right\| > T_r \tag{1}$$

where, $J \in R^{N*D}$ is the Jacobian matrix, $\hat{x} \in R^D$ represents the estimated state vector and $z \in R^N$ is the measurement vector. To maintain state estimation accuracy, the threshold T_r is defined. Beside their shortcoming of current BDD techniques in cyber-attack detection, these approaches are impractical for smart grid application due to the required measurement redundancy. Intelligent cyber-attacks, particularly FDIA attacks aim for controlling some of the actions and altering the state variables randomly that may be performed with a false data vector injection $z_a \in R^N$ to evade traditional BDD schemes. Assume the meter readings by z_a are maliciously attacked, so be manipulated so the attack suffered measurement adjustment can be written as

$$z = J\hat{x} + z_a + \varepsilon = J\left(\hat{x} + c_a\right) + q_a + \varepsilon, \hat{x}_a = \hat{x} + c_a \tag{2}$$

where, $\hat{x}_{\mathbf{a}}$ is the defective estimate state, te and $\boldsymbol{\varepsilon}$ represent the measurement noise. The injected manipulated data (z_a) can be decomposed into two elements $a = Jc_a$ and q_a is the only term which is detectable and compromises the corresponding space where: $J(J^TJ)^{-1}J^Tq_a = 0$.

Notably, the attack vectors ($\mathbf{z_a}$) can be constructed even though the rival can partially access the lines' parameters and network topology. Here, malicious attack construction absolutely lies in (J), i.e., $q_a = 0$, thus it can bypass the available BDD schemes [41].

As in the power network context, it is not convincing to assume simultaneous faulty measurements of all the sensors; it is considered that the attacker has just partial supplies and can balance some measurement values that can be for power flow or power injection data for a period $T_a \subseteq T$.

Realistically, acquiring full information of the system is not possible for an outsider and manipulating all the measurement readings escalates the cost and effort for attackers. Therefore, it is a working assumption that attackers have limited information of the system topology attained by statistical analysis of the data that is physically captured from the security information that is embedded in a node or by the data transferred between remote terminal units (RTUs) and the corresponding power control center.

To present the secure measurement, through the decomposition of the Jacobian matrix (J) in a row-wise tactic, a submatrix $J^s = (J_{ji,:}, J_{jN-|S|,:})$, is created; Where $J_{ji,:}$ is the ji-th row of J, which $J^sc_a = 0$. Likewise, submatrix J^A is built for measuring the attack. Finally, the attack plan is characterized as an optimization problem to find a solution c_a as follows

$$\begin{aligned} &\text{Minimize} \left\| J^A c_a \right\|_0 \\ &\text{Subject to } J^s c_a = 0, \\ &\qquad \|c_a\|_\infty \geq \tau \end{aligned} \tag{3}$$

where τ is a non-negative constant $\tau \geq 0$, the expressed optimization problem in (3) is solved by applying the least absolute shrinkage and selection operator (LASSO) and Regressor Selection algorithms [42].

As mentioned earlier, attackers aim to hack into the communication network to manipulate controller and sensor through FDI attack. For the distributed generator i, $\forall t \epsilon T_a$, the FDI attack's effect on the state of the system may be stated as

$$x_i^a(t) = x_i(t) + \beta_i x_i(t) + W_i \tag{4}$$

where W_i stands for a constant bias in the manipulated states and the β_i is a constant coefficient. In other word, attackers intend to modify the system states by β_i and W_i in such a way that the operator and existing BDD methods do not observe the attack vector. In the experiments, we presume that there is access to k measurements by attackers. Then k measurements are arbitrarily selected to create a k-sparse attack vector.

III. PROPOSED TECHNIQUE FOR DETECTION OF FALSE DATA INJECTION ATTACK

As expressed in Section II, due to the attackers' strategy to construct false data in such a way that satisfies Kirchhoff's circuit laws [26], well-built FDIA can avoid to be recognized by the existing BDD mechanisms in AC state estimation. Hence, distinguishing FDIA from regular SI incidents provided measurements from the identical sampling period is impossible for the operators; however, FDIA is not entirely unrecognizable. In SIs, over a time, synchro-phasor data is studied as temporal-spatial matrix/tensor. This would be commonly assumed which the data obtain spatial dependencies, were characterized by Kirchhoff's Laws. There is a temporal correlation among successive time slots in a power system, particularly the dynamic operations caused by the system's inertia. Existing FDIA constructions concentrate on creating attack vectors that satisfy the spatial correlation of AC power flow equations and the system variables, i.e. (2) [26] while the temporal dependence between successive states of the system, or SI dynamics is ignored. Thus, to discover FDIA occurrence while avoiding false alarms on regular incidents, this correlation can be employed in the system states. These methods are based on the proposed online FDIA detection technique that applies recent wavelet singular entropy methodologies. Therefore, in this work, the configuration and data of the suggested technique is elaborated, and then the detailed execution is stated in the rest of this section. Finally, the threshold of detection processes of the presented online FDIA detection technique is discussed.

A. WAVELET SINGULAR ENTROPY

1) WAVELET TRANSFORM THEORY

The proposed technique applies wavelets as practical tools in analyzing a signal that chops data, and after that, it translates and measures various versions of a signal function [43]. Harr wavelet that is the easiest wavelet tool, is characterized as:

$$haar\left(2^q+\delta,\emptyset\right)=\begin{cases}\sqrt{2^q}; & \delta/2^q\le\emptyset\le(\delta+0.5)/2^q\\ -\sqrt{2^q}; & (\delta+0.5)/2^q\le\emptyset\le(\delta+1)2^q\\ 0; & otherwise\end{cases}\quad(5)$$

where q = 1, 2, …. and $\delta = 0, 1, \ldots, 2^q - 1$

Next, if δ =0 and $2^q = 1$, then the Harr wavelet is

$$\Psi(\emptyset)=\begin{cases}1 & for\ 0\le\emptyset\le 0.5\\ -1 & for\ 0.5\le\emptyset\le 1\\ 0 & otherwise\end{cases}\quad(6)$$

where ϑ (t) is the scaling function [44] as follows:

$$\vartheta(\emptyset)=\begin{cases}1 & for\ 0\le\emptyset\le 1\\ 0 & otherwise\end{cases}\quad(7)$$

Typically, WT comprises band-pass filters series which include consecutive couples of high-pass and also low-pass filters. The specifications are high-frequency but low-scale components for high-pass and low-pass filters, whereas approximations can be low-frequency high-scale ones. Approximations and aspects are taken from the matrix of the WT coefficient are necessary.

B. SINGULAR VALUE DECOMPOSITION

Singular value decomposition (SVD) can be defined as a matrix decomposition way that breaks a matrix to three matrices. Assume $B_R \epsilon C^{m*n}$ and α_k (B_R) (k = 1, . . . , r ≤ min{m, n} become the nonzero singular values of B_R, hence according to [45], the SVD can be characterized as:

$$B_R = UQV^{T}\quad(8)$$

where: $U\epsilon C^{m*r}$, $V\epsilon C^{n*r}$ and $Q\epsilon C^{r*r}$, which Q defines a diagonal matrix as:

$$Q=\begin{bmatrix}\alpha_1 & 0 & \ldots & 0\\ 0 & & & \vdots\\ \vdots & & \alpha_k & 0\\ 0 & \ldots & 0 & \alpha_r\end{bmatrix};k=1,..,\quad(9)$$

Then in $F\epsilon C^{1*r}$ …matrix 'F' has made by diagonal elements 'Q'; so 'Q' is provided as:

$$F = diag[Q] = [\alpha_1\alpha_2\ldots\alpha_{r-1}\alpha_r]\quad(10)$$

where $\alpha_1 \ge \alpha_2 \ge \ldots \ge \alpha_{r-1} \ge \alpha_r > 0$ an…α_k (k= 1, ... ,r) represent the nonzero…singular values for the matrix B_R.

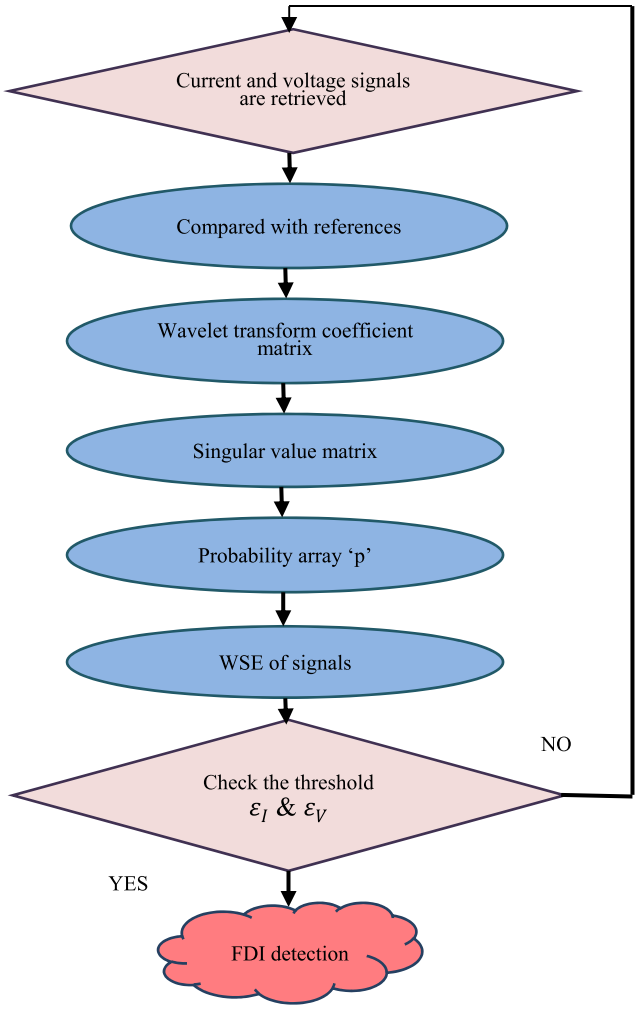

FIGURE 1. Suggested FDIA detector.

C. SHANNON ENTROPY

The concept of Shannon entropy in time domain defines a crucial measurement of signal uncertainty employed to assess patterns and structures of analyzed data. Hence, wavelet entropy-based signal analysis can indicate the signal in both time and frequency domains.

According to reference [46] and considering. '$\alpha_k{}'$, the probability is stated as follows:

$$P_k=\frac{\alpha_k}{\sum_{j=1}^{r}\alpha_j}\quad(11)$$

Finally, the entropy is planned as:

$$WSE=-10\sum_{k=1}^{r}(P_k*\ln P_k)\quad(12)$$

D. MECHANISM OF PRESENTED FDIA DETECTION

The presented FDIA detection technique is displayed in Figure 1. System states and measurements from consecutive sampling intervals, for example, time samples when performing standard state estimation, are considered in this method. These time intervals length may be anywhere from milliseconds to a few seconds. At an arbitrary sampling time

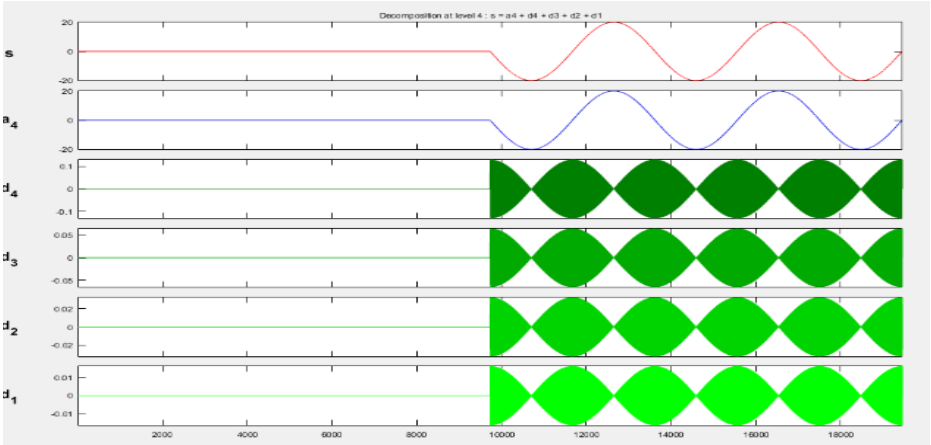

FIGURE 2. Wavelet decomposition levels (d1…, d4) of switching surface according to the sliding mode controller of voltage signals during cyber-attack conditions (cyber-attack has occurred at t = 1 s.)

interval t, the utility's information of the SI grid *h(0)* and real-time measurements z_t are the inputs to the mechanism, and the detection results are its output. First, the input data is fed to an AC state estimator that calculates the estimations of current and voltage system state as $\hat{x}_t$. Next, the estimated state is examined by BDD to trim any measurements manipulated by bad data. Then, as the bad data affected by communication error and sampling do not comply with the circuit laws and leave high residual values, they can be effectively detected [40].

The next step after the SE process is to apply a new FDIA detection procedure to provide additional analysis on the estimated system states. As illustrated in Figure 1, the detector comprises two data processing procedures. The estimated states of the $\hat{x}_t$ the system is taken from the prior state estimator as input. Also, the system state is saved in a database of state history. An attribute extractor determines the spatial data solidarities (details) of the previous system states. Then the following data implied by WSE is saved in a feature history database. Next, through the defined threshold, the WSE of the signals is applied FDIA attack detection. In the proposed FDIA detector model, it is apparent that the detection technique efficiency is affected by the attack detector and feature extractor. Two parts of the detection procedure should develop the state dynamics' distinctive spatial-temporal features and accurately classify attack incidents against others. In this paper, extracting the attack features is performed by WT algorithm that has excellent feature extraction capability [42]. SVD components are adopted to build a nonzero singular value to compute WSE then use a threshold to detect attack models from the extracted features.

We can observe from equations (6) and (7) that various wavelets and levels of decomposition 'm' could cause multiple factors of the decomposed signal. These factors will have more impact on the element extraction sufficiency of the feature extractor based on WT. So, they need an optimal setting for 'm' values and wavelets; however, it is not practical to examine all wavelets. Alternatively, they can be picked according to the properties of data and strategically [47], [48]. In particular, suppose there are sufficient data samples, because of their strength regardless of specific data characteristics, *db* and *sym* families of wavelets are influential.

Further, the wavelets, such as *bior* and coif members, struggle with longer filter length that can cause low amounts of decomposition and insufficient element extraction [47]. Thus, in this paper, 4 different wavelets of db and sym members are applied to decompose the input signal, including bus voltage and current. Figure 2 shows the wavelets and their corresponding M values. In general, the decomposed data series are very lengthy to be applied in subsequent computations. It has been illustrated that the crucial characteristics of the input signal can be represented via the statistical features of these data sequences [48]. Therefore, all factors' mean value and standard deviation are implemented to characterize the input signal's quality in our suggested feature extractor. The efficiency and proficiency of these statistical features in classified tasks are demonstrated in the literature [47], [48]. Subsequently, in an N bus SI and for each system state, coefficients, bus voltage and current features are computed and stored in the feature history database as a typical feature vector of the corresponding time interval (see Figure 1). In this paper, the WSE algorithm input comprises 200 samples. Besides, the WSE algorithm can be vulnerable to the magnitude altering frequency in the signal so that every alternation due to a cyber-attack causes a change in the signal frequency and can be detected by WSE. Figure 1 shows the wavelet singular entropy mechanism. The proposed FDIA method and SI are simulated in the MATLAB/Simulink environment, demonstrating and performing the technique.

IV. CASE STUDIES

A. CYBER-PHYSICAL MODEL

An Islanded MG with m parallel connected generators is shown in Figure 3. Some of the generation units in such MG can be divided into voltage and frequency mode, also can stabilize the MG voltage while other components are in load sharing state and current control mode [8]. The power electronic circuit of a 3-phase inverter connected to the MG is illustrated in Figure 4. In this work, first, we consider

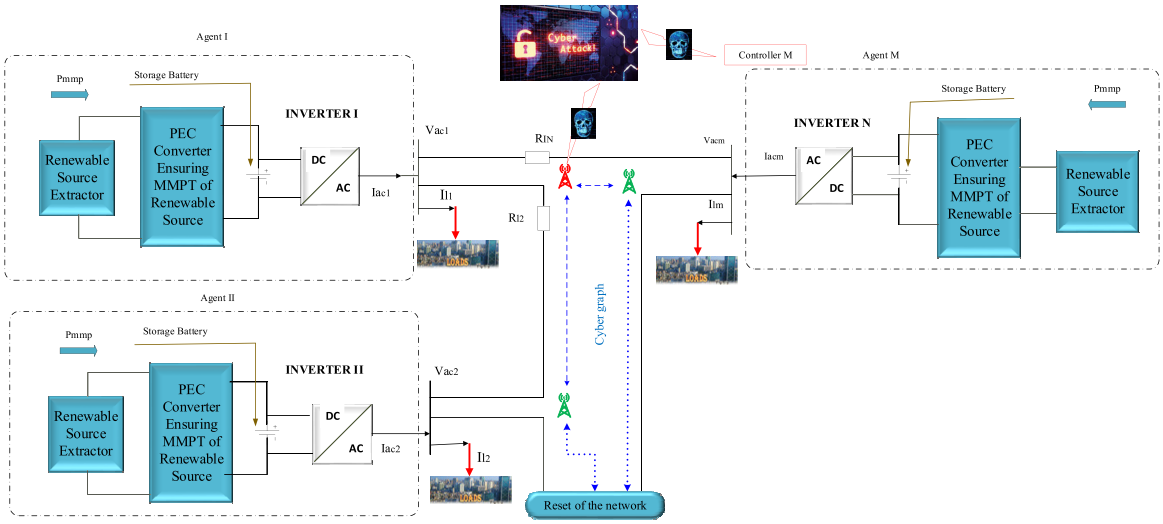

FIGURE 3. Standard cyber-physical paradigm of an AC Smart-Island where Blue arrows correspond to the cyber layer and black lines correspond to the physical circuit.

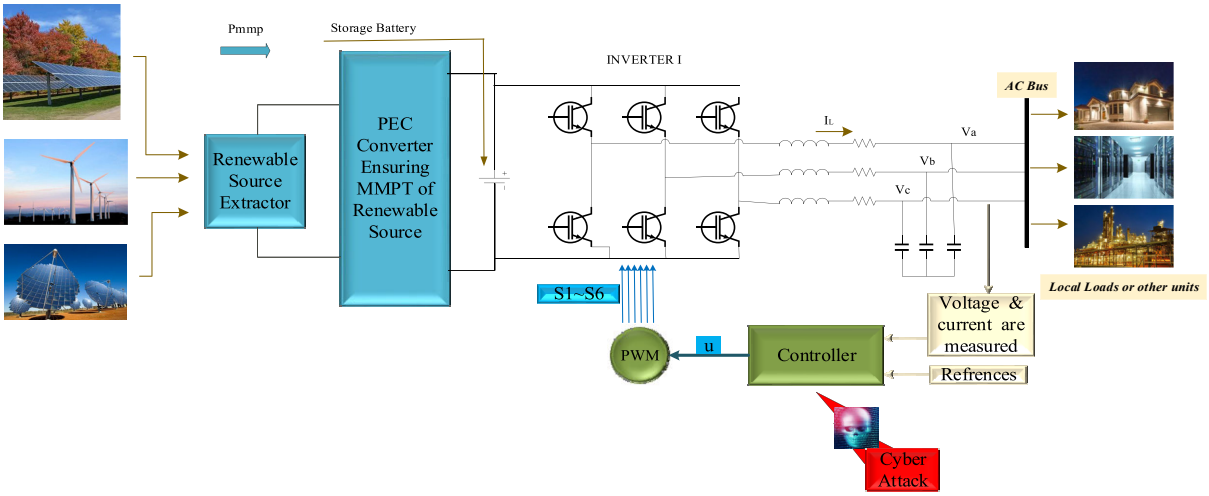

FIGURE 4. Generic scheme of a 3-phase microgrid in front of cyber-attack.

the single-phase system; next, we generalize the formulation to the 3-phase system where all phases have similar parameters. Figure 5 indicates the block diagram of a single-phase inverter. As illustrated in Figure 5, the output filter decreases the harmonics in the output voltage caused by PWM inverter.

For the single-phase inverter demonstrated in Figure 5, the state equations areas:

$$L_f \frac{dI_L}{dt} + V_o = V_{INV} \tag{13}$$

$$I_L = I_c + I_o, I_c = C_f \frac{dV_o}{dt} \tag{14}$$

where u is the controller's input signal, and $V_{INV} = uV_{dc}$ is the inverter output voltage. Combining equations (13) and (14) will result in:

$$\frac{d}{dt}\begin{bmatrix} V_o \\ \dot{I}_L \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{C_f} \\ -\frac{1}{L_f} & 0 \end{bmatrix}\begin{bmatrix} V_o \\ I_L \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{V_{dc}}{L_f} \end{bmatrix} u + \begin{bmatrix} -\frac{I_o}{C_f} \\ 0 \end{bmatrix} \tag{15}$$

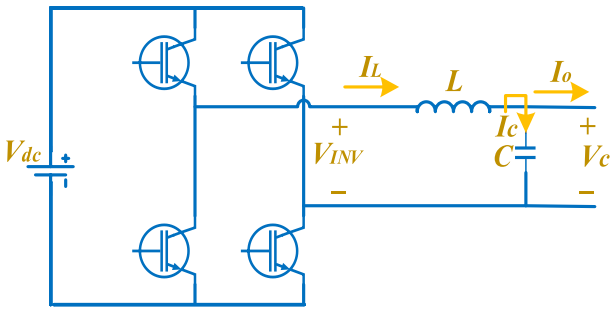

FIGURE 5. A full-bridge, single-phase inverter.

where V_{dc} is the voltage of tUninterruptibleble Power Supply (UPS) and the state variables are the capacitor voltage (V_o) and the inductive current (I_L). The output current of the capacitor and the filter are I_c and I_o, respectively. L_f and C_f are the inductive and capacitor of the filter, respectively.

According to reference [8], through the sliding mode controller, the index of cyber-attack detection for FDIA in

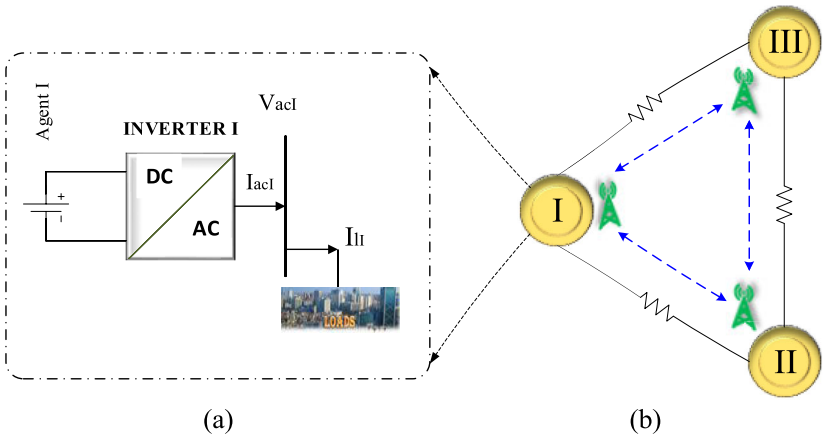

FIGURE 6. (a) Agent type and (b) Cyber-physical AC Smart-Island including 3 resources.

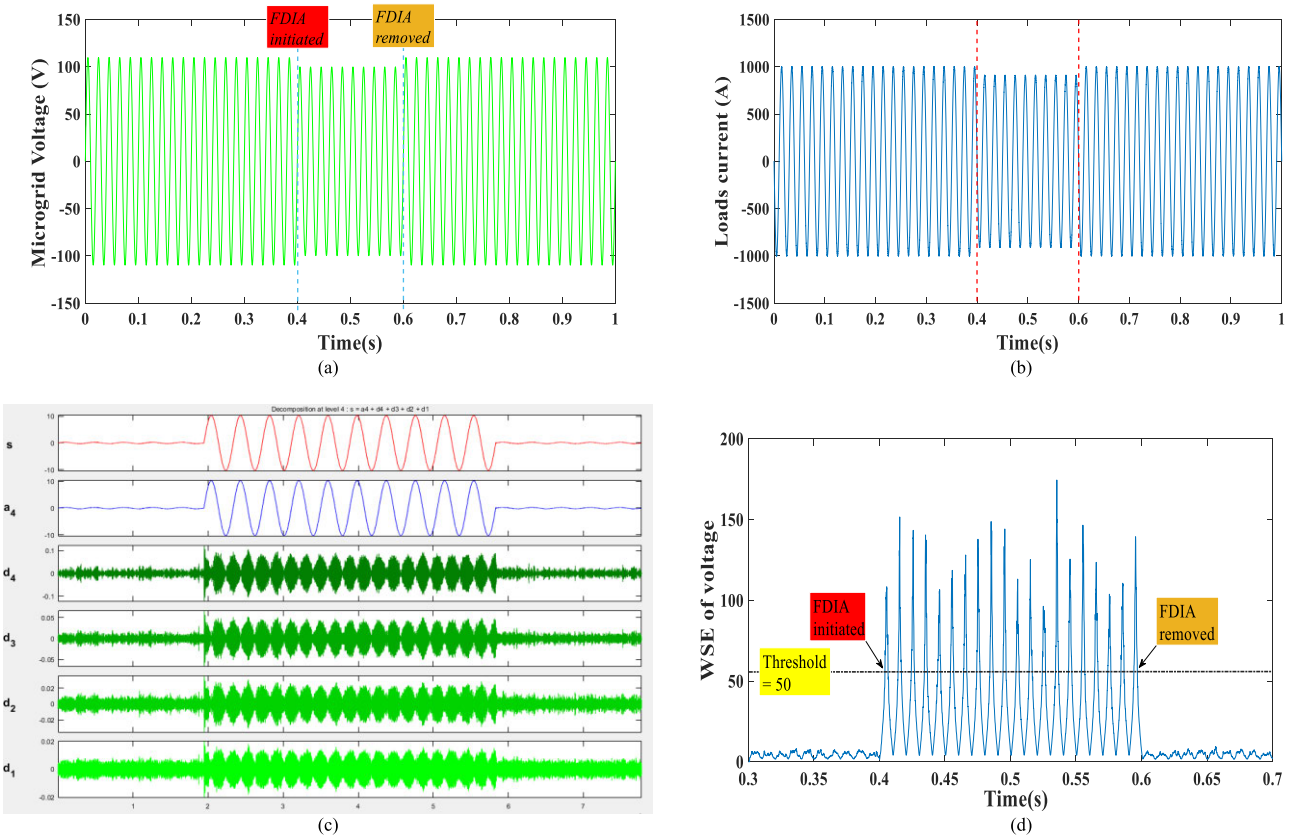

FIGURE 7. Instability caused by injecting an attack by altering the amplitude of the signal of voltage reference including a) Smart Island voltage, b) Load current, c) Wavelet decomposition, d) WSE of voltage where cyber-attack is happened at t = 0.4 s and is removed at t=0.6 s.

current and voltage parameters can be provided as:

$$S_V = \tilde{\tilde{x}} - \lambda\tilde{x}, \tilde{x} = x - x_{base} \tag{16}$$

where S_V (switching surface of voltage) represents the index of voltage to detect cyber-attack which input of wavelet transforms, and λ gives a positive number, x represents the SI voltage and x_{base} is the base voltage of SI that has a constant amplitude and frequency.

$$S_I = y - y_{base} \tag{17}$$

where S_I (switching surface of current) represents the current index to detect cyber-attack which input of wavelet transforms, y is the SI current generated by each distributed generator and y_{base} is the measured base current of SI loads.

Figure 3 shows the autonomous AC-SI considered in this work. DC sources connected through DC/AC inverters are inter-connected via tie-lines, thus comprising the SI physical layer. Inverters are operated to sustain the output voltage following the reference values produced through the local initial and secondary controller. A cyber graph of the communication network studied here transfer data to and from adjoining networks. In each unit, loads are coupled at the output of the converter.

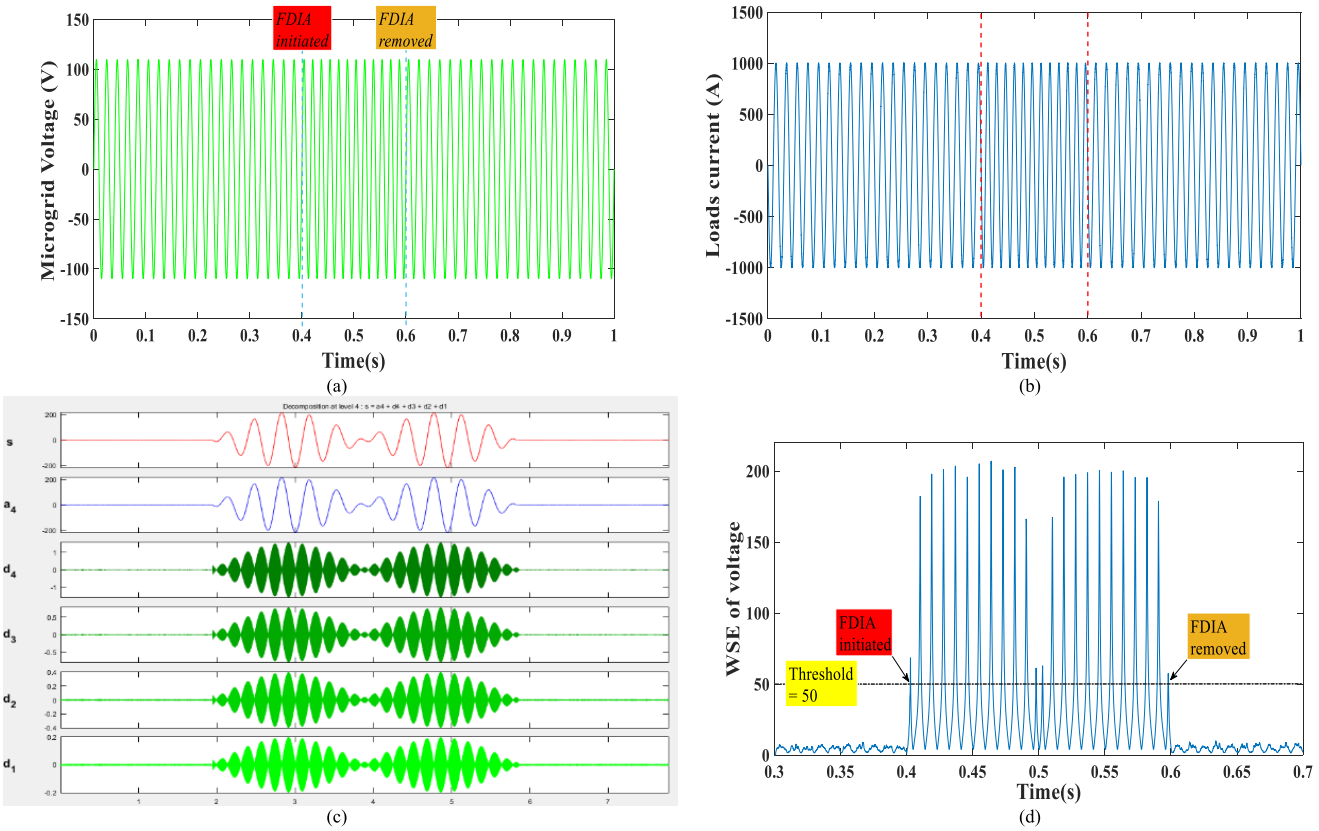

FIGURE 8. Instability caused by injecting an attack by altering the frequency of the signal of the voltage reference including a) Smart Island voltage, b) Load current, c) Wavelet decomposition, d) WSE of voltage where cyber-attack is happened at t = 0.4 s and is removed at t=0.6 s.

The communication network can be considered as digraph via links and edges with the adjacency matrix $A = [a_{jk}] \epsilon R^{M*N}$, and every source becomes an agent. The connection weights are:

$$a_{jk} = \begin{cases} > 0, & if\ (x_j, x_k)\ \epsilon E \\ 0. & else \end{cases} \tag{18}$$

In equation (18), E provides an edge that links 2 nodes, x_j represents the load node and x_k is the adjacent node. The communication weights only represent exchanged data between two consequent nodes that are indicated by the matrix with incoming data, $Z_{jn} = \sum j \epsilon M^{a_{jk}}$.

Thus, these 2 matrices match up each other, thus the Laplacian matrix L will be balanced, where $L = Z_{jn} - A$ and its components are provided as:

$$l_{jk} = \begin{cases} \deg(m_j), & j = k \\ -1, & j \neq k \\ 0, & otherwise \end{cases} \tag{19}$$

In equation (19), $L = [l_{jk}] \epsilon R^{MxN}$ and $\deg(m_j)$ is the degree of j^{th} node.

Remark I: all the units will attain consensus using $x(i+1) - x(i) = -\mu L x(i)$ for a well-spanned matrix L that $x_j(i) = c, \forall j \epsilon M$, where M provides the total number of the system's agents, μ is a positive parameter and c is constant.

V. NUMERICAL SIMULATION RESULTS

In this section, two systems are studied, and the simulation results are obtained and presented. Figure 6 shows two systems, including (a) agent type and (b) cyber-physical AC-SI with 3 resources.

As illustrated in Figure 6 (a), Smart-Island comprises three agents of the same capacities interconnected through resistive lines. Each of the agents in Figure 6(a) includes a battery and DC/AC inverters. As can be seen from Figure 6 (b), the cyber-attack detection technique proposed in this paper is examined on a cyber-physical AC SI with $V_{ref} = 110\sin(2*pi*60)$. The performance of the presented cyber-attack detection procedure in cooperative AC Smart-Island has examined applying multiple disturbances like FDIA, attack in various sensors that is likely to remain unrecognized by the distributed viewers, connection links to detect the distorted node so that the action is performed to obtain security. The control and system characteristics are given from the previous work [7]. To better understand the study, each incident in the scenarios is split by a specific time-gap.

A. CASE STUDY I

Here study, the attack is injected by changing the amplitude of the signal of a voltage reference, then the performance of WSE in FDIA detection is investigated by injecting the abovementioned attack.

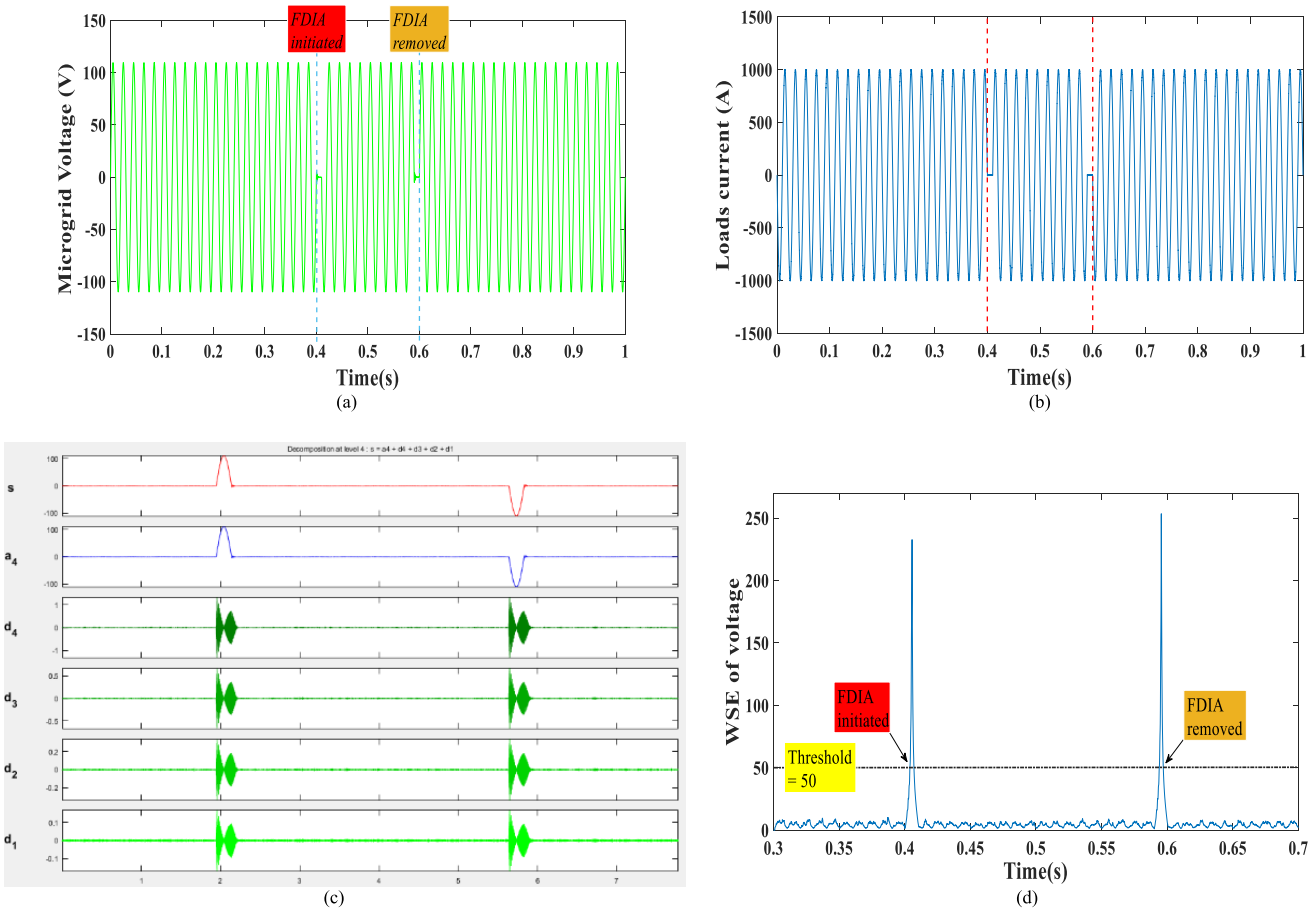

FIGURE 9. Instability caused by injecting an attack by shifting the voltage reference signal including a) SI voltage, b) Load current, c) Wavelet decomposition, d) WSE of voltage where cyber-attack is happened at t = 0.4 s and is removed at t=0.6 s.

At time t=.4 s, FDIA is started, and at t=.6 s, FDIA is cleared. It should be noted that under the attack influence, the reference voltage amplitude of the controller is reduced by 10%. Figure 7 shows the results of a simulation. Figure 7(a) and (b) demonstrate the SI's voltage and the current load, respectively. The wavelet transforms of the voltage sliding surface signal, and wavelet decomposition at various levels has been displayed in Figure 7(c). To get a practical singular value applied to compute the WSE for cyber-attack detection, the wavelet factors (d1…,d4) have been employed as shown in Figure 7(d), WSE of this scenario's signal considering the threshold as 50 successfully indicates the attack.

B. CASE STUDY II

Here study, the attack is injected by changing the frequency of the signal of the voltage reference and the performance of the WSE in FDIA detection is investigated.

At time t=.4 s FDIA is started, and at t=.6 s, FDIA is removed. It may be noted that the frequency of voltage is changed from 60 Hz to 50 Hz by cyber-attack in the controller reference signal. Figure 8 shows the simulation result for this scenario. The voltage of the SI and the loads current are displayed in Figure 8 (a) and (b), respectively. Figure 8(c) illustrates the wavelet transform of the voltage sliding surface signal and the wavelet decomposition at various levels. To acquiring practical singular values to compute the WSE to detect an SI attack, the wavelet coefficients (d1…,d4) are employed. Figure 8(d) shows WSE of the signal, and by selecting the threshold as 50, it can be viewed that the presented technique can successfully detect the attack.

C. CASE STUDY III

Here study, the attack is injected by shifting the signal of the voltage reference and the performance of the WSE in FDIA detection is investigated. At time t=.4 s, FDIA is started, and at t=.6 s, FDIA is cleared. Note that the cyber-attack shifts the SI output voltage in the controller reference signal. Figure 9 demonstrates the results of the simulation. Figure 9(a) and (b) show the smart grid's voltage and the load's current, respectively. Figure 9(c) illustrates the wavelet transform of the voltage sliding surface signal and wavelet decomposition at different levels. Figure 9(d) shows WSE of the signal in this case study, and by selecting the threshold as 50, the proposed technique successfully detects the mentioned cyber-attack.

D. CASE STUDY IV

Here, the attack is injected by adding white noise to signal voltage reference and the detection mechanism's performance. The attack is started at time t=.4 s and is cleared

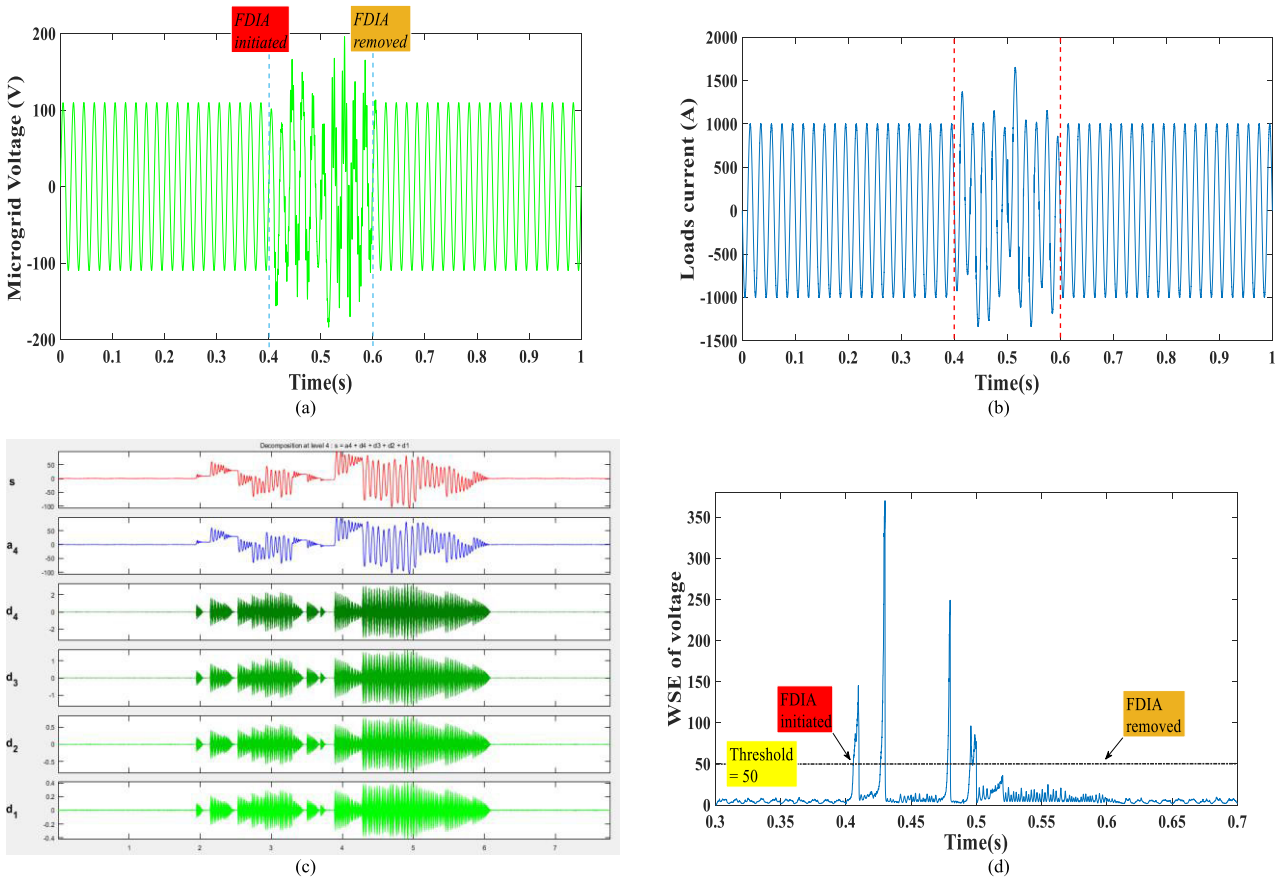

FIGURE 10. Instability caused by injecting an attack by plus noise with voltage reference signal including a) Smart Island voltage, b) Load current, c) Wavelet decomposition, d) WSE of voltage where cyber-attack is happened at t = 0.4 s and is removed at t=0.6 s.

at t=.6 s. Note that the white noise is added to the SI output voltage in the controller reference signal. Figure 10 shows the simulation results. In this scenario, Figure 10(a) and (b) illustrate the smart grid's voltage and the load's current, respectively. Figure 10(c) shows the wavelet transform of the voltage sliding surface signal and the wavelet coefficients at various levels. The wavelet coefficients (d1…d4) are applied to maintain efficient singular values employed to calculate the WSE for attack detection. Figure 10 (d) shows WSE of signal in this scenario, and by selecting the threshold as 50, it may be noticed that the presented technique can successfully detect the attack.

E. CASE STUDY V

In this scenario, the attack is on the voltage signal, and the detection technique's proficiency is examined. The attack is started at time t=.4 s and is cleared at t=.6 s. Figures 11 and 12 show the simulation results.

Here study, Figures 11(a) and 12 (a) show the voltage of SI. Figures 11(b) and 12(b) show the loads current. Figures 11(c) and 12(c) illustrate the wavelet transform of voltage sliding surface signal and the wavelet coefficients at various levels. The wavelet coefficients (d1…d4) are applied to maintain efficient singular values employed to calculate the WSE for attack detection.

Figures 11 (d) and 12 (d) show the WSE of signal in this scenario, and by selecting the threshold as 50, it can be noticed that the suggested technique can successfully detect the attack.

F. CASE STUDY VI

The performance and capability of the WSE in the attack caused by altering the load reference current signal on agent II and III are examined in this case study.

At t=.4 s, FDIA is started, and at t=0.6 s, FDIA is cleared. Note that during this attack, the controller's reference current amplitude is increased by 20%. Figure 13 shows the simulation result. Here, study, Figures 13(a) and 14(a) show the SI voltage, Figures 13(b) and 14(b) show the loads current, and Figures 13(c), (d) and (e) and 14(c), (d) and (e) display the current of DG1, DG2 and DG3, respectively. It can be seen that during the attack, the delivered current by each DG is increased, but the load is constant. Figures 13(f) and 14 (f) show the wavelet decompositions at various levels. The wavelet coefficients (d1…d4) are employed to maintain efficient singular values applied to calculate the WSE for attack detection. Figures 13(g) and 14(g) show WSE of this scenario signal, and by selecting the threshold as 20, the proposed technique successfully detects the cyberattack.

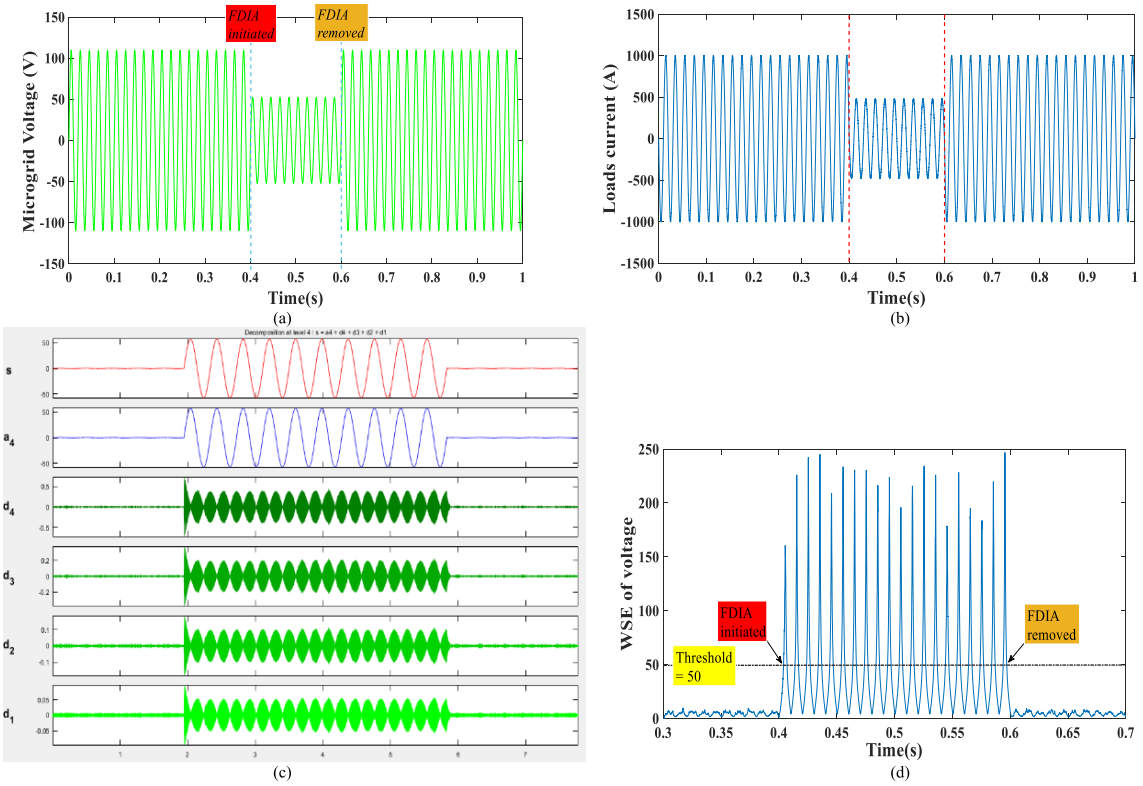

FIGURE 11. Instability caused by injecting an attack on voltage sensor (Smart Island voltage reduced) including a) SI voltage, b) Load current, c) Wavelet decomposition, d) WSE of voltage where cyber-attack is happening at t = 0.4 s and is removed at t=0.6 s.

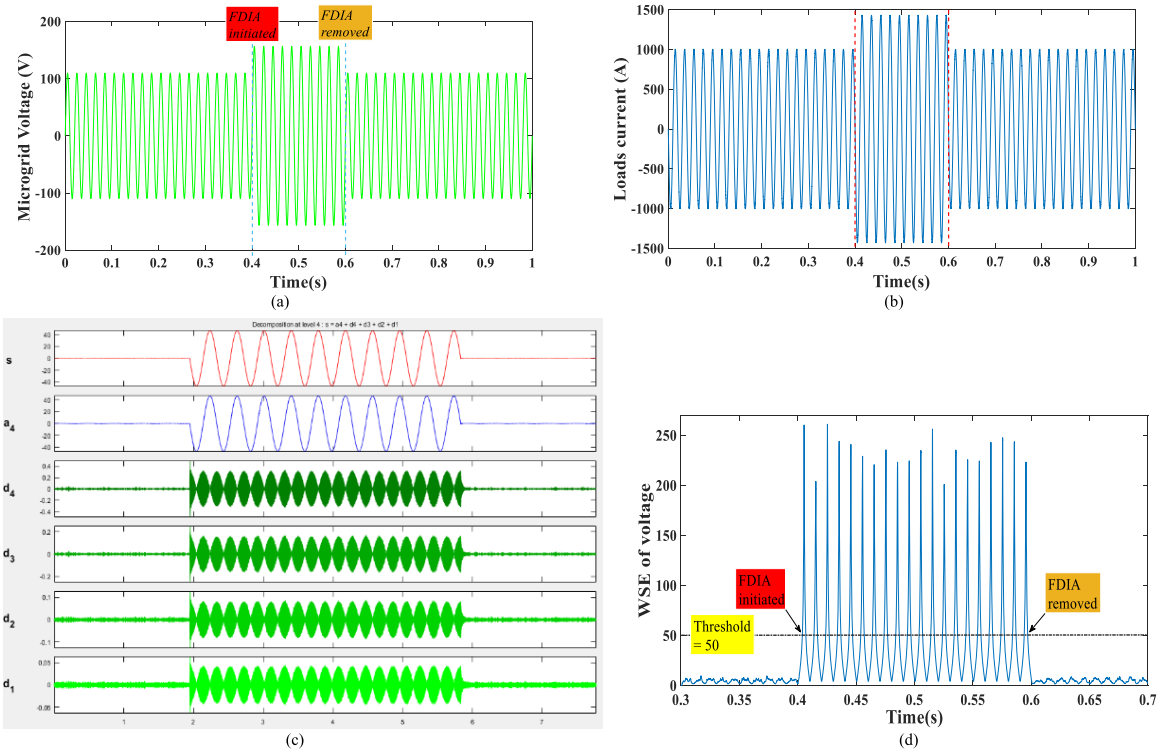

FIGURE 12. Instability caused by injecting an attack on voltage sensor (SI voltage increased): a) Smart Island voltage, b) Load current, c) Wavelet decomposition, d) WSE of voltage where cyber-attack is happening at t = 0.4 s and is removed at t=0.6 s.

G. CASE STUDY VII

Here study, the attack is injected into the current sensor to deteriorate the current sharing profile on agent II and III. At t=.4 s, FDIA is started, and at t=.6 s, FDIA is cleared. Note that the measured current of the Smart-Island affected by this kind of cyber-attack on its corresponding sensor has

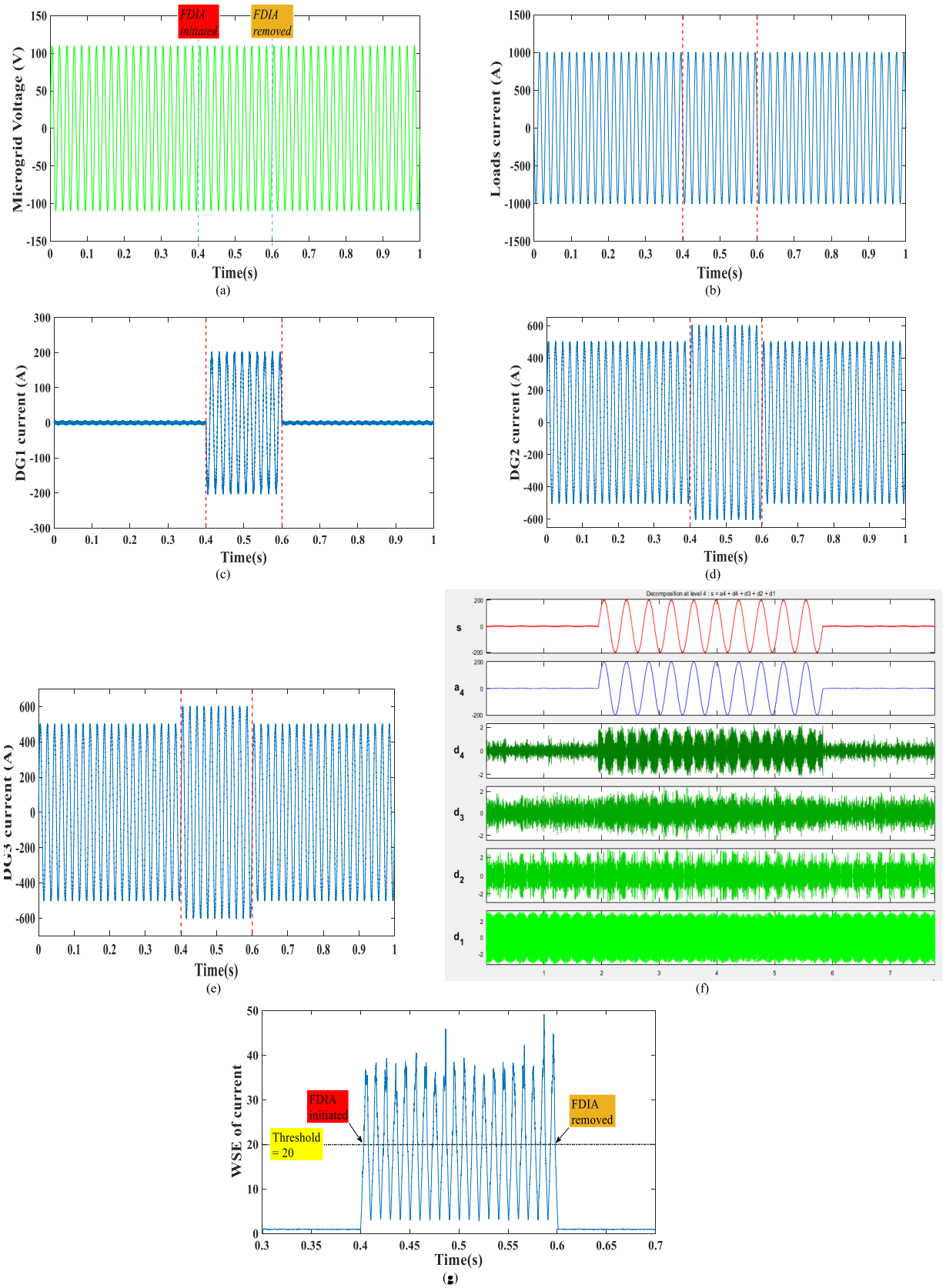

FIGURE 13. Instability caused by injecting an attack by altering the load current reference signal: Deteriorates current sharing profile on agent 2 and 3 including a) Smart Island voltage, b) Load current, c) Current of DG1, d) Current of DG2, e) Current of DG3, f) Wavelet decomposition, g) WSE of current where cyber-attack is happened at t = 0.4 s and is removed at t=0.6 s.

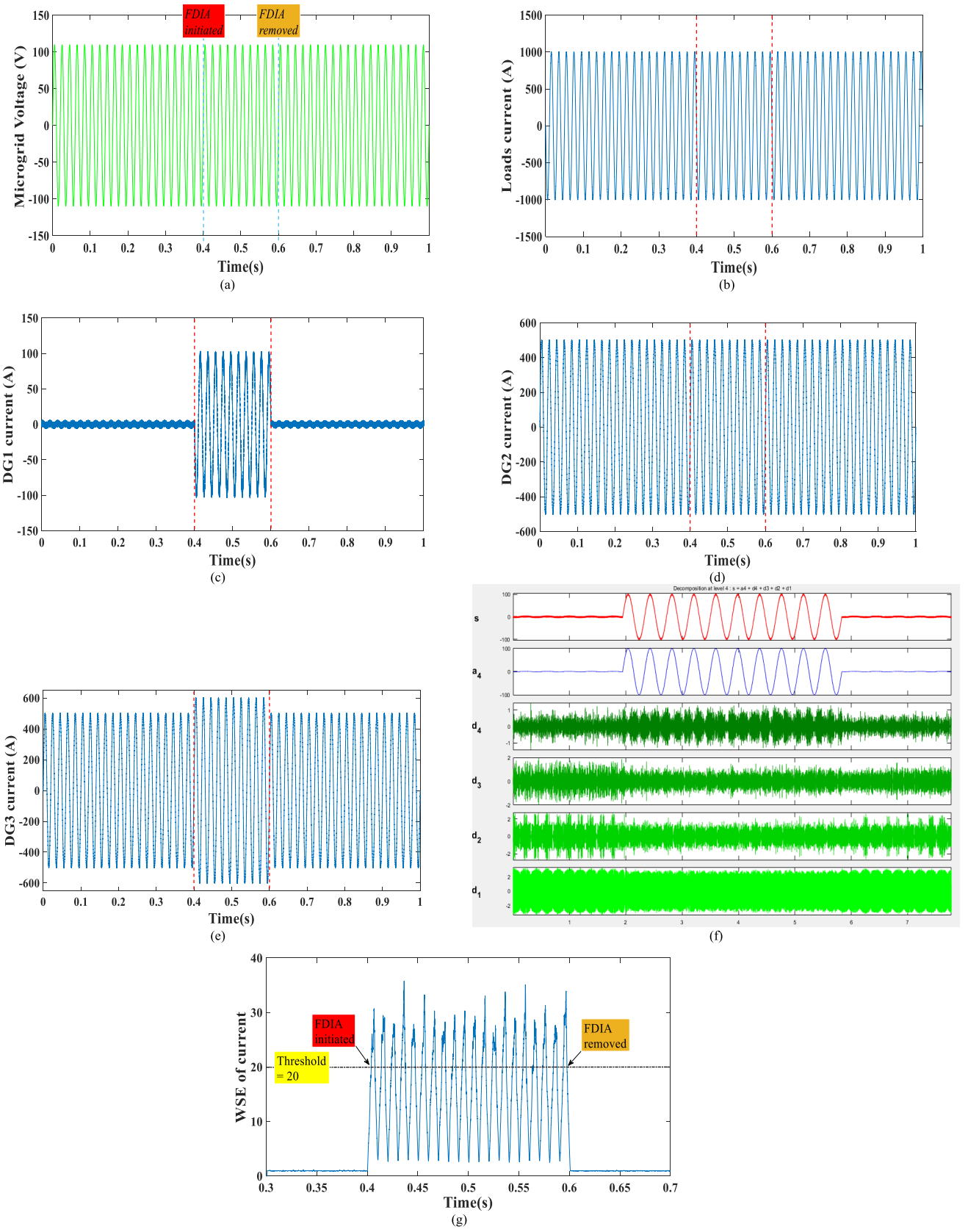

FIGURE 14. Instability caused by injecting an attack by altering the load current reference signal: Deteriorates current sharing profile on agent 2 including a) Smart Island voltage, b) Load current, c) Current of DG1, d) Current of DG2, e) Current of DG3, f) Wavelet decomposition, g) WSE of current where cyber-attack is happened at t = 0.4 s and is removed at t=0.6 s.

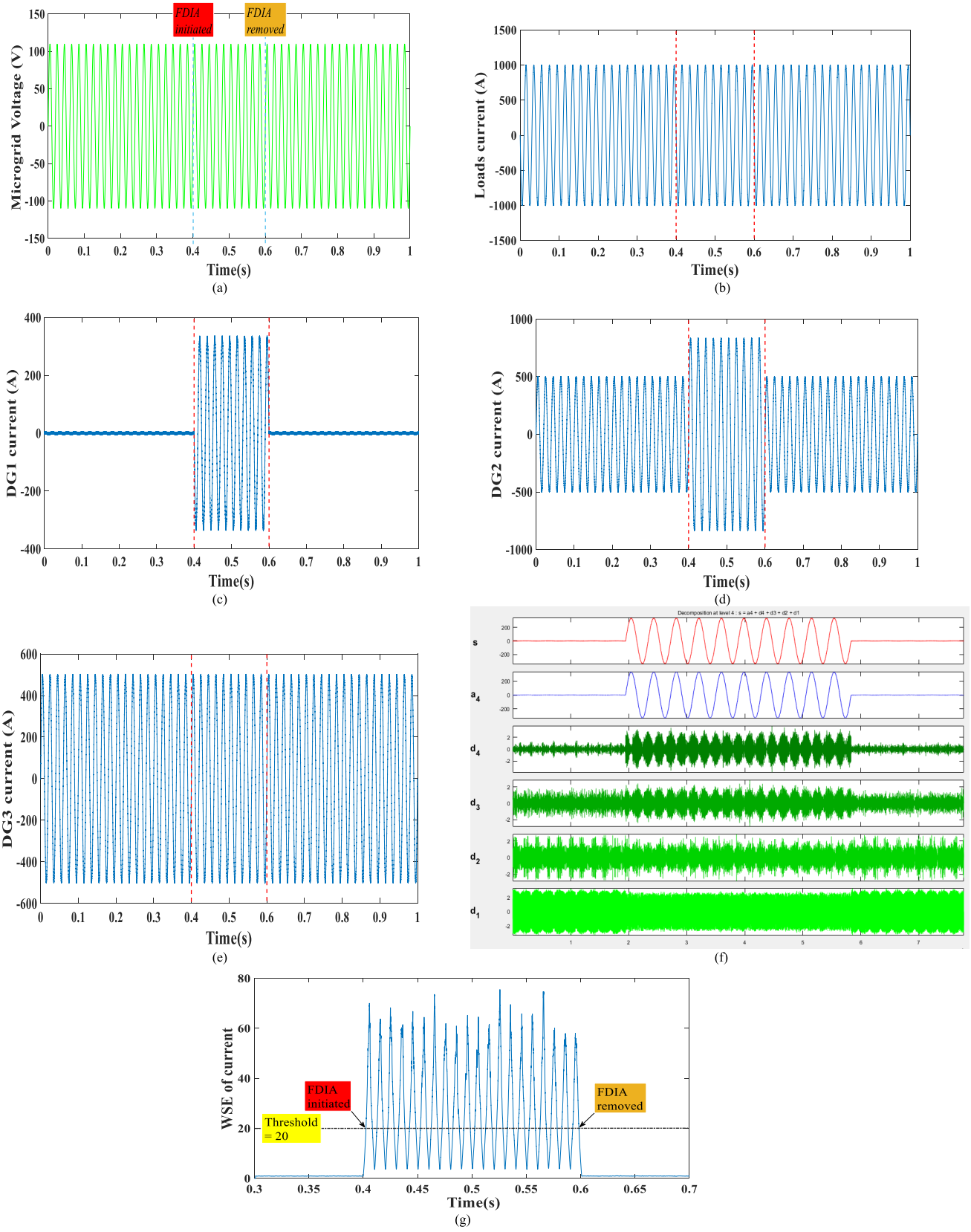

FIGURE 15. Instability caused by injecting an attack on the current sensor: Deteriorates current sharing profile on agent 2 and 3 including a) Smart Island voltage, b) Load current, c) Current of DG1, d) Current of DG2, e) Current of DG3, f) Wavelet decomposition, g) WSE of current where cyber-attack is happened at t = 0.4 s and is removed at t=0.6 s.

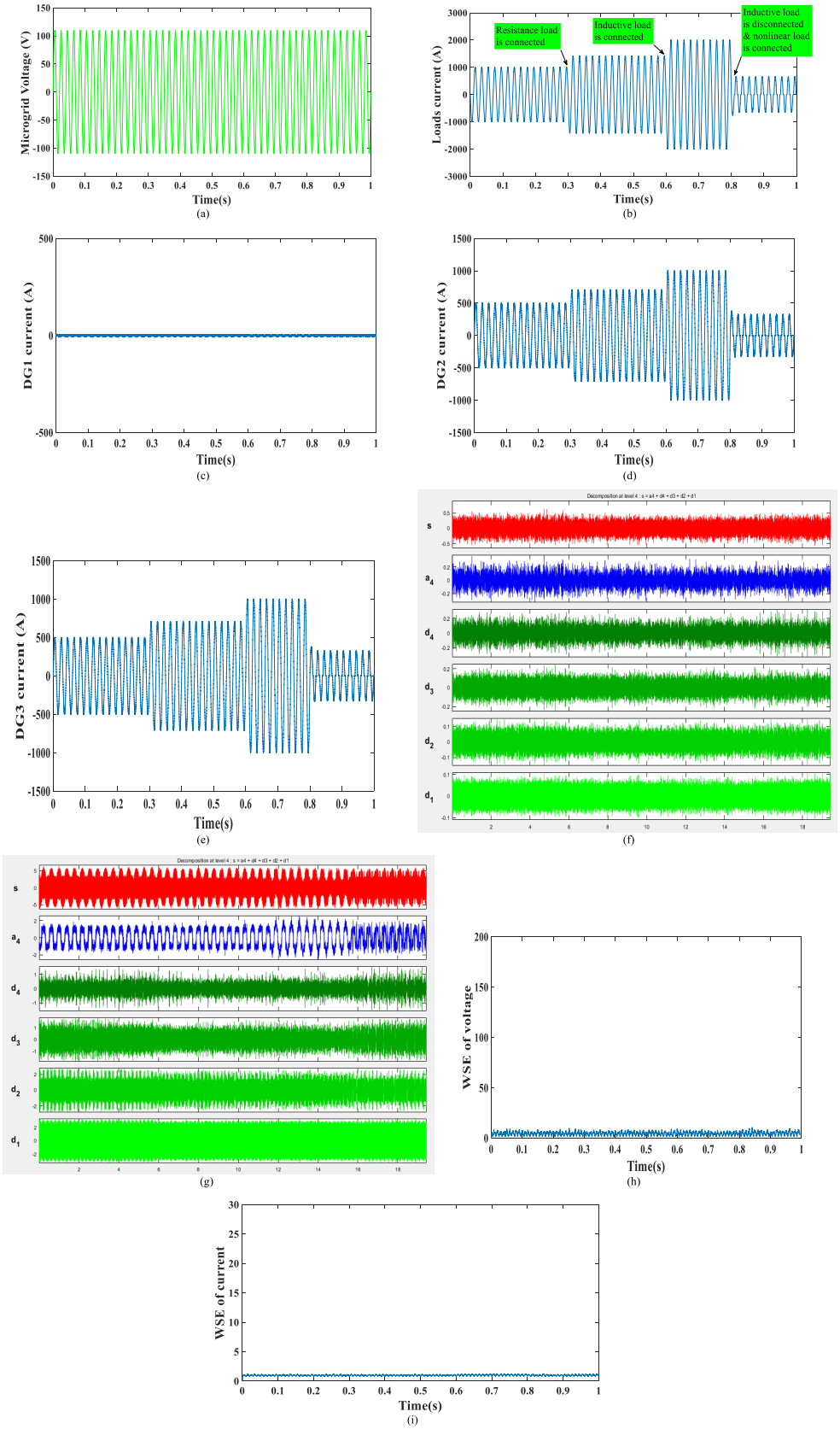

FIGURE 16. Loads changing: a) Smart Island voltage, b) Load current, c) Current of DG1, d) Current of DG2, e) Current of DG3, f) Wavelet decomposition of voltage, g) Wavelet decomposition of current, h) WSE of voltage, i) WSE of current.

less or more the real value. Figure 15 illustrates the results of the simulation. In this scenario, Figures 15(a) and (b) show the SI's voltage and the current loads current, respectively. Figures 15 (c), (d) and (e) show the DG1, DG2 & DG3 current, respectively. During the attack, the production of current DG2 increased while the load was constant and DG1 produced current in front of the attack current to eliminate the further current produced by DG2. Figure 15(f) illustrates the wavelet transform of the current sliding surface signal and wavelet decomposition at various levels. Besides, the wavelet factors (d1…d4) are employed to maintain efficient singular values that are applied to calculate WSE for attack detection in SI. Figure 15(g) shows WSE of the signal in this scenario and by selecting the threshold as 20; the successful attack detection effectiveness of the presented approach is shown.

H. CASE STUDY VIII: LOAD CHANGING

In this scenario, the proposed technique performance in detecting FDIA and under multiple load scenarios including resistive, inductive, balanced or unbalanced and nonlinear load is examined. At t=.3 s, a resistive load is connected to the system. Figure 16(a) indicates the voltage of the SI. At t=.6 s, an inductive load is connected, and at t=.8 s, these loads get disconnected, and a nonlinear load is connected (Figure 16 (b)). Figure 16(c), (d) & (e) show the DG1, DG2 & DG3 current signals, respectively. Fig. 16(f) & (g) illustrate the wavelet transform of voltage and current sliding surface signals, respectively and wavelet decomposition at various levels. Besides, the wavelet factors (d1…d4) are employed to maintain efficient singular values that are applied to calculate WSE for attack detection in SI. Fig. 15(h) & (i) show WSE of voltage and current signals in this scenario, respectively. As can be seen, the WSE method does not recognize loads changes as cyber-attacks and has a good response in separating FDI attacks from loads changes.

As shown from Figure 7 (d) to Figure 12 (d), by selecting the threshold as 50, the proposed procedure can identify the FDIA in voltage. Also, as can be seen from Figure 13 (g) to Figure 15(g), by selecting the threshold as 20, the proposed procedure can identify the FDIA in the current. As can be seen, the WSE technique can detect FDIA in various scenarios and identify the attack from load changing.

I. RESPONSE TIME

The response time of the presented algorithm under FDIA in the voltage and current signals are shown in figures 17(a) and 17(b), respectively. As can be observed, the proposed detection technique detects the attack in less than 10 ms from the moment the attack is started. Figure 17(a) indicates the response time of WSE of voltage. FDIA started at t=0.4s and is detected at t=0.406 s (in 6 ms). Figure 17(b) illustrates the response time of WSE of current. FDIA, in this case, begins at t=0.4 s and is detected at t=0.404 s (in 4 ms).

VI. DISCUSSION ABOUT SIMULATION RESULTS

In general, it is considered that when an issue is investigated as a cyber-activity, this will be a positive (Pos) decision.

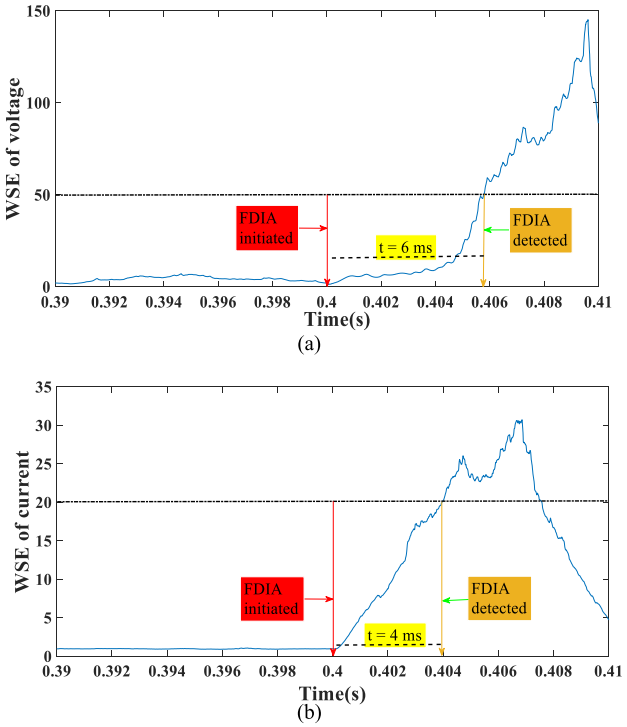

FIGURE 17. Time response: a) WSE of voltage, b) WSE of current.

TABLE 1. Confusion rate matrix of the introduced detection scheme.

		Actual Value	
		Pos	Neg
Detection scheme Response	Pos	Hit Rate Real Pos (TP)	False Alarm Rate False Pos (FP)
	Neg	Miss Rate False Neg (FN)	Correct Rejection Rate True Neg (TN)

It will be a negative (Neg) decision when the type of anomaly detection identifies as usual behaviour. The right decision will be made whenever the specimen of uncommon diagnosing is corrected. Therefore, an incorrect decision illustrates an incorrect response from the cyber-attack diagnosing type. According to this concept, it is concluded that a proper form of detection anomalies will be a model with a low false rate. Based on these definitions, four various types, namely False Alarm Rate (FAR), Miss Rate (MR), Correct Reject Rate (CRR) and Hit Rate (HR), are defined. To have a better understanding of these concepts, Table 1 provides the confusion matrix. Various test cases are applied to confirm the efficiency and validation of the presented wavelet transform in FDIA detection. The suggested detection plan's performance is evaluated by applying it into the FDIA layout, and the evaluation outcomes are illustrated. The presented detection plan's execution is investigated using the FDIA scheme and the evaluation outcomes shown in Table 2. To demonstrate the suggested cyber-attack detection model's sufficiency, it compares with WT and DNN presented in the reference [36]. Table 2 can remark that the proposed technique can detect the FDIAs with detection accuracy over 96.5 %.

The detection accuracy based on WT as the input of DNN can detect FDIAs over 95 % and the DNN training time

TABLE 2. Confusion result matrix of the introduced detection scheme.

	Method	Actual Value	Pos	Neg
Detection scheme Response	WSE	Pos	97.11 %	3.17 %
		Neg	2.89 %	96.83 %
	WT and DNN [36]	Pos	96.38 %	4.58%
		Neg	3.62%	95.42%

	Method	WSE	WT and DNN [36]
Response Time	Average Detection Time	5 ms	3.51 ms
	DNN Training Time	-	2713.2 s

is 2713.2 s where average detection time is 3.51 ms; but in the suggested method, the average detection time is 5 ms without the training time and complexity of DNN, so, it displays the sufficiency of the introduced detection plan to detect the FDIAs.

VII. CONCLUSION

A novel FDIA detection technique for the AC state estimation has been proposed in this paper. Other research works on FDIA detection were mostly concentrated on attacks and attack detection in DC state estimation. Current FDIA method focused on wavelet singular entropy technique. The wavelet singular entropy approach comprises the wavelet transform, singular value decomposition and Shannon entropy to obtain a programmed trait to characterize cyber-attack detection. Results find out wavelet singular entropy responds to unexpected alterations in signals and detect FDIA in various conditions. The reliable and quick performance of the presented technique is illustrated through different scenarios. The wavelet singular entropy can accurately detect FDIA in current and voltage, and they can be distinguished from the normal operating condition events.

In this paper, a series of comprehensive simulations on 3-bus Smart-Island have been performed. The proposed detector has been applied, and its performance was examined. The proposed FDIA detection technique shows a more reliable and accurate performance comparing to the existing FDIA detectors. In this paper, in a Smart-Island configuration and an extensive range of variations in the operating conditions, it is shown that the proposed mechanism is a reliable and fast FDIA detection method and the wavelet singular entropy can successfully and accurately detect FDIA under various types of attack. The suggested WSE-based FDIA detection plan is more straightforward and can be easily performed on the digital signal processing or field-programmable gate array (DSP/FPGA) boards for enhancing the anti-cyber-attack modules. Considering the proposed approach's notable performance, applying this model on real-time cyber-attack detection in an AC-SI hardware experimental setup can be a hot topic for future works.

REFERENCES

[1] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, and S. Padmanaban, "False data injection attack detection based on Hilbert-huang transform in AC smart islands," *IEEE Access*, vol. 8, pp. 179002–179017, 2020.

[2] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An ensemble deep learning-based cyber-attack detection in industrial control system," *IEEE Access*, vol. 8, pp. 83965–83973, 2020.

[3] M. Ghiasi, "Detailed study, multi-objective optimization, and design of an AC-DC smart microgrid with hybrid renewable energy resources," *Energy*, vol. 169, pp. 496–507, Feb. 2019.

[4] M. Dehghani, A. Kavousi-Fard, T. Niknam, and O. Avatefipour, "A robust voltage and current controller of parallel inverters in smart island: A novel approach," *Energy*, vol. 214, Jan. 2021, Art. no. 118879.

[5] H. Cui, X. Dong, H. Deng, M. Dehghani, K. Alsubhi, and H. M. A. Aljahdali, "Cyber attack detection process in sensor of DC micro-grids under electric vehicle based on Hilbert-Huang transform and deep learning," *IEEE Sensors J.*, early access, Sep. 29, 2020, doi: 10.1109/JSEN.2020.3027778.

[6] M. El-Hendawi and Z. Wang, "An ensemble method of full wavelet packet transform and neural network for short term electrical load forecasting," *Electric Power Syst. Res.*, vol. 182, May 2020, Art. no. 106265.

[7] M.-H. Khooban, M. Dehghani, and T. Dragievi, "Hardware-in-the-loop simulation for the testing of smart control in grid-connected solar power generation systems," *Int. J. Comput. Appl. Technol.*, vol. 58, no. 2, pp. 116–128, 2018.

[8] M. Dehghani, M. H. Khooban, T. Niknam, and S. M. R. Rafiei, "Time-varying sliding mode control strategy for multibus low-voltage microgrids with parallel connected renewable power sources in islanding mode," *J. Energy Eng.*, vol. 142, no. 4, Dec. 2016, Art. no. 05016002.

[9] Fathi and Ghiasi, "Optimal DG placement to find optimal voltage profile considering minimum DG investment cost in smart neighborhood," *Smart Cities*, vol. 2, no. 2, pp. 328–344, Jun. 2019.

[10] M. Dehghani, A. Kavousi-Fard, M. Dabbaghjamanesh, and O. Avatefipour, "Deep learning based method for false data injection attack detection in AC smart islands," *IET Gener., Transmiss. Distribution*, vol. 14, no. 24, pp. 5756–5765, Dec. 2020.

[11] P. Duan, H. Soleimani, A. Ghazanfari, and M. Dehghani, "Distributed energy management in smart grids based on cloud-fog layer architecture considering PHEVs," *IEEE Trans. Ind. Appl.*, early access, Jul. 21, 2020.

[12] M. Ghiasi, N. Ghadimi, and E. Ahmadinia, "An analytical methodology for reliability assessment and failure analysis in distributed power system," *Social Netw. Appl. Sci.*, vol. 1, no. 1, p. 44, Jan. 2019.

[13] M. Ghiasi, "Technical and economic evaluation of power quality performance using FACTS devices considering renewable generations," *Renew. Energy Focus*, vol. 29, pp. 49–62, Jun. 2019.

[14] C. Shang, D. Srinivasan, and T. Reindl, "Economic and environmental generation and voyage scheduling of all-electric ships," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 4087–4096, Sep. 2016.

[15] S. Mashayekh and K. L. Butler-Purry, "An integrated security-constrained model-based dynamic power management approach for isolated microgrids in all-electric ships," *IEEE Trans. Power Syst.*, vol. 30, no. 6, pp. 2934–2945, Nov. 2015.

[16] M. Ghiasi, M. Dehghani, T. Niknam, and A. Kavousi-Fard, "Investigating overall structure of cyber-attacks on smart-grid control systems to improve cyber resilience in power system," *IEEE Smart Grid Newslett.*, 2020.

[17] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.

[18] C. Iphar, C. Ray, and A. Napoli, "Data integrity assessment for maritime anomaly detection," *Expert Syst. Appl.*, vol. 147, Jun. 2020, Art. no. 113219.

[19] R. Khan, K. Mclaughlin, D. Laverty, and S. Sezer, "Design and implementation of security gateway for synchrophasor based real-time control and monitoring in smart grid," *IEEE Access*, vol. 5, pp. 11626–11644, 2017.

[20] A. Farraj, E. Hammad, and D. Kundur, "A distributed control paradigm for smart grid to address attacks on data integrity and availability," *IEEE Trans. Signal Inf. Process. over Netw.*, vol. 4, no. 1, pp. 70–81, Mar. 2018.

[21] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access*, vol. 5, pp. 13787–13798, 2017.

[22] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, and S. Mehraeen, "Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7300–7309, Nov. 2019.

[23] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Yang Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.
[24] 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.
[25] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1686–1696, Jul. 2015.
[26] X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239–2248, Sep. 2017.
[27] M. Mohammadpourfard, A. Sami, and A. R. Seifi, "A statistical unsupervised method against false data injection attacks: A visualization-based approach," *Expert Syst. Appl.*, vol. 84, pp. 242–261, Oct. 2017.
[28] 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.
[29] H. Karimipour and H. Leung, "Relaxation-based anomaly detection in cyber-physical systems using ensemble Kalman filter," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 1, pp. 49–58, Mar. 2020.
[30] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Trans. Signal Inf. Process. over Netw.*, vol. 4, no. 1, pp. 48–59, Mar. 2018.
[31] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.
[32] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.
[33] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical DC microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.
[34] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2208–2223, Mar. 2019.
[35] Y. Li, Z. Li, and L. Chen, "Dynamic state estimation of generators under cyber attacks," *IEEE Access*, vol. 7, pp. 125253–125267, 2019.
[36] 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.
[37] C. H. Li and S. C. Park, "An efficient document classification model using an improved back propagation neural network and singular value decomposition," *Expert Syst. Appl.*, vol. 36, no. 2, pp. 3208–3215, Mar. 2009.
[38] M. Nayer-Pour, A. H. Rajae, M. M. Ghanbaran, and M. Dehghan, "Fault detection and classification in transmission lines based on a combination of wavelet singular values and fuzzy logic," *Cumhuriyet Univ. Fac. Sci. Sci. J.*, vol. 36, p. 3, Sep. 2015.
[39] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.
[40] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.
[41] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. System Secur.*, vol. 14, no. 1, p. 13, 2011.
[42] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1306–1318, Jul. 2013.
[43] X. Xu and M. Kezunovic, "Automated feature extraction from power system transients using wavelet transform," in *Proc. Int. Conf. Power Syst. Technol.*, 2002, pp. 1994–1998.
[44] N. Bayati, H. R. Baghaee, A. Hajizadeh, and M. Soltani, "Localized protection of radial DC microgrids with high penetration of constant power loads," *IEEE Syst. J.*, pp. 1–12, Jan. 2020.
[45] M. Dehghani, M. H. Khooban, and T. Niknam, "Fast fault detection and classification based on a combination of wavelet singular entropy theory and fuzzy logic in distribution lines in the presence of distributed generations," *Int. J. Electr. Power Energy Syst.*, vol. 78, pp. 455–462, Jun. 2016.
[46] M. Karmellos and G. Mavrotas, "Multi-objective optimization and comparison framework for the design of distributed energy systems," *Energy Convers. Manage.*, vol. 180, pp. 473–495, Jan. 2019.
[47] D. Chen, S. Wan, and F. S. Bao, "Epileptic focus localization using discrete wavelet transform based on interictal intracranial EEG," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 25, no. 5, pp. 413–425, May 2017.
[48] J. J. Q. Yu, Y. Hou, A. Y. S. Lam, and V. O. K. Li, "Intelligent fault detection scheme for microgrids with wavelet-based deep neural networks," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1694–1703, Mar. 2019.

MOSLEM DEHGHANI was born in Shiraz, Iran, in 1990. He received the B.S. and M.S. degrees in electrical engineering from Islamic Azad University-Kazerun branch, in 2012 and 2014, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with the Shiraz University of Technology, Shiraz, Iran, in 2019. Since 2017, he has been an Electrical Design Engineer with Electrical Distribution Company, Fars, Shiraz, Iran. His current research interests include power electronic, control, and cyber security analysis of smart grids, microgrid, smart city, HVDC systems as well as protection of power systems, fuzzy logic, and signal processing.

MOHAMMAD GHIASI received the B.S. and M.S. degrees in electrical power engineering, in 2012 and 2016, respectively. He is currently a Research Assistant with the Shiraz University of Technology, Shiraz, Iran. His research on modeling, simulation, and optimization of power systems, integration and control of hybrid and distributed renewable energy resources, smart grids, as well as resilience and cyber security in power systems has led to multiple publications in these fields. He has two hot Articles and one highly-cited article, based on SciVal and Web of Science statistics. He is also the reviewer for several IEEE, IET, Elsevier, Springer, Wiley, Sage, and Taylor & Francis journals and conferences.

TAHER NIKNAM (Member, IEEE) was born in Shiraz, Iran. He received the B.S. degree from Shiraz University, Shiraz, Iran, in 1998, and the M.S. and Ph.D. degrees from the Sharif University of Technology, Tehran, Iran, in 2000 and 2005, respectively, all in power electrical engineering. He is a faculty member with the Electrical Engineering Department, Shiraz University of Technology. His research interests include power system restructuring, impact of distributed generations on power systems, optimization methods, and evolutionary algorithms.

ABDOLLAH KAVOUSI-FARD (Member, IEEE) received the B.Sc. degree from the Shiraz University of Technology, Shiraz, Iran, in 2009, the M.Sc. degree from Shiraz University, Shiraz, in 2011, and the Ph.D. degree from the Shiraz University of Technology, in 2016, all in electrical engineering. He was a Postdoctoral Research Assistant with the University of Michigan, MI, USA, from 2016 to 2018. He was a Researcher with the University of Denver, Denver, CO, USA, from 2015 to 2016, conducting research on microgrids. He is currently an Assistant Professor with the Shiraz University of Technology. His current research interests include operation, management and cyber security analysis of smart grids, microgrid, smart city, electric vehicles as well as protection of power systems, reliability, artificial intelligence, and machine learning. He is an Editor in Springer, ISTE ISI journal.

ELHAM TAJIK received the B.S. degree in electrical engineering from the Sharif University of Technology, the M.S. degree in electrical engineering from the Iran University of Science and Technology, Iran, and the Ph.D. degree from the University of Oklahoma, in 2018. Her research interests include control and modeling of power systems dynamics, microgrid, electricity market, and optimization.

SANJEEVIKUMAR PADMANABAN (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Bologna, Bologna, Italy, in 2012. He was an Associate Professor with VIT University, from 2012 to 2013. In 2013, he joined the National Institute of Technology, India, as a Faculty Member. In 2014, he was invited as a Visiting Researcher at the Department of Electrical Engineering, Qatar University, Doha, Qatar, funded by the Qatar National Research Foundation (Government of Qatar). He continued his research activities with the Dublin Institute of Technology, Dublin, Ireland, in 2014. Further, he served an Associate Professor with the Department of Electrical and Electronics Engineering, University of Johannesburg, Johannesburg, South Africa, from 2016 to 2018. Since 2018, he has been a Faculty Member with the Department of Energy Technology, Aalborg University, Esbjerg, Denmark. He has authored over 300 scientific articles. He was a recipient of the Best Paper cum Most Excellence Research Paper Award from IET-SEISCON'13, IET-CEAT'16, IEEE-EECSI'19, IEEE-CENCON'19, and five best paper awards from ETAEERE'16 sponsored lecture notes in electrical engineering, Springer book. He is a Fellow of the Institution of Engineers, India, the Institution of Electronics and Telecommunication Engineers, India, and the Institution of Engineering and Technology, U.K. He is an Editor/Associate Editor/Editorial Board for refereed journals, in particular the IEEE SYSTEMS JOURNAL, IEEE TRANSACTION ON INDUSTRY APPLICATIONS, IEEE ACCESS, *IET Power Electronics, IET Electronics Letters, and Wiley-International Transactions on Electrical Energy Systems*, Subject Editorial Board Member-*Energy Sources-Energies* Journal, MDPI, and the Subject Editor of the *IET Renewable Power Generation, IET Generation, Transmission and Distribution, and FACTS* journal (Canada).

HAMDULAH ALIEV received his B.Sc. M.Sc. and PhD in electrical and electronics engineering in 2008, 2010 and 2014 respectively. He is currently a researcher at Tajik Technical University, Dushanbe, Tajikistan. He is the reviewer for several IEEE, IET, and Elsevier journals.His research interests include renewable energy resources, power system stability, protection cyber-physical systems and energy conversion.