IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON EVOLVING TECHNOLOGIES IN ENERGY STORAGE SYSTEMS FOR ENERGY SYSTEMS APPLICATIONS

Received September 2, 2020, accepted September 25, 2020, date of publication September 29, 2020,
date of current version October 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3027782

False Data Injection Attack Detection based on Hilbert-Huang Transform in AC Smart Islands

MOSLEM DEHGHANI[1], MOHAMMAD GHIASI[1], (Graduate Student Member, IEEE), TAHER NIKNAM[1], (Member, IEEE), ABDOLLAH KAVOUSI-FARD[1], (Member, IEEE), AND SANJEEVIKUMAR PADMANABAN[2], (Senior Member, IEEE)

[1]Department of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz 71557-13876, Iran
[2]Department of Energy Technology, Aalborg University Esbjerg, 6700 Esbjerg, Denmark

Corresponding authors: Mohammad Ghiasi (m.ghiasi@sutech.ac.ir) and Taher Niknam (niknam@sutech.ac.ir)

ABSTRACT In Smart Island (SI) systems, operators of power distribution system usually utilize actual-time measurement information as the Advanced Metering Infrastructure (AMI) to have an accurate, efficient, advanced control and monitor of whole their system. SI system can be vulnerable to complicated information integrity attacks such as False Data Injection Attack (FDIA) on some equipment including sensors and controllers, which can generate misleading operational decision in the system. Hence, lack of detailed research in the evaluation of power system that links the FDIAs with system stability is felt, and it will be important for both assessment of the effect of cyber-attack and taking preventive protection measures. In this regards, time–frequency-based differential approach is proposed for SI cyber-attack detection according to non-stationary signal assessment. In this paper, non-stationary signal processing approach of Hilbert–Huang Transform (HHT) is performed for the FDIA detection in several case studies. Since various critical case studies with a small FDIA in data where accurate and efficient detection can be a challenge, the simulation results confirm the efficiency of HHT approach and the proposed detection frame is compared with shallow model. In this research, the configuration of the SI test case is developed in the MATLAB software with several Distributed Generations (DGs). As a result, it is found that the HHT approach is completely efficient and reliable for FDIA detection target in AC-SI. The simulation results verify that the proposed model is able to achieve accuracy rate of 93.17% and can detect FDIAs less than 50 ms from cyber-attack starting in different kind of scenarios.

INDEX TERMS False data injection attack, Hilbert-Huang transform, smart island, AC system.

I. INTRODUCTION

Cyber Physical Systems (CPSs) usually concentrate on connecting the physical globe to the cyber and digital world; also they are greatly utilized in the control of various industrial systems until several individuals can be able to grasp numerous kinds of required information in the real time [1]–[3]. The usage of CPS has a prominent potential of using in some fields including power distribution systems and sewage treatment plants. However, CPS safety subjects include integrity, confidentiality and availability, which are different from traditional cyber-security problems. The SI is responsible for monitoring, operation and control of transmission and distribution of electrical systems that can remarkably develop the reliability and efficiency of the power and energy systems. If such systems fail, they might have several negative and harmful effects on other systems, and can lead to short-term or long-term collapse in important infrastructures [4], [5]. Nowadays, numerous countries in the world regard the power network system as a pivotal infrastructure and have formed and stablished security and safety measures and related policies for this important issue [6]. Additionally, modern power systems, these days, are becoming more and more complex in the design and architecture; the phasor measurement units (PMUs) were accepted to develop the reliability of system. One of the advantages of this structure is the ability of making fast decisions by utilizing the collected information and data. Nevertheless, hackers are able to exploit vulnerabilities to intentionally causes of overloaded tripping of branches which might trigger a cascading fault and therefore impose considerable harms to the SIs [7], [8]. Consequently, the operators should take full account of the possibility of

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

grid attack in controlling, operation and monitoring to deal with the power network protection that requires the expertise of the grid and remarkable energy. As a main component of the proposed approach, Hilbert–Huang Transform (HHT) can be employed. References [9], [10] presented HHT for reduction and decomposition in the dimensionality of a signal. Generally, HHT includes two steps: first, performing a data-adaptive decomposition approach named Empirical Mode Decomposition (EMD), and second, applying Hilbert spectral assessment to the decomposed signals which named Intrinsic Mode Functions (IMF's). Additionally, EMD can have several advantages and benefits over the Fourier assessment in which firstly, the oscillations embedded in every signal would be extracted adaptively and automatically from the signals; secondly, it would be relatively simple to perform; and thirdly, it would be specifically robust for every non-stationary and non-linear signal. In addition to this, EMD efficiently can capture non-linear specifications with regards to the frequency and amplitude modulations by local time scale. While IMF's are taken, Hilbert spectral assessment gives frequency data changing over period of time which is a major component of assessment for every non-stationary signal including cyber-attack signals.

A. BACKGROUND

Concepts such as Microgrid (MG), Smart Grid (SG) and Smart Island (SI) in AC and DC power systems with advances in digital communication technologies have received more attention in the past few years. Recently, several researchers and studies have highlighted the vulnerability of traditional AC and DC state estimators to the FDIAs in that an adversary is able to present manipulated measurements to the mislead operation systems [11]. Some kind of attacks are able to bypass common Bad Data Detection (BDD) in the State Estimation (SE) as the measurement remnants with FDIAs are the same as the measurement residuals with no FDIAs. In the FDIAs, the attacker can have aims to mislead the SE of the system mechanism using sending corrupted measurements which in turn will successfully and effectively pass the BDD module and can bring mistake estimation in one or more of the state variables.

One important point is that choosing the suitable set of measurements to exploit between the accessible meters can be more complicated. AC state estimators have been safe against FDIA as long as the authors of the paper [12] showed that even though attacks aiming DC state estimators might not pass BDD in every AC-SE; nonetheless, an adversary still was able to inject false data attack into the AC-SE, thus, we observed that both AC and DC SE approaches were vulnerable and fragile to the FDIA. In reference [13], nonlinear FDI attacks with inaccurate and wrong data were introduced. Authors in the reference [14] displayed that an attacker was able to do FDI attack on the sub-grid without having full data about the whole power grid.

Another crucial point is that as an attacker, the issue of finding the attack vector could be in general NP-hard [15]. For this purpose, professionals and experts have suggested some attack vector construction approaches taking into account centralized and decentralized models. In reference [15] authors have presented a greedy approach to seek for a subsystem of measurement to be preserved by PMUs. Authors in paper [16] proposed a connection between grid observability and attack detectability by a graph-theoretic design. Machine learning approaches have also been presented in reference [17] to find stealth attacks (SA) in SE. Cyber-attacks, also, in systems like Supervisory Control And Data Acquisition (SCADA) can be very perilous, therefore, for such systems this should be used in a particular path [18]–[20]. There is a prominent amount of publications on CPS in recent years which a survey of this can be found in the paper [21]. Furthermore, authors of the paper [22] utilized noise fingerprint processing and sensors in order to address stealthy cyber-attack problems in CPS, and validated an approach in a data set from an actual-globe water treatment plant, which in this study the results displayed that the precision was about 98.1 percent. In reference [23] authors presented a Multi-Modal Luenberger observer that could be able to isolate the attacked sensors and SE of the basic dynamics of the remaining sensors and their methods could be able to be performed to large-scale CPSs. Reference [24] proposed a semantic system grid-based orientation detection to find attacks on control processing with utilizing grid traffic from water and sewage plants. Such kinds of studies display the emphasis on research in CPS safety; particularly, in the SGs that include CPSs. The PMU or synchro-phasor was built upon the cyber layer to serve real-time information [25] which can act as a bridge among physical and cyber amplitudes [26]. Besides, machine learning approaches have also been performed to intrusion detection related issues; following studies can be found in references [27]–[30]. Authors of the paper [27] presented a machine learning behavior-based method for the intrusion detection, and the data set that they utilized was Secure Water Treatment (SWaT)-generated information from eighteen attacks with ten type models. In paper [28] authors utilized a rapid one- class category method that overcomes the disadvantages of high sensitivity to the outliers; also, the presented approach was examined on an actual data set from distribution systems of drink water in France. In paper [29] authors utilized a method named One Class SVM (OCSVM) technology to discover SCADA grid intrusion.

B. MOTIVATION AND PRINCIPAL CONTRIBUTIONS OF THIS PAPER

In this study, we propose an HHT-based approach to draw out the dominant ingredients of a signal according to those ingredients. The suggested approach can be categorized into two parts: first, a signal will be decomposed using EMD; and second, meaningful IMF's ingredients will be opted using Hilbert spectrum. In this regards, the suggested approach will bring about development of FDI detection accuracy in AC-SI.

In the system, HHT is going to extract the state features of system, and define a threshold to detect AC-FDIA from

usual operation occurrences. The principal contributions of this study are mentioned as follows:

• This paper is located between the pioneering research of the use of HHT in the FDIA detection studies to diagnose an attack that is new and effective.

• The suggested method is going to identify FDIA in the AC-SI, specifically new attack templates with imperfect power grid data.

• In this work, the presented mechanism will be evaluated with the recently introduced FDIA template in SI case studies. The obtained results of the simulation confirm the accuracy and satisfactory of attack detection and the rate of false alarm.

• The test of parameter sensitivity is performed to assess the efficiency and accuracy of the suggested method.

C. PAPER STRUCTURE

The article will be organized as follows. In Section II, we will introduce the HHT approach and main concepts of FDI. In Section III, we will evaluate the SI information utilizing HHT, and also, their ability for FDI attack detection in different case studies will be presented. In Section IV, we will discuss obtained results of the simulation, and finally in Section V, we will present the conclusions of the study.

II. BASIC CONCEPTS

A. HILBERT–HUANG TRANSFORM (HHT)

The growth of HHT is basically caused by the requiring and describing nonlinear waves with changes in these signals in non-constant processes [31]. HHT consists of 2 different operations, Hilbert Transform (HT) and EMD, and these two operations have to be performed sequentially.

A) Experimental mode analysis: The basic part of the HHT is EMD. This is a sieving process that breaks down the signal into a number of internal states. The main signal $S(t)$ can be given in the equation (1).

$$S(t) = \sum_{i=1}^{n} c_i(t) + r_n(t) \tag{1}$$

It is noted that the first IMF (IMF1) $c_1(t)$ consists of the highest signal processing frequency and is often utilized as the input for subsequent processing with HT [31].

B) Hilbert transform (Conversion): by considering IMFs which is derived using the EMD approach, HT can be used for any component of the IMF which is defined in equation (2).

$$H[c_i(t)] = \int_{-\infty}^{\infty} \frac{c_i(\tau)}{\pi(t-\tau)} d\tau \tag{2}$$

Considering this equation, *ci(t)* and $H[c_i(t)]$ are able to figure a complicated conjugate pair, that generates the analytic signal $z_i(t)$.

$$z_i(t) = c_i(t) + jH[c_i(t)] \tag{3}$$

Meanwhile, $z_i(t)$ can be given as the equation (4)

$$z_i(t) = a_i(t)\exp(j\omega_i(t)) \tag{4}$$

Combined with instantaneous amplitude $a_i(t)$ and phase $\theta_i(t)$ gives equation (5);

$$a_i(t) = \sqrt{c_i^2(t) + H^2[c_i(t)]} \tag{5}$$

and

$$\theta(t) = \tan^{-1}\left[\frac{H[c_i(t)]}{c_i(t)}\right] \tag{6}$$

The instantaneous frequency $\omega_i(t)$ can be given by

$$\omega_i(t) = \frac{d\theta_i(t)}{dt} \tag{7}$$

As a result, the original data can be given in the form of equation (8):

$$S(t) = Re\sum_{i=1}^{n} a_i(t)\exp(j\int \omega_i(t)\,dt) \tag{8}$$

where, the remnant $r_n(t)$ is remained and $Re0$ represents the real part of a complicated quantity. Also, the signal spectral energy can be given in equation (9).

$$E(H) = (a_i(t))^2 \tag{9}$$

B. FDIAS THREATS

Owing to the complication and fragility of the data transfer procedure in power CPS, many hackers might attempt to manipulate sensor measurements, inject incorrect into controlling commands and topological parameters, replay or postpone sensor observations, and also carry out many other destructive measures. As can be seen from the Figure 1, the operations of achieving, transmitting, and integrating measurement are threatened using stealthy FDIAs, which are now recognized as one of the most dangerous threats to CPS of power network.

Depending on the different ways of attack, FDIA attack scenarios can be identified as follows:

A) Tune using readings of some sensors including different intelligent user meters, PMU and Remote Terminal Units (RTUs).

B) Directly attacks to communication grids.

C) Infiltrate the SCADA system and the Main Domain Controller (MDC).

The final aim is to divide the accuracy and integrity of the measurements to provide accurate and sufficient observations and operational limitations are used for SE to deduce the operating modes of the system in smaller quantities and then it helps the control center decide. Owing to the risk of the predetermined subset, hackers can infect SE results to mislead operators which lead to wrong decisions, and even touch additional problems and power outages [32].

Therefore, it is important to figure out the AC-FDIA attack mode, which can provide an opportunity for CPS of power systems to increase reliability and performance economics by developing appropriate interactions

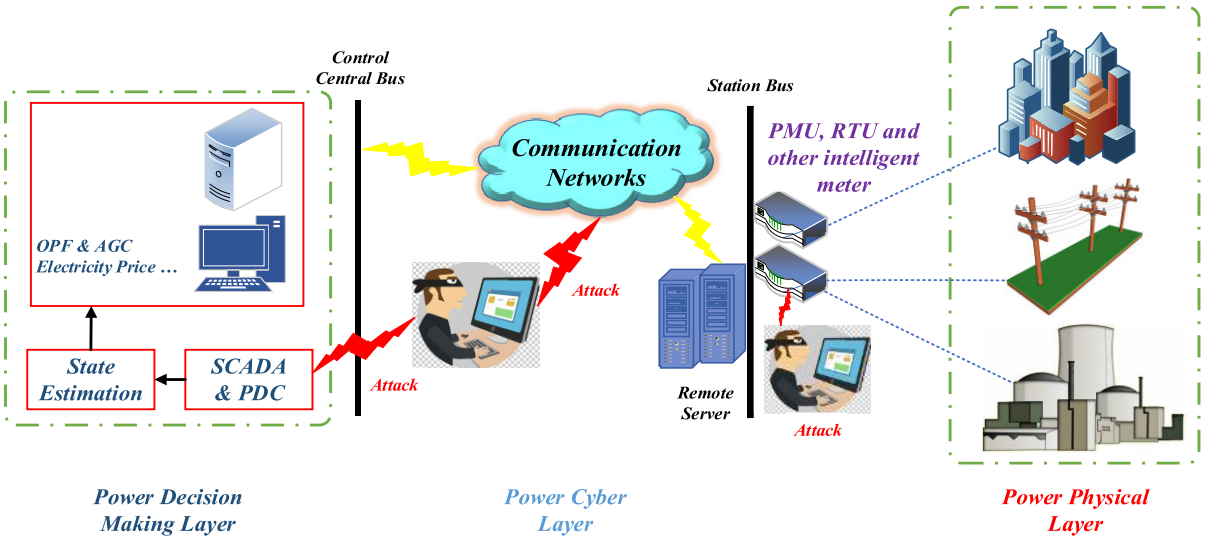


FIGURE 1. FDIAs threats in power CPS.

C. MAIN CONSTRUCTION OF AC-FDIAs

Hackers launched the FDIA by injecting false data into the attacker's vector $\mathrm{z} = [z_1, z_2, \ldots, z_m]^T$ in order to disrupt the AC-SE which is given in the equation (10), where, z generally consists of magnitudes of voltage and phase angles, complicated load injections at branches, complicated load flows on branches which included of forward and backward directions); $\mathrm{x} = [x_1, x_2, \ldots, x_n]^T$ defines the state vector (SV) that included of phase angles and voltage magnitudes; $h(\cdot)$ defines the nonlinear measurement function among SV x and measurement vector (MV) z, that belongs the physical parameters and features and also grid topology of the system. Hence, measurement error vector $\mathrm{e} = [e_1, e_2, \ldots, e_m]^T$ will be the matter for the Gaussian white noise (WN) division by covariance R. In experiment, weighted least square (WLS) approach is a common method to solve static ACSE [12].

$$z = h(x) + e \tag{10}$$

Due to the failure of communications or electromagnetic interference, bad data is often present in the measurement, which can bring about remarkable errors and faults in estimating system modes. Therefore, the BDD module of EMS is used to identify them that are based on the Largest Normal Residual (LNR) approach. By assuming that the change vector of the SV x is determined as c, the residuals of the system measurement before and after the attack would be r and r_a. In general, natural measurements z can cross the LNR-based BDD module, by calculating the $l_2 - norm$ of the residual measurement in order to detect bad measurements, we can define equation (11):

$$\|r\| = \|z - h(x)\| \leq \gamma \tag{11}$$

where in the equation (11), γ represents the detection threshold of LNR-based BDD module.

Whenever the z-measurement vector is injected into the false data, the effect of FDIAs on the BDD module can be as follows:

$$\begin{aligned} \|r_a\| &= \|z_a - h(x_a)\| \\ &= \|(z + a) - h(x + c)\| \\ &= \|(z - h(x)) + (a + h(x) - h(x + c))\| \end{aligned} \tag{12}$$

where in the equation (12), $\boldsymbol{z_a}$ defines the compromised measurement vector. In time of circumvent the BDD module to remain stealthy, whenever hackers become familiar with the topology of system and can have access to measurements, the attack vector have to be constructed which is given in equation (13).

$$a = h(x + c) - h(x) \tag{13}$$

It should be noted that, in this case, the LNR value would be unvaried after attack which means $\|r_a\| = \|r\| \leq \gamma$.

Unlike ideal conditions, it is highly unlikely for a hacker to gain full knowledge of the system in practice. To address this limitation, based on the attack model introduced in [14], we obtain a sufficient number of practical AC attack samples that they just need low prerequisites measurements in the attacking area along with the border buses.

D. SMART ISLAND

Defining an island as intelligent and smart is related to its ability to implement integrated solutions for managing infrastructure and natural sources, called energy, mobility and transportation, water and waste; all whenever promoting using new and comprehensive social programs, governance and funding plans. Introducing outstanding technologies along with proper environmental management consists of landscape protection and logical using of coastal and marine sources, is an important part to fostering sustainable economic and development activities on the islands. In addition, using information and communication technology (ICT) ensures the availability of reliable data to improve efficiency,

can decrease costs and increase the quality of local communities' life, is of paramount importance features the SI concept. With the growing trend towards a new type of energy market, in that energy supply has been increasingly decentralized, new forms of commercial models are emerging; consumers are controlling their energy generation and consumption, and technologies innovatively penetrate the market like smart meters and electric vehicles (EVs) with priority of demand management, so, islands appear as the ideal lands for testing new technologies and scalable processes with the participation of all relevant actors, such as government officials, water and electricity, market players, network operators, and citizens.

However, because of these common trends, the inactivity of politics and technology, along with the ongoing economic crisis, prevent the islands from completely exploiting their potential to host sustainable and innovative plans. This is because of a wide range of factors. Such tests and scales of innovative applications are considered as risky endeavor, thus, new technological solutions can have challenges in systems and economies of the island, and finally, technologies and their consequences are not often fully understood in different areas. In contrast with this drawback, the islands have to build the groundwork for better understanding of their potential and assessing priorities. This allows them to take a holistic approach when developing and performing new projects, including economic, social and environmental considerations. Therefore, before an island is able transform itself into a SI; it should be better first to find out precisely where it is in relation to other regions by setting appropriate indicators to measure, monitor, and evaluate effects. It allows sustainable islands to ensure that their ecosystems are exploited while taking advantage of their comparisons. Environmental CPSs are often utilized to monitor for understanding behaviors, and controlling the physical globe [33].

Because the representative CPS program is emerging, the expansion of SIs has been seen. SI is a relatively new form of power distribution system which connects power lines such as traditional power grids as well as ICT infrastructure to smart meters, which might be in the form of specialized tools including telephones, mobile, laptops or other gadgets in the island in oceans. Many of these SI devices allow data systems to accomplish predictive assessment, which can balance the generation and consumption of electricity in the network system. Real-time pricing, for instance, gives consumers and suppliers' worthwhile clues to aid manage their demand and energy resources. As a result, energy distribution that is able to control the processes of energy production, consumption and transmission can be carried out in a more efficient and dynamic way.

Nonetheless, the incongruity, variety, and intricacy of SIs provide fundamental challenges to ensuring the overall integrity of the system [34]. This matter is because in the SIs, network inference and decision-making might be carried out on local smart components than on preserved control centers. Thus, unlike common power networks where most attacks

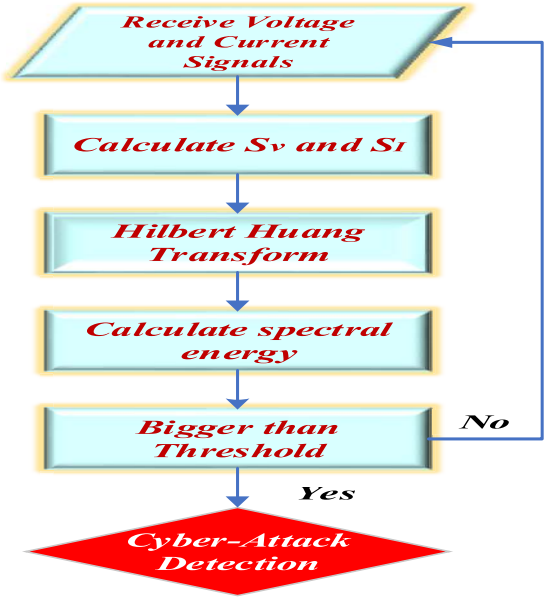


FIGURE 2. Proposed FDIA detection approach.

and failures are transferred from physical access to important facilities [35], the widespread use of SI components invites most of these anomalies from cyber substructures. A common SI attack is a FDI that can be utilized to distort real power demand and supply resources. Therefore, energy distribution might be incorrect, leading to further costs or even more destructive risks. It is necessary to trust such systems and achieve security because national security and not only cyber security can be compromised. Nonetheless, new countermeasures against the FDI have concentrated on the traditional state of the power systems [34], in that FDI attacks on physical meters are performed rather than intelligent and smart components [35]. Regardless of cyber-attacks and the distributed design of SI substructure, these methods might not dedicate any positive result with the full protection that need to quickly make a decision for any local smart device or component according to the status information. Considering all the above mentioned issues, in this paper, a method which can be easily performed on every smart island to detect FDI in real time is presented.

E. PROPOSED FDIAS DETECTION SCHEME

Because the false attack vector satisfies Kirchhoff's basic underlying rules, it can escape the remaining BDD and bring the system modes to deviate from normal events. Nevertheless, we are going to make it clear that there is time interdependence among dynamic system states, which allows hackers to monitor the system for a long time and continuously manipulate all relevant measurements to produce non-FDIA detection given a temporary correlation. This complicated form of attack would be infeasible to create in the actual power utilities [28].

Considering this issue, instead of out-of-line training and the scattering of recognizing attack behaviors in previous

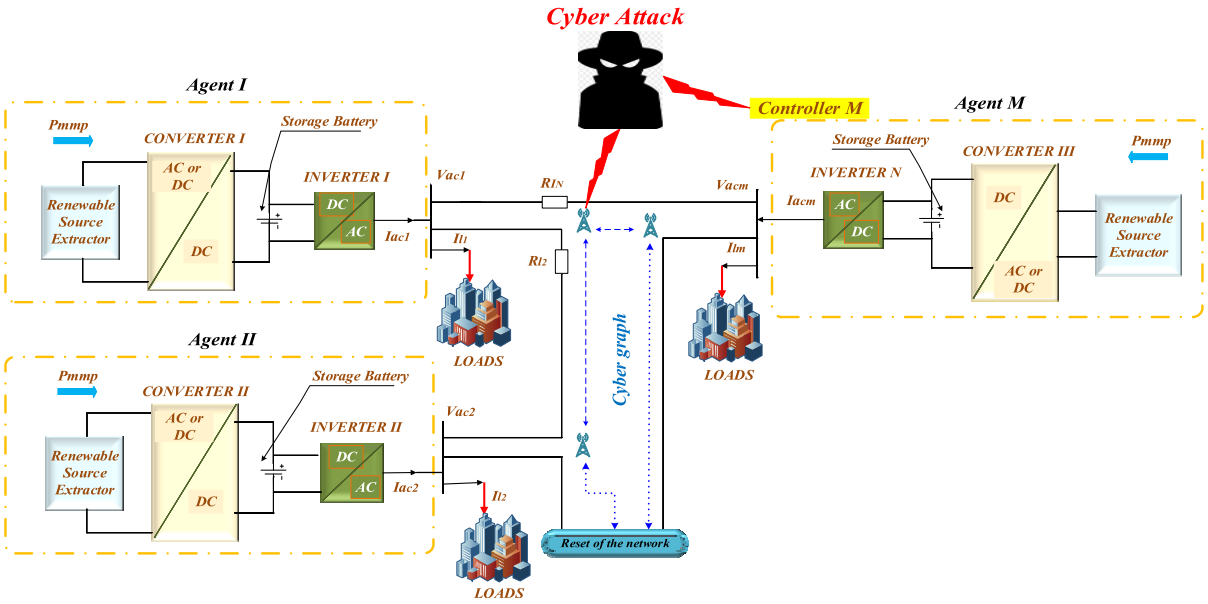


FIGURE 3. Cyber-physical type of AC smart islanding: Blue arrows give the cyber layer; Black lines give the physical circuit.

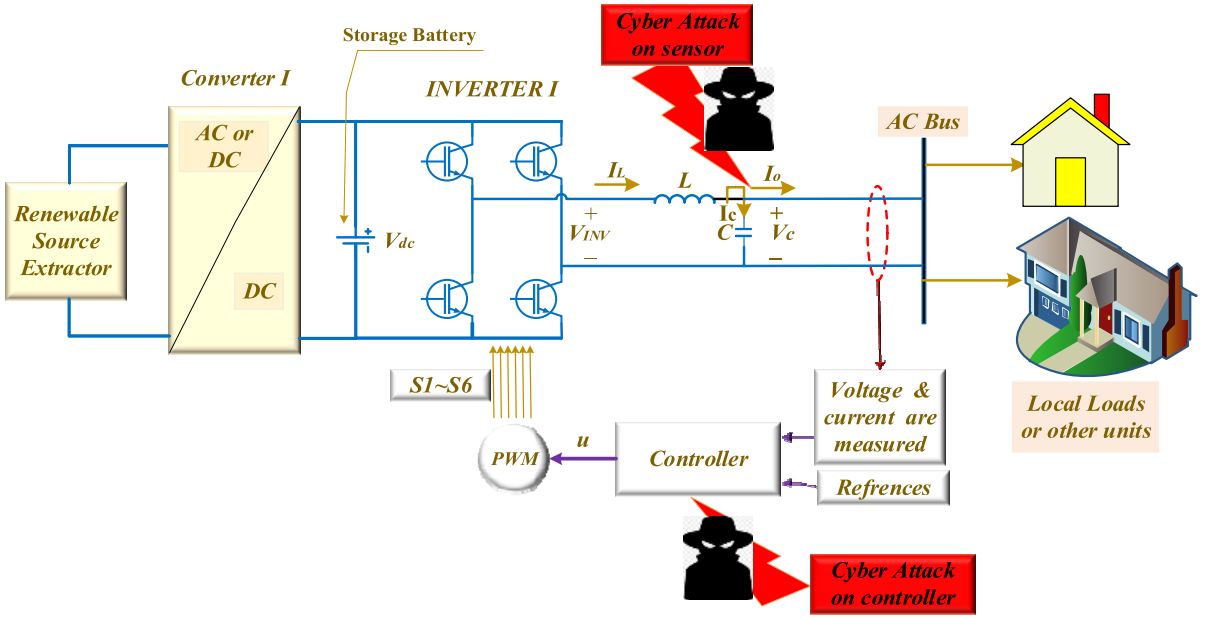


FIGURE 4. Typical diagram of a three-phase MG with cyber-attack.

works, in this part, a real-time FDIAs detection mechanism to identify possible attacks by recording changes in temporal correlation properties between states of the systems is introduces. Figure 2 displays the main structure of the presented FDIA identification mechanism in real time. The signals are retrieved and then the signal is processed by HHT to detect the cyber-attack in AC SI.

III. CASE STUDIES

A. SMART ISLAND MODEL

Figure 3 depicts the islanded MG by m-th distributed production units in the mode of parallel connection. Other units are working in load sharing mode and current control state [36], [37]. Some units in this MG are in the voltage frequency mode. They are responsible for stabilizing the voltage of MG. Figure 4 illustrates the power circuit of a typical three-phase inverter which connected to MG. For simplicity, in this study, the single-phase system is examined first; the equations are then generalized to these types of three-phase inverters that the topology of all three phases being the same as the single-phase system.

The block diagram of used single-phase inverter is displayed in Figure 5 [36, 37]. The LC output filter was used to reduce the harmonic components of the output

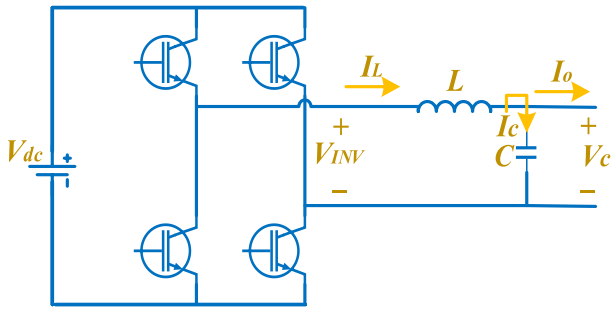


FIGURE 5. The scheme of a single-phase inverter.

voltage generated by the Pulse Width Modulation (PWM) inverter.

The state equations in the single-phase inverter depicted in the Figure 5 are given in formulas (14) and (15).

$$L\frac{dI_L}{dt} + V_o = V_{INV} \tag{14}$$

$$I_L = I_c + I_o, \quad I_c = C\frac{dV_o}{dt} \tag{15}$$

where, $V_{INV} = uV_{dc}$ is the output voltage of inverter; u represents the input signal of controller. By combining formulas (14) and (15) gives equation (16)

$$\frac{d}{dt}\begin{bmatrix} V_o \\ I_L \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{C} \\ -\frac{1}{L} & 0 \end{bmatrix}\begin{bmatrix} V_o \\ I_L \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{V_{dc}}{L} \end{bmatrix} u + \begin{bmatrix} -\frac{I_o}{C} \\ 0 \end{bmatrix} \tag{16}$$

where in this equation, both capacitor voltage (V_o) and inductive current (I_L) are chosen as the state variables. V_{dc} also represents the DC link voltage or Uninterruptable Power Supply (UPS). I_o and I_c define the filter output current and the capacitor current, respectively.

Based on sliding mode controller, the index of cyber-attack detection for FDIA in voltage and current parameters is defined in equation (17) and (18) [36], [37].

$$S_V = \dot{\tilde{x}} - \lambda\tilde{x}, \quad \tilde{x} = x - x_{base} \tag{17}$$

$$S_I = z - z_{base} \tag{18}$$

where S_V and S_I (switching surface of voltage and current) is the voltage index and current index for cyber-attack detection, respectively, which are applied as a input of Huilbert-Huang transform. λ is a positive number, x and z are the SI voltage and current, respectively. x_{base} and z_{base} are the base voltage and current of SI, respectively. x_{base} has a constant amplitude and frequency. z_{base} is measurable for each agent.

In this paper, the considered autonomous AC-MG is displayed in Figure 6.

DC sources are connected to each other by DC-AC inverters via tie lines, thus forming the physical layer of the MG. Every DC-AC inverter works to maintain the output voltage according to the values of reference generated by the main and secondary local controllers. In this article, the unexplained cyber chart from the communication grid has been considered to send and receive data from its neighbors. In addition, they are repeatedly connected at the output of the converter of each unit.

The suggested attack detection scheme is performed on a cyber-physical AC-MG as displayed in Figure 6(b) with $V_{ref} = 110sin(2 * pi * 60)$. V includes three factors of equal capacity connected to each other through resistance lines. It is important to mention that every agent includes a battery factor with DC / AC inverters are shown in Figure 6 (a). In order to test the performance and feasibility of the presented attack

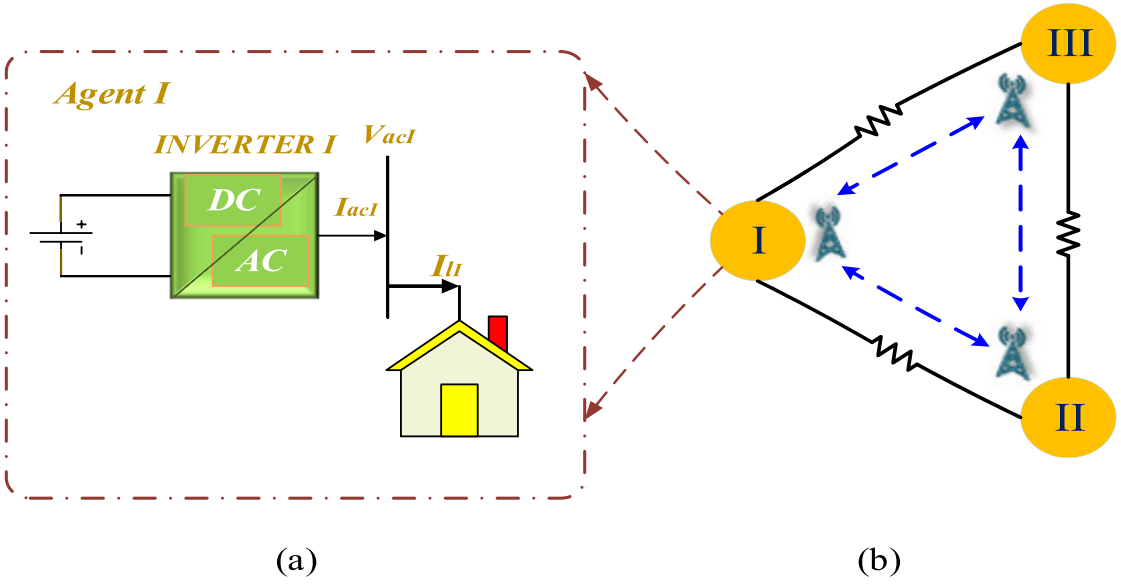


FIGURE 6. Intended system: (a) Agent model; (b) Cyber-physical AC-MG with three resources.

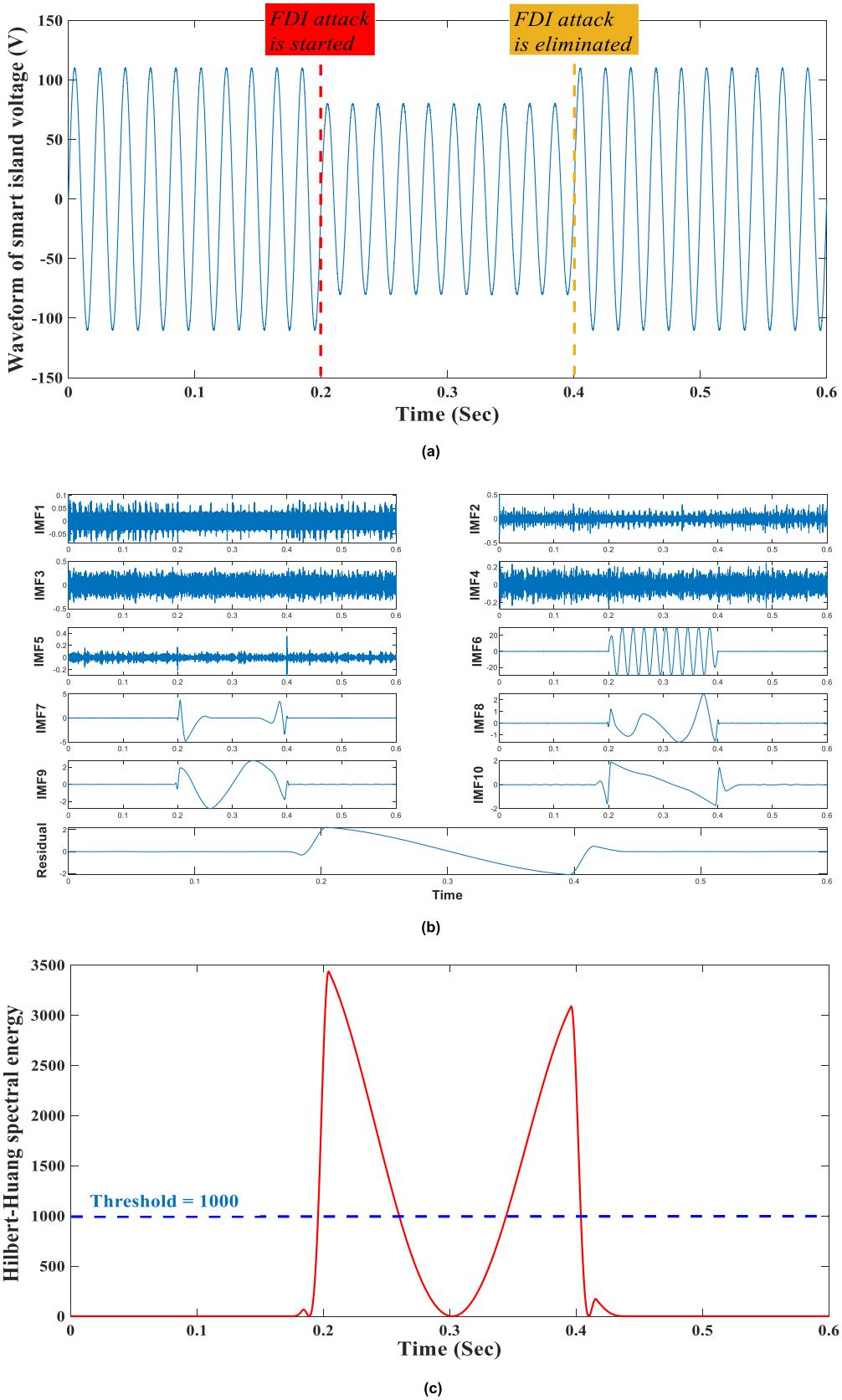
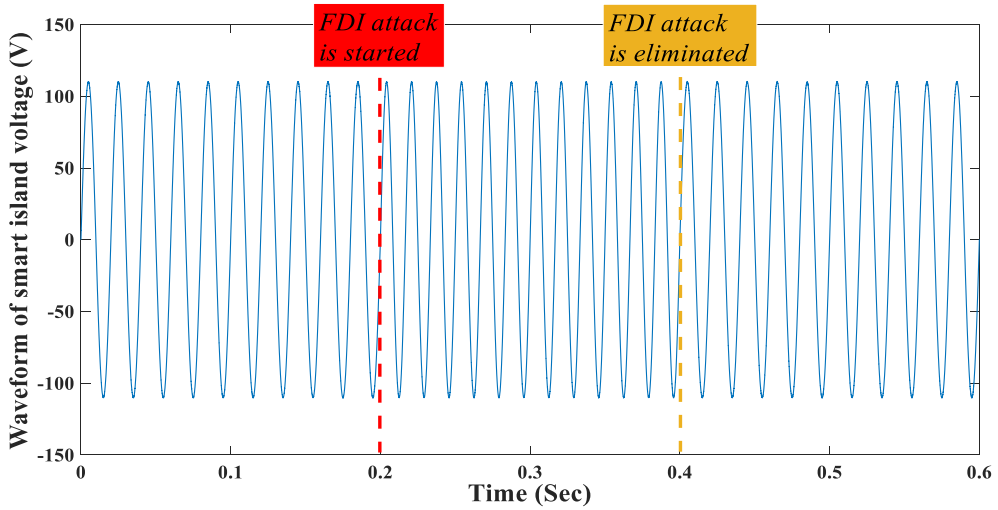
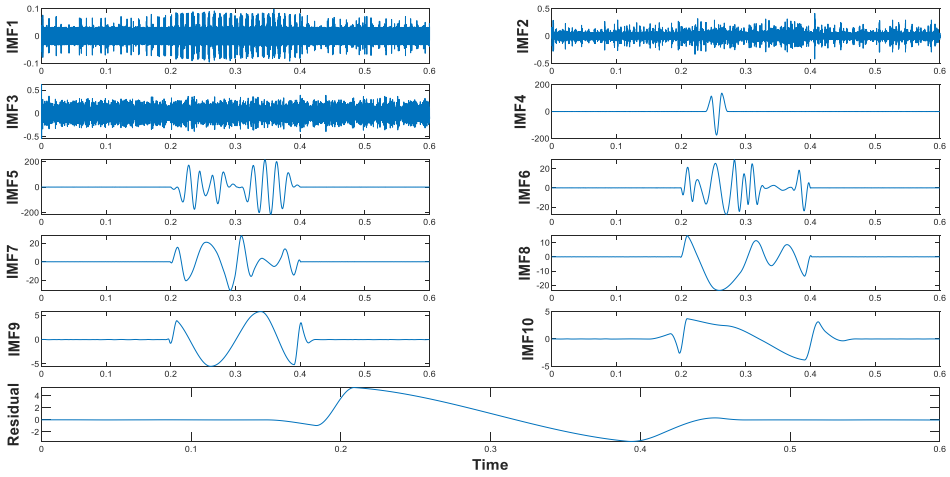


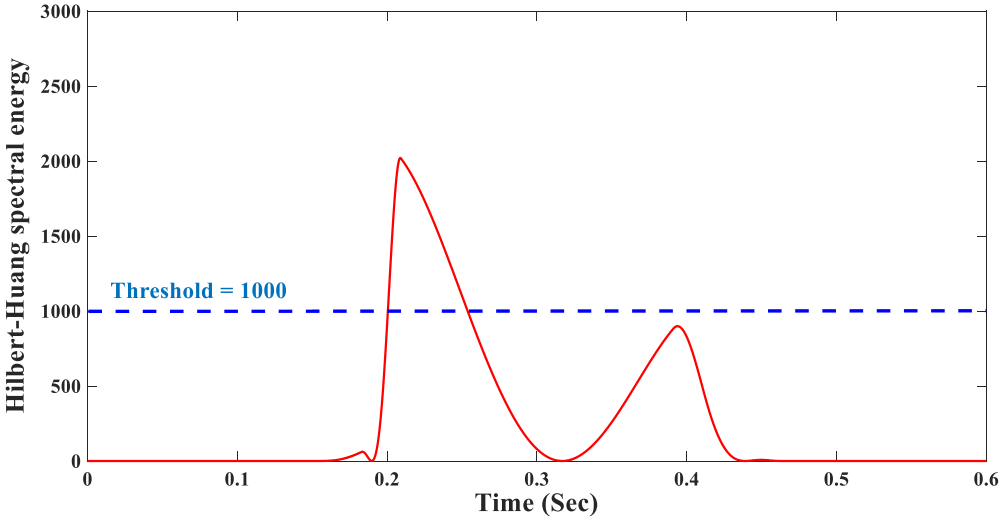
FIGURE 7. FDI attack to the amplitude of voltage signal (cyber-attack has started at t = 0.2 second and has eliminated at t = 0.4 second): a) Waveform of SI voltage, b) Empirical mode decomposition of input index of voltage, c) Hilbert-Huang spectral energy of input index of voltage.



(a)



(b)



(c)

FIGURE 8. FDI attack to the frequency of voltage signal (cyber-attack has started at t = 0.2 second and has eliminated at t = 0.4 second): a) Waveform of SI voltage, b) Empirical mode decomposition of input index of voltage, c) Hilbert-Huang spectral energy of input index of voltage.

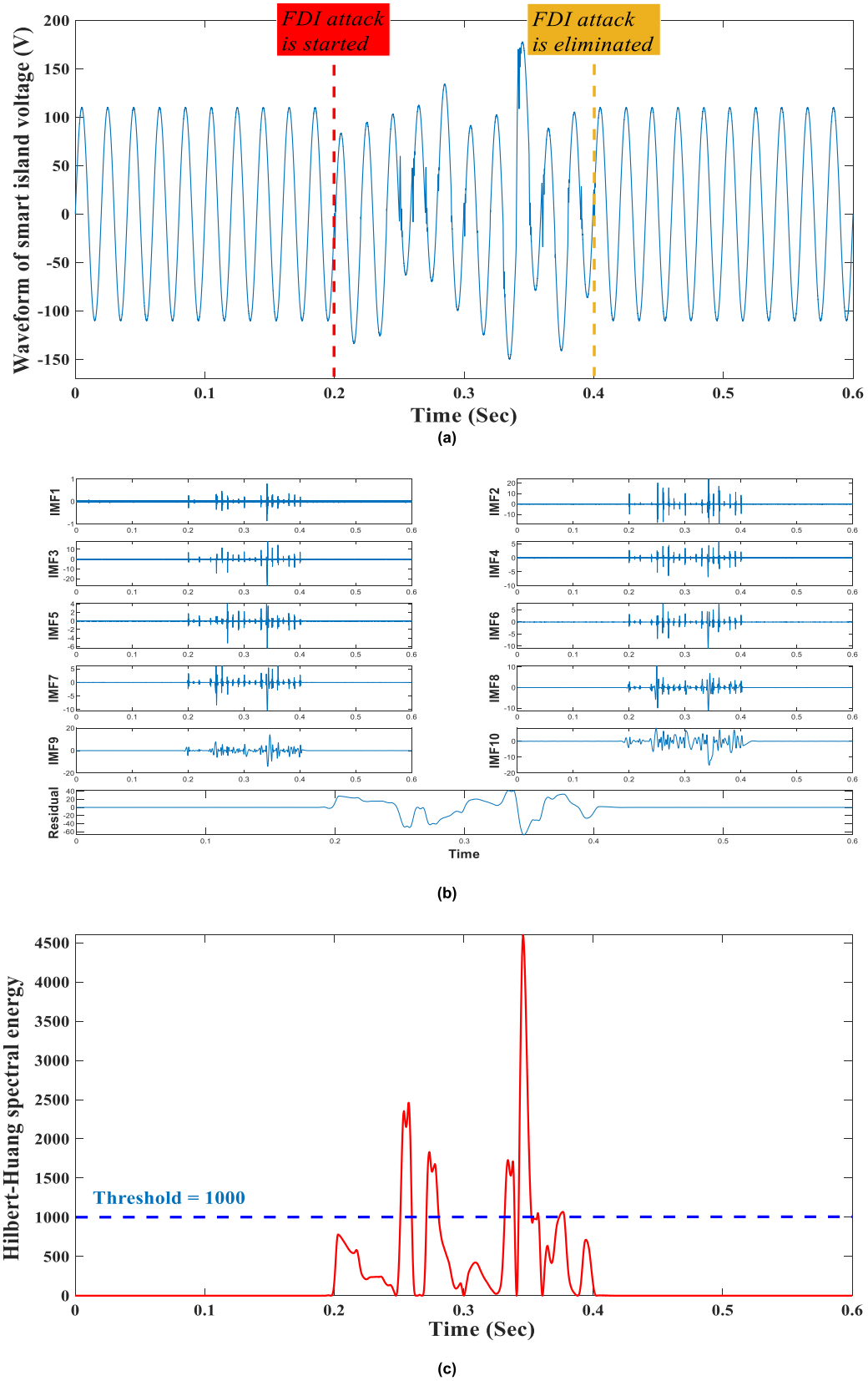
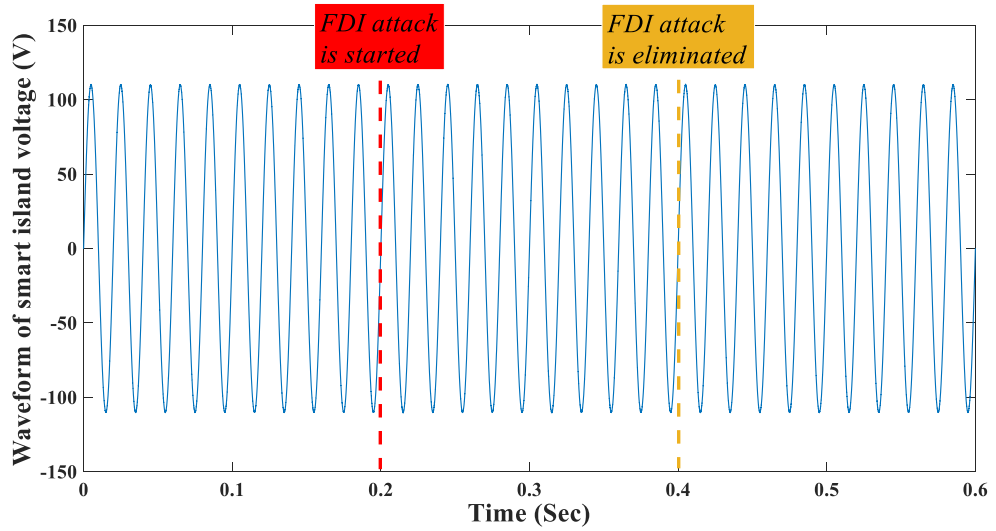
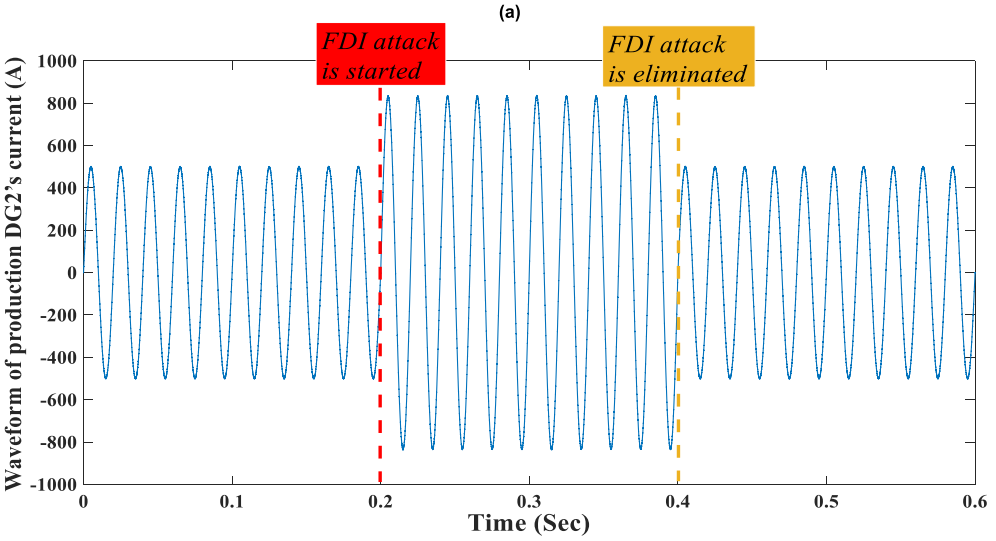


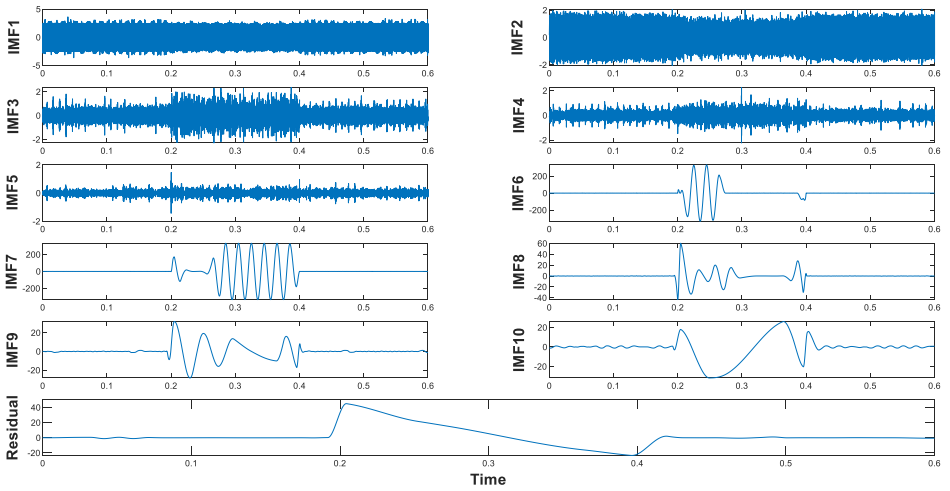
FIGURE 9. FDI attack by adding a white noise to the voltage signal (cyber-attack has started at t = 0.2 second and has eliminated at t = 0.4 second): a) Waveform of SI voltage, b) Empirical mode decomposition of input index of voltage, c) Hilbert-Huang spectral energy of input index of voltage.



(a)

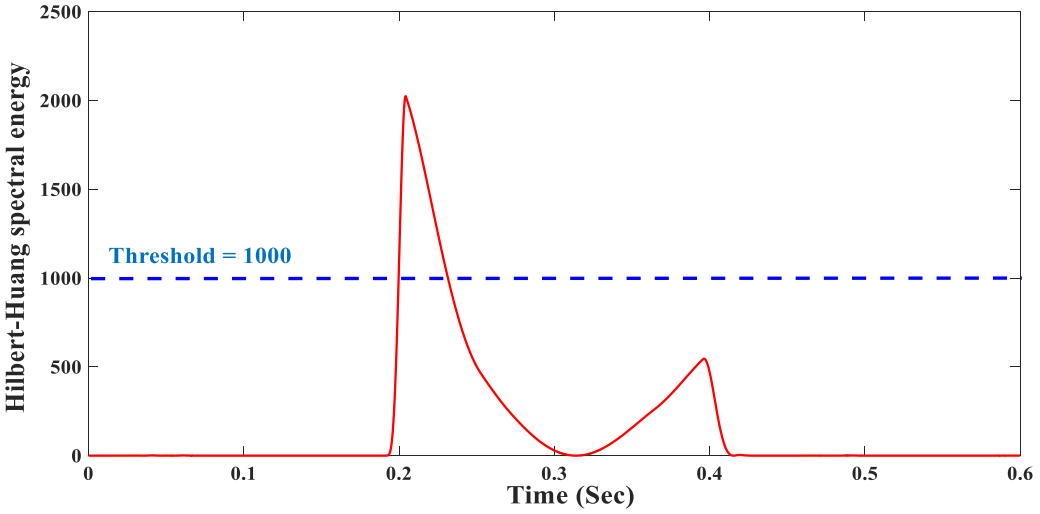


(b)



(c)

FIGURE 10. FDI attack to the current signal on agent II (cyber-attack has started at t = 0.2 second and has eliminated at t = 0.4 second): a) Waveform of SI voltage, b) Waveform of production DG2's current, c) Empirical mode decomposition of input index of current, d) Hilbert-Huang spectral energy of input index of current.



(d)

FIGURE 10. *(Continued.)* **FDI attack to the current signal on agent II (cyber-attack has started at t = 0.2 second and has eliminated at t = 0.4 second): a) Waveform of SI voltage, b) Waveform of production DG2's current, c) Empirical mode decomposition of input index of current, d) Hilbert-Huang spectral energy of input index of current.**

detection strategy for the AC-MG cooperative, several attacks including the FDIAs have been tested on multiple sensors, which are not usually detected by distributed observers an is necessary to confirm security. The control system and parameters were presented in our previous work in the reference [37]. Another important point is that every event in the above scenarios is divided by a certain time interval for a better understanding.

Case Study I: Instability arising from injecting an attack by changing the amplitude of voltage signals.

In this part, an example of a FDI cyber-attack on the voltage range is stated. An attack can be on a voltage measuring sensor, the amount sent via wireless or fiber optic, or the reference value given in the controller or changing the values of the controller. To better understanding the issue, the attack started and ended in a period of time. The attack started at 0.2 seconds and ended at 0.4 seconds. Sample simulation results are shown in Figure 7. Figure 7(a) is the intelligent island network voltage to which the FDI attack has been reported in time. Figure 7(b) shows the Hilbert-Huang conversion under different IMFs along with the residual value. Figure 7(c) Hilbert-Huang spectral energy shows the S_v index signal, which is able to detect a cyber-attack by determining the threshold at 1000. This value (1000) is obtained according to experimental results. The detection time is less than 5 ms from the FDIA occurred.

Case Study II: Instability arising from injecting an attack by changing the frequency of voltage signals.

In this part, an example of an FDI cyber-attack on the voltage signal frequency is described. The attack can be on a voltage measuring sensor, or the amount sent via wireless, or fiber optic, or the reference value given in the controller, or changes the values of the controller. To better understanding the issue, the attack began and ended over a period of time. The attack started at 0.2 seconds and ended at 0.4 seconds. The simulation results of the sample are shown in Figure 8. Figure 8(a) is the intelligent island network voltage to which the FDI attack has been reported in time. Figure 8(b) shows the Hilbert-Huang conversion under different IMFs with residual value. Figure 8(c) Hilbert-Huang spectral energy shows the S_v index signal, which can detect a cyber-attack by determining the threshold at 1000. The detection time is less than 5 ms from the FDIA occurred.

Case Study III: Instability arising from injecting an attack by adding a white noise to the voltage signals.

In this section, an example of a FDI cyber-attack on a voltage signal is expressed by adding white noise to the voltage signal. The attack can be on a voltage measuring sensor, the amount sent via wireless or fiber optic. To better understanding the issue, the attack began and ended over a period of time. The attack started at 0.2 seconds and ended at 0.4 seconds. Sample simulation results are shown in Figure 9. Figure 9(a) is the intelligent island network voltage to which the FDI attack has been reported in time. Figure 9(b) shows the Hilbert-Huang conversion under different IMFs along with the residual value. Figure 9(c) Hilbert-Huang spectral energy shows the S_v index signal, which is able to detect a cyber-attack by determining the threshold at 1000. The detection time is less than 50 ms from the FDIA occurred.

Case Study IV: Instability arising from injecting an attack by changing the current signal on agent II.

In this part, an example of a FDI cyberattack on signal flow of units II is described. An attack can be on a current measuring sensor, the amount sent via wireless or fiber optic, or the reference value given in the controller, or changing the values of the controller. In order to better understanding the

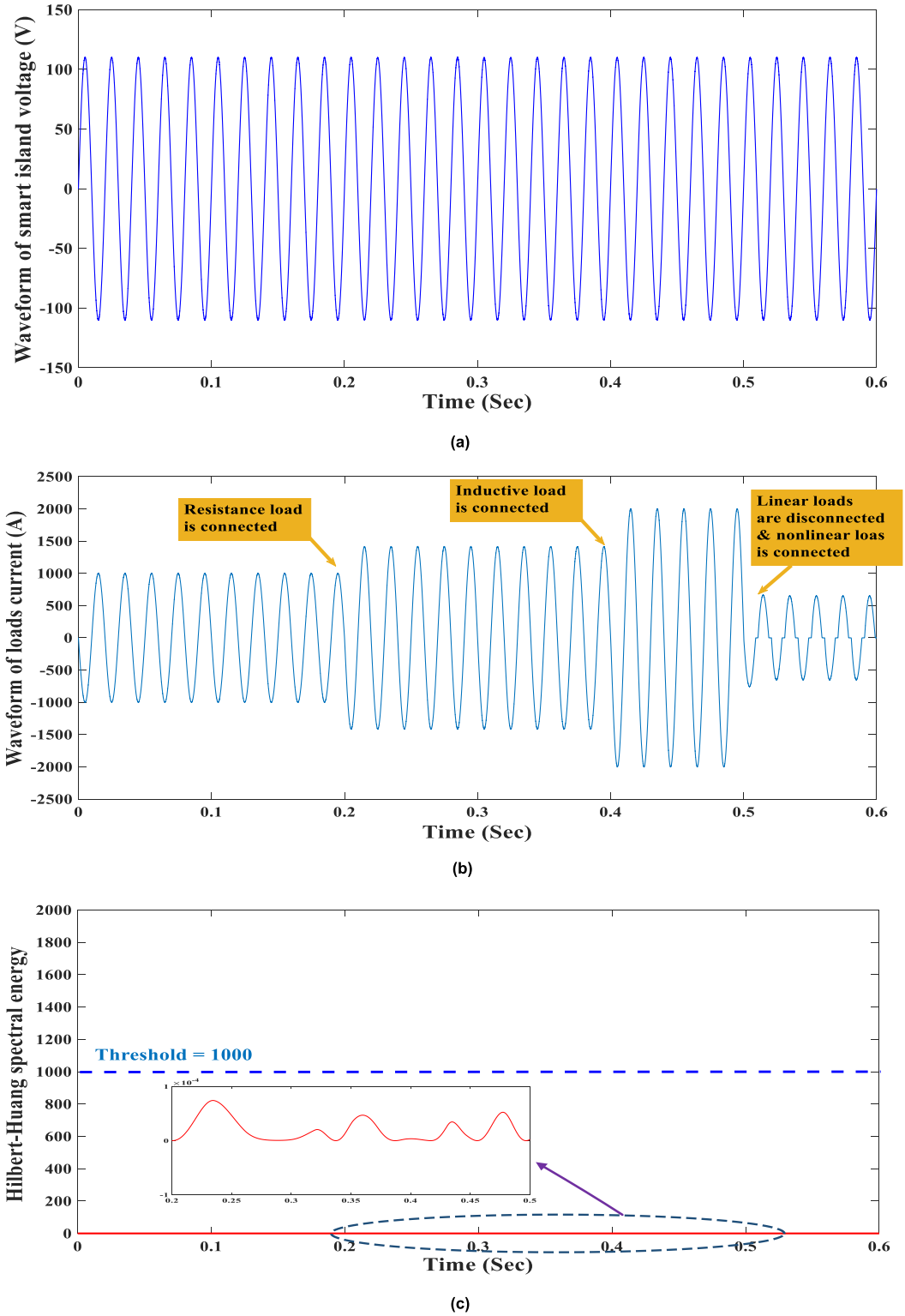
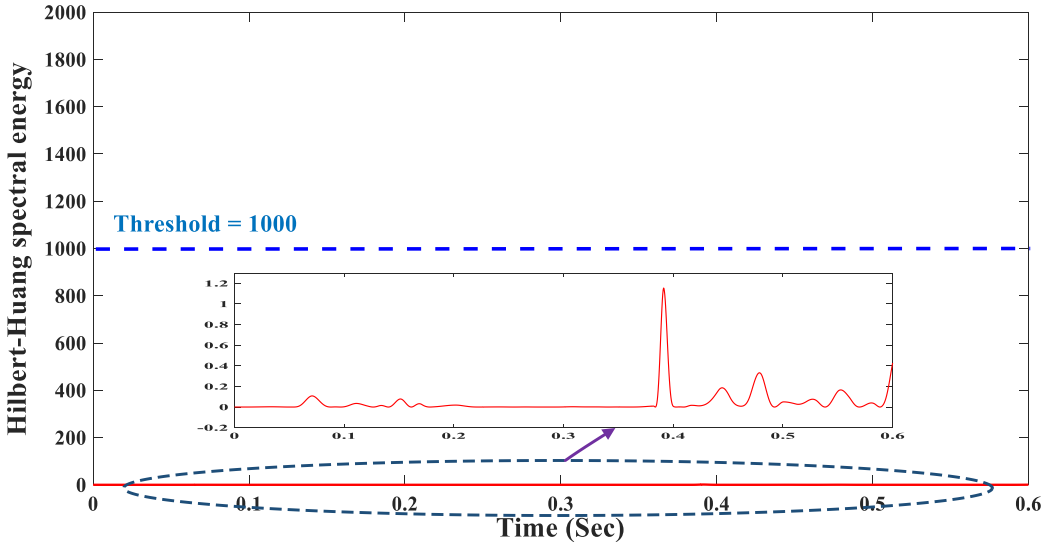


FIGURE 11. Load changing: a) Waveform of SI voltage, b) Waveform of loads current, c) Hilbert-Huang spectral energy of input index of voltage, d) Hilbert-Huang spectral energy of input index of current.

issue, the attack began and ended over a period of time. The attack started at 0.2 seconds and ended at 0.4 seconds. Sample simulation results are shown in Figure 10. Figure 10(a) is the intelligent island network voltage. Figure 10(b) shows the flow of the production unit II that was attacked by the FDI, which was declared the FDI attack. Figure 10(c) shows the



(d)

FIGURE 11. *(Continued.)* **Load changing: a) Waveform of SI voltage, b) Waveform of loads current, c) Hilbert-Huang spectral energy of input index of voltage, d) Hilbert-Huang spectral energy of input index of current.**

Hilbert-Huang conversion under different IMFs with residual values. Figure 10(d) Hilbert-Huang spectral energy shows the signal of the S_I index, which is able to detect cyber-attack by determining the threshold of 1000. The detection time is less than 5 ms from the FDIA occurred.

Case Study V: Load changing.

In this part, the behavior of the system under load changes is examined; the Hilbert-Huang spectral energy index of the S_v voltage index and the S_I current, which is used as the FDI detection index, has been investigated during load changes. Sample simulation results are shown in Figure 11. Figure 11(a) is the SI network voltage. Figure 11(b) shows the unit load current. As can be seen, the resistive and ohmic loads are connected to the network at 0.2 and 0.4, respectively, and are disconnected both times at 0.5. It is also connected to the system nonlinearly 0.5 times. Figures 11(c) and 8d show Hilbert-Huang spectral energy signals S_v and S_I, respectively. As can be seen, it is less than the threshold value for detecting a cyber-attack, and in this method, the FDI attack is distinguished from load changes.

TABLE 1. **Confusion rate matrix of the presented detection layout.**

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

TABLE 2. **Confusion result matrix of the presented detection layout.**

			Actual Value		Number of Testing Data	Identified to be Compromised	Identified to be Normal
			Pos	Neg			
Detection Model Response	Deep Learning	Pos	93.17 %	5.38 %	1274	1187	87
		Neg	6.83 %	94.62 %	1026	56	970
	Shallow Model	Pos	89.47 %	9.93	1147	1026	121
		Neg	10.53 %	90.07 %	981	103	878

IV. DISCUSSION ABOUT SIMULATION RESULTS

Generally, it is said that when an issue is considered as a cyber activity, it can be a positive decision. In contrast, it is a negative decision when the model of anomaly detection recognizes as a normal behavior. The true decision is made whenever the pattern of abnormal detection is correct. As a result, it is obvious that a wrong decision indicates a wrong reaction from the cyber-attack detection model. Based on this, it can be concluded that a suitable model for detection anomalies is a model with a low false rate. According to these definitions, we can define 4 different type named: False Alarm Rate (FAR), Hit Rate (HR), Correct Reject Rate (CRR), and Miss Rate (MR). In order to better understanding of these issues, Table 1 gives the confusion matrix.

To verify the efficiency and validation of suggested Hilbert-Huang transform in FDI attack detection, different sample test is applied. The performance of the proposed detection scheme is assessed through applying the FDIA layout and the evaluation results are displayed. The efficiency of suggested detection scheme is analyzed through applying the FDI attack model and the evaluation results are in Table 2. In addition, to show the efficiency of proposed cyber-attack detection frame, it has been compared with Shallow model.

Table 2 can remark that the suggested technique can detect the FDIAs with detection accuracy over 93%, and the detection accuracy based shallow model is able to detect FDIAs over 90%, so, it shows the efficiency of the proposed detection technique to detect the FDIAs.

V. CONCLUSION

The positive point of using HHT in cyber-attack detection is that the signals in the SI are unstable, meaning that their frequency changes with time. Hence, in this paper, HHT has been presented to compute spectral energy for FDI attack detection applications in AC Smart Islands. The presented technique successfully identified the true time of the cyber-attack by displaying a dramatic deviation in the time frequency spectrum at the time of the FDIA occurrence in AC-SI. The suggested scheme is able to detect FDIAs such as cyber-attacks in current and voltage signals of sensor or transmission data from wireless or fiber optic from common system operating status variations like load variation. The simulation results on a test SI demonstrated and proved the high performance and effectiveness of the proposed scheme, especially in the FDI attack detection, where the presented model was able to gain accuracy rate of 93.17% (3% more than detection based on shallow model). Additionally, the suggested protection scheme is able to detect FDI less than 50 ms after cyber-attack is started in different scenarios and it would be simple and easy to perform.

REFERENCES

[1] D. R. McKinnel, T. Dargahi, A. Dehghantanha, and K.-K.-R. Choo, "A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment," *Comput. Electr. Eng.*, vol. 75, pp. 175–188, May 2019.

[2] F. Darbandi, A. Jafari, H. Karimipour, A. Dehghantanha, F. Derakhshan, and K.-K. Raymond Choo, "Real-time stability assessment in smart cyber-physical grids: A deep learning approach," *IET Smart Grid*, vol. 3, no. 4, pp. 454–461, Aug. 2020.

[3] S. Kim and S. Park, "CPS(cyber physical system) based manufacturing system optimization," *Procedia Comput. Sci.*, vol. 122, pp. 518–524, Jan. 2017.

[4] R. Wei, T. P. Kelly, R. Hawkins, and E. Armengaud, "Deis: Dependability engineering innovation for cyber-physical systems," in *Proc. Fed. Int. Conf. Softw. Technol., Appl. Found.*, 2017, pp. 409–416.

[5] M. Fathi and M. 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.

[6] E. Irmak and I. Erkek, "An overview of cyber-attack vectors on SCADA systems," in *Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS)*, Mar. 2018, pp. 1–5.

[7] L. Che, X. Liu, Z. Shuai, Z. Li, and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6545–6556, Nov. 2018.

[8] 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.

[9] N. E. Huang, Z. Shen, and S. R. Long, "A new view of nonlinear water waves: The Hilbert spectrum," *Annu. Rev. Fluid Mech.*, vol. 31, no. 1, pp. 417–457, Jan. 1999.

[10] N. E. Huang, Z. Shen, S. R. Long, M. C. Wu, H. H. Shih, Q. Zheng, N.-C. Yen, C. C. Tung, and H. H. Liu, "The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis," *Proc. Roy. Soc. London. Ser. A, Math., Phys. Eng. Sci.*, vol. 454, no. 1971, pp. 903–995, Mar. 1998.

[11] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019.

[12] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[13] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2013, pp. 1–5.

[14] 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.

[15] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[16] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

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

[18] 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.*, Mar. 2020.

[19] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. Int. Conf. Internet Things 4th Int. Conf. Cyber, Phys. Social Comput.*, Oct. 2011, pp. 380–388.

[20] A. Sawas and H. E. Z. Farag, "Two-fold intelligent approach for successful FDI attack on power systems state estimation," in *Proc. IEEE Electr. Power Energy Conf. (EPEC)*, Oct. 2018, pp. 1–6.

[21] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv. (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.

[22] C. M. Ahmed, J. Zhou, and A. P. Mathur, "Noise matters: Using sensor and process noise fingerprint to detect stealthy cyber attacks and authenticate sensors in CPS," in *Proc. 34th Annu. Comput. Secur. Appl. Conf.*, Dec. 2018, pp. 566–581.

[23] Y. Shoukry, M. Chong, M. Wakaiki, P. Nuzzo, A. Sangiovanni-Vincentelli, S. A. Seshia, J. P. Hespanha, and P. Tabuada, "SMT-based observer design for cyber-physical systems under sensor attacks," *ACM Trans. Cyber-Phys. Syst.*, vol. 2, no. 1, pp. 1–27, Feb. 2018.

[24] D. Hadžiosmanović, R. Sommer, E. Zambon, and P. H. Hartel, "Through the eye of the PLC: Semantic security monitoring for industrial processes," in *Proc. 30th Annu. Comput. Secur. Appl. Conf. ACSAC*, 2014, pp. 126–135.

[25] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov. 2015.

[26] C. M. Ahmed, M. Ochoa, J. Zhou, A. P. Mathur, R. Qadeer, C. Murguia, and J. Ruths, "NoisePrint: Attack detection using sensor and process noise fingerprint in cyber physical systems," in *Proc. Asia Conf. Comput. Commun. Secur. ASIACCS*, 2018, pp. 483–497.

[27] K. N. Junejo and J. Goh, "Behaviour-based attack detection and classification in cyber physical systems using machine learning," in *Proc. 2nd ACM Int. Workshop Cyber-Phys. Syst. Secur. CPSS*, 2016, pp. 34–43.

[28] P. Nader, P. Honeine, and P. Beauseroy, "Detection of cyberattacks in a water distribution system using machine learning techniques," in *Proc. 6th Int. Conf. Digit. Inf. Process. Commun. (ICDIPC)*, Apr. 2016, pp. 25–30.

[29] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," in *Proc. Sci. Inf. Conf.*, Aug. 2014, pp. 626–631.

[30] R. C. Borges Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *Proc. 7th Int. Symp. Resilient Control Syst. (ISRCS)*, Aug. 2014, pp. 1–8.

[31] A. Bernadić and Z. Leonowicz, "Fault location in power networks with mixed feeders using the complex space-phasor and Hilbert–Huang transform," *Int. J. Electr. Power Energy Syst.*, vol. 42, no. 1, pp. 208–219, Nov. 2012.

[32] L. Che, X. Liu, and Z. Li, "Mitigating false data attacks induced overloads using a corrective dispatch scheme," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3081–3091, May 2019.

[33] E. A. Lee, "Cyber-physical systems-are computing foundations adequate," in *Proc. Position Paper NSF Workshop Cyber-Phys. Syst., Res. Motivat., Techn. Roadmap*, 2006, pp. 1–9.
[34] Y. Mo, T. Hyun-Jin Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.
[35] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, p. 15, 2009.
[36] 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.
[37] M. Dehghani, T. Niknam, M.-R. Tavana, and G. Asadi, "A rotating reference signal based on nonlinear control for multi-bus single phase microgrids," *Universal J. Control Automat.*, vol. 4, no. 3, pp. 29–41, 2016.

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, and the Ph.D. degree in electrical engineering from the Shiraz University of Technology, Shiraz, in 2019. His current research interests include power electronic, control, and cyber security analysis of smart grids, microgrid, smart city, and HVDC systems, and protection of power systems, fuzzy logic, and signal processing.

MOHAMMAD GHIASI (Graduate Student Member, IEEE) received the B.S. and M.S. degrees in electrical power engineering, in 2012 and 2016, respectively. Since 2007, he has been with the Power Control Center (PCC) of Tehran Metro as a Senior Control Power Engineer. He is currently a Research Assistant with the Shiraz University of Technology, Shiraz, Iran. His research interests include modeling, simulation and optimization of power systems, integration and control of hybrid and distributed renewable energy resources, smart grids, and resilience and cyber security in power systems has led to multiple publications in these fields. He is also a member of the Tehran Construction Engineering Organization (TCEO).

TAHER NIKNAM (Member, IEEE) was born in Shiraz, Iran. He received the B.S. degree from Shiraz University, Shiraz, 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 currently a Faculty Member with the Department of Electrical Engineering, 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, Ann Arbor, MI, USA, from 2016 to 2018. He was also 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, and electric vehicles, and protection of power systems, reliability, artificial intelligence, and machine learning. He is also an Editor in Springer and ISTE ISI journal.

SANJEEVIKUMAR PADMANABAN (Senior Member, IEEE) received the bachelor's degree in electrical engineering from the University of Madras, Chennai, India, in 2002, the master's degree (Hons.) in electrical engineering from Pondicherry University, Puducherry, India, in 2006, and 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 with 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. He was also 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, Esbjerg, Denmark. He has authored more than 300 scientific articles. He is also 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 was a recipient of the Best Paper cum Most Excellence Research Paper Award from IET-SEISCON 2013, IETCEAT 2016, the IEEE-EECSI 2019, the IEEE-CENCON 2019, and five best paper awards from ETAEERE 2016 sponsored Lecture Notes in Electrical Engineering, Springer book. He is also an Editor/Associate Editor/Editorial Board for refereed journals, in particular the IEEE Systems Journal, the IEEE Transactions on Industry Applications, IEEE Access, *IET Power Electronics*, and *International Transaction on Electrical Energy Systems* (Wiley), and the Subject Editor for the *IET Renewable Power Generation*, *IET Generation, Transmission & Distribution*, and *Obesity Facts* journal (Canada).