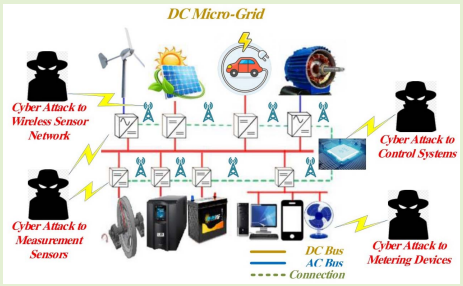
Cyber Attack Detection Process in Sensor of DC Micro-Grids Under Electric Vehicle Based on Hilbert–Huang Transform and Deep Learning

Hao Cui, Xiaorui Dong, *Member, IEEE*, Hongyan Deng, Moslem Dehghani, Khalid Alsubhi, *Member, IEEE*, and Hani Moaiteq Abdullah Aljahdali

***Abstract*—In this article, a new procedure is proposed on the basis of Hilbert-Huang Transform and deep learning for cyber-attacks detection in direct current (DC) micro-grids (MGs) as well as detection of the attacks in distributed generation (DG) units and its sensors. An advanced elective group deep learning method with Krill Herd Optimization (KHO) algorithm is proposed. At first, Hilbert-Huang Transform is used with the aim of extracting the signals feature and next these features are applied as the multiple deep input basis models are made with the aim of capturing automatically sentient traits from raw fluctuation signals. At third, to make sure the variety of the basis patterns, linear decoder, denoising autoencoder and sparse autoencoder are applied to make various deep autoencoders, respectively. Further, Bootstrap is applied with the aim of designing separate educational data subsets for any base model. Fourth, for implementing selective ensemble learning, a combination strategy of enhanced weighted voting (EWV) with class-particular thresholds is studied. Eventually, KHO algorithm is applied with the aim of adaptive selecting the optimal class-specific thresholds. In the offered tactic, firstly, a DC micro-grid is functioned and controlled with the lack of any false data injection attacks (FDIAs) to collect adequate information within the usual operation needed for the educating of deep learning networks. It is noteworthy that, in the procedure of datum production, load variable is also determined with the aim of having distinctive datasets for cyber-attack scenarios and load variables. Also, to provide more realistic method, the smart plug-in electric vehicle is also considered in the model. Outcomes of Simulation in various scenarios are applied with the aim of verifying the benefit of the offered procedure. The outcomes propose that the offered procedure is able to more accurate and robust know various type of false data injection attack over than 93.76% accuracy detection of true rate.**



***Index Terms*— False data injection attack, Hilbert-Huang transform, dc micro-grid, deep learning, krill herd optimization, electric vehicle.**

Manuscript received September 3, 2020; accepted September 25, 2020. Date of publication September 29, 2020; date of current version July 14, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 61262047 and in part by the Dongying Key Laboratory of Intelligent Information Processing. The associate editor coordinating the review of this article and approving it for publication was Dr. Alireza Jolfaei. *(Corresponding author: Xiaorui Dong.)*

Hao Cui is with the Department of Information Technology, Shengli College, China University of Petroleum, Dongying 257000, China, and also with the College of Computer Science and Technology, China University of Petroleum, Qingdao 266580, China (e-mail: 000447@slcupc.edu.cn).

Xiaorui Dong is with the Department of Information Technology, Shengli College, China University of Petroleum, Dongying 257000, China (e-mail: dongxiaorui@slcupc.edu.cn).

Hongyan Deng is with Dongying District Power Supply Company, State Grid Corporation of China, Dongying 257000, China.

Moslem Dehghani is with Software Energy Company, LLC, Detroit, MI 48128 USA (e-mail: moslem.dehghani6059@gmail.com).

Khalid Alsubhi is with the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: kalsubhi@kau.edu.sa).

Hani Moaiteq Abdullah Aljahdali is with the Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: hmaljahdali@kau.edu.sa).

Digital Object Identifier 10.1109/JSEN.2020.3027778

I. Introduction

DC micro-grids suggest important reliability advantages, cost and energy efficiency contrast to usual alternating current (AC) MGs [1], [2]. To control the DC micro-grids, the initial control acts locally on the basis of the droop manner, for regulating of grid voltage and load sharing among and standalone converters [3] and auxiliary, control is performed to restoration of DC bus voltage [4]. Two main purposes of cooperative auxiliary controllers are proportional load sharing and average voltage regulation [3].

Due to the essential of communication networks in cooperative control layouts, that makes DC micro-grids pretty vulnerable to cyber-attacks [5]. If a DC micro-grid acts on an undetected cyber-attack, the DC micro-grid energy management and the control strategy will be disturbed. Thus, the cyber-attacks detection has significant part for the efficient and reliable performance of the DC micro-grid [6]. Variant kinds of cyber-attacks are existed. For example, FDIA and denial of service (DoS) attack [7] are determined as cyber-attacks. One group of cyber-attacks is belonging to FDIAs which can

cause in altering the state of the system with the help of injecting false data toward sensors, while DoS attacks attempt to construct the communication network fully inaccessible in the MG [8], [9]. Other kind of cyber-attacks can be considered as replay attacks. A replay attacks model on cyber-physical system (CPS) is explained in [10]. On the basis of the description offered in [10], the replay attacks aim can be considered as recording the sensors reading for determined amount of time and afterward, repeating the perusals into the system with the aim of deceiving the operator. Because of variety of models of cyber-attack, discovering solutions with the aim of detecting the attempts of attacker is vital. FDIAs are focused in these articles that are considered as utmost commonly presented kind of attacks. FDIAs are able to harm control applications of the MGs like active power control or voltage control [6]. Developing solutions with the aim of reliably detecting them is important, Due to the FDI possible negative effects on MGs.

Formerly, several tasks have been presented with the aim of identifying FDIAs in smart power grids. For instance, a procedure with the aim of identifying FDIAs on voltage mensuration in MGs of DC via presenting a factor of cooperative vulnerability and observing the secondary sub-layer output with the aim of tracking the variations and so identifying the attacked elements has been proposed in [9].

Current task on the detection of FDIA, although in electrical power networks [11]–[17], extensively uses state estimation processes, for example applying Kalman filters [11], state forecasting [12], generalized likelihood ratio [13], sparse optimization [14], similarity matching and Chi-square detector [15], Kullback-Leibler distance [16], and machine-learning methods [17]. Although, to the best of understanding of researcher, diagnosis of FDIA in software- centralized DC micro-grids are not investigated in a systematic way so far. This task points with the aim of formalizing the FDIA diagnosis issue as a variation in collections of derived invariants; characteristics of the system which do not alter during time. In this study, invariants are described according to the output voltage bounds over and individual converters current.

On the basis of the procedure offered in [15], cosine similarity matching and a Chi-square detector were performed with the aim of identifying the attack in smart grids. The outcomes of [15] show that the detector on the basis of Chi-square is not able to detect the investigated FDIAs. The above tasks have several shortcomings that could be taken into account. For example, several of them have not taken into account current and voltage measurements in a uniform frame, and therefore they are not general ways with the aim of detecting the FDIAs on both current and voltage measurements. For instance, attacks on voltage measurements are discussed in [9] and attacks on current measurements are considered in [18].

In addition, several of them are specifically fitted ways for specific kinds of DC micro-grids. For example, the detection procedures offered in [9], [18] just significantly function in DC micro-grids, that are controlled on the basis of algorithms of cooperative consensus-based. Besides, the system mathematical model is needed with the aim of implementing the mentioned procedures, which is capable of increasing their complexity of implementation. For avoiding the mathematical pattern dependence of the cyber-attack detection, techniques of data-based are able to be applied when the layout of mathematical is not accessible and also with the aim of reducing the burden of computational. Some procedures have been offered with the aim of detecting FDIAs on the basis of deep learning and learning algorithms. For instance, a deep learning method-based with the aim of identifying FDIA in a smart grid (SG) has been proposed in [19]. On the basis of historic information, the FDIAs behavior properties are identified and performed with the aim of detecting FDIAs that attempt to thieve the electricity [19]. In addition, on the basis of the attack detection formulation in the role of a problem of machine learning-based, the efficiency of several procedures like semi-supervised and supervised learning, decision and feature-level fusion, and online learning mechanisms for FDIAs in SGs has analyzed [20]. This case of study will be demonstrated how a neural network is successfully able to be performed in the problem of FDIA detection with the aim of identifying the FDIA and as well as the attacked agent in DC micro-grids. This purpose is achieved only via comparing the neural networks outputs and measuring vales even if there is not any data about the system layout and with the lack of any heavy and extra statistical or analysis of mathematical.

To sum up, a new procedure named enhanced selective ensemble deep learning technique with Original Krill Herd Optimization (KHO) algorithm for diagnosis of cyber-attack in DC micro-grid is proposed in this article. At first, Hilbert-Huang transform extracts the signals features and in the second place, deep base models are made with the aim of adaptively learning hidden properties from signals of raw fluctuation. At third, two methods have been extracted with the aim of ensuring the variety of the base patterns. (I) Multiple deep autoencoders are made to use SAEs, DAEs, SLAEs and DLAEs, respectively. (II) Distinctive training datasets for any base pattern are planed via Bootstrap. Fourth, a combination strategy of EWV (enhanced weighted voting) with class-specific thresholds has been designed with the aim of implementing optional group. At the end, KHO algorithm has been applied with the aim of acquiring the EWV optimal class-particular thresholds. Empiric suffering datum have been applied with the aim of verifying the advantages of the offered method. The experimental outcomes offer which the offered technique is pretty efficient than the models of single deep and another method of ensemble learning, and as well the offered EWV is better in comparison with the standard WV.

The other sections of the article are followed as bellow: Section 2 introduces main concepts about HHT and offered method. Section 3 demonstrates cyber security in MGs and FDIA in full detail. Section 4 carries out simulations and analyzes results. Section 5 expresses the basic conclusion.

II. Basic Concepts

A. Signal Processing

The offered method includes differential energy-based protection layout applying both time–frequency HHT and

S-transform and comparison is created among the both. S-transform defines as a technique of time–frequency decomposition, which is achieved from continuous Wavelet transform and short-time Fourier transform. Which is on the basis of a scalable localizing Gaussian window that has an advanced frequency related resolvent that supplies it good utility and flexibility in the unstable signal processing. Which is totally inter- transformative among frequency domain and time domain. In addition, it owns greatly superior anti-noise efficiency in comparison with methods of traditional for processing of non-stationary signal. Therefore, on the basis of the better time–frequency resolution, it is able to be applied with the aim of describing the incoming signal structure in an effective way.

The HHT defines as a mixture of Hilbert spectral analysis (HSA) and empirical mode decomposition (EMD). It defines as a technique of adaptive used for unstable and non-linear datum and so is extremely effective. The acquired outcomes are extremely clearer in comparison with each of the techniques of traditional of time–frequency energy display. In that offered method, fault currents in two feeders' ends have been recovered, afterwards that have been processed by transforms and after that the content of spectral energy has been calculated. The contrast in energy add-up of time–frequency contours of the signals on the both ways shows the no-fault or fault situation.

1) S-Transform: S-transform defined as an expansion of short-term Fourier transform (STFT) and wavelet transform and Stock-well and his coworker offered it in the year 1996 [21]. It applies scalable window, which is recognized as Gaussian window, in contrast to STFT which applies constant window and so inappropriate for signals of non-stationary. Which is totally commutable from frequency domain to time domain and contrariwise. S-transform is able to be shown regarding magnitude $A(i,n)$ and phase spectrum $\emptyset(i,n)$ as

$$S(i,n) = A(i,n)e^{j\emptyset(i,n)} \tag{1}$$

The signal spectral energy is able to be gained through the equation as shown below

$$E_S = [A(i,n]^2 \tag{2}$$

2) Hilbert–Huang Transform: The HHT defines as NASA specified name and includes HSA and EMD. The main section is the EMD that breaks down a datum collection in smaller and limited components known as intrinsic mode functions (IMFs). Afterwards, these IMFs Hilbert transform has been computed with the aim of obtaining the instantaneous frequencies as a time of function [22].

a) Empirical mode decomposition: EMD elicits the mono detail and symmetrical details from the non-stationary and non-linear signals via sieving procedure. Sieving defines as the procedure of deleted the lowermost frequency of data till just the greatest frequency stays. A signal is analyzed into IMFs. The IMF shows an oscillating wave if it convinced the next two needs:

1. In a datum collection, the extreme's number and the zero-crossings' number should be either differ or equal at most by one.

2. At each point, the average extent of the envelope described through the local maximum and the local minimum is null.

The IMFs analysis from EMD has been accomplished through the below process;

I. In the test datum, exploration the local minimum and maximum and form both envelopes linking them, respectively, with cubical splines.

II. Average, $m(t)$ of the both envelopes has been measured. Minus it from the main signal $x(t)$, the primary component is gotten, $i_1(t)$

$$i_1 = x\,(t) - m(t) \tag{3}$$

III. If $i_1(t)$ convinced the mentioned two conditions, afterwards it is the first IMF else it has been behaved in the role of the original function and steps (1)–(3) have been recurred with the aim of obtaining component $i_{11}(t)$ like;

$$i_{11} = i_1\,(t) - m_1(t) \tag{4}$$

IV. After recurring sifting k times $i_{1k}(t)$ is first IMF, imf_1.

V. Separating IMF1 from $x(t)$ and letting it be $r_1(t)$, like

$$r_1 = x\,(t) - imf_1 \tag{5}$$

VI. $r_1(t)$ has been considered in the role of the main signal and equations (1) to (5) are recurred with the aim of obtaining the second IMF.

The mentioned method has been repeated n times and n like IMFs have been gained. The stopping criterion for the decomposition procedure describes when $r_n(t)$ a monotonic function is such a way that any more IMF is not able to be extracted from it.

b) Hilbert transform: The IMFs are analytical subordinate and with the aim of creating instant frequency of any IMF Hilbert transform has been applied. The Hilbert transform of a time domain signal $x(t)$ describes as the other time domain signal, defined through $\hat{x}(t)$, like $z(t) = x(t) + j\hat{x}(t)$ describes as an analytical signal. Amplitude $A(t)$ and phase $\emptyset(t)$ are be able to be measured like below:

$$A\,(t) = [x^2(t) + j\hat{x}^2(t)]^{1/2} \tag{6}$$

$$\theta\,(t) = tan^{-1}[\frac{\hat{x}(t)}{x(t)}] \tag{7}$$

Instant frequency is obtained through the below equation:

$$f_0\,(t) = \frac{1}{2\pi t} tan^{-1}[\frac{\hat{x}(t)}{x(t)}] \tag{8}$$

The signal spectral energy is be able to be gained through the below Equation:

$$E_H = [A\,(t)]^2 \tag{9}$$

B. Deep Learning Method

This article offers an advanced selective ensemble deep learning procedure with the algorithm of KHOA which stands for Krill Herd Optimization Algorithm for FDIA detection in DC micro-grids. at First, models deep base has been built with the aim of adaptively learning representation aspects

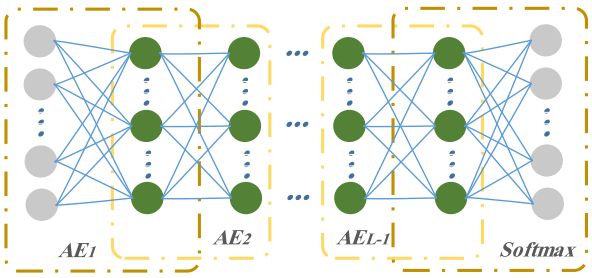


Fig. 1. Architecture of deep autoencoder.

from HHT of signals. At second, for ensuring the variety of the models constructed base, multiple deep autoencoders have been constructed applying SAE, DAE and linear decoder, respectively. Besides distinctive training datasets for any basis pattern have been planned via Bootstrap.

1) Multiple Diverse Deep Autoencoders Construction: Plenty methods are existed which can raise the variety of the base models, like training with various optimizers, adopting various type of models, choosing various hyperparameters, and etc. the below three methods are adopted in this case of study with the aim of ensuring variety.

I) Various autoencoders possess various features. so, for acquiring various base models, some DSAEs, DDAEs, DSLAEs and DDLAEs have been made through stacking several SAEs, DAEs, SLAEs and DLAEs, respectively. The structure procedure of mentioned deep autoencoders is same, that has been trained through layer-wise unsupervised learning. As has been illustrated in Fig. 1, the hidden output of prior autoencoder has been applied in the role of the input of subsequent autoencoder until the last autoencoder has been trained, and the top layer is soft max classifier.

II) This article conducts a supervised fine-tuning procedure after layer-wise unsupervised learning, and calculates the cost function of the fine-tuning procedure through following equation:

$$J_{DeepAE}(\theta) = -\frac{1}{n}\sum_{i=1}^{n}(\hat{y}_i log y_i) + \frac{\lambda}{2}\sum_{l=1}^{l}\sum_{i=1}^{n_l}\sum_{j=1}^{n_{l=1}}(W_{ij}^{l})^2 \tag{10}$$

in which $\hat{y}_i$ and y_i define as the real tag and forecasted tag of the ith instance, $(L-1)$ defines as the hidden layers number. The number of repetitions of fine-tuning procedure affects the efficacy of training, so various repetitions numbers of fine-tuning procedure have been chosen. If m various repetitions numbers of fine-tuning procedure have been chosen, afterwards there would exist 4 m base models.

III) In addition, making different deep basis patterns, unique training data subsets for any pattern have been also planned through Bootstrap with the aim of ensuring the variety of the base models. In particular, it is supposed that the all dataset has been defined as $X_w = \{X_1, X_2, ..., X_i, ..., X_s\}$, in which s defines as the sum number of the samples, $X_i = \{x_1, x_2, ..., x_j, ..., x_m\}$, m defines as the data points number of any sample. Afterwards X^w has been devided into three sections i.e. $X^{tr} = \{X_1, X_2, ..., X_n, ..., X_p\}$, $X^v = \{X_{p+1}, X_{p+2}, ..., X_q\}$, $X^t = \{X_{q+1}, X_{q+2}, ..., X_s\}$, in which X^{tr}, X^v and X^t show the training dataset, accuracy dataset and test dataset, respectively. for acquiring unique training datasets, Bootstrap have been applied with the aim of random selecting n instances from X^{tr} per time, and the training data subset for ith pattern has been defined as X^{tri}. About the architecture parameter election, further empirical guidelines have been defined as below. Two to five hidden layers have been suggested, and the number of hidden nodes inchmeal decreases from lower to higher layers. it should be considered which too plenty basis patterns would need high- efficiency hardware, 8–24 basis patterns are proper.

2) EWV With Class-Specific Thresholds: Standard WV just recourse to the generic efficiency diversity of any pattern with the aim of setting the voting weights, that doesn't care to the efficiency diversity of various basis patterns for any fault kind. so, a new combination strategy named EWV is designed in this paper. The advanced EWV takes into account the performance diversity of various models for any fault mode on the basis of a comprehensive index named F1-measure [22]. Firstly, class-specific thresholds have been adjusted with the aim of conducting elective ensemble, and afterwards class-particular weights have been devoted to any basis pattern per fault kind.

The EWV detailed are expressed as bellow. At first, a number of basis patterns have been made and trained. Afterwards the authenticity outcomes of any basis patterns have been obtained and the corresponding F1 extents are be able to be measured through

$$F = \frac{2P.P}{P+P} = \frac{2TP}{2TP+FP+FN} \tag{11}$$

In which

$$P = \frac{TP}{TP+FP} * 100\% \tag{12}$$

$$R = \frac{TP}{TP+FN} * 100\% \tag{13}$$

P shows the accurate factor, R shows the recall factor; TP, FN, FP show the number of false positive samples, true positive samples and false negative samples, respectively [22]. Afterwards, the class-particular F1 thresholds for any fault kind have been adjusted as $ft = [ft_1, ft_2, ..., ft_c]$. Comparing any F1 amount with the corresponding threshold, if F1 amounts are less in comparison with the corresponding thresholds, they would be adjusted to 0, that purposes the corresponding weights would be zero too.

$$F_{ij} = \begin{cases} 0, & F_{ij} < ft_j \\ F_{ij}, & Otherwise \end{cases}, i = 1, 2, \ldots, k; j = 1, 2, \ldots, c \tag{14}$$

In which

$$\min\{F_{ij}, i = 1, 2, \ldots k \le ft_j \le max F_{ij}, i = 1, 2, \ldots k\} \tag{15}$$

F_{ij} shows the $F1$ amount of fault state j of ith base model, ft_j shows the $F1$ threshold for fault state i, and c is the number of fault states.

then, allocate weights to any basis patterns for any fault state as:

$$w_{ij} = \frac{F_{ij}}{\sum_{i=1}^{k} F_{ij}} \tag{16}$$

In which

$$\sum_{i=1}^{k} w_{ij} = 1, w_{ij} \geq 0 \tag{17}$$

w_{ij} shows the weights of basis pattern i for fault state j.

At end, the decision is able to be made like below. Assume that Modeli (X_t) shows the forecasted label of basis pattern i for instance X_t. The sum scores which X_t pertains to fault state j has been measured through

$$Score_j\,(X_t) = \sum_{i=1}^{k} w_{ij}.G\,(X_t, j)\,, t = p+1, p+2, \ldots, q \tag{18}$$

In which

$$G\,(X_t, j) = \begin{cases} 1 & Model_i\,(X_t) = j \\ & Otherwise \end{cases} \tag{19}$$

The ultimate forecasted label $Pre\_L(X_t)$ of X_t is be able to be gained through

$$Pre_L\,(X_t) = T \tag{20}$$

In which

$$Score_r\,(X_t) = \max\{Score_r\,(X_t)\,, \mathrm{j} = 1, 2, \ldots \mathrm{c}\} \tag{21}$$

so, the ultimate authenticity precision of ensemble learning is be able to be gained through

$$Ensembel_{V_{acc}} = \frac{\sum_{t=p+1}^{q} g(X_t, Y_t)}{q-p} \tag{22}$$

In which

$$g\,(X_t, Y_t) = \begin{cases} 1 & Pre\_L(X_t) = Y_t \\ 0 & Otherwise \end{cases} \tag{23}$$

Y_t defines as the real label of instance X_t.

3) EWV Optimization Using Original Krill Herd Optimization Algorithm: An essential benefit of KHOA in comparison with the other optimization algorithm is the great level of variety in the research space that aids the algorithm to release from local optima. in addition, upkeeping the population various is a chief point in searching the whole research space so that any area is not remained behind [23].

With the aim of mimicking the krill manner, a swarm of krill has been produced and their position has been set pursuant to (24).

$$X_i^{Iter+1} = X_i^{Iter} + V_{r,i}^{Iter}\,\chi \sum_{j=1}^{N_v} (u_j - l_j) \tag{24}$$

The motion has been restricted through the upper and lower boundary of a position constant factor χ and control variables. Besides the speed of ith individual is the outcome of the velocities as below:

$$V_{r,i}^{Iter} = V_{ind,i}^{Iter} + V_{frgi,i}^{Iter} + V_{dif,i}^{Iter} \tag{25}$$

The mentioned velocities are on the basis of induction, foraging and random diffusion procedures. The representation of mathematical of these procedures has been described as below:

Induced Speed: The surrounding krill effect on a person movement has been modeled in the procedure. Any person sets its velocity pursuant to the repulsive effect, local effect and target effect described below:

$$V_{ind,i}^{Iter} = \alpha_{ind,i} V_{ind,i}^{max_{ind,i}^{Iter-1}} \tag{26}$$

The coefficient a_{ind} models the attractive/repulsive effect of surrounding krill and as well the effect of best person, so it includes two terms described below:

$$\alpha_{ind,i} = \sum_{j=1}^{N_s} [\frac{f_i - f_j}{f_w - f_b} \times \frac{X_i - X_j}{\left|X_i - X_j\right| + \varepsilon}] + 2[\rho_1 + \frac{i}{N_p}] f_i^b X_i^b \tag{27}$$

The election of neighbors for any krill is on the basis of an identifying area defined through the krill's situation in the research space. Any krill obtains the close persons as neighbors if their situation is in its identifiable area located through:

$$R_{Vicinity} = \frac{1}{5N_p} \sum_{j=1}^{N_p} \left|X_i - X_j\right| \tag{28}$$

Foraging Speed: The remembrance of finding food is the ruling idea behind updating foraging motion, where any person update its velocity pursuant to previous and current food position:

$$V_{frg,i}^{Iter} = 0.02[2(1 - \frac{i}{N_p}) f_i \frac{\sum_{i=1}^{N_s} \frac{X_i}{f_i}}{\sum_{i=1}^{N_s} \frac{1}{f_i}} + f_i^b X_i^b] + \omega_{frg} V_{frg,i}^{Iter-1} \tag{29}$$

Diffusion Speed: Random diffusion warrants the variety of the population during the total optimization procedure. therefore, the diffusion speed of krill individuals has been described as below:

$$V_{dif,i}^{Iter} = \upsilon \times \omega_{dif} \tag{30}$$

The procedure randomness has been modeled through the directional vector υ that has been divided uniformly among -1 and 1. The proposed process in KHOA brings altogether the experiments of swarm intelligence; although the traditional genetic operators (cross over and mutation) have been increased to the algorithm with the aim of speeding up the convergence feature.

C. General Scheme of the Offered Technique

As has been illustrated in Fig. 2, an advanced election ensemble deep learning procedure with KHO algorithm for cyber-attack detection in DC micro-grids is proposed in this article. At first, the signal characteristics has been exploited through Hilbert Huang transform. At second deep base models have been made with the aim of adaptively learning hidden

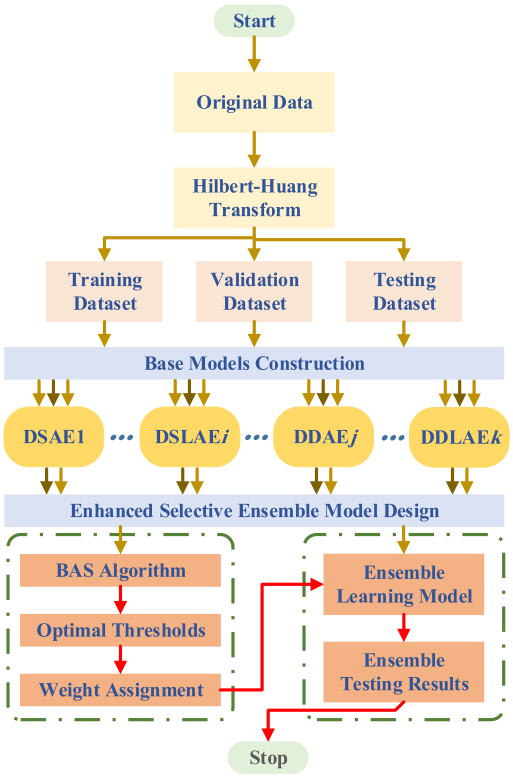


Fig. 2. Flowchart of the suggested FDI detection process.

characteristics from exploited indexes from Hilbert Huang transform of signals. For ensuring the variety of these basis patterns. (I) These deep autoencoders have been constructed applying SAE, DAE and linear decoder, respectively. (II) Unique training datasets for any basis pattern have been planned via Bootstrap. Afterwards, the syntax mechanism of WV with class-particular thresholds has been planned with the aim of conducting elective group. Eventually, KHO algorithm has been used to optimal thresholds.

III. Cyber Security in MGs With FDIAs

The MG cyber security is focused in this part and afterwards a scheme for cyber-attack in the MGs is explained.

A. MG Cyber Security

MG in a role of a small size electrical power grid contains both the consumption and generation spots that results in operating in two operation states of islanded and grid-connected. Alongside the physical layer such as various DGs and renewable energy resources, loads and power supply agents, a MG has an intercoupled cyber layer mostly trading datum transmission and decision making on the basis of information collected through advanced metering infrastructure (AMIs). Which is result that the MG an intricate CPS with a combinatory non-linear and correlated construction that is a remarkable aim for cyber hackers with the aim of penetrating into it and applying their malicious objectives. challenges to the reliable and secure operation of MGs have been posed by different factors like heterogeneous data resources, vulnerable sensors, vast volume interplays into the MG and

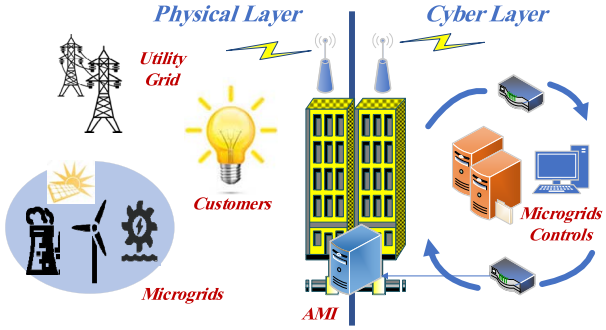
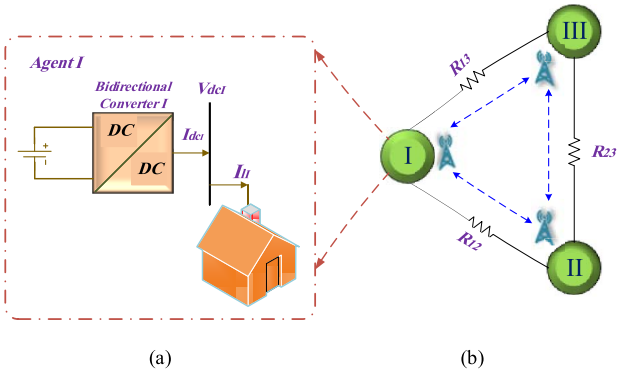


Fig. 3. MG construction as a cyber-physical layer.

among the MG and the main system, sensitivity to time synchronization and communication delays. In an MG, AMI is the principle layer creation a two-route communication path among the smart metering equipment with special IP addresses and consumers and the power producers. AMI is responsible for datum communication, data gathering and analysis of energy demand for the MG optimal running. AMI results the real-time decision making in both the consumption and generation spots. on the basis of the transmitted AMI data, DGs have been planned at their optimal operating part and electric consumers are be able to make suitable economic decisions for utmost energy saving and active taking part in the price of the market. the cyber physical construction of an MG incorporating the AMI is shown in fig. 3. As it shown in Fig. 3, via the wireless or wired communication links, the smart meters in the role of an essential section of AMI gather datum from generators, electric consumers and power supply agents for decision making and effective operation. Thus, smart meters have been supposed in the role of a gateway for gathering and decomposing the MG physical layer condition. This results in making them a vulnerable and penetration potential matter to be able to perform malicious attacks for affecting the entire MG efficiency. in point of fact, through colluding the datum offered via smart meters, one is able to influence the optimal dispatch of DGs and therefore decreasing the security, reliability and the quality of power in electrical services, intensely.

B. Cyber Attack

In an ordinary MG, the first and basic role of AMI defines as collecting load utilization datum and transferring it to the decision-making agent for suitable generator units planning. In each condition, an intact MG must meet the demand and generation balance equation with the aim of avoiding unanticipated interruptions or obligatory load shedding. Moreover, AMI is able to have a vital task in decreasing the whole cost of MG through making real-time datum about demand of the consumers. An MG should raise the content of power production within the maximum load hours to satisfy the electric requirements. Via the precise estimate of the load demand supplied through AMI, the MG is be able to apply demand reply technology to modify the maximum load hours and therefore decrease the whole MG costs, prevent useless feeder congestion and feasible frequency and voltage collapse.



(a) (b)

Fig. 4. Proposed MG: (a) unit plan and (b) Cyber-physical DC micro-grid with three resources.

TABLE I
TEST SYSTEM PARAMETERS

Parameter	Value
V_{dcref}	315 V
Δt	5 ms
L_f	5 mH
C_f	50 mF
R_{12}	1.8 Ω
R_{23}	2.3 Ω
R_{12}	1.3 Ω

This strategy is worth and hopeful as long as precise electric load demand data has been applied. Unluckily, AMI being made on the basis of communication junctions is weak to cyber-attacks like which a hostile professional user is be able to change the reported load demand for malicious purposes. Via manipulating the AMI, a hostile destroys the demand reply procedure and damage the demand and generation balance. This is able to cause further destroying results ranging from extra exploitation cost to permeability of exploitation and unplanned shutdowns. The reality that which of the issues might occur in the end for a MG belongs both on the cyber-attack capability and the MG state of exploitation. As said earlier, an MG is able to work in both modes including islanding or non-islanding mode. In the state of the non-islanding, the cyber-attack to the AMI is able to raise the costs of MG, losses of feeder power and collapse of voltage. In the next state which is islanded mode, the cyber-attack is able to cause in more serious outcomes like generation loss and balance of demand and impossibility of shutdown or operation.

In terms of intensity, the strength of cyber-attack is be able to be classified into two various instances. The prime one is a malicious attack with a powerful and immediate result leading to the greatest loss to the MG. Like an attack has been felt in the short-time window and is able to be identified because of its great magnitude. The latter one is that a malicious attack with clear and slow result dealing to variations in the long term. The basic goal of this kind of cyber-attack considers as avoiding being recognized through the system and making variations in the MG in the long terms. Both kinds of cyber-attacks on the MG would be analyzed in this case of study. And as well an intelligent model has been suggested with the aim of detecting the cyber-attack that has been described detailed in the prior part.

IV. Simulation Results

The suggested attack detection method has been examined on a DC micro-grid considering electric vehicle, as be seen in Fig. 4(b) with $V_{dcref} = 315V$ including three units of same capacities intercoupled to one another through lines. It is noteworthy that any unit includes a battery accompanies via DC/DC converters as be seen in Fig. 4(a). For testing the efficiency of the suggested attack detection mechanism for cooperative DC micro-grid, it has been examined versus some disturbances like FDIA, stealth attack in several sensors, that generally are not tracked through distributed observers, communication links with the aim of detecting the influenced node so that needful action is be able to be done with the aim of maintaining security. The control and system parameters have been supplied in Table I. It is noteworthy that any event in the aforesaid scenarios have been separated through a determined time-gap with the aim of providing clear understanding.

Case study I : In this section, the FDIA is occurred on voltage sensor in agent I. The behavior of the system is assayed in an instance of this FDIA kind and deep learning indicators are shown which is elicited based on Hilbert Huang transform.

FDIA has been began and deleted at time t = 0.3 and t = 0.5 second, respectively. The voltage reference signal amplitude has been altered (lessen by 30%). The outcomes of simulations of this case study has been indicated in Fig.5.

Fig. 5a is the DC micro-grid voltage to which the FDI attack has been defined in time. Fig. 5b illustrates the Hilbert-Huang conversion under various IMFs with residual value. Fig. 5c Hilbert-Huang spectral energy illustrates the index signal of suggested deep learning machine, that could distinguish a cyber-attack.

Case study II: In this part, the FDIA is occurred on voltage sensor in agent III. The behavior of the system is assayed in an instance of this FDIA kind and deep learning indicators are shown which is elicited based on Hilbert Huang transform.

FDIA has been began and deleted at time t = 0.3 and t = 0.5 second, respectively. The voltage reference signal amplitude has been altered (raised by 30%). The results of simulations of this case study has been indicated in Fig.6.

Fig. 6a is the DC micro-grid voltage to which the FDI attack has been defined in time. Fig. 6b illustrates the Hilbert-Huang conversion under various IMFs with residual value. Fig. 6c Hilbert-Huang spectral energy illustrates the index signal of suggested deep learning machine, that could distinguish a cyber-attack.

Case study III: In this part, the FDIA is on adding a noise signal to the voltage reference signal in agent II. The behavior of the system is assayed in an instance of this FDIA kind and deep learning indicators are shown which is elicited based on Hilbert Huang transform.

FDIA has been began and deleted at time t = 0.3 and t = 0.5 second, respectively. A noise is added to the voltage

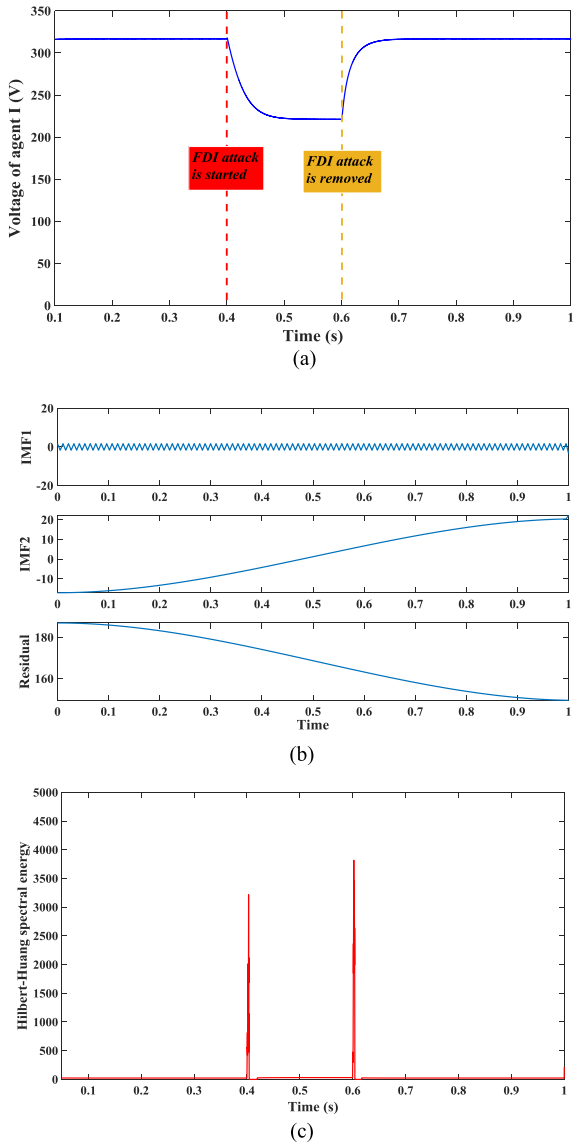


Fig. 5. FDIA on the basis of raising the amplitude of voltage reference signal: a) Waveform of voltage, b) Empirical mode decomposition of input index of voltage, c) Hilbert-Huang spectral energy of input index of voltage.

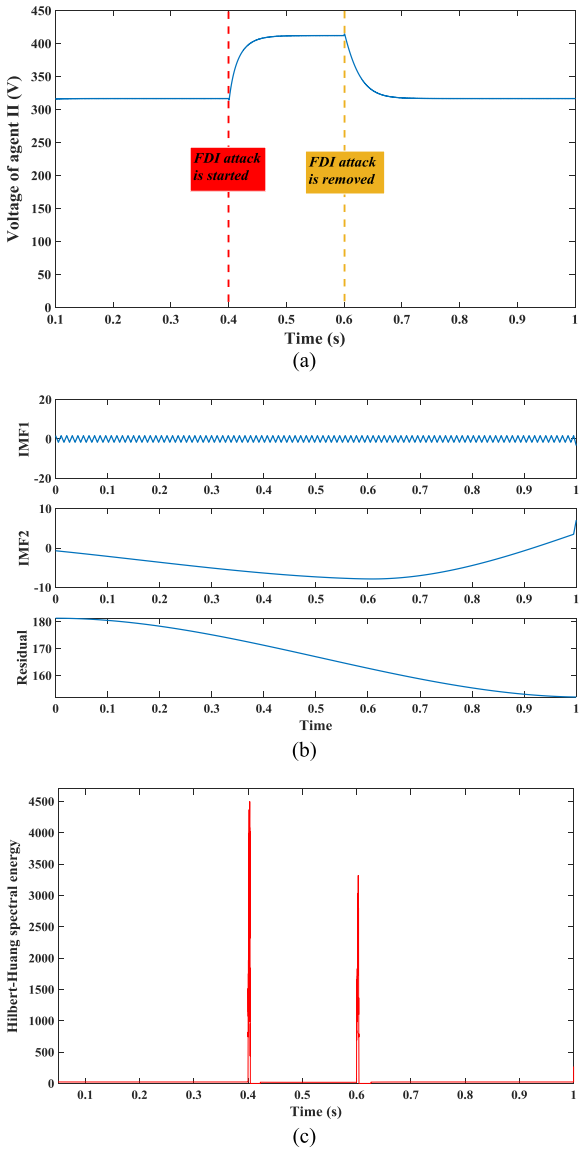


Fig. 6. FDIA on the basis of reducing the amplitude of voltage reference signal: a) Waveform of voltage, b) Empirical mode decomposition of input index of voltage, c) Hilbert-Huang spectral energy of input index of voltage.

reference signal. The results of simulations of this case study has been shown in Fig.7.

Fig. 7a is the DC micro-grid voltage to which the FDI attack has been defined in time. Fig. 7b is shown the Hilbert-Huang spectral energy which illustrates the index signal of proposed deep learning machine, that could distinguish a cyber-attack.

Discussion of simulation results: when decision is distinguished in a role of a cyber-attack, it is defined as positive. On the other side, when decision is recognized by the anomaly detection model in the role of ordinary situation, it is defined as negative.

When a correct decision has been made by the anomaly detection model, True decision has gained. So, obviously a wrong reaction from our cyber-attack detection pattern is shown by a false decision. Hence, it could be concluded that a proper detection pattern describes as one with low false rates. On the basis of these descriptions, four various indexes are able to be described: correct reject rate (CR), miss rate (MR), hit rate (HR), and false alarm rate (FR). Table II introduces the confusion matrix to have a clear comprehension of the proper index. Number of Testing Data is 1279 in Compromised situation and 1027 in ordinary situation. The offered cyber model detection is able to distinguish 1199 from Compromised situation and 978 from ordinary situation properly.

For verifying the accuracy of suggested deep learning in FDIA diagnosis, some instance tests have applied.

The performance of proposed detection manner has been tested through applying the FDI attack pattern and the assessment results have been proposed in table III. As can be seen in Table III, it is noteworthy that the offered manner can distinguish the FDIAs with diagnosis precision more than 93%, which shows the performance of the offered diagnosis procedure on diagnosis the FDIAs.

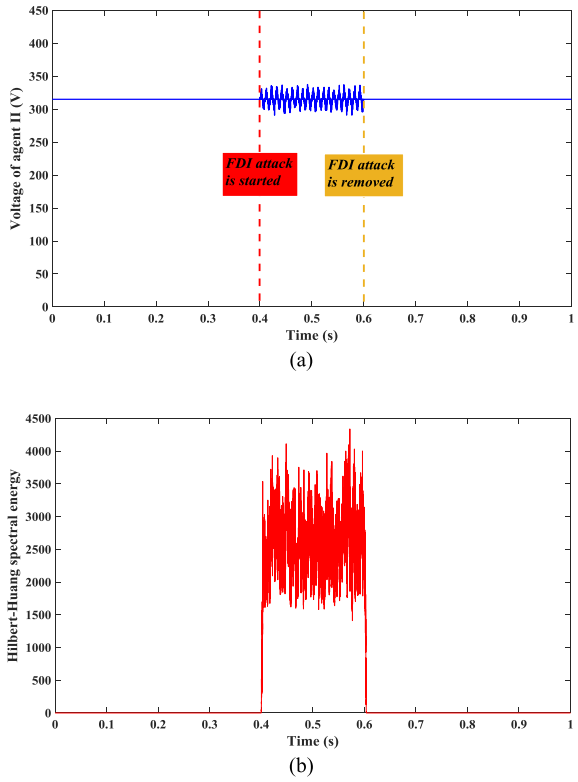


Fig. 7. FDIA on the basis of mixing a noise to voltage reference signal: a) Waveform of voltage, b) Hilbert-Huang spectral energy of input index of voltage.

TABLE II
CONFUSION MATRIX OF THE OFFERED DETECTION PLAN

		Real Amount	
		Positives	Negatives
Detection Layout Respond	Positives	HR True Positive (TP)	FR False Positive (FP)
	Negatives	MR False Negative (FN)	CR True Negative (TN)

TABLE III
CONFUSION MATRIX OF THE OFFERED DETECTION PLAN

		Real Amount	
		Positives	Negatives
Detection Layout Respond	Positives	93.75%	4.77 %
	Negatives	6.25 %	95.23 %

V. CONCLUSION

This article offers an advanced selective ensemble deep learning procedure with KHO algorithm with Hilbert Huang transform with the aim of modeling a cyber-attack detection procedure. Hilbert Huang transform has been exploited spectral energy of the input signals with the aim of using in the role of the input index of deep learning afterwards multiple deep basis patterns have been made with SAE, DAE and linear decoder, Bootstrap has been applied with the aim of designing determined training data subsets for them. This article proposes an EWV compound mechanism with class-specific thresholds with the aim of implementing selective ensemble, and uses KHO algorithm with the aim of optimizing the class-particular thresholds. And this article also uses simulation data with the aim of verifying the advantage of the suggested procedure. The outcomes propose that the suggested procedure is be able to more exactly and strongly detect FDI attacks in DC micro-grid. In addition, it could be concluded that the suggested model illustrates proper efficiency against destructive attacks with various intensities ranging from 10% to 100% datum injection. The outcomes of two various index of detection rate and confusion matrix outcomes support the precision and trustworthy efficiency of the suggested anomaly detection pattern. The efficiency of the suggested strategy has been verified through MATLAB/Simulink software environment.

REFERENCES

[1] T Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC Microgrids—Part I: A review of control strategies and stabilization techniques," *IEEE Trans. Power Electron.*, vol. 31, no. 7, pp. 4876–4891, Jul. 2016.

[2] 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.

[3] M. Dabbaghjamanesh, A. Kavousi-Fard, and J. Zhang, "Stochastic modeling and integration of plug-in hybrid electric vehicles in reconfigurable microgrids with deep learning-based forecasting," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 6, 2020, doi: 10.1109/TITS.2020.2973532.

[4] S. Adhikari, Y. Tang, and P. Wang, "Secondary control for DC microgrids: A review," in *Proc. Asian Conf. Energy, Power Transp. Electrific. (ACEPT)*, Oct. 2016, pp. 1–6.

[5] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of DC microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 1083–1085, Jan. 2019.

[6] 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.

[7] M. Dabbaghjamanesh, A. Moeini, and A. Kavousi-Fard, "Reinforcement learning-based load forecasting of electric vehicle charging station using Q-learning technique," *IEEE Trans. Ind. Informat.*, early access, Apr. 27, 2020, doi: 10.1109/TII.2020.2990397.

[8] 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 Newsletter*, early access, Oct. 2020.

[9] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragicevic, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[10] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2009, pp. 911–918.

[11] 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.

[12] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017.

[13] S. Li, Y. Yilmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.

[14] 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.

[15] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[16] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.
[17] M. Dehghani, A. Kavousi-Fard, M. Dabaghjamanesh, and O. Avatefipour, "Deep learning based method for false data injection attack detection in AC smart islands," *IET Gener., Transmiss. Distrib.*, early access, May 2020.
[18] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragicevic, "On detection of false data in cooperative DC Microgrids—A discordant element approach," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6562–6571, Aug. 2020.
[19] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.
[20] 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.
[21] S. S. Sahu, G. Panda, and N. V. George, "An improved S-transform for time-frequency analysis," in *Proc. IEEE Int. Advance Comput. Conf.*, Mar. 2009, pp. 315–319.
[22] S. Tang, H. Ma, and L. Su, "Filter principle of Hilbert–Huang transform and its application in time series analysis," in *Proc. 8th Int. Conf. Signal Process.*, 2006, pp. 1–5.
[23] A. H. Gandomi and A. H. Alavi, "Krill herd: A new bio-inspired optimization algorithm," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 12, pp. 4831–4845, Dec. 2012.

Hao Cui was born in Hunan, China, in 1979. He received the B.S. degree in communication engineering and the M.S. degree in computer application technology from the China University of Petroleum, Shandong, China, in 2002 and 2006, respectively.

He is currently an Associate Professor with the Shengli College, China University of Petroleum. He is the author of two books and more than ten articles. His current research interests include network security, the IoT security, scalable software systems, data mining, and ensemble learning.

Xiaorui Dong (Member, IEEE) was born in Shandong, China, in 1988. He received the B.S. degree in software engineering and the M.S. degree in computer science and technology from Nanchang University, Jiangxi, China, in 2010 and 2013, respectively.

Since 2017, he has been a Lecturer with the Shengli College, China University of Petroleum, Shandong. He is the author of one book and more than 20 articles. His research interests include data and computation security, data fusion, deep learning, distributed computing, and soft sensor applications.

Hongyan Deng was born in Shandong, China, in 1984. She received the B.S. degree in electronic information engineering from the Shandong University of Technology in 2007. She is currently pursuing the M.E. degree in electrical engineering with Shandong University.

She is a Senior Engineer with Dongying District Power Supply Company, State Grid Corporation of China, Shandong. Her current research interests include electric vehicles, power system reliability, and smart electricity grid applications.

Moslem Dehghani is currently cooperating with Software Energy Company, LLC, Detroit, MI, USA. His current research interests include power electronics, control, and cybersecurity analysis of smart grids, microgrid, smart city, protection of power systems, fuzzy logic, and signal processing.

Khalid Alsubhi (Member, IEEE) received the B.Sc. degree in computer science from King Abdulaziz University (KAU) in 2003 and the M.Math. and Ph.D. degrees in computer science from the University of Waterloo, Waterloo, Canada, in 2009 and 2016, respectively. He is currently an Assistant Professor of Computer Science with KAU. His research interests include network security and management, cloud computing, and security and privacy of healthcare applications.

Hani Moaiteq Abdullah Aljahdali was born in Jeddah, Saudi Arabia, in 1983. He received the B.Sc. degree in computer science from King AbdulAziz University, Jeddah, in 2005, and the M.Sc. degree in information technology and the Ph.D. degree in computer science from the University of Glasgow in 2009 and 2015, respectively. From 2005 to 2007, he worked at Saudi Electricity Company as a Budget and System Analyst. In 2011, he has appointed as a Lecturer at the Department of Information Systems, King AbdulAziz University. He is currently appointed as an Associate Professor at the Faculty of Computing and Information Technology in Rabigh, King AbdulAziz University. His research interests include information security, human–computer interaction, and machine learning.