electronics

MDPI

Article

Cyber-Attack Detection in DC Microgrids Based on Deep Machine Learning and Wavelet Singular Values Approach

Moslem Dehghani [1], Taher Niknam [1,*], Mohammad Ghiasi [1], Navid Bayati [2,*] and Mehdi Savaghebi [2]

[1] Department of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz 7155713876, Iran; mo.dehghani@sutech.ac.ir (M.D.); m.ghiasi@sutech.ac.ir (M.G.)
[2] Electrical Engineering Section, Department of Mechanical and Electrical Engineering, University of Southern Denmark, Campusvej 55, 5230 Odense, Denmark; mesa@sdu.dk
* Correspondence: niknam@sutech.ac.ir (T.N.); navib@sdu.dk (N.B.)

Abstract: Nowadays, the role of cyber-physical systems (CPSs) is of paramount importance in power system security since they are more vulnerable to different cyber-attacks. Detection of cyber-attacks on a direct current microgrid (DC-MG) has become a pivotal issue due to the increasing use of them in various electrical engineering applications, from renewable power generations to the distribution of electricity and power system of public transportation and subway electric network. In this study, a novel strategy was provided to diagnose possible false data injection attacks (FDIA) in DC-MGs to enhance the cyber-security of electrical systems. Accordingly, to diagnose cyber-attacks in DC-MG and to identify the FDIA to distributed energy resource (DER) unit, a new procedure of wavelet transform (WT) and singular value decomposition (SVD) based on deep machine learning was proposed. Additionally, this paper presents a developed selective ensemble deep learning (DL) approach using the gray wolf optimization (GWO) algorithm to identify the FDIA in DC-MG. In the first stage, in the paper, to gather sufficient data within the ordinary performance required for the training of the DL network, a DC-MG was operated and controlled with no FDIAs. In the information generation procedure, load changing was considered to have diagnosing datasets for cyber-attack and load variation schemes. The obtained simulation results were compared with the new Shallow model and Hilbert Huang Transform methods, and the results confirmed that the presented approach could more precisely and robustly identify multiple forms of FDIAs with more than 95% precision.

Keywords: deep learning; DC microgrid; GWO; false data injection attack; singular value decomposition; Wavelet transform

Citation: Dehghani, M.; Niknam, T.; Ghiasi, M.; Bayati, N.; Savaghebi, M. Cyber-Attack Detection in DC Microgrids Based on Deep Machine Learning and Wavelet Singular Values Approach. *Electronics* **2021**, *10*, 1914. https://doi.org/10.3390/electronics10161914

Academic Editor: Taha Selim Ustun

Received: 15 June 2021
Accepted: 6 August 2021
Published: 9 August 2021

1. Introduction

1.1. Background

Recent studies have confirmed that with the increasing development of power electronics, DC microgrids (DC-MGs) provide significant efficiency and reliability compared to conventional AC microgrids (AC-MGs), and they are also more cost-effective [1–4]. In general, to control DC-MGs, the primary control is performed according to the droop technique to adjust the output voltage and divide the current between individual converters locally [5,6]. Ancillary control is executed to restore the voltage of the DC bus. The main goals of cooperative ancillary controllers have been divided into load sharing and voltage adjustment [7,8].

As the importance of communication systems in the cooperative control strategies, DC-MGs are assailable to different kinds of cyber-attack. It has been shown that if a DC-MG operates under undetected cyber-attacks, the DC-MG power control and management scheme can be affected or disrupted. Accordingly, cyber-attack detection has a vital role in reliable and effective operation in a DC-MG [9]. Some new research has focused on several kinds of cyber-attack in electrical power grids. Good examples here can be the denial of service (DoS) and false data injection (FDI) attacks [10,11]. In DoS attacks, the hacker tries

to keep the microgrid (MG) communication network fully inaccessible, whereas, in an FDI attack (FDIA), hackers change the status of the system by injecting incorrect data into the sensors [12,13].

Replay attacks (RAs) are considered as another form of cyber-attacks. The purpose of RAs is to record the readings of the sensors for a specified period, and then these readings are repeated to deceive the operator in the system. In [14], a concept of RAs in CPS was presented. Given the variety of cyber-attack schemes, it is vital to find different solutions to identify the hacker's efforts. Paper [15] has concentrated on FDIA as the most prevalent kind of cyber-attack. FDI attacks (FDIAs) can also damage control programs in DC-MGs, including voltage and power control. As the potential negative impacts of FDIA on DC-MGs, it is pivotal to enhance different solutions for their reliable detection.

Previous research like [16,17] has worked on the protection of DC-MGs to increase the reliability of power systems. In Reference [18], a technique for identifying FDIAs on voltage measurement sensors in DC-MG has been proposed. It introduced a cooperative vulnerability agent and monitored the secondary output sublayer to identify the attacked parts.

Some research works on FDIA detection in power systems can be found in [19–23], which widely employ state estimation procedures, for instance, by using Kalman filters in [24], sparse optimization and state forecasting provided in [20], generalized likelihood ratio in [19], Kullback–Leibler distance in [25], Chi-square detector and also similarity matching in [26], and machine learning methods in [27]. But in this paper, FDIA detection has been considered in DC-MGs to detect FDIAs in voltage/current sensors and in the reference amount, actual amounts used in the controllers.

According to the presented technique in reference [28], a Chi-square-based detector and cosine similarity matching have been performed to distinguish the cyber-attack in smart grids (SGs) [29]. Most of them do not consider the voltage and current measurements in an integrated framework. Thus, there are no general methods for detecting FDIAs in both current and voltage measurements because the attackers can attack both measurements, so it is better to consider FDIAs in both voltage and current measurements. An example is [30], which discussed some forms of attacks on voltage measurements; also, in [31], attacks on current measurements were considered.

Several FDIA detection ways rendered for CPSs have been considered and analyzed. Based on the control information, the CPSs controllers have been classified as various distributed and centralized controllers [32–35]. Extant centralized cyber-attack detection techniques have been considered in several forms, including 1- linear time-invariant systems, 2- actuator/sensor attacks, 3- nonlinear systems, and finally, 4- systems with noise. Additionally, the advancement of distributed cyber-attack detection has been surveyed based on various decoupling approaches. Furthermore, future research paths and different forms of challenges in cyber-attack detection methods have been listed. In [36], a review of recent developments on security concepts and cyber-attack detection in CPSs is presented from a control theory viewpoint.

Recently, new techniques for detecting FDIA according to machine learning and deep learning (DL) frameworks have been presented; for instance, Reference [37] provided an in-depth learning-based approach to detect FDIA in the smart grid (SG). In [38], according to the attack detection formula as a problem based on machine learning, the possibility of some techniques, including supervised and semi-supervised learning approaches, decision fusion and level features, and online learning frameworks for FDIA in smart grids have been examined. Some of the previous works have been summarized in Table 1.

Table 1. Exiting literature of FDIA detection.

Reference	Methodology	Detection Technique	Limitation	Advantages of Our Proposed Technique
[12]	Cooperative vulnerability factor	Considering attacks on measurements in DC-MG	Criteria indexes of the accuracy rate like miss rate (MR), false alarm rate (FAR), hit rate (HR), and correct reject rate (CRR) are not considered and not compared to the other FDIA detection methods based on the accuracy criteria indexes	Both voltage and current measurement are investigated in the proposed study. Criteria indexes of the accuracy rate are considered and compared to the other FDIA detection methods; The technique is free-model-based
[24]	Kalman filter	Applying the mathematical method in smart grids to detect the FDIAs	Criteria indexes of the accuracy rate like MR, FAR, HR, and CRR are not considered and not compared to the other FDIA detection methods based on the accuracy criteria indexes; DC system is not considered;	This work is not dependent on the system's mathematical model. Criteria indexes of the accuracy rate are considered and compared to the other FDIA detection methods; DC-MG has been investigated
[38]	Deep learning	Applying DL schemes to identify the properties behavior of FDIA with the historical measurement information and using the captured properties to diagnose the FDIA	Criteria indexes of the accuracy rate like MR, FAR, HR, and CRR are not considered for the FDIA detection; DC system is not considered;	Applying WT and SVD to extract features to use as input of deep learning and deep base models are built to adaptively learn hidden properties. Criteria indexes of the accuracy rate are considered and compared to the other FDIA detection methods;
[39]	Kullback–Leibler	The ability to diagnose different attacks. Has difficulty diagnosing FDIAs in some state variables	Using historical data so it cannot detect small FDIA to the system. Criteria indexes of the accuracy rate like MR, FAR, HR, and CRR are not considered for the FDIA detection;	This work is not dependent on the state variable for detection FDIAs and is based on signals features. Various criteria indexes are considered and compared. It does not depend on the historical data
[40]	Chi-square detector and cosine similarity matching were applied	The results illustrated that detection based Chi-square could not detect the examined FDIAs	Criteria indexes of the accuracy rate like MR, FAR, HR, and CRR are not considered for the FDIA detection; and is not compared to the other FDIA detection methods based on the accuracy criteria indexes; DC system is not considered;	This paper is capable to detect various FDIAs in smart MG; Criteria indexes of the accuracy rate are considered and compared to the other FDIA detection methods; DC-MG has been investigated;
[41]	Discordant Element Approach	Considering attacks on current measurements in DC-MG	Criteria indexes of the accuracy rate like MR, FAR, HR, and CRR are not considered for the FDIA detection; and not compared to the other FDIA detection methods based on the accuracy criteria indexes; does not consider the attack on voltage sensors	Both voltage and current measurement are investigated in the proposed study. Criteria indexes of the accuracy rate are considered and compared to the other FDIA detection methods;

1.2. Motivation and Main Contribution

In this paper, we provide a strategy to diagnose possible FDIA in DC-MGs to enhance cyber-physical security. Accordingly, a new procedure of wavelet transform (WT) and singular value decomposition (SVD) based on DL has been presented to diagnose cyber-attacks in DC-MG and identify the attack. Additionally, this paper presents a developed selective ensemble DL approach using a gray wolf optimization algorithm (GWOA). In this regard, in the first step, the WT has been applied to extract the features of the signals. Afterward, these features have been decomposed according to SVD to reach wavelet singular values (WSVs). Additionally, the WSVs have been utilized as the input for the multiple deep base concepts to obtain sensitive features automatically from raw vibration signals.

In the second stage, to ensure the variety of the base concepts, several encoders, and decoders including sparse auto-encoder, de-noising auto-encoder, and linear decoder, have been utilized to build different deep auto-encoders. Besides, bootstrapping was utilized to plan distinctive training information subsets for every base concept.

The third part presents a developed weighted voting (DWV) combination scenario with class-defined thresholds to perform selective ensemble learning.

In the final phase, a grey wolf optimization (GWO) approach is used to choose the optimal class-specific thresholds adaptively.

Briefly, the main contributions of this paper are explained as follows:

- WT and SVD are combined to extract features from signals and obtained singular values (SVs) of the signals.
- A singular value of the signals has been used as input of DL to diagnose FDIA in DC-MG for the first time.
- Deep base models have been built to learn hidden properties from signals adaptively.
- Several deep base patterns are obtained with AE and bootstrap types.
- DWV is designed with particular class thresholds to perform elective ensembles.
- The DWV's class-specific thresholds are optimized by applying the GWO algorithm.

1.3. Paper Structure

Part 2 presents the concepts about WT, SVD, and presented approach. In part 3, cyber-security in DC-MGs and FDIA will be demonstrated in detail. Part 4 will carry out the simulations, and the gained outcomes will be considered. Finally, in Part 5, the main conclusion will be expressed.

2. Basic Concepts

2.1. Wavelet Singular Values

In this section, the mechanism of the FDIA detection applies the benefits of WT and SVD analysis to exploit the exact features to utilize as the input indicator for the DL method. To begin with, we define the structure of the proposed technique; then, we state the efficiency of the technique involved in the short term.

2.1.1. Wavelet Transform

Typical 1-D decomposition includes a time-domain resolution or amplitude frequency that can usually not achieve an attack pattern. Moreover, it would be difficult to diagnose a DC-MG cyber-attack based solely on data provided by the time or frequency domain.

Time-frequency display is an efficient way of analyzing sensor signals to detect an attack by presenting visibility to the basic data in time. Various approaches include S transform (ST), WT, and short-time Fourier transform (STFT), which can discover time-frequency imaging. However, due to the constant resolution of the STFT frequency and the frequency darkness for the ST frequency band, WT was accepted to convert the transform of 1-D oscillation signals in this paper.

WT is a beneficial method for accurate time-frequency extraction due to the lesser time and higher frequency decompositions in the low-frequency part. Hence WT has been

called a microscope for signal assessment. In addition, it could depict low-frequency data on a wide scale and locally specify the high-frequency property on a small scale. WT is understood by calculating the inner signal efficiency of the status resolution of signal $z(t)$ and also by the wavelet function base $\theta_{a,\tau}(t)$. Accordingly, WT can be determined in below [33,42,43]:

$$WT_z(\alpha,\tau) = \int_{-\infty}^{+\infty} z(t)\theta_{\alpha,\tau}(t)dt = \int_{-\infty}^{+\infty} z(t)\theta\left(\frac{t-\tau}{\alpha}\right)dt \quad (1)$$

In which, α and τ provide the dilation factor and the translation factor in transformation.

2.1.2. Singular Value Decomposition

It proposes which of the main discrete signals $Z = z(1), z(2), \ldots, z(N)$ have been collected.

According to the References [13,33], the Hankel matrix can form the basis of the idea of phase reconstruction as below:

$$H = \begin{bmatrix} z(1) & z(2) & \ldots & z(n) \\ z(2) & z(3) & \ldots & z(n+1) \\ \ldots & \ldots & \ldots & \ldots \\ z(N-n+1) & z(N-N+2) & \ldots & z(N) \end{bmatrix} \quad (2)$$

where in, we have: $1 < n < N$, let $m = N - n + 1$, then $Y \epsilon R^{m*n}$. The mentioned matrix rebuilds the attack circuit matrix. The N matrix incorporates the dynamic properties of the invader into the reconstruction area by reconstructing the characteristic of the aggressor. Therefore, H can present as $H = D + W$, which D displays the $(N - n + 1) * n$ matrix of the soft signal in the reconstruction area, W also shows the $(N - n + 1) * n$ matrix of the noise intervention signal. The SVD can be used to the above-noted matrix H, where the bellow formula is achieved [13,33]:

$$H = USV^T \quad (3)$$

In Equation (3), U and V^T represent $(N - n + 1) * (N - n + 1)$ and $n * n$ matrices. S defines a diagonal matrix of $(N - n + 1) * n$, the basic diagonal parts provide $\delta_i (i = 1, 2, \ldots, j)$ and $j = min((N - n + 1), n)$, which is given in the Equation (4).

$$S = diag(\delta_1, \delta_2, \ldots, \delta_k) \quad (4)$$

In Equation (4), $\delta_1, \delta_2, \ldots, \delta_k$ give the SVs of matrix H, and $\delta_1 \geq \delta_2 \geq \ldots \geq \delta_k \geq 0$ has been convinced, V^T and U represent the left and right singular matrix.

2.2. Deep Learning Method

In this work, we proposed a developed selective ensemble DL approach using GWOA for FDIA detection in DC-MGs to enhance cyber-physical security.

In this regard, in the first step, DL base types are constructed to learn representative features adaptively from the WSV of signals. Then, to warranty the variety of the constructed base types, several deep auto-encoders are built with deforming auto-encoders (DAE), stacked auto-encoders (SAE), and linear decoder. In addition to this, distinguished training datasets for every basis type were planned using bootstrap. The DWV combination framework with particular class thresholds is planned to perform an elective ensemble in the third stage. In the final part, the GWO algorithm was carried out to achieve the optimal class-specific thresholds. The structures of the presented approach are introduced below:

2.2.1. Multiple Diverse Deep Auto-Encoders Construction

Various approaches have been proposed for developing the diversity of basic models, including adopting different types, choosing various hyperparameters, teaching with various optimizers, etc. To satisfy these diversities, this article adopted three methods as follows:

(a) Various auto-encoders usually have different features. Therefore, to obtain diverse base types, multiple DDAEs, DSAEs, DDLAEs, and DSLAEs were constructed through accumulating several SAEs, SLAEs DAEs, and DLAEs. The construction procedures of these deep automated encoders were the same as those taught by learning without layer supervision.

As shown in Figure 1, the latent output of the prior automatic encoder is utilized as the input of the subsequent automatic encoder until the final automatic encoder is trained, and the upper layer will be the soft-max arranger.

(b) A fine-tuning procedure was performed after learning without layered supervision, and the fine-tuning cost function procedure is computed through Equation (5).

$$J_{DeepAE}(\varphi) = -\frac{1}{n}\sum_{i=1}^{n}(\hat{x}_i log x_i) + \frac{\beta}{2}\sum_{k=1}^{k}\sum_{i=1}^{n_l}\sum_{j=1}^{n_{l=1}}\left(\omega_{ij}^{l}\right)^2 \quad (5)$$

where x_i and $\hat{x}_i$ represent the real and anticipated labels of the ith sample, also $(K-1)$ gives the number of hidden layers. The important point is that the iteration number of fine-tuning procedures impresses the impact of training; therefore, diverse iteration numbers of fine-tuning procedures have opted. If m diverse iteration numbers of fine-tuning procedures have opted, afterward there will be 4 m base types.

(c) In addition to constructing different deep base types, distinct training information sets for every type have also been planned through bootstrap to warranty the variety of such base types.

In particular, the entire dataset is assumed to be specified as $Z_w = \{Z_1, Z_2, \ldots, Z_i, \ldots, Z_s\}$, where s represents the sum number of the instances, $Z_i = \{z_1, z_2, \ldots, z_j, \ldots, z_m\}$, and m gives the information points number of every sample. Then Z^w represents disarticulate into three segments such as $Z^{tr} = \{Z_1, Z_2, \ldots, Z_n, \ldots, Z_\rho\}$, $Z^v = \{Z_{\rho+1}, Z_{\rho+2}, \ldots, Z_q\}$, and $Z^t = \{Z_{q+1}, Z_{q+2}, \ldots, Z_s\}$; where Z^{tr}, Z^t, and Z^v are the training dataset, test dataset, and validation dataset. To obtain distinctive training datasets, bootstrap was utilized to randomly choose n instances from Z^{tr} per time, and the training information subset for ith type was signified as Z^{tri}.

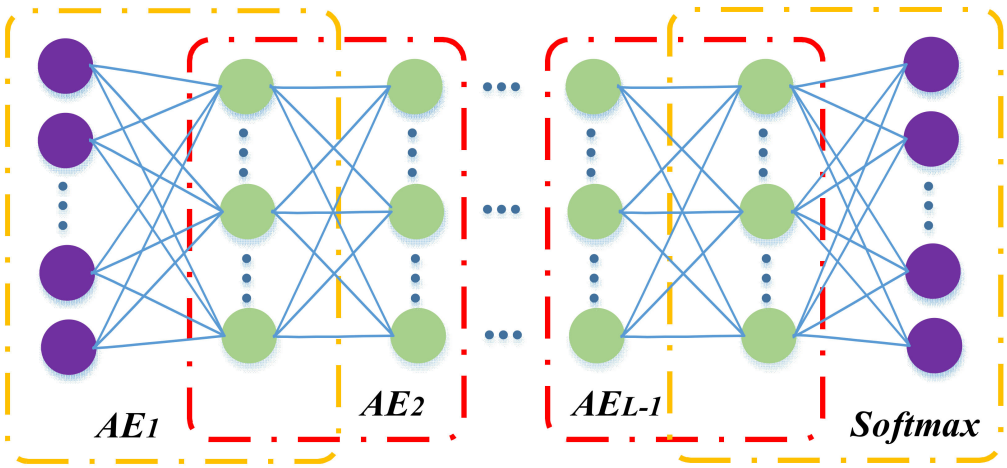


Figure 1. The framework of deep auto-encoder [43].

The method or architecture of selecting parameters is based on the empirical guidelines. In this regard, 2–5 hidden layers are suggested firstly, and then, gradually, the

number of hidden nodes decreases from the lower layer to the top layer. It is noteworthy that high-performance hardware has been required for lots of deep bases kinds. Therefore, 8–24 deep base types will be suitable.

2.2.2. DWV with Class-Specific Thresholds

Weighted voting (WV) criteria only provide the overall implementation diversity of every type to set the voting weights and usually do not pay attention to the efficiency variety of multiple base types for every attack type. As a result, in this paper, a novel compound platform called DWV was planned. The DWV is given, including the efficiency of diverse types for every fault mode according to a general term called $\mathcal{F}1$-measure [43,44]. To begin with, class-specific thresholds are adjusted to run the selected group; afterward, the class-specific weight is allocated to every base pattern in each error state.

Details of the DWV are presented as follows: In the first stage, several basic layouts are built and trained. After that, the confirmation outcomes of every base type are obtained; moreover, the corresponding $\mathcal{F}1$ values are computed using Equation (6).

$$\mathcal{F} = \frac{2\mathcal{P}\cdot P}{\mathcal{P}+\mathcal{P}} = \frac{2T\mathcal{P}}{2T\mathcal{P}+\mathcal{F}\mathcal{P}+\mathcal{F}N} \tag{6}$$

where:

$$\mathcal{P} = \frac{T\mathcal{P}}{T\mathcal{P}+\mathcal{F}\mathcal{P}} * 100\% \tag{7}$$

$$R = \frac{T\mathcal{P}}{T\mathcal{P}+\mathcal{F}N} * 100\% \tag{8}$$

$\mathcal{P}$ is defined as the accuracy rate, R gives the recall rate; $T\mathcal{P}$, $\mathcal{F}N$, $\mathcal{F}\mathcal{P}$ provide the number of true positive, false negative, and false-positive samples. After this step, the class-specific $\mathcal{F}1$ thresholds for every error type are defined like $ft = ft_1, ft_2, \ldots, ft_c$ [43,44].

By comparing each value of $\mathcal{F}1$ with the relevant threshold, if the amounts of $\mathcal{F}1$ are less than the relevant threshold amounts, the value is fixed to 0, which defines the corresponding weight will also be equal to 0. As a result, we need to define Equation (9) as:

$$\mathcal{F}_{ij} = \begin{cases} 0\,,\ \mathcal{F}_{ij} < ft_{\,j} \\ \mathcal{F}_{ij},\ Otherwise \end{cases}, \qquad i = 1,\ 2,\ \ldots,\ k; j = 1,\ 2,\ \ldots,\ \delta \tag{9}$$

In which:

$$\min\{\mathcal{F}_{ij}, i = 1,\ 2,\ \ldots k\} \le ft_j \le \max\{\mathcal{F}_{ij}, i = 1,\ 2,\ \ldots k\} \tag{10}$$

$\mathcal{F}_{ij}$ provides the $\mathcal{F}1$ value for error mode j of ith base type, ft_j gives the $\mathcal{F}1$ threshold for error type i, and δ represents the number of error types. After that, we should devote weights to every base type for every error mode as given in Equation (11).

$$\omega_{ij} = \frac{\mathcal{F}_{ij}}{\sum_{i=1}^{k}\mathcal{F}_{ij}} \tag{11}$$

where:

$$\sum_{i=1}^{k}\omega_{ij},\ \omega_{ij} \ge 0 \tag{12}$$

ω_{ij} is the weights of base type i for error type j.

In the final stage, the decision is made as follows; we should suppose that type i(Z_t) gives the expected label of base type i for instance Z_t. The sum score that Z_t appertains to error type j is computed through Equation (13).

$$Score_j(Z_t) \ = \sum_{i=1}^{k}\omega_{ij}\cdot H(Z_t, j),\ t = \rho+1,\ \rho+2,\ \ldots,\ q \tag{13}$$

where:

$$H(Z_t, j) = \begin{cases} 1 & Model_i(Z_t) = j \\ 0 & Otherwise \end{cases} \quad (14)$$

The final predicted label $Pre\_K\ (Z_t)$ of Z_t is acquired by Equation (15).

$$Pre_K(Z_t) = T \quad (15)$$

where:

$$Score_r(Z_t) = \max\{Score_r(Z_t),\ \mathrm{j} = 1,\ 2,\ \ldots \delta\} \quad (16)$$

As a result, the accuracy of the final confirmation of ensemble learning is computed as follows:

$$Ensembel_{V_{acc}} = \frac{\sum_{t=\rho+1}^{q} h(Z_t, X_t)}{q - \rho} \quad (17)$$

where:

$$h(Z_t, X_t) = \begin{cases} 1 & Pre\_K(Z_t) = X_t \\ 0 & Otherwise \end{cases} \quad (18)$$

X_t also represents the actual label of the sample Z_t.

2.2.3. Gray Wolf Optimization

GWO is a relatively novel intelligence algorithm presented by Mirjalili and his colleagues, designed through the hunting behaviors and the social hierarchy of gray wolves [45]. In GWO, the rest of the solutions are named as ω wolves that chase the α, β and δ wolves within their hunting. The grey wolves' hunting behavior can be formulated as follows:

$$\begin{cases} D_p = \left|C \cdot X_p(t) - X(t)\right| \\ X(t+1) = \frac{1}{3} \sum\limits_{p=\alpha,\beta,\delta} \left(X_p(t) - A \cdot D_p\right) \end{cases} \quad (19)$$

where D_p gives the absolute amount of every dimension in the vector, t shows the running iteration, X and X_p represent the situation vectors of grey wolf and prey. Also, A and C provide coefficient vectors that are computed in Equation (20):

$$\begin{cases} A = 2a \cdot r_1 - a \\ C = 2a \cdot r_2 \\ a = 2 - 2t / t_{max} \\ r_1, r_2 = rand(0, 1) \end{cases} \quad (20)$$

where in Equation (20), a signifies control parameter, t_{max} provides the maximum number of iterations. r_1, r_2 show the random vectors of (0, 1). Multi-objective gray wolf optimization (MOGWO) is an extended form of the GWO where two added components are dedicated to accommodating multipurpose optimization problems. One component is the archive used to store Pareto solutions (non-dominated solutions). Another component acts as a leader election framework that aims to opt wolves α, β, and δ from the set while hunting. Exact explanations of the two components are provided as follows:

(a) The external archive

In MOGWO, an outer archive was performed to save Pareto solutions achieved. During every iteration, Pareto solutions are reserved while the dominant members are removed. Besides, while there is mutual non-dominate from the new solution to archive residents, a new solution can be embedded into the archive. When the archive is full, the procedure of the network, according to Reference [46], is used to replace one of the archive members in the busiest set with a new solution that assists in maintaining the variety of archive residents.

(b) The leader selection framework

Since the non-dominated solutions cannot be easily sorted, it would be hard to straightly choose the leader of wolves with considering the first, 2nd, and 3rd best solutions. In reply to this, according to [46], the leader chosen framework selected with the roulette-wheel approach can be used to select such leaders from the archive, including the entire non-dominated solutions achieved. In this strategy, the probability of being opted as new leaders is inversely proportional to the severity of the parts that increase the variety of solutions.

2.3. Procedure of the Proposed Technique

As shown in Figure 2, in this paper, we propose a developed selective ensemble DL approach by GWO method to detect cyber-attack in DC-MGs.

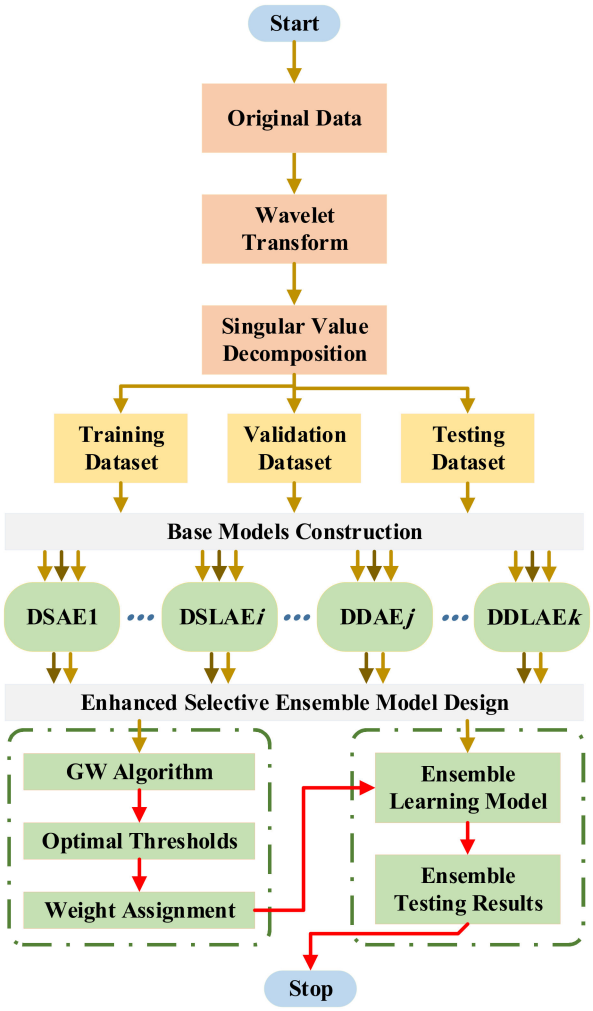


Figure 2. Diagram of the offered FDIA detection procedure.

In the first stage, the signal feature is extracted using WSVs. Then, deep base types are built to adaptively learn hidden characteristics from extracted indexes by WSVs of signals to ensure the variety of the base types. In this way: (1) the deep auto-encoders are produced by applying DAE, SAE, and linear decoder; (2) the datasets of distinctive training for every base type are planned by bootstrap. After that, the DWV combination framework with particular class thresholds is planned to conduct an elective ensemble. In the final stage, the GWO algorithm is applied to find optimal thresholds.

3. CYBER PHYSICAL LAYER in DC-MGs

In this section, we focus on the cybersecurity of DC-MG and then explaining a type of cyber-attack in such systems.

3.1. Cyber Security in DC-MG

As a small electrical power grid, the MG encompasses both production and consumption, allowing it to operate in both network and island operation modes. In addition to the physical layer like distributed generations (DGs) and green energy units, storage and loads units, an MG with an interconnected cyber layer, basically with transferring information and decision-making according to collected datum, deals with advanced measurement infrastructures (AMIs).

Such factors make MG a complicated CPS with a nonlinear, hybrid correlated structure, which in turn is an accessible target point for hackers to infiltrate and exploit their malicious targets. Several items including heterogeneous information resources, vulnerable sensors, and a high amount of interactions within the MG and from the MG to the main network, sensibility to synchronization of time and communication postpones usually create different challenges to ensure a secure and reliable operation strategy in MGs. AMI plays a pivotal key layer in an MG that creates a two-rout communication way from the smart metering components with special IP addresses to the electrical suppliers and users. Additionally, AMI is responsible for information collection, information communication, and energy expenditures assessment for optimal MG performance.

AMI enables to make real-time decisions on both production and consumption sides. According to AMI, DGs are timely optimized for their operation, and electricity consumers can take appropriate economic decisions to maximize energy savings and actively participate in market pricing. Figure 3 displays the cyber-physical framework of an MG with AMI. As depicted in Figure 3, through links of wireless/wired communication, smart meters, which act as the main section of AMI, get information from electrical consumers, generations, and storage agents for efficient decision making and exploitation.

As a result, smart sensors are given into account as a gateway to gather and assess the state of the physical layers to fine dust. This factor makes them a vulnerable and potential point of intrusion to carry out malicious attacks because they affect the efficiency of the whole MG. By compromising the information reported by smart sensors, it is possible to infiltrate the optimal dispatch of DGs, thereby greatly lessening the reliability, security, and energy quality of electrical power services.

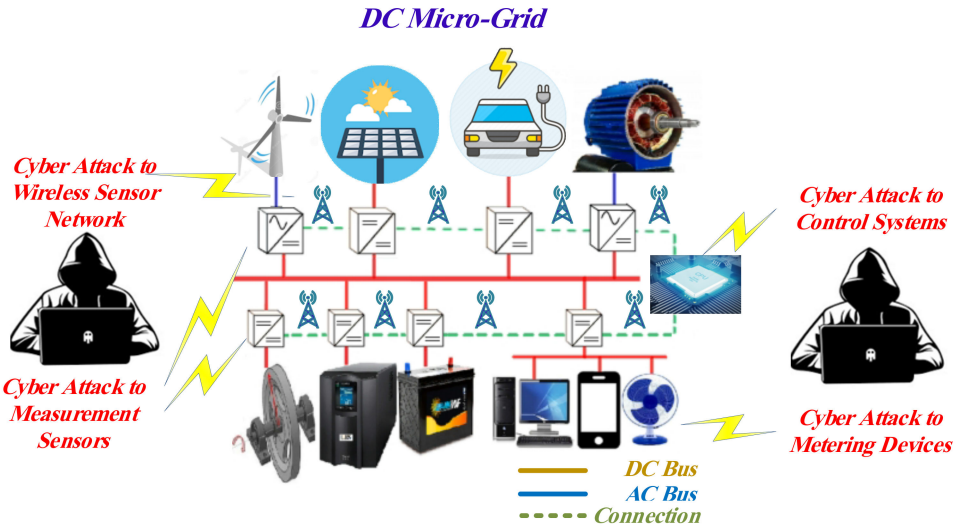


Figure 3. The framework of MG as a CPS layer.

3.2. Cyber-Attack

In a generic MG, the main task of AMI can be to collect load consumption information and exchanged it to the decision-making program for appropriate planning of generating units. In every case, a healthful MG must meet the production and demand equilibrium equation to eschew unanticipated interruptions or obliged load shedding. Furthermore, AMI can do an important duty in diminishing the entire cost of MGs via offering real-time information regarding consumers' demands. To meet electrical requirements, an MG should gain power generation during peak load times.

By accurately estimating the load demand offered by AMI, the MG can use demand response techniques to change peak load times, thereby reducing the total costs of MG, using unnecessary feeder combustion, and preventing frequency and voltage drops. This would be a valuable and applicable strategy while accurate data on electrical load demand is presented. Unfortunately, AMI, which is according to the communication interfaces, can be assailable from cyber hackers so an expert enemy can change the reported load.

By hacking AMI, the other party disrupts the demand response procedures and upsets the balance of production and demand. This can lead to other damaging results, including additional operating costs, impractical operations, and unplanned shutdowns. As a result, the issue of which events might ultimately occur for an MG depends on both the stability of the cyber-attack and how the MG works. As noted earlier, an MG can act as a network-connected mode or islanded mode. A cyber-attack on AMI can gain the MG's costs, power loss, and voltage drop when in network-connected mode. For example, in the islanded operation of a power system, a cyber-attack can bring about more intense consequences, including loss of production and demand balance and inaccessibility of exploitation or even shutting down of units. In terms of severity, cyber-attack power can be categorized into two diverse states: Firstly, a malicious attack by strength and immediate impact causes the most detriment to the MG. Such kinds of attacks should be felt quickly and should be recognizable because of their large size. Secondly, a destructive attack with a smooth and slow impact causes a change in the long term. The significant aim of the form of cyber-attack is to prevent the system from being detected and changes in MG's accessibility in the long run.

In this regard, in this article, both forms of cyber-attacks on MGs are analyzed. An intelligent type is presented to detect a cyber-attack, which is described in detail.

4. Simulation Outcomes

In the simulation, we tested the presented strategy for attack detection on the cyber-physical DC-MG, which is depicted in Figure 4b with $V_{dcref} = 315$ V, including four different agents with equal capacities interconnected with others with resistive lines. It should be stated that every production agent includes a battery accompanied by boost converters, as depicted in Figure 4a. To confirm the efficiency of the offered strategy for attack detection in cooperative DC-MG, it was tested against numerous disturbances. This included FDIA and stealth attacks in sensors that often go undetected with distributed observers, and also communication links to diagnose the affected nodes so that the intransitive measures can be derived to maintain cyber-security. In the FDIAs, the attacker can access the datum of the sensors, communication links, and controllers. To simulate the FDIA, it has been assumed that the attacker can manipulate the data; therefore, the data has been manipulated to show the attack at the attack's time. The parameters of the system are presented in Table 2. Because the main goal in this paper is FDIA detection in DC-MGs, the system details and control parameters in [47] are used to simulate the physical system and controller. It has to be stated that every attack in the defined strategies has been separated using a certain time gap to present a better understanding.

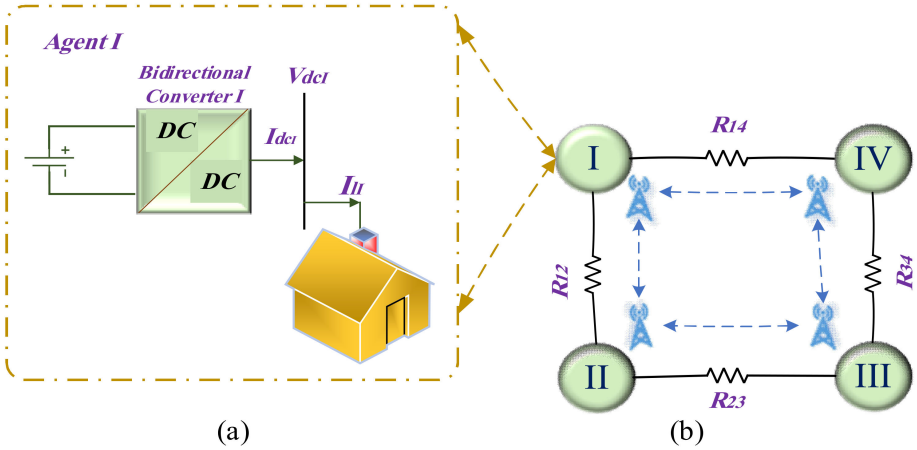


Figure 4. Simulated system: (**a**) unit type; (**b**) Cyber-physical DC-MG with four resources.

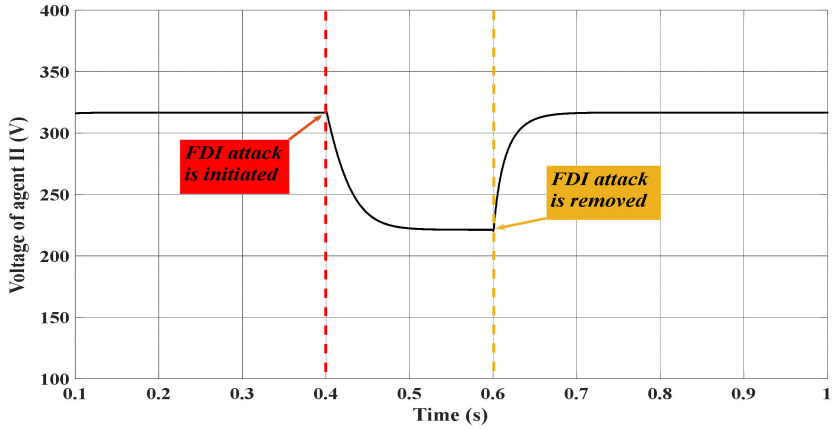
Table 2. Simulated system parameters.

Parameter	Value
V_{dcref}	315 V
Δt	5 ms
L_f	5 mH
C_f	50 mF
R_{12}	1.8 Ω
R_{14}	2.3 Ω
R_{23}	1.3 Ω
R_{34}	1.5 Ω

4.1. Case Studies

The proposed strategy was implemented into three different study cases.

Study Case 1: In this part, the FDIA on the voltage sensor occurs in the 2nd unit. System behavior is considered in an example of a defined type of FDIA, and DL indicators have been indicated which one has been extracted based on the WSVs. The FDIA starts at t = 0.4 and finishes at t = 0.6 s, respectively. Moreover, the voltage reference signal amplitude changes and is reduced by about 30%. The outcomes of this study case are displayed in Figure 5. Figure 5a shows that the DC-MG voltage on that the FDIA was reported in a timely manner. Additionally, Figure 5b displays the signal wavelet decomposition in db4, which is used to extract SVs utilized as machine learning input for detecting cyber-attacks.



(**a**)

Figure 5. *Cont.*

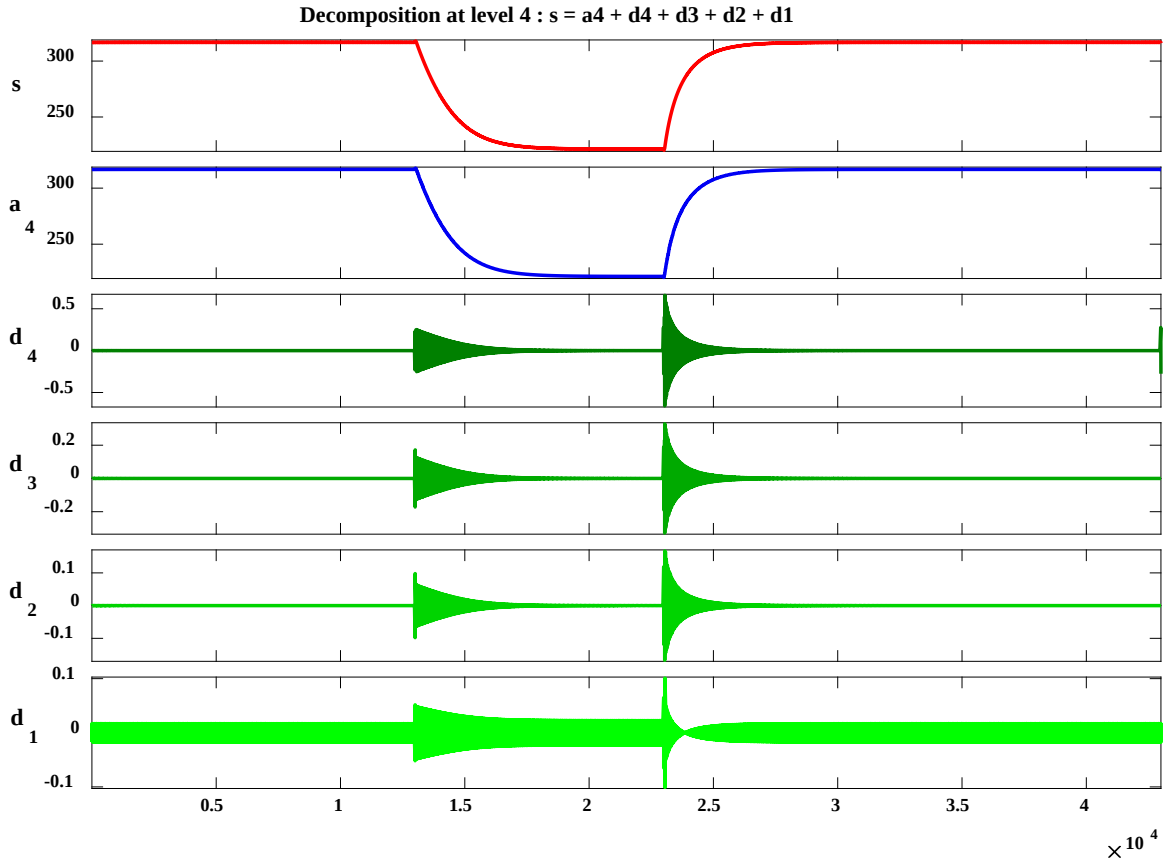
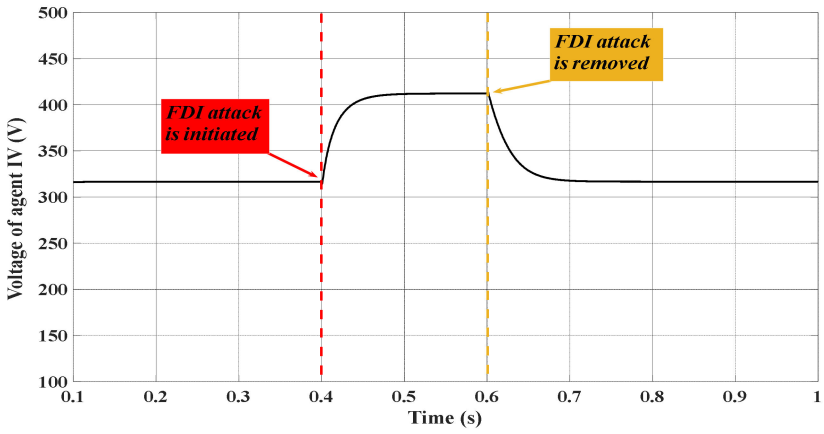


Figure 5. FDIA based on raising the voltage reference waveform amplitude: (**a**) Voltage waveform,(**b**) Wavelet decomposition.

Study Case 2: In this part, the FDIA on the voltage sensor occurs in the 4th agent. System behavior is considered in an example of this type of FDIA, and deep machine learning indicators show which one has been extracted based on the WSVs. The FDIA starts at t = 0.4 and finishes at t = 0.6 s, respectively. Moreover, the voltage reference signals amplitude changes and increases about 30%. The outcomes of this study case have been displayed in Figure 6. Figure 6a shows that the DC-MG voltage on that the FDIA was reported in a timely manner. Additionally, Figure 6b displays the signal wavelet decomposition in db4, which is used to extract SVs utilized as machine learning input for detecting cyber-attacks.



(**a**)

Figure 6. *Cont.*

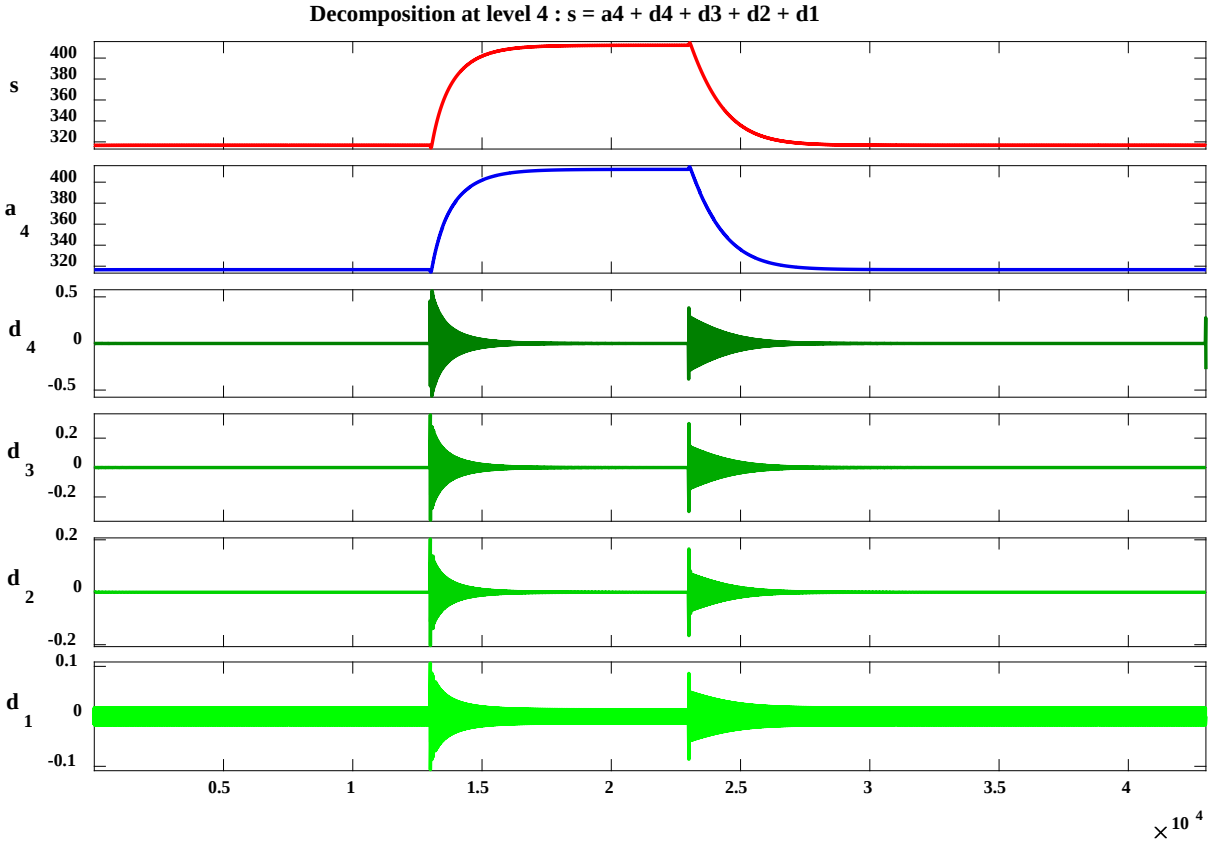
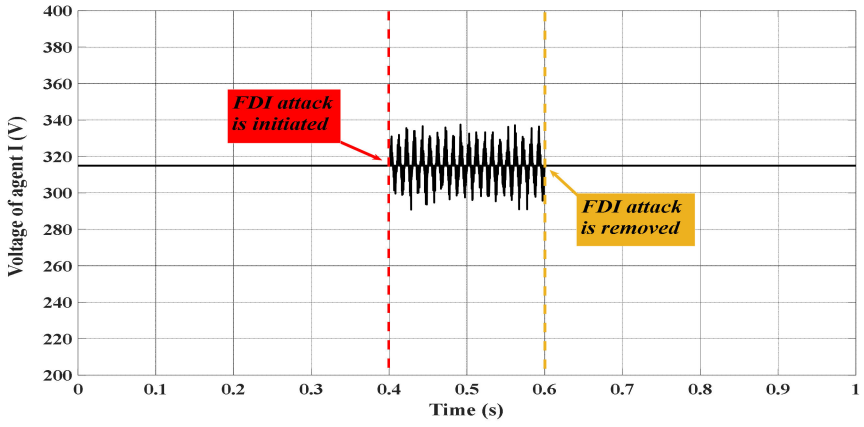


Figure 6. FDIA according to decreasing the voltage reference waveform amplitude: (**a**) Voltage Waveform, (**b**) Wavelet decomposition.

Study Case 3: In this part, the FDIA on the voltage sensor occurs in the 1st unit. System behavior is considered in an example of this type of FDIA, and DL indicators displayed which one has been extracted based on the WSVs. The FDIA starts at t = 0.4 and finishes at t = 0.6 s, respectively. Moreover, the voltage reference signal amplitude changes, and noise adds to the signal. The outcomes of this study case have been displayed in Figure 7. Figure 7a shows that the DC-MG voltage on that the FDIA was reported in a timely manner. Additionally, Figure 7b displays the signal wavelet decomposition in db4, which is used to extract SVs utilized as machine learning input for detecting cyber-attacks.



(**a**)

Figure 7. *Cont.*

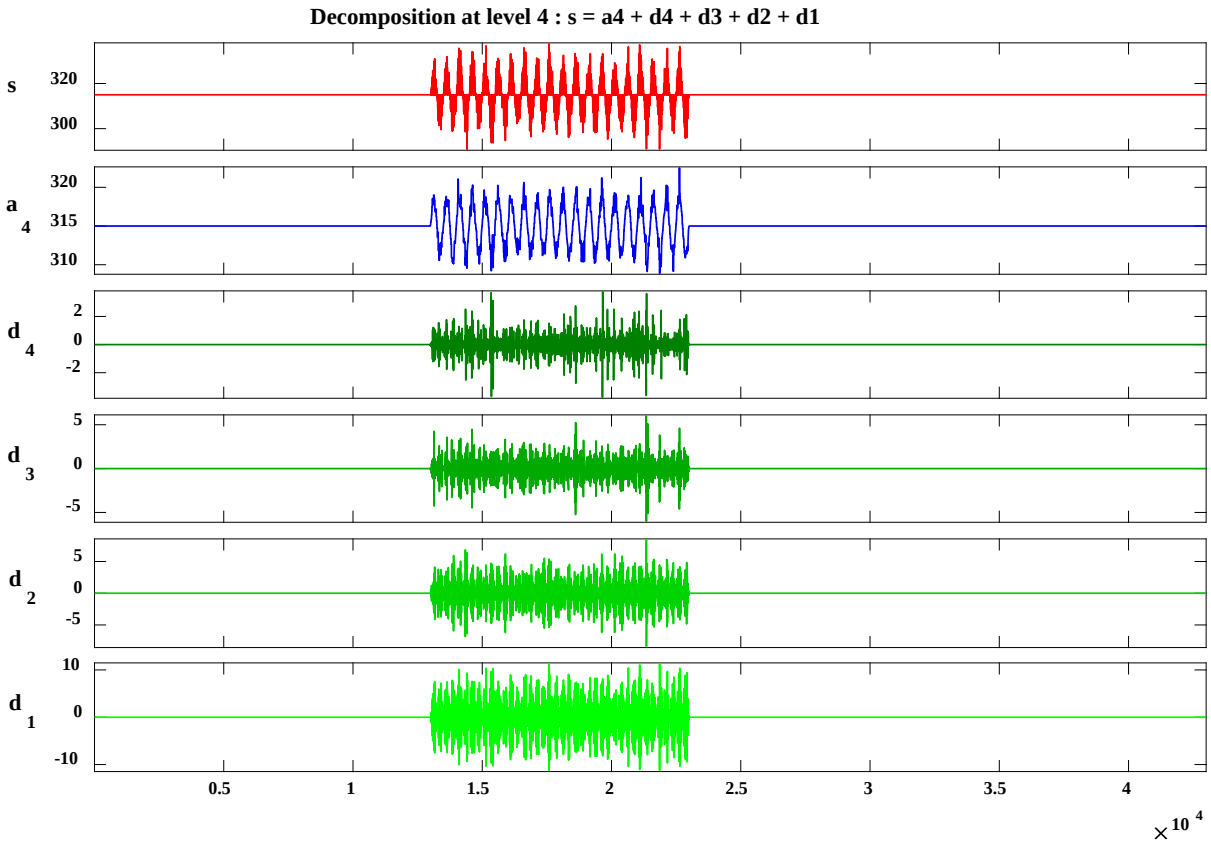


Figure 7. FDIA according to combining a noise to voltage reference waveform: (**a**) Voltage waveform, (**b**) Wavelet decomposition.

4.2. Discussion

On the one hand, a decision would be positive when it is recognized as a cyber-attack. On the other hand, a decision would be negative when the anomaly detection type identifies it as a usual condition. The real decision has been taken when the type of anomaly detection is the true decision. An incorrect decision displays a false reaction of the type of detection of the cyber-attack.

In this regard, it is inferred that a proper type of anomaly detection is a type with a low false rate. Based on these definitions, four various criteria can be determined as follows: miss rate (MR), false alarm rate (FAR), hit rate (HR), and correctly reject rate (CRR). To aid a clear understanding of the issue, Table 3 provides a matrix of the suggested detection method to show the accuracy rate of the suggested method to detect attacked conditions and normal conditions correctly. Hit rate (true positive) shows the percentage of correct detection when FDIAs occur in the system, and the method can detect it as attacked. Miss rate (false Negative) shows the percentage of incorrect detection of the method when FDIAs occur in the system, and the detection method cannot detect it as attacked. Correct rejection rate (true negative) represents the percentage of correct diagnosis of the normal conditions; in other words, when there is no attack in the system, and the condition is normal, the method does not alarm as the attacked condition. False alarm rate (false positive) is the percentage of incorrect diagnosis in the normal conditions and the detection method alarm in the normal condition as the attacked.

The number of test data in attacked conditions is 1348 and in normal conditions is 1174. The proposed cyber-attack detection method could detect 1285 from 1348 (number of test data in attacked conditions) as the manipulated or attacked condition and accurately identify 1125 from 1174 (number of test data in normal conditions) as the normal condition.

Table 3. The proposed detection matrix framework.

Type	Real Value		
	Form	**Positives**	**Negatives**
Detection Type Response	Positives	Hit Rate True Positive	False Alarm Rate False Positive
	Negatives	Miss Rate False Negative	Correct Rejection Rate True Negative

Various case tests have been executed to validate the presented deep machine learning approach in the FDIA detection. The FDIA type has analyzed the efficiency/performance of offered detection method, and the appraisal results are depicted in Table 4. Besides, to indicate the performance of the proposed cyber-attack detection approach, it compares the Shallow model and deep neural network (DNN) with Hilbert–Huang Transform (HHT) presented in the [48] in Table 4. As shown in Table 4, it can be argued that the proposed method could diagnose the FDIAs by detection precision over 95% that indicates the performance of the offered diagnosing approach on detecting the FDIAs.

According to the Shallow model and HHT as DNN inputs, the detection methods can diagnose FDIAs with over 90% and 93% accuracy, respectively. The DNN training time in HHT as DNN inputs are 1759 s that means detection time is 50 ms; but in the proposed technique, the average detection time is 10 ms and the DNN training time is 1638 s. As a result, it provides the competency of the stated detection approach for detecting the FDIAs.

Table 4. The value matrix of the presented detection framework.

Type	Method	Real Value		
		Form	**Positives**	**Negatives**
Detection Type Response	WT and DL	Positives	95.36%	4.16%
		Negatives	4.64%	95.84%
	Shallow Model	Positives	90.13%	8.36%
		Negatives	9.87%	91.64%
	HHT and DL [48]	Positives	93.75%	4.77%
		Negatives	6.25%	95.23%
	Method		**WT and DL**	**HHT and DL [48]**
Response Time	Average Detection Time		10 ms	50 ms
	DNN Training Time		1638 s	1759 s

5. Conclusions

This research work presents an advanced selective DL approach with a GWO algorithm using WSV to type a cyber-attack detection procedure. WSVs have been extracted from the spectral energy of the input signals to be used as an indicator of DL input, and then numerous types of deep bases are produced via SAE, DAE, and linear encoder. Bootstrap has also been used for them to design distinctive training information subsets. In addition, a hybrid DWV strategy with class-specific thresholds has been presented to perform the selected group, and the GWO algorithm has been used for class-specific thresholds optimization. Accordingly, simulation data has been applied to confirm the effectiveness of the presented framework. The gained results of the simulation have been compared with the new Shallow model and Hilbert–Huang transform methods. The simulation results suggested that the presented approach can detect FDIAs more accurately and robustly in DC-MG. Besides, it was seen that the presented type illustrates suitable efficiency in the face of FDIAs with numerous severities ranging from 10% to 100% information changed. The outcomes of two diverse criteria for the rate of diagnosis and the outcomes of the confusion matrix confirm the integrity and valuable proficiency of the proposed anomaly type of diagnosis. The efficiency of the presented method has been verified using simulations by

offline digital time-domain in the MATLAB software. The obtained outcomes of 2 various criteria of detection rate and matrixes support the integrity and significant sufficiency of the presented anomaly detection type.

Evaluating the efficiency of the suggested cyber-attack detection scheme on a real-time "hardware experiment" can be a hot subject for future research. The FPGA and DSP boards can also be used as the processor. Other cyber-attacks like a man-in-the-middle attack, reply attacks, etc., can consider in the DC-MG in future studies.

Author Contributions: M.D. and M.G.: investigation, methodology, writing-original draft; N.B. and M.S.: writing-review and editing; T.N.: supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Aghaee, F.; Mahdian Dehkordi, N.; Bayati, N.; Hajizadeh, A. Distributed control methods and impact of communication failure in AC microgrids: A comparative review. *Electronics* **2019**, *8*, 1265. [CrossRef]
2. Ghiasi, M. Detailed study, multi-objective optimization, and design of an AC-DC smart microgrid with hybrid renewable energy resources. *Energy* **2019**, *169*, 496–507. [CrossRef]
3. Ghiasi, M.; Niknam, T.; Dehghani, M.; Siano, P.; Haes Alhelou, H.; Al-Hinai, A. Optimal Multi-Operation Energy Management in Smart Microgrids in the Presence of RESs Based on Multi-Objective Improved DE Algorithm: Cost-Emission Based Optimization. *Appl. Sci.* **2021**, *11*, 3661. [CrossRef]
4. Ghiasi, M.; Dehghani, M.; Niknam, T.; Baghaee, H.R.; Padmanaban, S.; Gharehpetian, G.B.; Aliev, H. Resiliency/Cost-based Optimal Design of Distribution Network to Maintain Power System Stability against Physical Attacks: A Practical Study Case. *IEEE Access* **2021**, *9*, 43862–43875. [CrossRef]
5. Dehghani, M.; Ghiasi, M.; GhasemiGarpachi, M.; Niknam, T.; Kavousi-Fard, A.; Shirazi, H. Stabilization of DC/DC Converter with Constant Power Load using Exact Feedback Linearization Method based on Backstepping Sliding Mode Control and Nonlinear Disturbance Observer. In Proceedings of the 2021 12th Power Electronics, Drive Systems, and Technologies Conference (PEDSTC), Tehran, Iran, 2–4 February 2021; pp. 1–6.
6. Esfahani, M.S.G.; Savaghebi, M. A Decentralized Control Strategy Based on VI Droop for Enhancing Dynamics of Autonomous Hybrid AC/DC Microgrids. *IEEE Trans. Power Electron.* **2021**, *36*, 9430–9440.
7. Bayati, N.; Baghaee, H.R.; Hajizadeh, A.; Soltani, M. A Fuse Saving Scheme for DC Microgrids With High Penetration of Renewable Energy Resources. *IEEE Access* **2020**, *8*, 137407–137417. [CrossRef]
8. Ghiasi, M.; Dehghani, M.; Niknam, T.; Kavousi-Fard, A.; Siano, P.; Alhelou, H.H. Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform. *IEEE Access* **2021**, *9*, 29429–29440. [CrossRef]
9. Shirazi, H.; Ghiasi, M.; Dehghani, M.; Niknam, T.; Garpachi, M.G.; Ramezani, A. Cost-Emission Control Based Physical-Resilience Oriented Strategy for Optimal Allocation of Distributed Generation in Smart Microgrid. In Proceedings of the 2021 7th International Conference on Control, Instrumentation and Automation (ICCIA), Tabriz, Iran, 23–24 February 2021; pp. 1–6.
10. Wang, H.; Ruan, J.; Ma, Z.; Zhou, B.; Fu, X.; Cao, G. Deep learning aided interval state prediction for improving cyber security in energy internet. *Energy* **2019**, *174*, 1292–1304. [CrossRef]
11. Dehghani, M.; Ghiasi, M.; Niknam, T.; Kavousi-Fard, A.; Shasadeghi, M.; Ghadimi, N.; Taghizadeh-Hesary, F. Blockchain-Based Securing of Data Exchange in a Power Transmission System Considering Congestion Management and Social Welfare. *Sustainability* **2021**, *13*, 90. [CrossRef]
12. Sahoo, S.; Mishra, S.; Peng, J.C.-H.; Dragičević, T. A Stealth Cyber-Attack Detection Strategy for DC Microgrids. *IEEE Trans. Power Electron.* **2018**, *34*, 8162–8174. [CrossRef]
13. Dehghani, M.; Ghiasi, M.; Niknam, T.; Kavousi-Fard, A.; Tajik, E.; Padmanaban, S.; Aliev, H. Cyber Attack Detection based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack. *IEEE Access* **2021**, *9*, 16488–16507. [CrossRef]
14. Kim, S.; Park, S. CPS (cyber physical system) based manufacturing system optimization. *Procedia Comput. Sci.* **2017**, *122*, 518–524. [CrossRef]
15. Ahmed, M.; Pathan, A.-S.K. False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure. *Complex Adapt. Syst. Model.* **2020**, *8*, 1–14. [CrossRef]
16. Bayati, N.; Baghaee, H.R.; Hajizadeh, A.; Soltani, M.; Lin, Z. Mathematical morphology-based local fault detection in DC Microgrid clusters. *Electr. Power Syst. Res.* **2020**, *192*, 106981. [CrossRef]
17. Mola, M.; Meskin, N.; Khorasani, K.; Massoud, A. Distributed Event-Triggered Consensus-Based Control of DC Microgrids in Presence of DoS Cyber Attacks. *IEEE Access* **2021**, *9*, 54009–54021. [CrossRef]

18. Wang, B.; Dabbaghjamanesh, M.; Fard, A.K.; Mehraeen, S. Cybersecurity Enhancement of Power Trading Within the Networked Microgrids Based on Blockchain and Directed Acylic Graph Approach. *IEEE Trans. Ind. Appl.* **2019**, *55*, 7300–7309. [CrossRef]
19. Liang, G.; Weller, S.R.; Luo, F.; Zhao, J.; Dong, Z.Y. Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism. *IEEE Trans. Smart Grid* **2017**, *9*, 3820–3829. [CrossRef]
20. Zhao, J.; Zhang, G.; Dong, Z.Y.; Wong, K.P. Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation. *IEEE Trans. Smart Grid* **2015**, *7*, 6–8. [CrossRef]
21. Wang, Q.; Tai, W.; Tang, Y.; Ni, M. Review of the false data injection attack against the cyber-physical power system. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 101–107. [CrossRef]
22. Zhao, J.; Mili, L.; Wang, M. A Generalized False Data Injection Attacks Against Power System Nonlinear State Estimator and Countermeasures. *IEEE Trans. Power Syst.* **2018**, *33*, 4868–4877. [CrossRef]
23. Dehghani, M.; Ghiasi, M.; Niknam, T.; Kavousi-Fard, A.; Padmanaban, S. False Data Injection Attack Detection based on Hilbert-Huang Transform in AC Smart Islands. *IEEE Access* **2020**, *8*, 179002–179017. [CrossRef]
24. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Trans. Control. Netw. Syst.* **2014**, *1*, 370–379. [CrossRef]
25. Bobba, R.B.; Rogers, K.M.; Wang, Q.; Khurana, H.; Nahrstedt, K.; Overbye, T.J. Detecting false data injection attacks on dc state estimation. In Proceedings of the Preprints of the First Workshop on Secure Control Systems, CPSWEEK, Stockholm, Sweden, 12–16 April 2010.
26. Foroutan, S.A.; Salmasi, F.R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *2*, 161–171. [CrossRef]
27. Esmalifalak, M.; Liu, L.; Nguyen, N.; Zheng, R.; Han, Z. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Syst. J.* **2014**, *11*, 1644–1652. [CrossRef]
28. Mohammadi-Ivatloo, B.; Shiroei, M.; Parniani, M. Online small signal stability analysis of multi-machine systems based on synchronized phasor measurements. *Electr. Power Syst. Res.* **2011**, *81*, 1887–1896. [CrossRef]
29. Aghajani, G.; Ghadimi, N. Multi-objective energy management in a micro-grid. *Energy Rep.* **2018**, *4*, 218–225. [CrossRef]
30. Mehrdad, S.; Mousavian, S.; Madraki, G.; Dvorkin, Y. Cyber-physical resilience of electrical power systems against malicious attacks: A review. *Curr. Sustain. Renew. Energy Rep.* **2018**, *5*, 14–22. [CrossRef]
31. Habibi, M.R.; Baghaee, H.R.; Dragi ˇcevi, T.; Blaabjerg, F. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**. [CrossRef]
32. Dehghani, M.; Khooban, M.H.; Niknam, T.; Rafiei, S.M.R. Time-varying sliding mode control strategy for multibus low-voltage microgrids with parallel connected renewable power sources in islanding mode. *J. Energy Eng.* **2016**, *142*, 05016002. [CrossRef]
33. Dehghani, M.; Khooban, M.H.; Niknam, T. Fast fault detection and classification based on a combination of wavelet singular entropy theory and fuzzy logic in distribution lines in the presence of distributed generations. *Int. J. Electr. Power Energy Syst.* **2016**, *78*, 455–462. [CrossRef]
34. Giraldo, J.; Urbina, D.; Cardenas, A.; Valente, J.; Faisal, M.; Ruths, J.; Tippenhauer, N.O.; Sandberg, H.; Candell, R. A survey of physics-based attack detection in cyber-physical systems. *ACM Comput. Surv.* **2018**, *51*, 1–36. [CrossRef]
35. Tan, S.; Guerrero, J.O.; Xie, P.; Han, R.; Vasquez, J.C. Brief Survey on Attack Detection Methods for Cyber-Physical Systems. *IEEE Syst. J.* **2020**, *14*, 5329–5339. [CrossRef]
36. Ding, D.; Han, Q.-L.; Xiang, Y.; Ge, X.; Zhang, X.-M. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing* **2018**, *275*, 1674–1683. [CrossRef]
37. He, Y.; Mendis, G.J.; Wei, J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Trans. Smart Grid* **2017**, *8*, 2505–2516. [CrossRef]
38. Ozay, M.; Esnaola, I.; Vural, F.T.Y.; Kulkarni, S.R.; Poor, H.V. Machine learning methods for attack detection in the smart grid. *IEEE Trans. Neural Netw. Learn. Syst.* **2015**, *27*, 1773–1786. [CrossRef]
39. Chaojun, G.; Jirutitijaroen, P.; Motani, M. Detecting false data injection attacks in ac state estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483. [CrossRef]
40. Rawat, D.B.; Bajracharya, C. Detection of false data injection attacks in smart grid communication systems. *IEEE Signal Process. Lett.* **2015**, *22*, 1652–1656. [CrossRef]
41. Sahoo, S.; Peng, J.C.-H.; Devakumar, A.; Mishra, S.; Dragičević, T. On detection of false data in cooperative dc microgrids—A discordant element approach. *IEEE Trans. Ind. Electron.* **2019**, *67*, 6562–6571. [CrossRef]
42. Biswal, B.; Vyshnavi, E.; Sairam, M.V.S.; Rout, P.K. Robust retinal optic disc and optic cup segmentation via stationary wavelet transform and maximum vessel pixel sum. *IET Image Process.* **2019**, *14*, 592–602. [CrossRef]
43. Dehghani, M.; Kavousi-Fard, A.; Dabbaghjamanesh, M.; Avatefipour, O. Deep learning based method for false data injection attack detection in AC smart islands. *IET Gener. Transm. Distrib.* **2020**, *14*, 5756–5765. [CrossRef]
44. Shao, H.D.; Jiang, H.K.; Li, X.Q.; Wu, S.P. Intelligent fault diagnosis of rolling bearing using deep wavelet auto-encoder with extreme learning machine. *Knowl. Based Syst.* **2018**, *140*, 1–14. [CrossRef]
45. Mirjalili, S.; Mirjalili, S.M.; Lewis, A. Grey wolf optimizer. *Adv. Eng. Softw.* **2014**, *69*, 46–61. [CrossRef]
46. Mirjalili, S.; Saremi, S.; Mirjalili, S.M.; Coelho, L.D.S. Multi-objective grey wolf optimizer: A novel algorithm for multi-criterion optimization. *Expert Syst. Appl.* **2016**, *47*, 106–119. [CrossRef]

47. Nasirian, V.; Moayedi, S.; Davoudi, A.; Lewis, F.L. Distributed cooperative control of DC microgrids. *IEEE Trans. Power Electron.* **2014**, *30*, 2288–2303. [CrossRef]
48. Cui, H.; Dong, X.; Deng, H.; Dehghani, M.; Alsubhi, K.; Aljahdali, H.M.A. Cyber Attack Detection Process in Sensor of DC Micro-Grids Under Electric Vehicle based on Hilbert-Huang Transform and Deep Learning. *IEEE Sens. J.* **2021**, *21*, 15885–15894. [CrossRef]