frontiers | Frontiers in Energy Research

ORIGINAL RESEARCH
published: 30 May 2022
doi: 10.3389/fenrg.2022.903370

An Advanced Accurate Intrusion Detection System for Smart Grid Cybersecurity Based on Evolving Machine Learning

Tong Yu[1]*, *Kai Da*[1], *Zhiwen Wang*[2], *Ying Ling*[1], *Xin Li*[1], *Dongmei Bin*[1] *and Chunyan Yang*[1]

[1]Guangxi Power Grid Co.,Ltd., Electric Power Research Institute, NanNing, China, [2]Guangxi Power Grid Co.,Ltd., Hechi Power Supply Bureau, Hechi, China

Smart grids, the next generation of electricity systems, would be intelligent and self-aware of physical and cyber activity in the control area. As a cyber-embedded infrastructure, it must be capable of detecting cyberattacks and responding appropriately in a timely and effective manner. This article tries to introduce an advanced and unique intrusion detection model capable of classifying binary-class, trinary-class, and multiple-class CDs and electrical network incidents for smart grids. It makes use of the gray wolf algorithm (GWA) for evolving training of artificial neural networks (ANNs) as a successful machine learning model for intrusion detection. In this way, the intrusion detection model's weight vectors are initialized and adjusted using the GWA in order to reach the smallest mean square error possible. With the suggested evolving machine learning model, the issues of cyberattacks, failure forecast, and failure diagnosing would be addressed in the smart grid energy sector properly. Using a real dataset from the Mississippi State Laboratory in the United States, the proposed model is illustrated and the experimental results are explained. The proposed model is compared to some of the most widely used classifiers in the area. The results show that the suggested intrusion detection model outperforms other well-known models in this field.

Keywords: smart grid, cyberattack, intrusion detection system, advanced machine learning, smart city

Edited by:
Loiy Al-Ghussain,
University of Kentucky, United States

Reviewed by:
Mohamed A. Mohamed,
Minia University, Egypt
Mostafa Rezaei,
Griffith University, Australia

Correspondence:
Tong Yu
Yutongpgco@gmail.com

Specialty section:
This article was submitted to
Smart Grids,
a section of the journal
Frontiers in Energy Research

Received: *24 March 2022*
Accepted: *11 April 2022*
Published: *30 May 2022*

Citation:
Yu T, Da K, Wang Z, Ling Y, Li X, Bin D and Yang C (2022) An Advanced Accurate Intrusion Detection System for Smart Grid Cybersecurity Based on Evolving Machine Learning. Front. Energy Res. 10:903370. doi: 10.3389/fenrg.2022.903370

1 INTRODUCTION

A smart grid (SG) is a complicated system that combines processing technologies, modern communication, and recognition in the current electrical grid. In the SG, intelligent control applications are utilized, which necessitates the usage of error-free data of high quality, as well as rapid and dependable performance (Mohamed et al., 2021a). While SGs are yet under development, they present a risk of misoperation as vital infrastructure and a cyber–physical system, which is the result of intruders injecting malicious or false data (Alnowibet et al., 2021). In recent years, cybersecurity is an important concern faced by power system operators with the advent of SG implementation at large scales. Increasingly, high-speed networks and critical cyber–physical devices are being used now in power grids, making them vulnerable to attacks (Ma et al., 2021). The large-scale energy systems generate high-volume, high-speed data that are difficult for conventional attack detection systems to process. Cybersecurity systems still need to be efficient and resilient to deal with such new threats and detect malicious data on the network effectively (Chen et al., 2021). Cyberattacks (CAs) that target the electric grid belong typically to data intrusion attacks. Denial-of-service (DoS), load redistribution (LR), and false data injection (FDI) attacks are the three main forms of data intrusion attacks. Such attacks allow CAs for manipulating data with which the power grid manages and controls operations, disrupting the power system's safe operation, gaining financial benefit, and even destroying it physically (Meng et al., 2021). Modern intrusion detection systems (IDSs) rely heavily on the ability to detect and separate abnormal data from normal data. IDSs maintain data availability while maintaining the integrity and confidentiality of networks from unauthorized access (Nazir and Khan., 2021). Technically, IDS is based on the intrusion detection model. Users and utilities may suffer important losses as a result of unreliable or inadequate intrusion detection (Xue., 2021). Intrusion detection models address engineering issues, which are nonlinear, undefined, and accompanied by noise. It is essential to implement an intrusion detection model that is robust, reliable, and cost-efficient in order to resolve such problems. In this way, an overview of recent investigations on the improvement of intrusion-diagnosing models for electrical grids has been provided in the rest.

Several procedures and countermeasures for malicious data attacks on control centers are defined in Zhang et al. (2021). In order to obtain small yet extremely damaging attacks, they proposed the minimum residue energy heuristic (Zhang et al., 2021). Non-identifiable but detectable attacks are examined in Varmaziari and Dehghani (2017) and Cheng et al. (2019). The power flow layout using the supervisory control and data acquisition (SCADA) communication framework layout is integrated in Pan et al. (2018), and some algorithms in order to improve attack detection and system security factors are examined. Countermeasures vs. unobservable attacks are suggested in Dehghani et al. (2020). PMUs are assumed to be sufficiently secure and known to prevent attacks. Since CAs appear as a natural occurrence in the process, they can be complicated and hard to distinguish malicious from non-malicious data in communication systems. Chattopadhyay et al. (2017) distinguished CAs and disturbances since the disruption appear as the CA, and *vice versa*. This leads to incorrect classification, inappropriate actions, and other problems for the power systems (Liu et al., 2021). Power system disturbances can be categorized and grouped by a number of data-mining techniques. When DoS attacks are present, resilient cooperative event-triggered control and scheduling have been taken into account (Cong et al., 2021).

The precision and speed of the detection method can be considerably affected by the size of the feature set for intrusion detection applications. There is no guarantee that more features will result in improving efficiency since more features would need more memory, take longer time to process, and possibly have higher noise-to-signal ratios. Feature selection has been shown to be critical to faster intrusion detection in networks with a lot of information traffic (Panthi, 2021). An intrusion detection model in Liang et al. (2020), which uses feature selection as well, provided good detection accuracy based on varied features. As compared to other feature selection techniques, that model had great true-positive (TP) criteria and small false-positive (FP) criteria. An artificial neural network (ANN) has been widely applied in deep learning for its efficiency and simplicity. In addition, this is used for intrusion detection in electrical grids (Reddy et al., 2021). Currently, it is difficult to train an ANN since conventional training algorithms face problem to deal with slow convergence and local optima. In one recent trend, the ANNs are trained by applying heuristic optimization methods based on physical or biological principles for determining the most effective weights and biases (Cui et al., 2020).

The present study proposes the use of ANN training with the gray wolf algorithm (GWA) for creating an intrusion diagnosing layout. GWA–ANN is the name for this model. In general, an ANN structure and its arrangement of neurons are classified as follows: self-organizing maps, feed-backward, and forward. The multilayer perceptron (MLP), which can be the feed-forward neural network (FFNN), uses the hidden layer to transform the inputs into outputs. In this case, the network has been trained using the back-propagation algorithm as the supervised learning model. A GWA method, which is a powerful swarm-based intelligent search approach (Qiao et al., 2021), has been applied to identify attacks while overcoming the slow convergence issue and "local minima" traps related to ANNs. In general, GWA is well-known for its ability to determine the identified surrounding area for the universal optimal and has been considered to be very accurate and efficient for solving optimization problems. A GWA algorithm is applied as a trainer for FFNN for overcoming the challenges related to the learning method. This can be a flexible and gradient-free method that could prevent local optimum and has the ability to address many optimization issues and outperform the other current optimization methods to train MLPs. Based on the proven outcomes from the research, this study uses the GWA for training an ANN to detect cyber intrusions in SGs. In our model, the GWA would minimize the mean square error (MSE) and find the best weights for usage in the ANN. The effectiveness of the GWA–ANN model is evaluated using diverse statistical measures, like recall, F_1 score precision, and accuracy. A comparison is also made between the suggested GWA–ANN model and other intrusion detection models that utilize the databases of CAs in electrical grids held at Mississippi State University (MSU). In the large-scale power system intrusion datasets, it is shown that the GWA–ANN is able to produce better perceptions for most cases and diagnose among diverse categories of unknown entities.

Following are the sections of this study: The GWA–ANN-based intrusion detection model is presented in section 2. The power system structure and the datasets applied in this study are described in section 3. Experimental outcomes are presented in section 4 to show the algorithm's effectiveness. Section 5 discusses conclusions and future work.

2 INTRUSION DETECTION SYSTEM BASED ON THE GRAY WOLF ALGORITHM–ARTIFICIAL NEURAL NETWORK

2.1 Artificial Neural Network

ANNs are well-known methods for classification, which simulates the activity of biological neurons inside the brain

(Lan et al., 2021). ANNs are different from conventional classification techniques since they generate relationships dynamically through training inputs, instead of relying on predefined relationships (Zou et al., 2021). Training and testing phases are included in the ANN classification method (Kumar et al., 2018). The input weight summation has been determined as follows:

$$S_j = \sum_{i=1}^{m} I_i w_{jk} + \beta_j. \tag{1}$$

Here, the input variable is shown by I_i; the linkage weight among the input node i and the latent node j has been represented by w_{ij}; and the latent node's bias j is shown by β_j. Every latent layer node's output has been determined by using the sigmoid activation function described as follows:

$$f_j = \frac{1}{1 + e^{-S_j}}. \tag{2}$$

The last output for every node k in the network's output layer has been determined as follows:

$$\hat{O}_k = \sum_{j=1}^{h} f_j w_{jk} + \beta_k. \tag{3}$$

Here, the link weight among latent node j and the output node k has been shown *via* w_{jk} and the output node's bias k is represented by β_k.

2.2 Gray Wolf Optimizer

The hunting behavior and leadership style of gray wolves have been mimicked by GWO, a swarm-based optimization algorithm. The mathematical formulation of GWO is described in Mirjalili et al. (2020).

2.2.1 Gray Wolf Optimizer Inspiration

A gray wolf's behavior when hunting makes it one of the top predators on the food chain. **Figure 1** shows the four subgroups of gray wolves based on their dominance, namely, alpha (α), beta (β), delta (δ), and omega (ω). In the gray wolf pack hierarchy, the alpha wolf occupies the top position because of its experience in deciding on habitats and hunting prey for the pack. Beta wolves are found at the second level of wolf packs. Beta wolves help the alpha wolf manage the pack and perform other functions. In third in the pack hierarchy, delta wolves serve mainly as a protector of the pack vs. dangers and as a helper for weaker members. Omega wolves are the remaining wolves in the pack, at the bottom of the pack's hierarchy. Because of its role to manage and maintain the gray wolf pack, the social hierarchy of the pack is its basis. The social hierarchy also aids in the pack's ability to hunt prey systematically, in which, once the prey is found, the alpha will lead the pack to track and encircle it. Delta and beta are commanded for attacking the target by the alpha wolf. As soon as the prey escapes, omega wolves will assist delta and beta for catching target.

2.2.2 Gray Wolf Optimization Method

According to the hunting strategy in gray wolves, the GWO algorithm search encircles and attacks prey. The GWO algorithm, similar to other meta-heuristic layouts, begins *via* selecting a random set of solutions (wolves). Every solution contains one wolf position vector X in a search space. Vector X' s length shows an issue dimension. For PSPSH, the length of vector X showing the numbers of SAs m and their amounts show the beginning time for every SA, so $X^2 = (X_1^z, X_2^z, \ldots, X_m^z)$, in which X_i^z is a set of SA i at z^{th} iteration. In every iteration, the alpha wolf is the optimal solution, while the beta and delta are the second and the third, respectively. The rest of the solutions are assigned as omega wolves. By encircling alpha, beta, and delta, the omega wolves will assist them in hunting target with the following formulas:

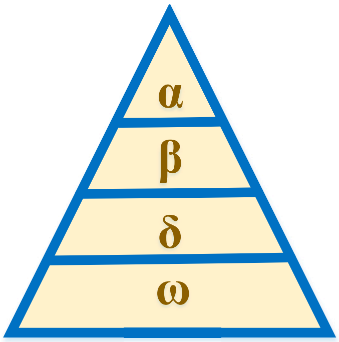

FIGURE 1 | Levels of gray wolves packs.

$$d = \left|c \cdot X_{p,z} - X_z\right|, \tag{4}$$

$$X_{z+1} = X_{p,z} - \mu \cdot d, \tag{5}$$

$$\mu = 2 \cdot b \cdot r_1 - b, \tag{6}$$

$$c = 2 \cdot r_2. \tag{7}$$

Here, prey position at z^{th} iteration is shown by $X_{p,z}$, wolf position at z^{th} iteration is represented by X_z, wolf position at $(z+1)^{th}$ iteration is shown by X_{z+1}, μ and c represent two coefficient vectors, b linearly reduces from 2 to 0 across the course of iterations, and r_1 and r_2 represent two random vectors between (0, 1). The GWO equation formulations have been revised to be greatly reasonable, realistic, and not a conflict with the PSPSH formula represented in Gosain and Sachdeva (2020).

The whole of the omega wolves solutions must be updated in every iteration based on the three best solutions (viz., delta, alpha, and beta delta solutions) applying these formulations as follows:

$$d_\alpha = |c_\alpha \cdot X_\alpha - X|, \tag{8}$$

$$d_\beta = \left|c_\beta \cdot X_\beta - X\right|, \tag{9}$$

$$d_\delta = |c_\delta \cdot X_\delta - X|, \tag{10}$$

$$X_1' = X_\alpha - \mu_\alpha \cdot d_\alpha, \tag{11}$$

$$X_2' = X_\beta - \mu_\beta \cdot d_\beta. \tag{12}$$

$$X_3' = X_\delta - \mu_\delta \cdot d_\delta \tag{13}$$

$$X_{z+1} = \frac{X_1' + X_2' + X_3'}{3} \tag{14}$$

In GWO, exploration and exploitation can be effectively balanced, while local optima stagnation can be avoided

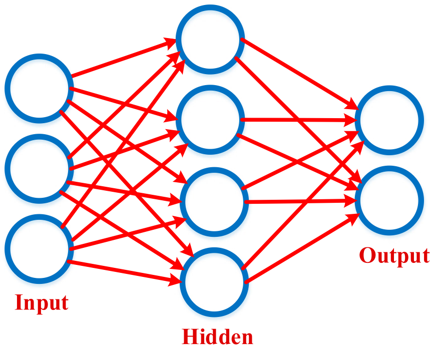

FIGURE 2 | Generic structure of the MLP.

utilizing μ. GWO explores and exploits a quest space during $|\mu| > 1$ and $|\mu| < 1$, respectively. Local search avoidance relies primarily on the value of c, altering randomly throughout iterations.

2.2.3 Gray Wolf Optimizer on the Basis of the Local Search Algorithm Process

Recent optimization investigations have presented hybrid optimization layouts for improving the efficiency of main layouts and enhancing their outcomes (Al-Ghussain et al., 2021a). This part proposes GWO–MCA, a hybrid algorithm that combines GWO and local search algorithms (MCA). GWO–MCA proposes for meeting the shortcomings for GWO causing its optimal solution to be poor, like low accuracy and slow convergence speed (Zhou and Lei, 2021). MCA has been applied for its easy and quick search process without requiring the use of equations. MCA is also one of the most widely used layouts offered for dealing with CSPs like PSPSH.

The A_1 parameter has been used for equipping MCA at the exploitation section of GWO. In GWO, the A_l variable behaves like the μ parameter; so if $A_l| > 1$, then GWO explores the search, and when $A_l| < 1$, GWO exploits the search. A_l is determined in the following way:

$$A_l = 2 \times a_l \times r_1 - a_l. \tag{15}$$

Here, r_1 is chosen randomly between (0, 1], and a_1 linearly reduces from 2 to 0 during iterations according to Eq. 36.

$$a_l = 2 - \left(2 \times \frac{itr}{I}\right). \tag{16}$$

Here, this indicates the present iteration and I represents the iteration's maximum number. The first step in the GWO–MCA process is to initialize the CSP and GWO variables. Then, fitness values are calculated for every solution. Furthermore, X_α, X_β, and X_δ are the three best solutions, respectively. The suggested parameters, namely, r_1, a_1, and A_l are calculated in the next step. When $|A_l| < 1$, so MCA would select one of the optimal solutions (i.e., X_α, X_β, and X_δ) randomly and try to minimize the

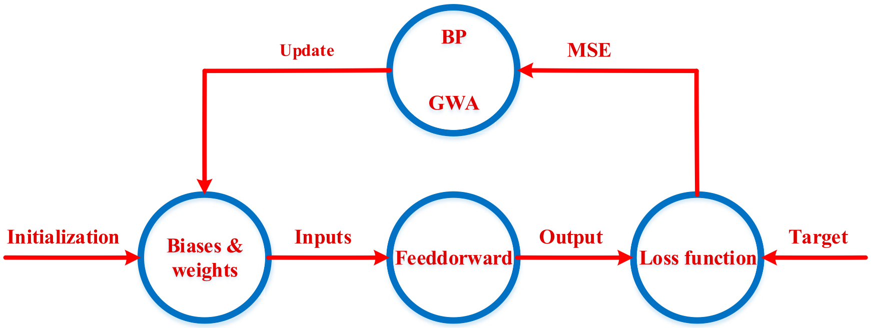

FIGURE 3 | Training method of the MLP.

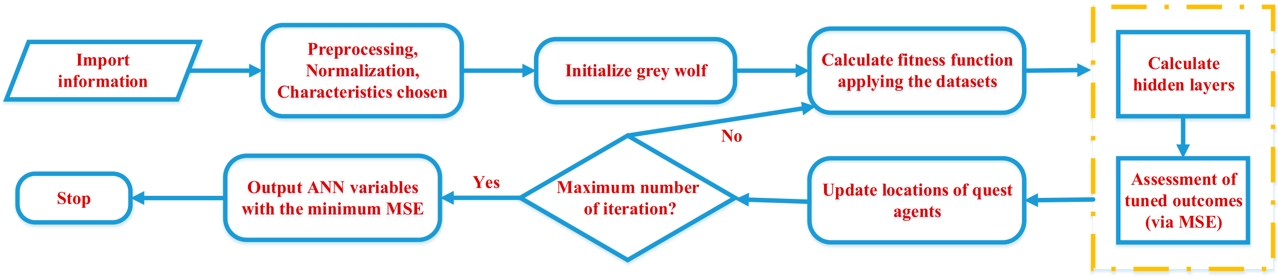
Import information
Preprocessing, Normalization, Characteristics chosen
Initialize grey wolf
Calculate fitness function applying the datasets
Calculate hidden layers
Assessment of tuned outcomes (via MSE)
Update locations of quest agents
Maximum number of iteration?
No
Yes
Output ANN variables with the minimum MSE
Stop

FIGURE 4 | GWA–ANN training scheme.

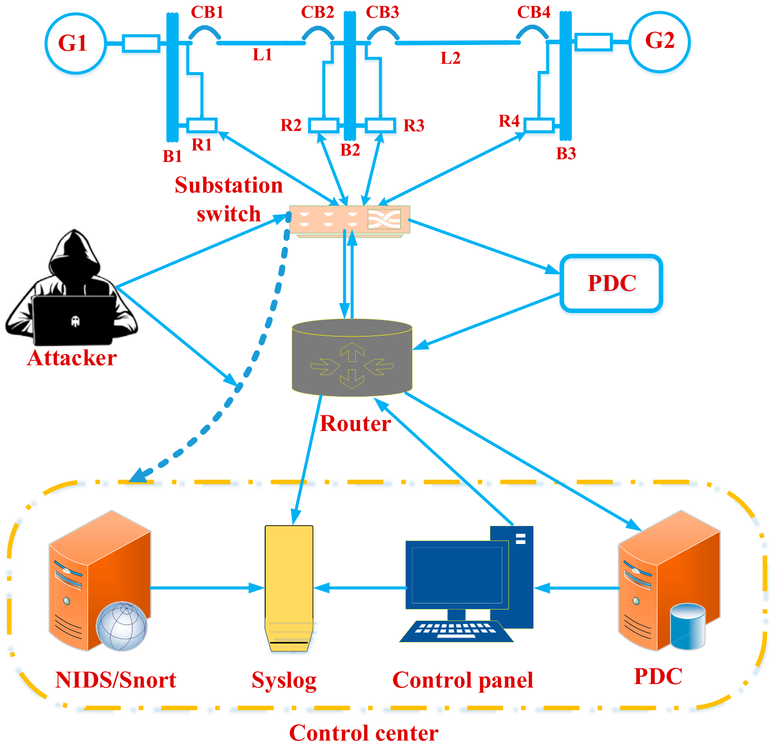

FIGURE 5 | Power grid structure.

TABLE 1 | Problem kinds and case studies.

Kind of problem		Trinary (15 datasets)	Binary (15 datasets)	Multiple (15 datasets)
Number of case studies	CA	28	28	Each case study alone is an apart class
	Normal	-	9	
	Natural	8	-	
	No event	1	-	
	Total	37	37	37

TABLE 2 | Natural event case studies in MSU/ORNL information.

Case study tag				
Usual occurrences (SLG: single line to ground fault)	Fault occurs in L1	1	From	10%
			To	19%
		2	From	20%
			To	79%
		3	From	80%
			To	90%
	Fault occurs in L2	4	From	10%
			To	19%
		5	From	20%
			To	79%
		6	From	80%
			To	90%
Usual occurrences (line maintenance)		13: L1 14: L2		

TABLE 3 | CA occurrence case studies for MSU/ORNL information.

	Case study tag and CA kind			
Data injection: SLG fault replay attack	Fault occurs in L1 with tripping command	7	From	10%
			To	19%
		8	From	20%
			To	79%
		9	From	80%
			To	90%
	Fault occurs in L2 with tripping command	10	From	10%
			To	19%
		11	From	20%
			To	79%
		12	From	80%
			To	90%
Tripping command injection in remote mode: command injection vs. relays	Injected command	15	R1	
		16	R2	
		17	R3	
		18	R4	
		19	R1 and R2	
		20	R3 and R4	
	Fault occurs in L1 with R1 deactivated and fault	21	From	10%
			To	19%
		22	From	20%
			To	90%
	Fault occurs in L1 with R2 deactivated and fault	23	From	10%
			To	49%
		24	From	50%
			To	70%
		25	From	80%
			To	90%
	Fault occurs in L2 with R3 deactivated and fault	26	From	10%
			To	19%
		27	From	20%
			To	49%
		28	From	50%
			To	90%
	Fault occurs in L2 with R4 deactivated and fault	29	From	10%
			To	79%
		30	From	80%
			To	90%
Relay adjustment alteration: deactivating relay action-2 relays deactivated and fault	Fault occurs in L1 with R1 and R2 deactivated and fault	35	From	10%
			To	49%
		36	From	50%
			To	90%
	Fault occurs in L1 with R3 and R4 deactivated and fault	37	From	10%
			To	49%
		38	From	50%
			To	90%
Relay adjustment alteration: deactivating relay action-2 relays deactivated and maintain the line	Maintain L1	39	R1 and R2 deactivated	
		40	R1 and R2 deactivated	

TABLE 4 | No occurrence case studies for MSU/ORNL information.

Case studies tag (sans occurrences)	
41	Usual action and load alternations

numbers of conflicts among the chosen solution parameters. The MCA will choose and improve one of the three optimal solutions because of their impacts on the other solutions. Furthermore, the fitness amount of the new solutions is computed and assigned again. Then, GWO updates X_α, X_β, X_δ, and the rest of the

TABLE 5 | Features in the datasets.

Characteristics and signal references	No.	1	2	3	4	5	6	7	8	9	10
Relay	1	R1-PA1:VH	R1-PM1:V	R1-PA2:VH	R1-PM2:V	R1-PA3:VH	R1-PA3:V	R1-PA4:IH	R1-PM4: I	R1-PA5:IH	R1-PA5: I
	2	R2-PA1:VH	R2-PM1:V	R2-PA2:VH	R2-PM2:V	R2-PA3:VH	R2-PA3:VH	R2-PA4:IH	R2-PM4: I	R2-PA5:IH	R2-PA5: I
	3	R3-PA1:VH	R3-PM1:V	R3-PA2:VH	R3-PM2:V	R3-PA3:VH	R3-PA3:VH	R3-PA4:IH	R2-PM4: I	R3-PA5:IH	R3-PA5: I
	4	R4-PA1:VH	R4-PM1:V	R4-PA2:VH	R4-PM2:V	R4-PA3:VH	R4-PA3:VH	R4-PA4:IH	R4-PM4: I	R4-PA5:IH	R4-PA5: I
Integrated relay and PMU		Snort_log1	Snort_log2	Snort_log3	Snort_log4	Relay1_log	Relay2_log	Relay3_log	Relay4_log	Control_panel_log1	Control_panel_log2
No		11	12	13	14	15	16	17	18	19	20
Relay	1	R1-PA6:IH	R1-PM6: I	R1-PA7:VH	R1-PA7:V	R1-PA8:VH	R1-PM8:V	R1-PA9:VH	R1-PM9:V	R1-PA10:IH	R1-PM10: I
	2	R2-PA6:IH	R2-PM6: I	R2-PA7:VH	R2-PA7:V	R2-PA8:VH	R2-PM8:V	R2-PA9:VH	R2-PM9:V	R2-PA10:IH	R2-PM10: I
	3	R3-PA6:IH	R3-PM6: I	R3-PA7:VH	R3-PA7:V	R3-PA8:VH	R3-PM8:V	R3-PA9:VH	R3-PM9:V	R3-PA10:IH	R3-PM10: I
	4	R4-PA6:IH	R4-PM6: I	R4-PA7:VH	R4-PA7:V	R4-PA8:VH	R4-PM8:V	R4-PA9:VH	R4-PM9:V	R4-PA10:IH	R4-PM10: I
Integrated relay and PMU		Control_panel_log3	Control_panel_log4								
	No	21	22	23	24	25	26	27	28	29	
Relay	1	R1-PA11:IH	R1-PM11: I	R1-PA12:IH	R1-PM12: I	R1: F	R1: DF	R1-PA:Z	R1-PA:ZH	R1: S	
	2	R2-PA11:IH	R2-PM11: I	R2-PA12:IH	R2-PM12: I	R2: F	R2: DF	R2-PA:Z	R2-PA:ZH	R2: S	
	3	R3-PA11:IH	R3-PM11: I	R3-PA12:IH	R3-PM12: I	R3: F	R3: DF	R3-PA:Z	R3-PA:ZH	R3: S	
	4	R4-PA11:IH	R4-PM11: I	R4-PA12:IH	R4-PM12: I	R4: F	R4: DF	R4-PA:Z	R4-PA:ZH	R4: S	

solutions for finding better solutions. Fitness values are calculated and solutions are improved until the stop criterion is reached.

2.3 The Artificial Neural Network Architecture

This study implements two MLP networks. There are three layers in an MLP: the output, input, and latent layers. **Figure 2** shows the typical architecture for MLP methods. The numbers of input node is m, the latent node's number is h, and the output node's number is k. Various numbers have been given for binary problems, trinary-class problems, and multiple-class problems. **Figure 3** shows the training method of the MLP. Inputs are taken and outputs are generated according to the current weights and biases. A loss function is used to compare the output from the feed-forward route with the goal result. Next, the Levenberg–Marquardt back-propagation method (Kaveh et al., 2020) has been applied for updating the bias and weight for the subsequent iteration in the conventional MLP method. A GWA is used for updating the weights for the subsequent iteration for the suggested MLP method.

2.4 The Proposed Gray Wolf Algorithm–Artificial Neural Network

An ANN is trained to organize CAs from usual occurrences in the energy systems using the GWA here. The GWA–ANN first initializes every search agent for optimizing a candidate neural network (NN). There are vectors of weights and biases in an MLP network indicating the relations among the input and hidden layers, and also between the hidden and the output layers (Qiao et al., 2021). **Equation 17** illustrates the whole number of bias and weight parameters in MLP networks to be optimized using the GWA. Here, the whole number of input nodes is shown by q and the whole number of neurons in the hidden layer is represented by p.

$$V = pq + 2p + 1. \tag{17}$$

By using the MLP method's MSE as a fitness function, the search agents (whales) can determine a difference among the predicted and actual classes. **Equation 18** illustrates MSE, in which O_i represents the real output for input instance i, $\hat{O}i$ shows the estimated output for input instance i, and n represents the numbers of instances.

$$MSE = \frac{\sum_{i=1}^{n}\left(O_i - \hat{O}i\right)^2}{n}. \tag{18}$$

MATLAB R2018a was used to implement the GWA trainer for the experiments. Normalization would be crucial for an MLP if dataset attributes have multiple ranges (Qiao et al., 2021). The min–max normalization is shown in **Eq. 19**.

$$u' = \frac{u - u_{min}}{u_{max} - u_{min}}. \tag{19}$$

Here, u' shows the normalized value of u between $[u_{min}, u_{max}]$.

A flowchart of the GWA-ANN training method is shown in **Figure 4**. Once importing the data, data cleansing is used for

TABLE 6 | Symbols applied in the names of characteristics.

Symbols and descriptions			
PA1-PA3	In (A, B, C) sequence	Phase angle	Voltage signal
PM1-PM3		Magnitude	
PA4-PA6		Phase angle	Current signal
PM1-PM9		Magnitude	
PA7-PA9	In (+, -, 0) sequence	Phase angle	Voltage signal
PM7-PM9		Magnitude	
PA10-PA12		Phase angle	Current signal
PM10-PM12		Magnitude	
F	Relay	Frequency	Frequency
DF		Delta frequency	
Z		Impedance	Impedance
ZH		High impedance	
S		Status flag	
Snort log	Binary	0 or 1	
Relay log			
Control panel log			

TABLE 7 | Matrix of confusion.

Genuine class	Predicated class	
Normal	Normal	CA
	TN	FP
CA	FN	TP

preprocessing it. Prior to using the GWA–ANN to classify the data, the data have been normalized, and feature selection has been performed for determining the number of input features. Next, Gaussian random distribution is used for dividing the datasets into subgroups, 20 percentage for testing, 80 percentage for confirmation (16 percentage), and 64 percentage training that can be according to the most usual ANN research action. GWA–ANN classification has been combined with feature selection (dimension reduction). With the aim of determining the accuracy of the model, the testing data have been employed to feed the classification of an ANN layout with optimum bias and weight achieved from the training step.

GWA–ANN can be effective at avoiding local optima. For the suggested model, this would make it easier to find the best MLP's bias and weight related to great accuracy and great performance (Qiao et al., 2021).

3 POWER GRID STRUCTURE AND EXPLANATIONS OF THE DATASET

3.1 Description of the Power Grid

This study's power system structure is illustrated in **Figure 5**. This system includes two generators, G_1 and G_2, three bus bars B_1 *via* B_3, two transmission lines, L_1 and L_2, and four circuit breakers, CB_1 *via* CB_4 that have been controlled *via* four relays, R_1 *via* R_4. A substation switch and a router connect those relays to the SCADAs. Distance protection schemes are used by the relays for tripping the breakers on diagnosed error and fault, regardless of whether the fault is actual or not since they do not have any internal validation to determine whether the fault is real or not. These intelligent relays can also be controlled manually by operators so that breakers can be manually tripped by relays (Wang et al., 2021; Zeng et al., 2021). These scenarios suppose that attackers have already accessed a substation's grid and have been able to access to the switch of substation's commands, as illustrated in the figure. Electricity is distributed to various equipment by means of the power distribution center (PDC). There are many smart electronic tools, like the control panel, Syslog, and Snort at the bottom of the figure that can monitor the whole grid.

3.2 Datasets and Attack Case Studies

The GWA–ANN is evaluated using the CAs in SG datasets in the ORNL and MSU (Morrison et al., 2021). The types of issues and the segments of case studies are shown in **Table 1**. A total of 45 diverse datasets are available. In total, there are 15 binary, multiple, and trinary-class datasets. There are no two datasets that can be identical. There are over 5,000 samples in every dataset. The samples correspond to one of the 37 occurrence scenarios. As an example, one trinary-class

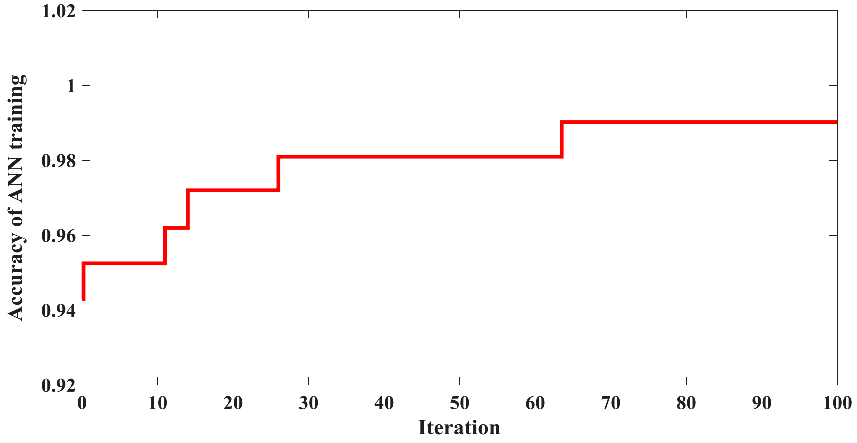

FIGURE 6 | Convergence curve of the ANN accuracy during the GWA-tuning process.

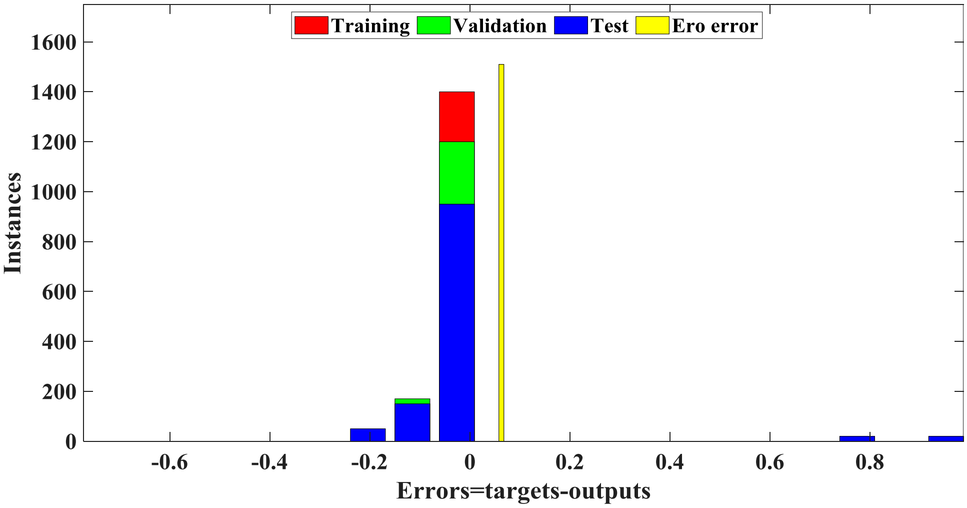

FIGURE 7 | Training error histogram, confirmation, and testing with the GWA–ANN.

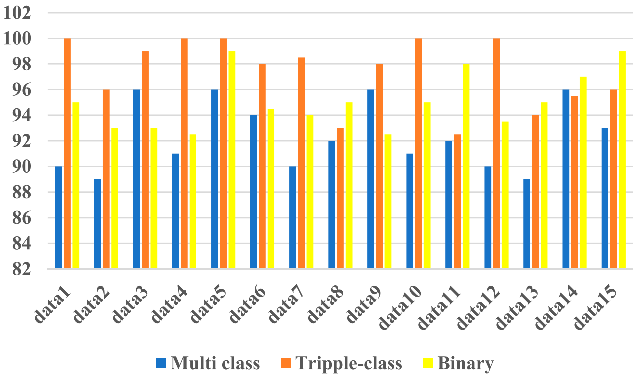

FIGURE 8 | Accuracy across 15 multiple-class, 15 trinary-class, and 15 binary datasets.

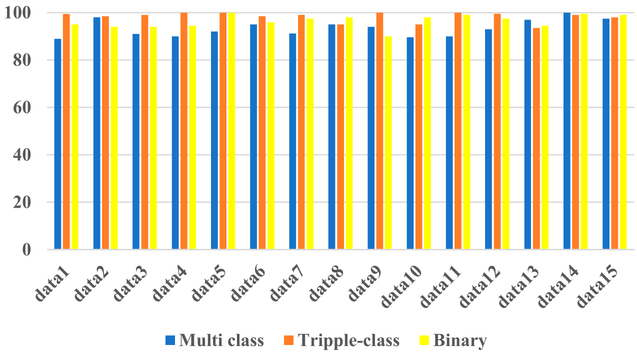

FIGURE 10 | Recall across 15 multiple-class, 15 trinary-class, and 15 binary datasets.

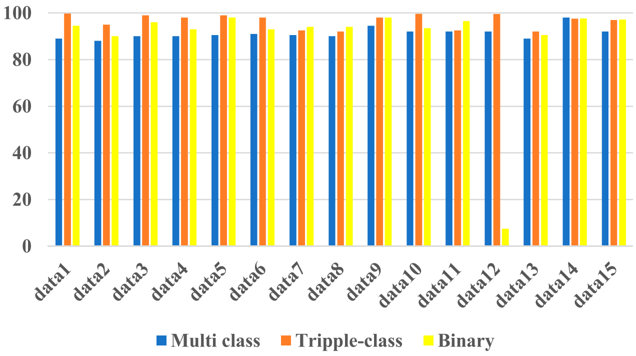

FIGURE 9 | Precision across 15 multiple-class, 15 trinary-class, and 15 binary datasets.

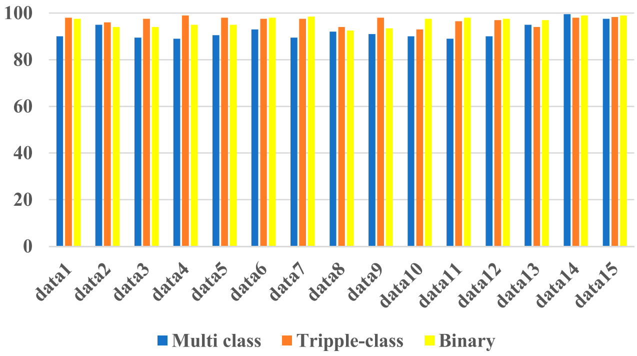

FIGURE 11 | F_1 score across 15 binary, 15 trinary-class, and 15 multiple-class datasets.

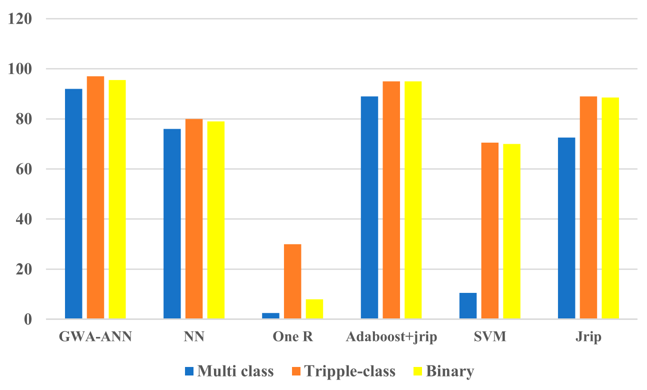

FIGURE 12 | Mean precision amounts of diverse classifiers of the 45 datasets.

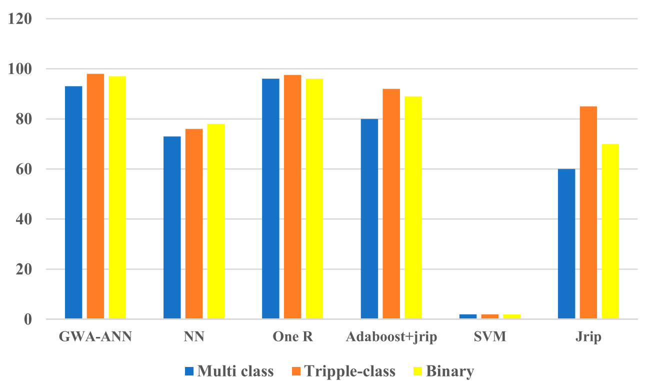

FIGURE 14 | Mean recall amounts of diverse classifiers of the 45 datasets.

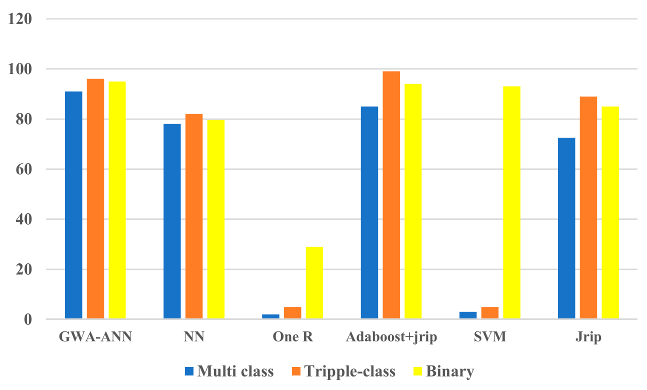

FIGURE 13 | Average precision amounts of diverse classifiers of the 45 datasets.

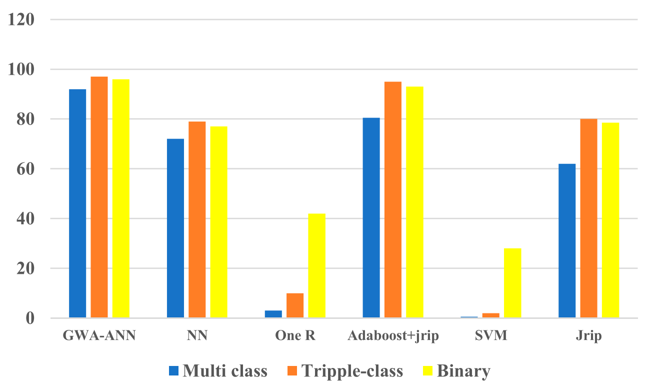

FIGURE 15 | Mean F_1 score amounts of diverse classifiers of the 45 datasets.

datasets contains 5,236 observations, consisting of 292 sans occurrences, 3,713 attack, and 1,212 natural observations (Mohamed et al., 2021b). This scenario employed in Kumar et al. (2018) is similar to what is employed here; 1,212 natural similar to Kumar et al. (2018), attack scenarios like short circuits, input of remote command, and maintenance of line, relay adjusting changes, and FDIs are considered. Among the 37 event scenarios in binary datasets, 28 are CAs case studies and nine are usual operation case studies. There are 28 and seven CAs and usual case studies, and one case study sans occurrence for trinary-class datasets. All the 37 case studies in a multiple-class dataset is a class on its own.

A comprehensive list of 37 case studies (one sans occurrence, 28 CAs, and eight normal) is presented in **Table 2**, **Table 3**, **Table 4** in the MSU/ORNL dataset.

There are 129 columns in each dataset, including 128 properties columns and one class tag column. The short names for the properties have been shown in **Table 5**. All 128 features are generated by four PMUs. PMUs or synchrophasors measure electrical waves from an electrical network utilizing a common time resource for synchronization. The measurements of four PMUs are shown in the first four columns, each measuring 29 relay features. Twelve extra properties from the control panel, Snort, and relay logs are included in the last column.

Table 6 lists the symbols employed in the feature names. As an instance, (R2-PM2:V) (in column Relay 2 and row #4) denotes Relay 2's Phase B voltage magnitude as determined using PMU R2, while (R3-PA:ZH) (in column Relay 3 and row #28) denotes Relay 3's impedance angle as determined using PMU R3.

Each of the 45 datasets contains around 650,000 data points (5,000 rows by 129 columns), and the 45 datasets contain an overall of 29 × 10^6 data spots.

4 EXPLANATIONS AND OUTCOMES OF EXPERIMENTS

Our research sets the maximum number of iterations to 100 and the numbers of quest units to 50. The parameters listed here are typical for the GWA, and they work perfectly in most cases. Preprocessing and the feature selection lead to the selection of 76, 92, and 92 properties from the 128 properties for binary, trinary, and multiplex-class issues. In other words, these three kinds of problems have MLP network architectures of 76-20-1, 92-20-1, and 92-20-1, respectively. Part 4.1 describes the model training and validation method utilizing Dataset 15 binary classification problem. As previously described in Part 4.1, Part 4.2 displays the outcomes for all 45 datasets and issue kinds.

4.1 Pattern Training and Verification

The efficiency of the suggested GWA–ANN model will be measured by recall, F_1 score precision, and accuracy. The binary classification confusion matrix of this suggested pattern has been presented in **Table 7**. Outcomes of actual (rows) and predicted (columns) classes are included in the matrix. TP indicates a real CA occurrence that is indicated as an CA; TN (true negative) indicates the usual occurrence that is indicated as usual; FP indicates a usual occurrence that is indicated as the CA, and FN (false negative) indicates a real CA that is indicated as the usual occurrence.

Eqs. 20–23 summarize the recall, F_1 score precision, and accuracy from **Table.7**. The accuracy, represented in **Eq. 20**, generally calculates when the classifier can be right (Al-Ghussain et al., 2021b; Al-Ghussain et al., 2022). Precision, described in **Eq. 21**, calculates that whenever the classifier predicts the CA, when it can be right. Recall, described in **Eq. 22**, calculates that when a CA really happens, how often it can be indicated accurately. F_1 score, described in **Eq. 23**, combines precision and recall.

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN}, \tag{20}$$

$$Precision = \frac{TP}{TP + FP}, \tag{21}$$

$$Recall = \frac{TP}{TP + FN}, \tag{22}$$

$$F_1 \quad Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}. \tag{23}$$

The accuracy curve of convergence throughout the adjusting method for the ANN *via* GWA employing Dataset 15 binary classification issue is shown in **Figure 6**. Based on the figure, increasing the number of iterations slowly raises the accuracy of the model. Beginning from 64 number of iteration, the accuracy has jumped up and rapidly stabilized at approximately 99%.

Figure 7 illustrates the histogram's error with 20 bins representing training, confirmation, and error of trials for Dataset 15 binary classification. This figure illustrates how the trained pattern can fit the dataset. The majority of errors have been concentrated in the tiny area near zero, with 0.02592 being the most prominent error.

4.2 Trail Outcomes for the Mississippi State University/ORNL Datum

These classification outcomes in this subsection are based on all 45 MSU/ORNL datasets. **Figures 8–11** show the classification outcomes from this suggested pattern for trinary-class, multiple-class, and binary issues regarding recall, F_1 score precision, and accuracy.

Figures 12–15 have compared the mean amounts for the recall, F_1 score, precision, and accuracy for the 45 datasets utilizing typically employed classifiers for the research, like the OneR, JRip, AdaBoost + JRip, SVM (Panthi, 2021), and NN with no GWA. According to the figure, GWA–ANN performs better than other algorithms for most applications.

5 CONCLUSION

Detecting suspicious or anomalous events with a very high speed and accuracy is essential for a reliable SG operation and management. As power systems are highly dependent on cyber infrastructure, cybersecurity is a significant problem. This infrastructure is necessary to distribute and process huge amounts of real-time data produced throughout system operation. This study overcomes several weaknesses associated with conventional algorithms on the basis of ANNs, like the trapping of local minima. This study uses the GWA-ANN model for classifying the CAs and detecting failures in the electrical grid by applying the MSU/ORNL datasets at diverse difficulty levels (binary, trinary-class, and multiple-class). The GWA is used to train the ANN for achieving the best bias and weight with minimum MSE in the classification task. The efficiency of the suggested GWA-ANN is evaluated applying different standard metrics, like F_1 score recall, precision, and accuracy. Experiments demonstrated that the suggested method is capable of detecting the CA data in electrical systems efficiently. Compared to other classification methods, like OneR, JRip, AdaBoost + JRip, SVM, and NN (with not GWA), the GWA-ANN is superior due to its powerful capability to explore and prevent local optimization. A periodic update of the suggested model is possible. In the event that an unidentified event has been later confirmed as a CA by humans, it must achieve the confirmed tag and has been added to the library of training and be employed to detect potential CAs in the future.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

REFERENCES

Al-Ghussain, L., Abubaker, A. M., and Ahmad, A. D. (2021). Superposition of Renewable-Energy Supply from Multiple Sites Maximizes Demand-Matching: Towards 100% Renewable Grids in 2050. *Appl. Energ.* 284, 116402. doi:10.1016/j.apenergy.2020.116402

Al-Ghussain, L., Ahmad, A. D., Abubaker, A. M., Abujubbeh, M., Almalaq, A., and Mohamed, M. A. (2021). A Demand-Supply Matching-Based Approach for Mapping Renewable Resources towards 100% Renewable Grids in 2050. *IEEE Access* 9, 58634–58651. doi:10.1109/ACCESS.2021.3072969

Al-Ghussain, L., Subaih, M. A., and Annuk, A. (2022). Evaluation of the Accuracy of Different PV Estimation Models and the Effect of Dust Cleaning: Case Study a 103 MW PV Plant in Jordan. *Sustainability* 14 (2), 982. doi:10.3390/su14020982

Alnowibet, K., Annuk, A., Dampage, U., and Mohamed, M. A. (2021). Effective Energy Management *via* False Data Detection Scheme for the Interconnected Smart Energy Hub-Microgrid System under Stochastic Framework. *Sustainability* 13 (21), 11836. doi:10.3390/su132111836

Chattopadhyay, A., Ukil, A., Jap, D., and Bhasin, S. (2017). Toward Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation. *IEEE Trans. Ind. Inform.* 14 (6), 2442–2451. doi:10.3390/su14020982

Chen, J., Mohamed, M. A., Dampage, U., Rezaei, M., Salmen, S. H., Obaid, S. A., et al. (2021). A Multi-Layer Security Scheme for Mitigating Smart Grid Vulnerability against Faults and Cyber-Attacks. *Appl. Sci.* 11 (21), 9972. doi:10.3390/app11219972

Cheng, G., Song, S., Lin, Y., Huang, Q., Lin, X., and Wang, F. (2019). Enhanced State Estimation and Bad Data Identification in Active Power Distribution Networks Using Photovoltaic Power Forecasting. *Electric Power Syst. Res.* 177, 105974. doi:10.1016/j.epsr.2019.105974

Cong, M., Mu, X., and Hu, Z. (2021). Sampled-data-based Event-Triggered Secure Bipartite Tracking Consensus of Linear Multi-Agent Systems under DoS Attacks. *J. Franklin Inst.* 358 (13), 6798–6817. doi:10.1016/j.jfranklin.2021.07.012

Cui, H., Dong, X., Deng, H., Dehghani, M., Alsubhi, K., and Aljahdali, H. M. (2020). Cyber Attack Detection Process in Sensor of DC Micro-grids under Electric Vehicle Based on Hilbert-Huang Transform and Deep Learning. *IEEE Sensors J.* 21, 15885–15894. doi:10.1109/jsen.2020.3027778

Dehghani, M., Kavousi-Fard, A., Dabbaghjamanesh, M., and Avatefipour, O. (2020). Deep Learning Based Method for False Data Injection Attack Detection in AC Smart Islands. *IET Generation, Transm. &amp; Distribution* 14 (24), 5756–5765. doi:10.1049/iet-gtd.2020.0391

Gosain, A., and Sachdeva, K. (2020). "Random Walk Grey Wolf Optimizer Algorithm for Materialized View Selection (RWGWOMVS)," in *InNovel Approaches Inf. Syst. Des.*. PA, United States: IGI Global, 101–122. doi:10.4018/978-1-7998-2975-1.ch005

Kaveh, K., Kaveh, H., Bui, M. D., and Rutschmann, P. (2020). Long Short-Term Memory for Predicting Daily Suspended Sediment Concentration. *Eng. Comput.* 8, 1–5. doi:10.1007/s00366-019-00921-y

Kumar, M. N., Koushik, K. V., and Sundar, K. J. (2018). Data Mining and Machine Learning Techniques for Cyber Security Intrusion Detection. *Int. J. Scientific Res. Comput. Sci. Eng. Inf. Technol.* 3 (3), 162–167. doi:10.1109/TII.2017.2770096

Lan, T., Jermsittiparsert, K., T. Alrashood, S., Rezaei, M., Al-Ghussain, L., and A. Mohamed, M. (2021). An Advanced Machine Learning Based Energy Management of Renewable Microgrids Considering Hybrid Electric Vehicles' Charging Demand. *Energies* 14 (3), 569. doi:10.3390/en14030569

Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., et al. (2020). Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems. *Electronics* 9 (7), 1120. doi:10.3390/electronics9071120

Liu, Y., Jin, T., Mohamed, M. A., and Wang, Q. (2021). A Novel Three-step Classification Approach Based on Time-dependent Spectral Features for Complex Power Quality Disturbances. *IEEE Trans. Instrum. Meas.* 70, 1–14. doi:10.1109/tim.2021.3050187

Ma, F., Wang, B., Zhou, J., Jia, R., Luo, P., Wang, H., et al. (2021). An Effective Risk Identification Method for Power Fence Operation Based on Neighborhood Correlation Network and Vector Calculation. *Energ. Rep.* 7, 6995–7003. doi:10.1016/j.egyr.2021.10.061

Meng, F., Zou, Q., Zhang, Z., Wang, B., Ma, H., Abdullah, H. M., Almalaq, A., and Mohamed, M. A. (2021). An Intelligent Hybrid Wavelet-Adversarial Deep Model for Accurate Prediction of Solar Power Generation. *Energ. Rep.* 7, 2155–2164. doi:10.1016/j.egyr.2021.04.019

Mirjalili, S., Aljarah, I., Mafarja, M., Heidari, A. A., and Faris, H. (2020). Grey Wolf Optimizer: Theory, Literature Review, and Application in Computational Fluid Dynamics Problems. *Nature-inspired optimizers.*, 87–105. doi:10.1007/978-3-030-12127-3_6

Mohamed, M. A., Almalaq, A., Abdullah, H. M., Alnowibet, K. A., Alrasheedi, A. F., and Zaindin, M. S. A. (2021). A Distributed Stochastic Energy Management Framework Based-Fuzzy-PDMM for Smart Grids Considering Wind Park and Energy Storage Systems. *IEEE Access* 9, 46674–46685. doi:10.1109/access.2021.3067501

Mohamed, M. A., Mirjalili, S., Dampage, U., Salmen, S. H., Obaid, S. A., and Annuk, A. (2021). A Cost-Efficient-Based Cooperative Allocation of Mining Devices and Renewable Resources Enhancing Blockchain Architecture. *Sustainability* 13 (18), 10382. doi:10.3390/su131810382

Morrison, R., Liu, X., and Lin, Z. (2021). Anomaly Detection in Wind Turbine SCADA Data for Power Curve Cleaning. *Renew. Energ.* 184, 473–486. doi:10.1016/j.renene.2021.11.118

Nazir, A., and Khan, R. A. (2021). A Novel Combinatorial Optimization Based Feature Selection Method for Network Intrusion Detection. *Comput. Security* 102, 102164. doi:10.1016/j.cose.2020.102164

Pan, K., Teixeira, A., Cvetkovic, M., and Palensky, P. (2018). Cyber Risk Analysis of Combined Data Attacks against Power System State Estimation. *IEEE Trans. Smart Grid* 10 (3), 3044–3056. doi:10.1109/TSG.2018.2817387

Panthi, M. (2021). Identification of Disturbances in Power System and DDoS Attacks Using Machine Learning. *InIOP Conf. Ser. Mater. Sci. Eng.* 1022 (No. 1), 012096. IOP Publishing. doi:10.1088/1757-899x/1022/1/012096

Qiao, W., Khishe, M., and Ravakhah, S. (2021). Underwater Targets Classification Using Local Wavelet Acoustic Pattern and Multi-Layer Perceptron Neural Network Optimized by Modified Whale Optimization Algorithm. *Ocean Eng.* 219, 108415. doi:10.1016/j.oceaneng.2020.108415

Reddy, D. K., Behera, H. S., Nayak, J., Vijayakumar, P., Naik, B., and Singh, P. K. (2021). Deep Neural Network Based Anomaly Detection in Internet of Things Network Traffic Tracking for the Applications of Future Smart Cities. *Trans. Emerging Telecommunications Tech.* 32 (7), e4121. doi:10.1002/ett.4121

Varmaziari, H., and Dehghani, M. (2017). "Cyber-attack Detection System of Large-Scale Power Systems Using Decentralized Unknown Input Observer," in 2017 Iranian Conference on Electrical Engineering (ICEE) 2017 May 2 (IEEE), 621–626. doi:10.1109/iraniancee.2017.7985114

Wang, Q., Jin, T., Mohamed, M. A., and Deb, D. (2021). A Novel Linear Optimization Method for Section Location of Single-phase Ground Faults in Neutral Noneffectively Grounded Systems. *IEEE Trans. Instrum. Meas.* 70, 1–10. doi:10.1109/tim.2021.3066468

Xue, P. (2021). Impact of Large-Scale Mobile Electric Vehicle Charging in Smart Grids: A Reliability Perspective. *Front. Energ. Res.*, 101–122. doi:10.3389/fenrg.2021.688034

Zeng, L., Xia, T., Elsayed, S. K., Ahmed, M., Rezaei, M., Jermsittiparsert, K., Dampage, U., and Mohamed, M. A. (2021). A Novel Machine Learning-Based Framework for Optimal and Secure Operation of Static VAR Compensators in EAFs. *Sustainability* 13 (11), 5777. doi:10.3390/su13115777

Zhang, Z., Deng, R., Yau, D. K. Y., and Cheng, P. (2021). Zero-Parameter-Information Data Integrity Attacks and Countermeasures in IoT-Based Smart Grid. *IEEE Internet Things J.* 8 (8), 6608–6623. doi:10.1109/jiot.2021.3049818

Zhou, B., and Lei, Y. (2021). Bi-objective Grey Wolf Optimization Algorithm Combined Levy Flight Mechanism for the FMC green Scheduling Problem. *Appl. Soft Comput.* 111, 107717. doi:10.1016/j.asoc.2021.107717

Zou, H., Tao, J., Elsayed, S. K., Elattar, E. E., Almalaq, A., and Mohamed, M. A. (2021). Stochastic Multi-Carrier Energy Management in the Smart Islands Using Reinforcement Learning and Unscented Transform. *Int. J. Electr. Power Energ. Syst.* 130, 106988. doi:10.1016/j.ijepes.2021.106988

Conflict of Interest: TY, KD, ZW, YL, XL, DB, and CY were employed by the company Guangxi Power Grid Co., Ltd.

This work was supported by the Guangxi Power Grid Co., Ltd., Research on vulnerability defense technology of power monitoring system based on interdependent network (047000KK52210031), Research and application of security attack monitoring technology for power intranet terminal equipment based on counter deep learning (047000KK52200012).

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.