A Machine-Learning-Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids

Abdollah Kavousi-Fard, *Senior Member, IEEE*, Wencong Su, *Senior Member, IEEE*, and Tao Jin, *Senior Member, IEEE*

***Abstract*—In this article, an accurate secured framework to detect and stop data integrity attacks in wireless sensor networks in microgrids is proposed. An intelligent anomaly detection method based on prediction intervals (PIs) is introduced to distinguish malicious attacks with different severities during a secured operation. The proposed anomaly detection method is constructed based on the lower and upper bound estimation method to provide optimal feasible PIs over the smart meter readings at electric consumers. It also makes use of the combinatorial concept of PIs to solve the instability issues arising from the neural networks. Due to the high complexity and oscillatory nature of the electric consumers' data, a new modified optimization algorithm based on symbiotic organisms search is developed to adjust the NN parameters. The high accuracy and satisfying performance of the proposed model are assessed on the practical data of a residential microgrid.**

***Index Terms*—Microgrid, monitoring, optimization, prediction, smart sensor.**

I. Introduction

MICROGRID as a supportive concept for the wide integration and deployment of renewable energy sources such as wind turbine and solar panels has improved the electrical services and transmitted power quality, in the last years. Microgrid technology brings many benefits to the electric grid including but not limited to higher social welfare, lower costs, and power losses, higher voltage profile, improved reliability, less air pollutions, and higher green energy economy [1]–[3]. It is anticipated that the installed microgrid capacity at the United States (US) will reach 30% increase by 2020 [4]. In this situation, it is clear that an intelligent operation of the microgrid is closely tied with secure and reliable monitoring of the local power consumption and generation. Metering devices such as smart meters are the key enablers for the two-way information interaction between the consumers and microgrid decision making units (either microgrid central control or distributed decision makers), eventually leading to the efficient and effective operation of the microgrid. Therefore, the security of smart meters in the microgrid plays a significant role in the optimal operation and management of these systems.

With the wide spread growth of microgrids, serious concerns regarding the cyber attacks to these systems involving smart meters' hacking have emerged. According to a recent report from the US Department of Homeland Security, 224 malicious cyber attacks were reported in local electric power companies during the years 2013 and 2014 [5]. The malicious attack of Stuxnet worm to the supervisory control and data acquisition (SCADA) system in 2010 could damage part of the industrial electric grids [6]. In 2008, several cyber attacks were reported in European power utilities trying to penetrate into the system and injecting false data [7]. Therefore, it is quite unsurprising to see a growing concern regarding the possible cyber attacks threatening the vulnerable points of microgrid as a newly introduced technology in the modern power system. In this way, data integrity attacks are among the most destroying and dangerous cyber attacks which can affect the microgrid operation by injecting false data replacing the real monitored data reported by smart meters. Such an attack silently manipulates the transmitted data and affects the healthy data monitored advanced metering infrastructure (AMI) including meters, sensors, or communication channels. In [8], authors develop a method to determine the smallest set of attacked metering devices damaging the electric grid observability through a graph-based approach. It tried to provide a trade-off between maximizing the estimation error at the central control and minimizing the probability of cyber attack. In [9], a Gaussian-based detection model is introduced to limit the data integrity attack in electric grids by defining a minimum and maximum value for the measuring parameters. In [10], the effect of data integrity attacks on the distributed dc power flow algorithms is investigated. Their mechanism fits into the distributed power flow framework to neutralize the severe and dangerous cyber attacks. In [11], the possibility of data

Manuscript received October 29, 2019; revised December 18, 2019 and December 29, 2019; accepted January 2, 2020. Date of publication January 7, 2020; date of current version October 23, 2020. Paper no. TII-19-4801. *(Corresponding authors: Wencong Su and Tao Jin.)*

A. Kavousi-Fard is with the Department of Electrical Engineering, Fuzhou University, Fuzhou 350116, China, and also with the Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz 715555-313, Iran (e-mail: kavousi@sutech.ac.ir).

W. Su is with the Department of Electrical and Computer Engineering, University of Michigan-Dearborn, Dearborn, MI 48128, USA (e-mail: wencong@umich.edu).

T. Jin is with the Department of Electrical Engineering, Fuzhou University, Fuzhou 350116, China (e-mail: jintly@fzu.edu.cn).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2020.2964704

TABLE I
REVIEW OF SOME CYBER ATTACKS IN POWER SYSTEM IN RECENT YEARS

Cyber Attack Type	Attack Point	Effect
Slammer Worm	Ohio Nuclear Power Plant, USA, 2002	Shut-down safety alert system
Stuxnet worm	SCADA System in Iran, 2010	Damaging the Industrial Components
DoS Attack	SCADA, Ukraine, 2015	Service outage to customers by disconnecting 110kV and 35 kV substations for three hours
DDoS Attack	electric power infrastructure, USA, 2007-2010	Causing problem in the control system
Havex malware	ICSs (Industrial Control Systems), United States and Europe, 2014	Damaging and destroying ICSs

integrity attack in the optimal power flow is first investigated and then a resistive framework is constructed to defense the system. Similar works for assessing the data integrity attacks in power systems are implemented in [12]–[16]. Table I shows a review on some of the well-known cyber attacks in the power system in recent years.

While each of the above research works has investigated a specific aspect of data integrity attack, none of them has addressed this harsh cyber attack in microgrids. In fact, microgrids with advanced sophisticated AMIs are a very good target for hackers to implement their malicious attacks. In [17], false data injection attack is investigated in a dc microgrid. In their method, the candidate variants are selected and compared with the actual variants so that any mismatch reveals the existence of a cyber attack.

Unfortunately, the analysis is limited to the dc microgrid and the method is not smart enough to detect different attack severities. In addition, the high complexity and nonlinearity of microgrid local consumers (residential, industrial, or agricultural) make it impossible to reach all points for comparison. This article proposes a new intelligent framework to deal with the data integrity attack in microgrids and defend them against these malicious activities. The proposed framework is capable of detecting cyber attacks with different severities (let us call attack strength) by measuring specific features of the microgrid and learning their behavior during the normal operation. The proposed cyber resilient model is constructed based on the lower and upper estimation (LUBE) method to make optimal prediction interval (PI) with high confidence level [18]. Based on the constructed PIs, any anomaly behavior in the local consumer smart meters' recordings is detected, quickly. In order to overcome the instabilities existing in the neural network (NN) models, the idea of combined NNs is employed. Due to the high complexity and nonlinearity of the microgrid local consumer's dataset, a new optimization algorithm based on symbiotic organisms search (SOS) algorithm is developed to find the optimal values of LUBE parameters. SOS is an evolutionary optimization algorithm which is inspired from the symbiotic interaction strategies adopted by organisms to survive and propagate in their ecosystem [19]. In addition, a three-phase modification method based on crossover and mutation operators from genetic algorithm (GA) is introduced to increase the search ability of SOS while avoiding the possibility of trapping in local optima. The proposed anomaly-based detection model uses the practical data readings recorded by smart meters in AMI to construct a sufficient cyber resilient framework for a secured microgrid operation. To be short, the main contributions of this article can be summarized inthe groups as follows:

1) introducing an intelligent data anomaly detection model for secured microgrid operation based on PIs against data integrity attacks;
2) assessing the effects of attack severity covering stealthy false data injection to severe data attacks making the microgrid operation infeasible;
3) proposing a new SOS-based approach to enhance the LUBE training by accurate adjusting of the setting parameters;
4) introducing a novel two-phase modification method for equipping SOS with global and local search mechanisms for the optimization applications.

The feasibility and high accuracy of the proposed model are examined on the real datasets gathered by AMIs for a practical residential microgrid with three neighborhood and 114 houses (aggregated and individual circuits).

The rest of this article is organized as follows. Section II explains cyber security in microgrids and the proposed data integrity attack model. Section III describes the proposed anomaly detection model based on combined LUBE. This section also explains the two-phase modified SOS optimization algorithm. The simulation results are discussed in Section IV. Finally, Section V concludes this article.

II. CYBER SECURITY IN MICROGRIDS WITH DATA INJECTION ATTACKS

This section focuses on the microgrid cyber security and then explains a model for cyber attack in these systems.

A. Microgrid Cyber Security

Microgrid as a small-size power system covers both the generation and consumption sides which make it possible to operate in two operation modes of grid-connected and islanded. Beside the physical layer including different distributed generations (DGs) and renewable energy sources, loads and storage units, a microgrid has an interconnected cyber layer mainly dealing with data transmission and decision making based on data gathered by AMIs. This makes the microgrid a complex cyber–physical system with a combinatorial nonlinear and correlated structure which is a very good target for cyber hackers to penetrate into it and apply their malicious purposes. Various factors such as vulnerable sensors, heterogeneous data sources, high volume interactions within the microgrid and between the microgrid and the main grid (in the grid-connected mode), sensitivity to time synchronization and communication delays pose challenges to the secure and reliable operation of microgrids. In a microgrid, AMI is the key layer creating a two-way communication road between the smart metering devices with specific IP addresses and the power suppliers and consumers. AMI is in charge of data gathering, data communication, and energy consumption analysis for optimal running of the microgrid. AMI

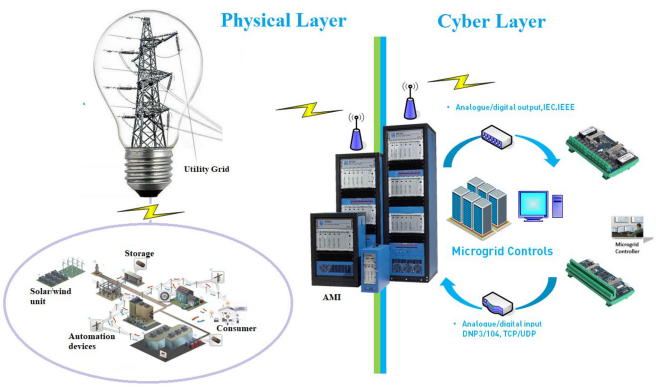

Fig. 1. Microgrid structure as a cyber–physical layer.

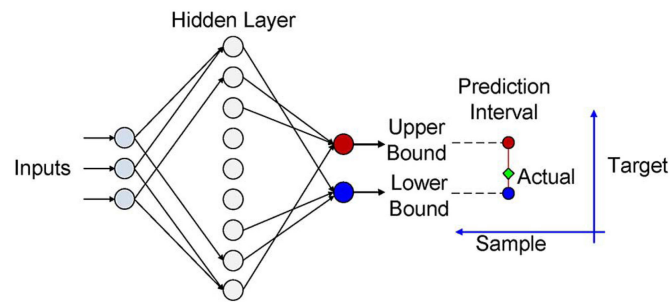

Fig. 2. PIs constructed by LUBE model [18].

makes the real-time decision making in both the generation and consumptions sides possible. Based on the transmitted AMI data, DGs are scheduled at their optimal operating point and electric consumers can make appropriate economic decisions for maximum energy saving and actively participating in the market price. Fig. 1 shows the cyber–physical structure of a microgrid incorporating the AMI. As it can be seen in Fig. 1, through the wired or wireless communication links, the smart meters as a key part of AMI collect data from electric consumers, generators, and storage units for decision making and efficient operation. Therefore, smart meters are assumed as a gateway for collecting and analyzing the microgrid physical layer situation. This makes them a vulnerable and potential penetration point to run malicious attacks for affecting the whole microgrid performance. In fact, by compromising the data reported by smart meters, one can affect the optimal dispatch of DGs and thus reducing the reliability, security, and power quality of electrical services, severely.

B. Cyber Attack

In a typical microgrid, the first and main AMI role is to gather load consumption data and transfer it to the decision making unit for proper scheduling of generator units. In any situation, a healthy microgrid should satisfy the generation and demand balance equation to avoid unexpected interruptions or mandatory load shedding. In addition, AMI can play a significant role in reducing the total microgrid cost by providing real-time data about consumers demand. A microgrid has to increase the amount of power generation during the peak load hours to meet the electric needs. Through the accurate estimation of the load demand provided by AMI, the microgrid can make use of demand response technology to shift the peak load hours and thus reduce the total microgrid costs, avoid unnecessary feeder congestion and possible voltage and frequency collapse. This is a valuable and promising strategy as long as accurate electric load demand information is provided. Unfortunately, AMI being constructed based on communication interfaces is vulnerable to cyber attacks such that an expert adversary can manipulate the reported load demand. By hacking the AMI, an adversary damages the demand response process and destroy the generation and demand balance. This can result in further damaging consequences ranging from additional operating cost to infeasibility of operation and unscheduled shutdowns. The fact that which of these events may happen at the end for a microgrid depends both on the cyber-attack strength and the microgrid mode of operation. As mentioned before, a microgrid can operate in either grid-connected or islanded mode. In the grid-connected mode, the cyber attack to the AMI can increase the microgrid costs, feeder power losses, and voltage collapse. In the islanded mode, the cyber attack can result in more severe results such as loss of generation and demand balance and infeasibility of operation or shutdown. From the severity point of view, the cyber-attack strength can be categorized into two different cases. First, a malicious attack with a strong and instantaneous effect causing the highest damage to the microgrid. Such an attack is sensed in the short-time window and can be recognized due to its high magnitude. Second, a malicious attack with smooth and gradual effect causing changes in the long term. The main purpose of this type of cyber attack is to avoid being detected by the system and make changes in the microgrid in the long terms. In this article, we will analyze both types of cyber attacks on the microgrid. An intelligent model is also proposed to detect the cyber attack which is explained in detail in the next section. The proposed anomaly detection model makes use of the PI concept which represents some smart thresholds which can detect any normality in the system.

III. Proposed Anomaly Detection Method Based on Prediction Intervals

This section proposes a new modified anomaly detection model based on LUBE and modified SOS algorithm to diagnose and stop malicious cyber attacks in the microgrid.

A. Constructing PI Based on LUBE

The LUBE method makes use of the feedforward NN model to construct optimal PIs surrounding the forecast target. In order to detect data integrity attack in the smart sensors installed in the microgrid local consumers' side, each PI is in charge of modeling the forecast uncertainty existing in the electric consumption data. Each PI is made up of a lower bound (LB) and an upper bound (UB) such that any forecast sample will fall between these two bounds. Fig. 2 shows the conceptual illustration of the PI construction by LUBE. According to Fig. 2, the LUBE model has two output values; one value constructing the UB and one value constructing the LB. The number of input features as well as the LUBE structure are determined according to the

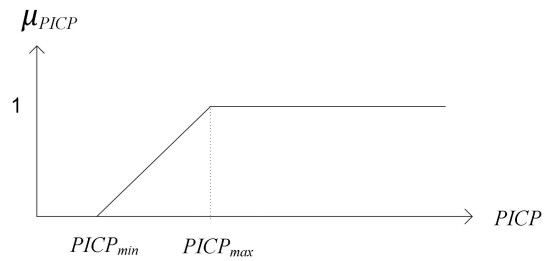

Fig. 3. Fuzzy membership function for PICP.

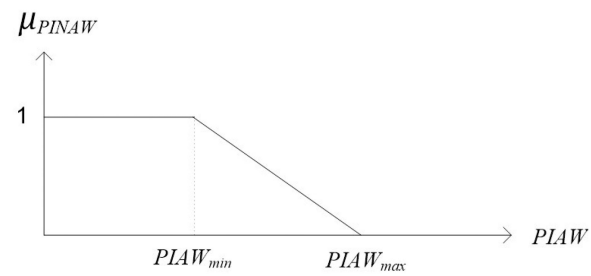

Fig. 4. Fuzzy membership function for PINAW.

data characteristics and complexity. It should be noted that none of these bounds exist during the NN training process. In order to solve this problem and connect the produced PIs with the required confidence level, two fitness functions are defined in the literature [19] which are explained in the rest.

The first fitness function determines the required confidence level of PIs, namely called PI coverage probability (PICP). PICP shows the percentage of forecast points falling in the PIs and is calculated as follows:

$$\mathrm{PICP} = \frac{1}{N}\sum_{i=1}^{N}\varepsilon_i \tag{1}$$

where N is the number of samples and ε_i is a Boolian value that is evaluated as follows:

$$\varepsilon_i = \begin{cases} 1; & y_i \in [\mathrm{LB}_i, \mathrm{UB}_i] \\ 0; & y_i \notin [\mathrm{LB}_i, \mathrm{UB}_i] \end{cases} \tag{2}$$

where y_i is the forecast target. The NN is trained such that the least requirement for the confidence level of $(1-\alpha)\%$ is satisfied. Any PI with a lower confidence level is discarded and a new PI is produced and replaces the low-quality PI.

According to (2), PICP is a significant criterion to determine the quality of PIs. Nevertheless, a PI with a high PICP and a large bandwidth is not applicable for our case. In other words, a very wide PI cannot contain much information about the forecast data and may get useless. Therefore, a second criterion is needed to be defined, mainly calculating the PI bandwidth. The PI average width (PIAW) is defined to compute the PI bandwidth as follows:

$$\mathrm{PIAW} = \frac{1}{\mathrm{NR}}\sum_{i=1}^{N}(U_i - L_i) \tag{3}$$

where R is the range of the underlying targets used for normalizing PIs.

As it can be seen from (1)–(3), the PICP and PIAW have a conflicting interaction such that improving one can devastate the other one and vice versa. This trend brings to the mind the idea of multiobjective optimization which needs a proper mechanism to optimize both fitness functions. This problem will get into several optimal points, making the set of nondominated solutions. In order to extract the most satisfying solution from this set, we make use of the fuzzy min–max approach. To this end, first proper fuzzy sets are assigned to PICP and PIAW, as shown in Figs. 3 and 4. In these figures, the $\mathrm{PICP}_{\min/\max}$ and $\mathrm{PIAW}_{\min/\max}$ show the minimum/maximum values of PICP and PIAW, respectively.

For each nondominated solution (optimal PI), the fuzzy membership value of PICP (μ_{PICP}) and PIAW (μ_{PICP}) are calculated using Figs. 3 and 4. Now, the min–max fuzzy approach is employed to extract the most compromised solution from the set of nondominated solutions as follows [20]:

$$F(X) = \min_{x\in\Omega}\left\{\max_{k=1,\ldots,n}|\mu_{\mathrm{ref},k} - \mu_{f,k}(X)|\right\}, \quad k = 1, 2. \tag{4}$$

Having PICP and PIAW as the fitness functions, the parameter n becomes two here. In (4), $\mu_{f,k}$ shows the fuzzy membership value of kth fitness function. The reference membership functions $\mu_{\mathrm{ref},k}$ are determined by the decision maker in the range (0,1] showing the significance of the corresponding fitness function for the operator. Therefore, the higher $\mu_{\mathrm{ref},k}$ value is, the more significance (weighting factor) is assigned to the corresponding function.

Please note it that $\mathrm{PICP}_{\min/\max}$ and $\mathrm{PIAW}_{\min/\max}$ are generally determined based on the data characteristics. Nevertheless, $\mathrm{PICP}_{\max}$ is set 100 which states that all forecast points are in between the PIs.

Also, $\mathrm{PICP}_{\min} = 0$ represents a very bad scenario in which none of the forecast samples are in the range. For $\mathrm{PIAW}_{\min}$, its value is calculated through the single-objective optimization of $\mathrm{PIAW}_{\min}$ when $\mathrm{PICP}_{\min} > \mathrm{PICP}_{\mathrm{worst}}$. Also, the $\mathrm{PIAW}_{\max}$ may vary in the range [1]–[4] multiple of $\mathrm{PIAW}_{\min}$ based on the data features. As mentioned before in Section I, one main deficiency of NNs is their instable response due the complex nonlinear structure and random training initialization process. This can affect the performance of LUBE and thus the quality of PIs. In other words, any change in the training set can affect the NN response, which is not appropriate in an anomaly detection model. In order to overcome this issue, here we make use of the combination concept for the forecast PIs. It is demonstrated in the literature [21] that combinatorial forecast can enhance the NN performance, effectively. In a similar way, we first train n_c NNs using the LUBE approach. This will result in n_c PIs which are sorted according to their quality [which is determined by (4)]. The first best n_b NNs are picked up and employed for constructing the combined PI based on the test data. The rest of NNs with low quality are discarded. By the use of simple median or average operators, the final n_b PIs are combined to construct the final combined PI.

Through the above process, the proposed probabilistic model can create optimal combined PI for the microgrid electric power consumptions which are monitored by the smart meters in a real-time manner. As mentioned before in Section II, AMI in

a power system is in charge of transferring data of the smart metering devices and sensors to the central control unit. With the aid of AMI, real-time power consumption of the microgrid is monitored and analyzed in the central control unit, which the result will be the optimal power dispatch of units (it means optimal operation). The data integrity attack tries to alter the monitored data of customers' metering devices in the microgrid and affect its optimal operation. By constructing optimal PIs for each group of consumers, any deterioration from the UB or LB shows a possible anomaly data injection activity. Due to the high complexity and nonlinearity of the dataset, a new optimization algorithm based on SSO is developed to help the LUBE training process for constructing more optimal PIs. This is explained in the next part. In this article, authors have made use of (4) instead of the traditional CWC criterion for constructing optimal PIs.

B. Modified Symbiotic Organisms Search Algorithm

The LUBE method developed in the last section is employed for constructing optimal PIs around the smart meters recordings of the microgrid consumers. This part proposes a new optimization algorithm to help adjusting the proposed anomaly detection model parameters. SOS was introduced in 2014 for the first time by inspiring the cooperative interactions happening among different organisms to live and spread in an ecosystem [19]. Similar to the other metaheuristic optimization algorithms, SOS starts with a random initial population (called ecosystem). Each member of this ecosystem is an organism representing a promising solution for the optimization problem. The SOS is constructed based on the specific relationships existing among different organisms in an ecosystem. Depending on that, three core ideas can form the population relationships: 1) mutualism, 2) commensalism, and 3) parasitism. These three types of relationships are used to update the organisms (solutions) position in the ecosystem (population). In a mutualism relationship, both interacting sides benefit from this event. In the commensalism, only one side of the interacting parts most benefit from the relationship. In the parasitism interactions, one side of the relationship (which is most of the time host organism) is harmed. Using the above three rules, all individuals in the population can enhance their position to improve their adaptation (here the fitness function) as time passes. To simulate the above phenomenon, an initial population of organisms is generated. Each solution in this population is a vector representing the LUBE model adjusting parameters. After calculating the fitness function for each solution, the best one is stored X_g. From now on, the population position is improved through several iterations. In the first step, the mutualism interaction is simulated between any two random organisms X_n and X_m as follows:

$$X_n^{\mathrm{Iter}+1} = X_n^{\mathrm{Iter}} + \rho_1 \left(X_g - \omega_1 \times \frac{X_n^{\mathrm{Iter}} + X_m^{\mathrm{Iter}}}{2} \right) \tag{5}$$

$$X_m^{\mathrm{Iter}+1} = X_m^{\mathrm{Iter}} + \rho_2 \left(X_g - \omega_2 \times \frac{X_m^{\mathrm{old}} + X_n^{\mathrm{old}}}{2} \right) \tag{6}$$

where $\rho_1, \ldots, \rho_6$ are random numbers in the range (0, 1] in this article. According to (5) and (6), both organisms are improved in this interaction depending on their benefiting level, i.e., ω_1 and ω_2.

In the second step, the commensalism interaction is simulated. Therefore, a solution X_n is chosen from the population randomly to improve its position as follows:

$$X_n^{\mathrm{Iter}+1} = X_n^{\mathrm{Iter}} + \rho_3 \left(X_g - X_n \right). \tag{7}$$

In the last step, the parasitism interaction is simulated. For each solution X_n, a random individual is chosen as the host to replace X_n. The above three steps are repeated until the algorithm converges.

The SOS algorithm has special features which makes it a powerful optimizer for the nonlinear and nonconvex constraint optimization problems. Some of the main characteristics of the SOS algorithm can be named as simple concept, few adjusting parameters, ease of implementation, having powerful global search mechanisms, and multimodal structure. Nevertheless, the performance of this algorithm can still be improved by equipping it with powerful search mechanisms. Therefore, in this article, we propose a two-stage modification method to improve the SOS algorithm performance. Each of these three phases is explained in the rest.

1) *Modification Phase* 1: This modification method makes use of Levy flight to construct a powerful local search

$$X_n^{\mathrm{Iter}+1} = X_n^{\mathrm{Iter}} + \rho_4 \oplus \mathrm{Le'vy}(\theta). \tag{8}$$

Here, the operator Levy(θ) simulates a random walking around the relevant solution as follows:

$$\mathrm{Le'vy}(\theta) \approx \tilde{\tau} = \mathrm{Iter}^{-\theta} \; 1 \leq \theta \leq 3. \tag{9}$$

2) *Modification Phase* 2: This modification method makes use of the crossover and mutating operators from the GA to increase the ecosystem diversity and avoid premature convergence. To this end, for each random solution X_n, three dissimilar solutions X_{m1}, X_{m2}, and X_{m3} are chosen such that $n \neq m_1 \neq m_2 \neq m_3$. Then, a mutated solution is generated as follows:

$$\begin{aligned} X_{\mathrm{mut}} &= X_{m1} + \rho_5 (X_{m2} - X_{m3}) \\ X_{\mathrm{mut}} &= [x_{\mathrm{mut},1}, \ldots, x_{\mathrm{mut},j}, \ldots, x_{\mathrm{mut},d}]. \end{aligned} \tag{10}$$

Now, the crossover operator is employed for generating new test solutions as follows:

$$\begin{aligned} x_j^{\mathrm{Test1}} &= \begin{cases} x_{\mathrm{mut},j}; & \rho_5 \leq \rho_6 \\ x_g; & \rho_5 \succ \rho_6 \end{cases} \\ X_g &= [x_{g,1}, \ldots, x_{g,j}, \ldots, x_{g,d}] \end{aligned} \tag{11}$$

$$\begin{aligned} x_j^{\mathrm{Test2}} &= \begin{cases} x_{\mathrm{mut},j}; & \rho_6 \leq \rho_7 \\ x_n; & \rho_6 \succ \rho_7 \end{cases} \\ X_n &= [x_{n,1}, \ldots, x_{n,j}, \ldots, x_{n,d}]. \end{aligned} \tag{12}$$

The best solution among (11) and (12) is compared with X_n and will replace it if it has a better position. Fig. 5 shows the flowchart of the proposed MSOS algorithm.

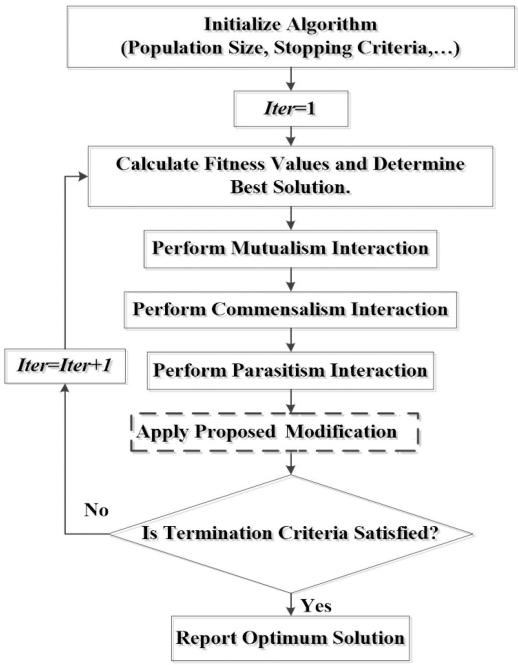

Fig. 5. Flowchart of the proposed modified optimization algorithm.

C. Anomaly Detection Model Based on LUBE and MSOS

As it can be seen from the last parts, the proposed anomaly detection model makes use of PI concept to see whether smart meter readings of electric consumers in the microgrid is showing a normal behavior or an abnormal one. Fig. 6 shows the conceptual illustration of the proposed anomaly detection method to detect data integrity attack in the microgrid. According to this figure, constructing PIs around the smart meter readings of the electric consumers can determine the normal or abnormal behaviors in the system. In the case of cyber security, the proposed anomaly detection method may make any of these four decisions: 1) true positive, 2) false positive, 3) true negative, and 4) false negative. These decisions are made depending on the real system data and the proposed anomaly detection model response. The PIs created by the proposed LUBE-based method will make boundaries which will help detecting anomalies as shown in the figure.

A decision is said to be positive when it is identified as a cyber activity. On the opposite, a decision is negative when the anomaly detection model recognize it as normal behavior. True decision is made when the anomaly detection model has made a correct decision. Therefore, it is clear that a false decision shows a wrong response from our cyber-attack detection model. Accordingly, it can be deduced that an appropriate anomaly detection model is one with low false rates. Based on these definitions, four different criteria can be defined: hit rate (HR), false alarm rate (FR), miss rate (MR), and correct reject rate (CR). To help better understanding of these criteria, Fig. 7 provides the confusion matrix.

Considering C_A and C_N as the total real malicious data and normal data, four criteria of HR, FA, MR, and CR are formulated

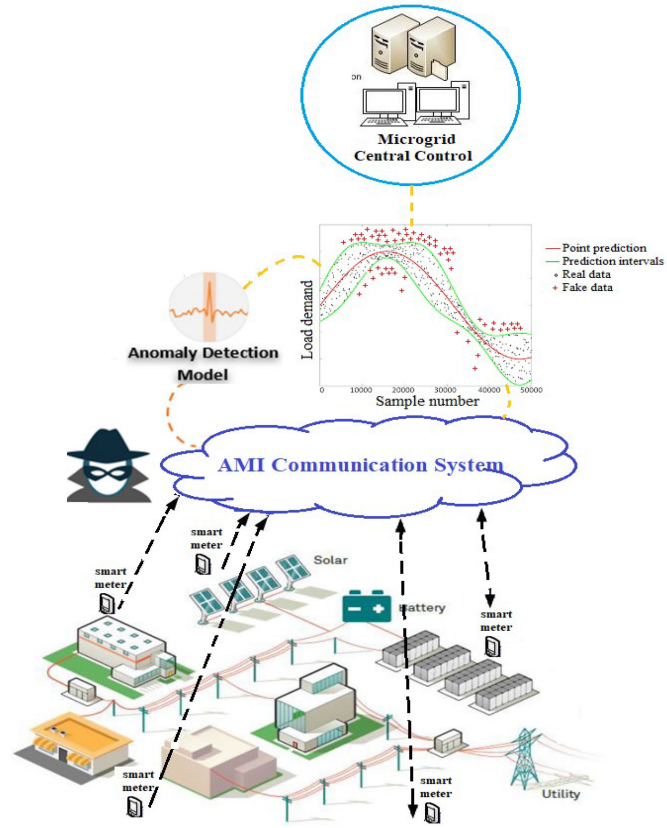

Fig. 6. Proposed anomaly detection model based on PIs to secure microgrid smart meters.

Anomaly Detection Model Reponse		Actual Value From Experiment	
		positives (C_A)	negatives (C_N)
	positives (C_O)	Hit Rate True Positive (TP)	False Alarm Rate False Positive (FP)
	negatives (C_I)	Miss Rate False Negative (FN)	Correct Rejection Rate True Negative (TN)

Fig. 7. Confusion matrix for the proposed anomaly detection model.

for the proposed anomaly detection model as follows:

$$\mathrm{HR} = \frac{|H_i|}{|C_A|} \quad ; \quad H_i = \{X \in D \,|\, X \in C_A \,\&\, X \in C_O\} \quad (13)$$

$$\mathrm{FR} = \frac{|F_A|}{|C_N|} \quad ; \quad \mathrm{F}_A = \{X \in D \,|\, X \in C_N \,\&\, X \in C_O\} \quad (14)$$

$$\mathrm{MR} = \frac{|M_i|}{|C_A|} \quad ; \quad \mathrm{M}_i = \{X \in D \,|\, X \in C_A \,\&\, X \in C_I\} \quad (15)$$

$$\mathrm{DR} = \frac{|C_R|}{|C_N|} \quad ; \quad \mathrm{C}_R = \{X \in D \,|\, X \in C_N \,\&\, X \in C_I\} \quad (16)$$

where D is the set of total data received from the smart meter, C_I is the set of inliers, and C_O is the set of outliers. By the help of these four criteria, the performance of the proposed anomaly detection method can be assessed.

According to the above explanations, the following steps are needed to construct the proposed anomaly detection model.

Steps 1: Input data including the microgrid data (grid topology, sensor locations, sampling frequency, load, and generation values), the MSOS data (the initial population, the termination criterion, the population size, and objective function), the anomaly detection model data (the minimum and maximum values $\text{PICP}_{\text{min/max}}$ and $\text{PIAW}_{\text{min/max}}$, the required confidence level, the training dataset, validation dataset, and the test dataset).

Step 2: Read the recording load data from the microgrid and store it.

Step 3: Construct the anomaly detection model dataset. Divide the recorded dataset into training, validating, and testing group. Determine the appropriate features for input to the model.

Step 3: Train n_c NNs using the LUBE approach. To this end, n_c PIs are trained and sorted according to their quality.

Step 4: Optimize the anomaly detection model using the proposed MSOS algorithm. Run the MSOS algorithm as shown in Fig. 5 to adjust the weighting and biasing factors in in such that more optimal PIs are constructed by each NNs.

Step 5: Construct the combined PIs. In order to increase the model robustness and accuracy, the first best n_b NNs are picked up and employed for constructing the combined PIs.

Step 6: Compare the microgrid test data with the PIs bandwidth to find the HR, FR, MR, and CR.

IV. Numerical Simulations

This section examines the performance of the proposed anomaly detection model to detect cyber attack to the smart sensors in a practical residential microgrid with 342 houses which are divided into three neighborhood, each supporting 114 houses. The electric power consumption of each residential neighborhood is recorded by two different types of metering devices. First, aggregated meters which are installed at the front of each neighborhood. Second, smart meters which are installed for each individual house in a neighborhood area. Since in the reality, only portion of the houses are equipped with smart meters and not all of them, here we apply our method only on the aggregated meters installed upfront of each neighborhood. It is clear that checking the individual smart meters is also quite possible in the similar way. The metering devises record data every 30 min, which are stored in excel files of the anomaly detection model. At the first, in order prove the satisfying performance of the proposed anomaly detection method in constructing optimal PIs around smart meters data readings, Table II shows the optimal PIs characteristics generated by the proposed LUBE-MSOS algorithm. To have a better comparison, the LUBE model is trained by three different methods of GA, particle swarm optimization algorithm, original SOS, and proposed MSOS. As it can be seen from this table, the proposed MSOS algorithm could help the LUBE to get into higher fuzzy membership value, which results in a lower PIAW and a higher PICP.

TABLE II
Characteristics of the PIs Constructed by the Proposed Anomaly Detection Method

Algorithm	PICP	PIAW	Membership Function value
GA	82.47028	28.30582	0.104781
SOS	89.68038	25.97342	0.070244
Proposed MSOS	91.69504	23.66935	0.060587

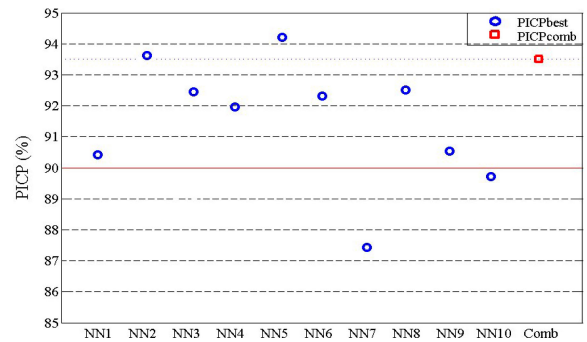

Fig. 8. Comparative plot of the n_b NNs and the combined PI using the fuzzy fitness function.

In order to perceive the positive role of combined LUBE in improving the final PI, Fig. 8 shows the PICP values attaining for the best $n_b = 10$ NNs. According to this figure, except two of NNs which could into higher PICPs, all the other eight NNs have low PICP values (representing less-qualified PIs). Nevertheless, the final combined PI achieved through the proposed combinatorial approach has appropriate quality, with high PICP value. This verifies the satisfying performance of the proposed combined LUBE method in comparison with the single ones. In order to avoid repetition, the final PI is shown later along with the data integrity attacks in the same frame (Fig. 9).

So far, the satisfying performance of the proposed LUBE model for constructing optimal PIs is proved. In order to assess its performance in the face of cyber attacks as well, we need to launch a cyber attack to the microgrid. In order to simulate a cyber attack, the compromised aggregated meter will report overload situations, repeatedly. Therefore, attacks of different severity are generated every 24 h which will last for around a few hours depending on the severity. Based on the fact that our smart meters record the data every 30 min, then the attack effect should be seen in the next few samples. Having the peak load demand of the aggregated meter as 200 kW, several ranges of data injection attacks in the range 20–200 kW are launched to simulate the severity from a smooth attack (10% overload) to a very severe attack (100% overload). Fig. 9 shows the performance of the anomaly detection model for data integrity attack detection with different severities. The attacks are lunched two times (in two successive days) in the microgrid (shown by small red squares) such that the attacks of less severity are lunched at the beginning and attacks of higher severities are lunched later after sample

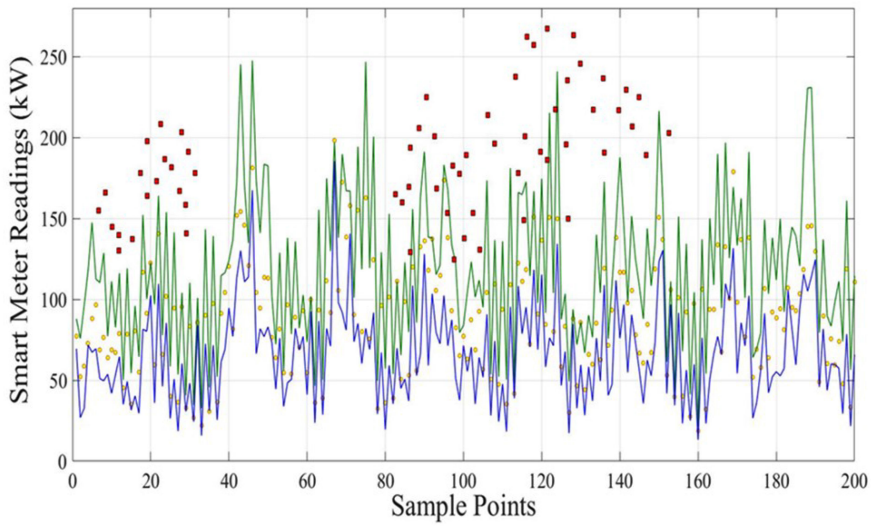

Fig. 9. Performance of the proposed anomaly detection model for data integrity attacks of different severities. (Green line: upper bound, Blue line: lower bound, Yellow circles: real smart metering, Red squares: fake data).

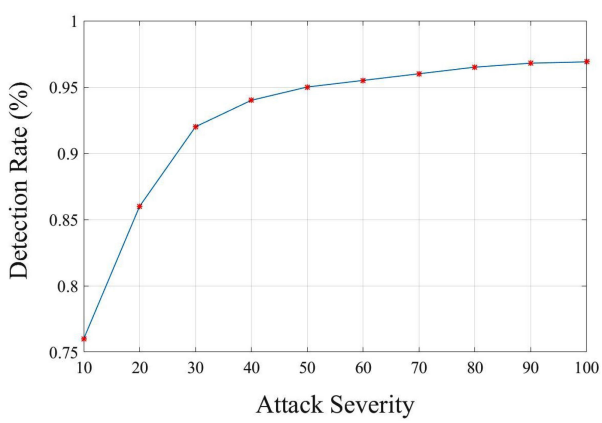

Fig. 10. Detection rate versus the attack severity using the proposed anomaly detection model.

point 80. In Fig. 9, the PI constructed by the proposed optimal probabilistic framework is depicted to detect the normality in the dataset. The PCIP and PINAW values of this PI are 91.69504 and 23.66935, respectively. As it can be seen from this figure, in both attacking cases, the constructed PIs could highlight the abnormal smart meter' readings, properly. In fact, the UB generated for the sample points show the highest possible values that each aggregated customer can get at each time considering the uncertainty effects. As a result, any value out of the PI shows a suspicious case which needs to be assessed, carefully. Still, there is a possibility to assign probability values to samples according to their distance from the PIs.

In order to better see the performance of the proposed method, the detection rate value versus the attack severity is plotted in Fig. 10. The detection rate is considered as the percentage of smart meter readings which are affected by the adversary and that are recognized as false data, correctly. As can be seen from this figure, at stealthy false data injections, the detection rate is not very high. But as the injection attack severity increases, the detection rate increases to very high values. This is an acceptable response since attacks of high severity can make the microgrid operation infeasible or forcing to operate in the islanding mode. On the other hand, attacks of stealthy data injection can only affect the optimality of the power dispatch for the power generators. Still, both values are in the acceptable range and appropriate for a microgrid. It is also seen that the detection rate is saturated at the attack severity of almost 60%. This means that any attack with a severity higher than this value is highly detected by the model.

TABLE III
CONFUSION MATRIX VALUES FOR DIFFERENT ANOMALY DETECTION MODEL

Outlier Algorithm	HR(%)	MR(%)	FR (%)	CR (%)
Conventional LUBE	83.14%	16.86%	17.17%	82.83%
Method LUBE-SOS	88.78%	11.22%	13.52%	86.48%
Proposed Anomaly Detection Model	92.43%	7.57%	8.36%	91.64%

Finally, the overall performance of the proposed anomaly detection model based on the confusion matrix is shown in Table III. In order to get into a better perception about the model performance, the simulation results of the conventional LUBE, LUBE-SOS, and proposed LUBE-MSOS are shown, comparatively. According to these results, the proposed data integrity attack detection model has shown superior performance over the other models by providing higher HR% and CR%. Such a progress in the results shows the significance of optimal setting of NNs in constructing the more fitting PIs.

V. CONCLUSION

In this article, data integrity attack can endanger the total microgrid operation and management by misleading the central control unit in correct estimation of the total demand. This can result in not only nonoptimal operation of the units, but can also force the microgrid to schedule its units at an infeasible point, causing mismatch between the generation and demand.

Therefore, this article proposed a highly accurate and intelligent anomaly detection model for securing the microgrids against data integrity attacks. The proposed method, a modified LUBE, and MSOS model, was constructed based on the PI concept to prevent hackers from fake data injection to the central control unit. The proposed MSOS helped to adjust the NNs setting parameters and help LUBE for getting into higher PICP and lower PIAW values. The simulation results on the experimental dataset recorded for a residential microgrid with 342 houses including three neighborhood, reveal the satisfying performance of the proposed method to detect the fake data injections in the smart meter readings. Also, it was seen that the proposed model shows appropriate performance in the face of malicious attacks with different severities ranging from 10% to 100% data injection. The results of two different criteria of detection rate and confusion matrix results advocate the accuracy and valuable performance of the proposed anomaly detection model.

References

[1] W. R. Issa, A. H. El Khateb, M. A. Abusara, and T. K. Mallick, "Control strategy for uninterrupted microgrid mode transfer during unintentional islanding scenarios," *IEEE Trans. Ind. Electron.*, vol. 65, no. 6, pp. 4831–4839, Jun. 2018.

[2] M. Dab, A. Kavousi-Fard, and S. Mehraeen, "Effective scheduling of reconfigurable microgrids with dynamic thermal line rating," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1552–1564, Feb. 2019.

[3] K. W. Hu and C. M. Liaw, "Incorporated operation control of DC microgrid and electric vehicle," *IEEE Trans. Ind. Electron.*, vol. 63, no. 1, pp. 202–215, Jan. 2016.

[4] Greentech Media reports, 2018. [Online]. Available: https://www.utilitydive.com

[5] J. Pagliery, Hackers Attacked the U.S. Energy Grid 79 Times This Year, 2014. [Online]. Available: http://money.cnn.com/2014/11/18/technology/security/energy-grid-hack/, Accessed on: 10 March 2017.

[6] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[7] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "Survey on advanced metering infrastructure," *Int. J. Elect. Power Energy Syst.*, vol. 63, pp. 473–484, 2014.

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

[9] X. Yang, P. Zhao, X. Zhang, J. Lin, and W. Yu, "Toward a Gaussian-mixture model-based detection scheme against data integrity attacks in the smart grid," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 147–161, Feb. 2017.

[10] J. Duan, W. Zeng, and M. Y. Chow, "Resilient distributed DC optimal power flow against data integrity attack," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3543–3552, Jul. 2018.

[11] Q. Yang *et al.*, "Toward data integrity attacks against optimal power flow in smart grid," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1726–1738, Oct. 2017.

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

[13] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[14] Q. Yang, J. Yang, W. Yu, N. Zhang, and W. Zhao, "On a hierarchical false data injection attack on power system state estimation," in *Proc. IEEE Global Telecommun. Conf.*, USA, Dec. 2011, pp. 1–5.

[15] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, New York, NY, USA, 2009, pp. 21–32.

[16] Y. Feng, C. Foglietta, A. Baiocco, S. Panzieri, and S. D. Wolthusen, "Malicious false data injection in hierarchical electric power grid state estimation systems," in *Proc. 4th Int. Conf. Future Energy Syst.*, New York, NY, USA, 2013, pp. 183–192.

[17] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber–physical DC microgrids," *IEEE Trans. Ind. Inform.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[18] A. Khosravi, S. Nahavandi, D. Creighton, and A. F. Atiya, "A lower upper bound estimation method for construction of neural network based prediction intervals," *IEEE Trans. Neural Netw.*, vol. 22, no. 3, pp. 337–346, Mar. 2011.

[19] M. Y. Cheng and D. Prayogo, "Symbiotic Organisms Search: A new metaheuristic optimization algorithm," *Comput. Struct.*, vol. 139 pp. 98–112, 2014.

[20] T. Niknam, A. Kavousifard, and J. Aghaei, "Scenario-based multiobjective distribution feeder reconfiguration considering wind power using adaptive modified particle swarm optimization," *IET Renewable Power Gener.*, vol. 6, no. 4, pp. 236–247, Jul. 2012.

[21] S. Hashem and B. Schmeiser, "Improving model accuracy using optimal linear combinations of trained neural networks," *IEEE Trans. Neural Netw.*, vol. 6, no. 3, pp. 792–794, May 1995.

Abdollah Kavousi-Fard (Senior Member, IEEE) received the B.Sc. degree from the Shiraz University of Technology, Shiraz, Iran, in 2009, the M.Sc. degree from Shiraz University, Shiraz, in 2011, and the Ph.D. degree from the Shiraz University of Technology, Shiraz, in 2016, all in electrical engineering.

Dr. Kavousi-Fard is currently an Assistant Professor with Shiraz University of Technology, Shiraz, Iran.

He was a Postdoctoral Research Assistant with the University of Michigan, Ann Arbor, MI, USA, from 2016 to 2018. He was a Researcher with the University of Denver, Denver, CO, USA, from 2015 to 2016 conducting research on microgrids. His research interests include operation, management and cyber security analysis of smart grids, microgrid, smart city, electric vehicles, as well as protection of power systems, reliability, artificial intelligence, and machine learning.

Dr. Kavousi-Fard is an Editor in Springer, ISTE ISI Journal.

Wencong Su (Senior Member, IEEE) received the B.S. degree (with distinction) from Clarkson University, Potsdam, NY, USA, in 2008, the M.S. degree in instrument science and technology from Virginia Tech, Blacksburg, VA, USA, in 2009, and the Ph.D. degree in instrument science and technology from North Carolina State University, Raleigh, NC, USA, in 2013.

He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Michigan-Dearborn, Dearborn, MI, USA. His research interests include power systems, electrified transportation systems, and cyber–physical systems.

Dr. Su is an Editor for the IEEE Transactions on Smart Grid and an Associate Editor for the IEEE Access. He is a registered Professional Engineer with the the State of Michigan, USA.

Tao Jin (Senior Member, IEEE) was born in Hubei Province, China, in 1976. He received the B.S. and M.S. degrees in electrical engineering from Yanshan University, Qinhuangdao, China, in 1997 and 2001, respectively, and the Ph.D. degree in electrical engineering from Shanghai Jiaotong University, Shanghai, China, in 2005.

He is currently a Research Professor in the School of Electrical Engineering & Automation at Fuzhou University, China.

He has worked as a Research Fellow with Virginia Polytechnic Institute, Blacksburg, VA, USA and Imperial College London, London, U.K. Since 2009, he has been a Researching Professor with Fuzhou University, Fuzhou, China. His research interests include measurement technology and new technologies in smart grid.