IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 12, 2021, accepted June 22, 2021, date of publication June 28, 2021, date of current version July 5, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3092834

A Secured Advanced Management Architecture in Peer-to-Peer Energy Trading for Multi-Microgrid in the Stochastic Environment

MOHAMED A. MOHAMED[1,2], (Member, IEEE), ALI HAJJIAH[3], KHALID ABDULAZIZ ALNOWIBET[4], ADEL FAHAD ALRASHEEDI[4], EMAD MAHROUS AWWAD[5], AND S. M. MUYEEN[6], (Senior Member, IEEE)

[1]Electrical Engineering Department, Faculty of Engineering, Minia University, Minia 61519, Egypt
[2]Department of Electrical Engineering, Fuzhou University, Fuzhou 350116, China
[3]Electrical Engineering Department, College of Engineering and Petroleum, Kuwait University, Safat 13060, Kuwait
[4]Statistics and Operations Research Department, College of Science, King Saud University, Riyadh 11451, Saudi Arabia
[5]Electrical Engineering Department, College of Engineering, King Saud University, Riyadh 11421, Saudi Arabia
[6]School of Electrical Engineering Computing and Mathematical Sciences, Curtin University, Perth, WA 6845, Australia

Corresponding author: Mohamed A. Mohamed (dr.mohamed.abdelaziz@mu.edu.eg)

This work was supported by the Deanship of Scientific Research at King Saud University under Grant RG-1436-040.

This work did not involve human subjects or animals in its research.

ABSTRACT Careful consideration of grid developments illustrates the fundamental changes in its structure which its developments have taken place gradually for a long time. One of the most important developments is the expansion of the communication infrastructure that brings many advantages in the cyber layer of the system. The actual execution of the peer-to-peer (P2P) energy trading is one core advantage which also may lead to the systematic risks such as cyber-attacks. Consequently, it is necessary to form a useful way to cover such challenges. This paper focuses on the online detection of false data injection attack (FDIA), which tries to disrupt the trend of optimal peer-to-peer energy trading in the stochastic condition. Moreover, this article proposes an effective modified Intelligent Priority Selection based Reinforcement Learning (IPS-RL) method to detect and stop the malicious attacks in the shortest time for effective energy trading based on the peer to peer structure. The presented method is compared with other methods such as support vector machine (SVM), reinforcement learning (RL), particle swarm optimization (PSO)-RL, and genetic algorithm (GA)-RL to validate the functionality of the method. The proposed method is implemented and examined on three interconnected microgrids in the form of peer-to-peer structure wherein each microgrid has various agents such as photovoltaic (PV), wind turbine, fuel cell, tidal system, storage unit, etc. Eventually, the unscented transformation (UT) is applied for uncertainty analysis and making the near-reality simulations.

INDEX TERMS Peer-to-peer energy trading, microgrid, reinforcement learning, uncertainties, intelligent priority selection method, cyber-attack detection, stochastic modeling, combinatorial optimization.

NOMENCLATURE

Sets/Indices

j/Ω^i	Set/index of number of microgrid.
i/Ω^i	Set/index of number of renewable energy resource.
t/Ω^T	Set/index of time where $\Omega^T = \{1 \ldots 24\}$.

Constants

κ_t	Attack time.
$X_{bad,t}$	False data.
R^{loss}	Power loss related to PV.
S_t^W	Wind speed.
T_t^V	Tidal current.
S_{cutin}^W, S_{rated}^W	The cut-in and rated wind speeds.
T_{cutin}^V, T_{rated}^V	Cut-in and rated tidal current speeds.
Q	Direct irradiation.
γ	Sea water density.
λ	Swept area of the turbine blades.

The associate editor coordinating the review of this manuscript and approving it for publication was Behnam Mohammadi-Ivatloo.

U_t	Capacity of the PVs.
$P^{\min}/P^{\max}$	Min/max limits of battery power.
$V^{\min}/\leq V^{\max}$	Min/max limits of battery energy.
$P_t^{load1}, P_t^{load2}, P_t^{load3}$	Loads of microgrid 1 to 3, respectively.
γ^k	Persistent sequence.
CW_t, CTI_t, CPV_t, CB_t	Prices of the WT, tidal, PV and storage system, respectively.
m, σ	Value of the average and variance.
c	The injected malicious data.
κ	Attack time.
λ	Attack vector.

Variables

$PB_t, PW_t, TI_t, PV_t, FC$	Power output of the storage, WT, tidal system, PV, fuel cell, respectively.
u_t	Binary variable related to reward.
r_t	Received Reward at time t.
φ_t	Estimate of likelihood.
PB_t	Battery power.
P_t^{13}	Power transaction between microgrid 1 and 3.
P_t^{12}	Power transaction between microgrid 1 and 2.
P_t^{23}	Power transaction between microgrid 2 and 3.
V_t^{fc}, I_t^{fc}, R	Voltage, current and resistance of inverter converter connected to fuel cell unit.
P_j	The power generations of the microgrid.
H_t^j	Slackness variable of each microgrid j.
$PS_{j,t}^k$	Power set point of microgrid j in iteration k.
$P_t^{jj'}$	The power transaction among microgrids.
PB_t^{ch}/PB_t^{dis}	Charging/Discharging power of storage.
$R_t^{jj'}$	Auxiliary coefficient related to microgrids.
VB_t	Energy of the storage system.
$\beta_t^{jj'}$	The trading prices among the microgrids.
$mic1, mic2, mic3$	Costs of the microgrid 1 to 3, respectively.

I. INTRODUCTION

Due to the changing grid structure in the past decade, the power energy trade is going up at a startling pace. As the communication tools have been expanding in the electrical grids, the volume of the real-time trade has been rising at the same rate. In the sense that creating safe and secure infrastructures in the field of developing real-time energy transactions will be provided a more desire for participation in the real-time energy market among the agents. In this situation, the penetration of renewables and microgrids is also growing in the main grid. So the power production, in order to meet the consumers' needs, plays a more important role in almost every microgrid in the power system, and energy markets now tempt agents that never get much worried about sales beyond their inner customers. Hence, this research addresses peer-to-peer energy trading and it's providing security. Therefore, the following three parts are addressed in this paper: A) peer to peer (P2P) energy trading, B) Detecting false data injection attack (FDIA), C) Applying modified approach: Intelligent Priority Selection based Reinforcement Learning (IPS-RL).

A. P2P ENERGY TRADING

P2P energy trading is a new model of power electric market, where generation units can generate their output electric power independently and sell it to each customer locally. In [1], authors have explained effective methods for P2P energy trading, and surveyed their similarities and differences. Several projects on P2P energy trading have been experimentally carried out in recent years. A project was implemented in the UK [2] in which industrial consumers can purchase electricity directly from the local generations based on renewable energy resources. Similar to the UK project, the P2P energy trading platform in the Netherland functions performs such as an energy provider that connects customers and agents, and equilibrates the whole market [3].

On the other hand, a few studies have been carried out which present a new method for executing P2P energy trading independently from the practical projects. In more complex situations such as a multi-agent trading agreement, a consensus can be a bilateral contract verified among all agents. In reference [4], bilateral contract networks have been proposed as new scalable market designs for P2P energy trading. Recently, the game theory method has received a lot of attention for resolving mathematical problems. In some aspects, game theory is a strategic issue or at least the optimal decision-making of autonomous players is met in a competing environment. Authors in [5] have briefly carried out an overview of the application of game-theoretic methods for P2P energy trading as a pragmatic and executable solution of the energy management. Authors in [6], [7] have expanded an optimization model and blockchain-based architecture to manage the operation of distributed energy systems, with P2P energy trading. Despite applying the blockchain-based structure mentioned in references [6], [7], the power grid is not only a software platform for achieving a consensus. Therefore, lack of diagnosis of FDIA can damage the system components. Unfortunately, there are still too few studies in this field which shows the big gap existing in this area. In this research, the FDIA detection has been considered such that

the implementation of P2P energy trading is reconciled with the modified IPS-RL method.

B. DETECTING FDIA AND PROPOSED SOLUTION

Nowadays, the electrical power grid, as the most important infrastructure in every country, is under threat from cyber-attack point of view. FDIA is widely brought up in cyber-physical systems e.g. electricity market [8], power grid [9], [10], control systems [11], [12], and water distribution system [13]. The FDIA in cyber-physical systems refers to a category of cyber-attacks in which the attacker desires to change the integrity of the network by influencing a set of sensor devices and sending incorrect readings of data to the controller. So, this attack impacts physical devices that operators and some attackers can access. On the other hand, owing to sending data by devices of the system, the output of FDIA is valid for cyber-security systems based on data mining such as blockchain. Consequently, the motivation behind the attack will be different. The former is often sought destruction over the system (a malicious adversary), the latter benefit (internal beneficiaries). The power grid with varied types of resources, transmission lines, distribution networks, and numerous protection devices, is one of the largest infrastructures in the human life. Since the measurement devices in these systems are smart equipment (e.g., smart meters and protection relays), they can always be an attractive purpose for the cyber hacking. Cyber-attacks that impact the system operation have been reported in several researches such as in [8], [14]–[18]. A blockchain-based architecture and optimization model has been developed [8] for energy management systems and it is mentioned that an uncontrollable risk exists in the blockchain-based energy market, i.e., the attacks from the malicious trading operator. Monitoring of the system is needful to guarantee the reliable operation of the power network, and state estimation is an output of it to reach the best estimate of the power grid. In [14], the authors have presented an FDIA, against state estimation in power grids. In [15], malicious cyber-attacks against some devices in the smart grid have been investigated, in which an attacker controls a set of meters and is able to change the measurements from those meters. In [16], [17], the researchers have analyzed the cyber security of state estimators in SCADA operating in power grids. A bad data detection schemes have been presented for state estimation algorithms to detect random outliers in the measurement data. Reference [18] has also introduced analytical techniques with the aim of analyzing the vulnerability of state estimation when it is subject to a hidden false data injection attack on a power grid's SCADA system. Research about FDIA in kinds of literature are generally included three points of view: 1) theoretical investigates on generating or creating a valid FDIA [19]–[22], 2) application studies on the general impact of FDIA [23]–[26], 3) techniques adopted to protect against FDIAs [27]–[29]. Reference [30] has presented a review of false data injection impact in modern power systems. In [31], the authors have formulated detection of FDAI with the binary classification machine learning problem. It's worth mentioning that interrupting power electric is a notable disorder; therefore, online detection of the FIDA can considerably contribute to the increasing system reliability. Research [32] has addressed the issue of joint distributed secure estimation and distributed attack detection for a cyber-physical system under cyber and physical attacks. In this reference, a malicious adversary simultaneously starts up an FDIA at the physical system layers. In [33], the authors have considered the problem of data detection in distributed systems in the presence of falsification data injection attacks. This type of attack is also known as Byzantine attacks. Detection methods considered in the reference [33] are based on distributed consensus algorithms. In [34], researchers have formulated the online attack detection based on the reinforcement learning (RL) method. In this investigation, the effective data in a consensus of P2P energy trading are sifted by the proposed algorithm then it is broadcasted. Consequently, the speed of FDIA detection goes up strongly. The RL method is used for widespread applications. For example, a distributed multi-agent-based RL method has been proposed in [35] for optimal reactive power flow. In order to bring the simulation closer to the reality, the load and production uncertainty are considered and the UT method is used to simulate the uncertainty. Some of the significant applications of UT are reported in several literature [36]–[39].

C. CONTRIBUTIONS

Returning to the hypothesis posed at the beginning of this study in the abstract, cyber-physical attacks such as FDIA are increasingly recognized as a serious distributed smart grid concern. Proposing an application solution is the most important challenge in this investigation. A key aspect of detection FDIA in P2P systems is attention to the time issue. Therefore, this paper tries to address the online detection of FDIA in the power system and optimal peer-t-peer energy trading process. In this regard, a novel intrusion detection system, called modified intelligent priority selection based reinforcement learning (IPS-RL) is developed to detect and stopover the malicious cyber-hacking activities in the very short time. The proposed method is compatible with the peer-to-peer energy trading in a multi-agent mechanism and consists of the advanced machine learning techniques such as support vector machine (SVM), reinforcement learning (RL), particle swarm optimization (PSO)-RL, and genetic algorithm (GA)-RL. In order to validate the performance of the proposed intrusion detection system, an interconnected microgrid with three microgrids in a P2P structure is deployed as the test system. However, there isn't limitation for applying case study. For example, in future studies can be adopted virtual power plant as a case study [40]. Varied types of generation units such as photovoltaic (PV), wind turbine, fuel cell, tidal system and storage unit are considered in the model. Considering the high uncertainty effects, a stochastic framework based on UT is deployed in this work.

Given all the above discussions, the main contributions can be summarized as follows:

- Suggesting a fruitful intrusion (anomaly) detection scheme based on the IPS-RL approach to get into the minimum detection delay.
- This article investigates and proposes an effective P2P energy trading framework equipped by a security platform based on the IPS-RL method against malicious cyber-attacks.
- Modeling the attack of FIDA type to assess the security of the proposed detection method in the P2P energy market.
- Developing a stochastic framework based on UT for the proposed P2P based energy management under uncertainty conditions.

The remaining sections of the paper are arranged as follows: Section II presents the proposed security management architecture based on the proposed attack detection method. Section III introduces the secured P2P energy market structure. The uncertainty framework based on UT is explained in section IV to deal with the stochastic effects. Section V discusses the simulation results on the proposed case study. Finally, the main results of the proposed method are described in section VI.

II. CYBER ATTACK DETECTION APPROACH BASED ON THE PROPOSED IPS-RL SCHEME

The growing occurrence of malicious attacks in the cyber-physical systems (CPSs) is one of the main reasons to propose different detection methods. In this regard, the CPSs need to develop their communications with the use of the detection technologies in order to preserve actual data against cyber-attacks. In a special attack such as FDIA, hackers try to get into the most social/economic benefits in the shortest possible time. Therefore, the detection scheme should be able to recognize the attacks launched to the CPSs with the aim of minimizing the detection delay. Therefore, this part aims first to present how an attack of FDIA type is modeled and introduces an appropriate detection method based on IPS-RL approach against the malicious attacks.

A. FDIA MODEL

Modeling the cyber-attacks is one of the most significant tasks in a problem in order to analyze the varied fields of the system security, including the security defenses and the destructive effects of attacks. This section introduces the mathematical formulation for stealthy attacks in the power systems. Modeling the cyber-attacks can be usually modeled and categorized in different classes, such as attack networks, attack trees and attack graphs [41]. The attack tree method is modeled by the use of the acyclic directed graph in accordance with the nodes of network. All proposes related to hackers can be discovered by the attack graph model when launching a given attack in the network. The third method (attack networks) is a trusty model, which is capable of simulating the attack with regards to the malicious decision of hackers. One of the most destructive attacks is FDIA type in power cyber-physical systems that are regarded in the class of third model. A successful FDIA can make harmful economic and physical effects on the power systems by manipulating data. Accordingly, impacts of FDIA on the power system can be mainly categorized in three aspects: 1) the economic impacts 2) the load redistribution attack 3) the energy deluding attack. For instance, the energy market can be one of the targeting purposes of hackers to deceive an amount of energy in order to acquire the economic profits over the energy exchanging among participants. To elaborate on FDIA model, let us assume that the hacker is able to make access to the data through the relevant communications in the system. Keeping this in mind, the problem function is indicated by (1) in which X and S are defined as the data and objective function for the system, respectively. Making altered data by an attacker, the problem function of system (S) is turned into the new function ($S\gamma$) in which X_{bad} is the manipulated data as shown in (2). In order to get into a successful FDIA, it is essential that the residue norm pertaining to the false function should be zero or a slight error in comparison with the function one as that it is shown in (3).

$$S = h(X_t) \tag{1}$$

$$S_\lambda = h(X_{bad,t}) \tag{2}$$

$$\left\| S_\lambda - h(X_{bad,t}) \right\| = \| S - h(X_t) \| \tag{3}$$

Also, FDIA assessment can be checked by using a significant criterion defined as follows:

$$\lambda = h(X_t + c_{t=\kappa}) - h(X_t) \tag{4}$$

where c donates the injected malicious data at time κ and λ is the structured attack vector, by which hacker can check the needed variation to get into a successful FDIA. To make a targeting attack, the injected false data is defined as below:

$$X_{bad,t} = \begin{cases} X_t + c_t & if\ t \geq \kappa \\ X_t & otherwise \end{cases} \tag{5}$$

where index κ is described as the change-time for injecting false data in the system.

B. THE PROPOSED DETECTION METHOD BASED ON IPS-RL APPROACH

In the literature, the learning machine technology can be mainly used in classification cases in order to declare attacks in the different ways, i.e. the supervised learning, unsupervised learning and RL, which is introduced as the most important and effective method in the classification cases [42]. In other words, the learning phase of RL method is more general than other models due to interaction with environment to achieve a special goal. The RL method performance is shown in Fig. 1. As it can be seen, the RL approach mainly comprises of two general parts: 1) agent 2) environment. In the learning phase of RL method, the agent should choose an effective action with regards to the environment condition. Then, the agent receives a scalar feedback signal

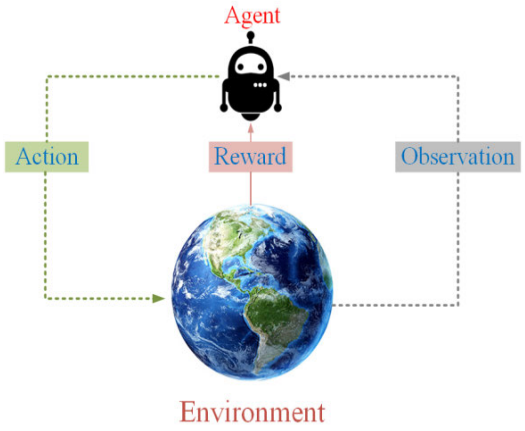

FIGURE 1. The reinforcement learning approach.

named the reward from environment considering the selected action in interaction with environment. This trend is achieved to get into the received maximum reward by the agent. It is vital to say that the environment may be unknown from the respective of agent and it should choose the best action even in the stochastic and uncertain conditions of the environment. Accordingly, at each step t related to the learning phase, each of the RL elements briefly serves as follows:

The agent: 1) Executes action 2) Receives observation 3)Receives scalar reward.

The environment: 1) Receives action 2) Emits scalar reward 3) Emits observation.

Hence, this section concentrates on providing an appropriate attack detection approach based on the RL method using the observable Markov decision process (POMDP) concept. Also, the detection method is developed by an Intelligent Priority Selection algorithm to get into two main goals, including the minimum detection delay and attack alarm. It is needed to first present a POMDP setting before explaining the proposed IPS-RL method. Given an environment and an agent, a POMDP problem is described by using different elements, i.e. the set of states (hidden) of the environment (s), set of observations (o), and set of transition probabilities among states (T), set of rewards (r), and set of actions (a). Note it that in a POMDP problem, the environment is defined in an invisible state. After determining the observation of the environment with regards to the current state, the agent chooses an appropriate action and receives a reward from the environment depending on its selected action and current state at each time t. Then, the environment tries to take the next state (s_{t+1}) by considering the probability pertaining to s_{t+1}. This is continued until the environment reaches a terminal state.

To clarify the proposed method, it is essential that the attack detection problem is explained as a POMDP function in the first place and then suggests the solution approach to get into the main goals described before. Let us assume that a hacker tries to launch a malicious attack to the system with unknown strategy at time κ. The detection function is aimed to minimize the detection delay and declare the attack.

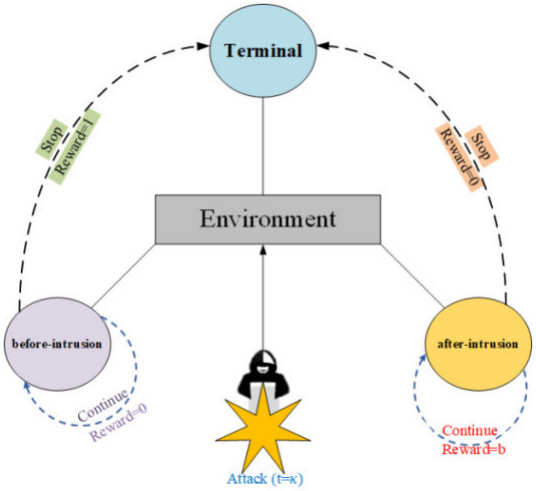

FIGURE 2. The cyber-attack detection scheme.

The proposed function, in fact, can be considered as a POMDP problem by defining actions, rewards and states related to problem (see Fig. 2).

Since the attack strategy is unknown, the environment hidden states are based on the "before-intrusion", "after-intrusion" and "terminal" states. At each time t, the agent is permissible to select two actions of "continue" and "stop" in each state. The agent can choose the "stop" action to move from the present state (before-intrusion or after-intrusion) to "terminal" state and declare the attack. On the other hand, the current state will be per-state if the agent decides to select the "continue" action. It receives the different rewards arising from the action choice in each state. Let us assume that the rewards *1* and *0* are considered as penalty coefficients for action selecting of "stop" and "continue" in "before-intrusion" state when the environment is under normal condition, respectively. Once attack is occurred in the environment, if the agent selects the "continue" action in "after-intrusion" state, it would take the penalty coefficient b due to the detection delay in "after-intrusion" state. Keeping the above argument in mind, the objective function of agent is to minimize the sum of the penalty coefficients emanating from action election for all states. Considering the environment observations, the agent tries to provide the stopping time at which the attack is launched. To this end, the objective function of the agent is developed as below:

$$minR^{penalty} = E^{\kappa}\left[(r_t|t_s < \kappa_t) + \sum_{t=\kappa}^{\infty} b|t_s > \kappa_t\right] \quad (6)$$

Let t_s shows the stopping time and $R^{penalty}$ is defined as the expected value of the penalty coefficient received by the agent. As it can be seen, the objective function includes two main terms pertaining to the received rewards before and after time κ. In the first term, the agent takes the penalty coefficient for the sake of selecting the "stop" action at time $t_s < \kappa$. On the contrary, the second term donates the sum of the

TABLE 1. The learning phase.

Initialize $P(o, a)$ with arbitrary action-observation pair,
for $s=1:S$ Episode
$t=0$
U="before-intrusion" state
Select "continue" action and an observation relaying to the "before-intrusion" state.
for $t=1:T$
$t=t+1$
if a^t="stop" and $t<\kappa$
$r^t=1$.
U^t="terminal" sate.
$P^t(o^t, a^t) = P(o^t, a^t) + \alpha(r^t - P^t(o^t, a^t))$.
end
if a^t="continue" and $t>\kappa$
$r^t=b$.
U^t="after-intrusion" sate.
else
$r=0$.
end
obtain Xt and compute observation signal (o^{t+1})
Select the optimal action (a^{t+1}) based on the observation signal (o^{t+1}) by using ε-greedy policy.
Update the action value (P^{t+1}) by relaying to SARSA algorithm as follows:
$P^t(o^t, a^t) = P(o^t, a^t) + \alpha(r^t + P^{t+1}(o^{t+1}, a^{t+1}) - P^t(o^t, a^t))$.
Revise Y table (that is being learned).
$o^t=o^{t+1}$
$a^t=a^{t+1}$
end
end

TABLE 2. The detection phase.

Input Y table trained by the first phase.
U="before-intrusion" state
Select "continue" action and an observation relaying to the "before-intrusion" state.
for $t=1:T$
$t=t+1$
if a^t="stop"
$t_s=t$ the stopping time
Declare attack.
end
obtain Xt and compute observation signal (o^{t+1})
Select the optimal action (a^{t+1}) based on the observation signal (o^{t+1}) by using ε-greedy policy.
Update the action value (P^{t+1}) by relaying to SARSA algorithm as follows:
$a^t=a^{t+1}$
end

penalty coefficients taken by the agent due to the "continue" action choice in the "after-intrusion" state at time $t_s > \kappa$.

After providing the proposed problem, it is needed to describe an effective solution method to get into the main goals, including the detection delay minimizing and attack alarm as described in [38]. The proposed method contains two underlying phases, 1) learning phase 2) detection phase, as shown in Table 1 and Table 2. The first phase is developed with regards to the proposed problem and is aimed to learn an action value, shown by $P(o,a)$, for each action-observation pair with many experience episodes. All learning action values are saved in Y table to deploy in the second phase. Based on Table 1, it is needed to first define an arbitrary action and observation based on the "before-intrusion" state (U) at time 1. After collecting X_t, the observation signal (o^{t+1}) is determined by using the estimate of likelihood φ_t for time $t+1$. Then, the optimal action (a^{t+1}) for o^{t+1} is obtained with regards to ε-greedy policy, opting the action with the minimum action value (P) and probability 1-ε. Also, the current action value is updated by using SARSA control algorithm, which can perform well over PODMP problem [38].

As the last step, the Y table is revised with the new action value P and the action-observation pair are updated to determine and check the new reward value and state for times $t < \kappa$ and $t > \kappa$ (refer to Table 1). This training procedure continues until the "stop" action is chosen for all episodes. The second phase concentrates on detecting the unknown attack in accordance with trained Y table by the learning phase as indicated in Table 2. In other words, this phase determines the stopping time t_s and declares the online attack with "stop" action choice. All to all, according to the proposed method, the agent is developed to train in such a way that the optimal action is chosen with regards to the minimum penalty coefficient. Such as the trained agent can be able to detect the online attack in the shortest stopping time. It should be mentioned that the action value updating based on the SARSA algorithm is notably dependent on a coefficient α, which is an efficient and significant coefficient to get into an optimal learning phase. Let us employ an appropriate approach based on Intelligent Priority Selection (IPS) algorithm with the aim of optimizing the α value.

C. INTELLIGENT PRIORITY SELECTION ALGORITHM

This document offers a different strong algorithm to assign the value of α to the learning method optimization. Different techniques are created and commonly employed to solve optimal problem depending on mathematical modeling or artificial intelligence [43]. But then again, long solving time and inadequate precision are dictated by the use of mathematical modeling and artificial intelligence tools. This document additionally recommends a new and strong method relying on stochastic approaches to improve precision and to efficiently decrease the overall runtime, simultaneously. Firstly, in statistical point of view, the number of combinations of N things taken n is defined as follows:

$$\binom{N}{n} = \frac{N!}{(n!).(N-n)!} \tag{7}$$

The mentioned equation demonstrates that the sample space consists of a large amount of possible results for choosing n samples from N. In this model, the answer would be precise by using the brute force search, but the method takes a long time owing to the huge sample space. To solve such an issue, the model suggested will smartly decrease and limit the amount of sample spaces. In this respect, it is the following measures that indicate the suggested technique of optimization:

Step1: First, assume that the primary set P of the possible choices includes the optimal values of the issue. The vector K matrix for the control variables is randomly defined in the first step. The remaining candidate points (P-K) are shown in the set W. All possible sets were subsequently replaced by the sets of K members for each of the W members, resulting in the matrix KT being created. As defined in (11), each part of the set H is computed by the replacement of the i-th member of the W into the set K which is then followed by calculating the optimal value of the objective function among the members of the i-th H_{W_i}, defined as $F^{best}_{W_1,K'_n}$. It is worth to say that K'_n in (13) shows the n-th element of the K which is replaced by the elements of the W. Eqs (8)–(11), as shown at the bottom of the page.

The components of i-th H_{W_i}, as shown in (12)-(13), are arranged according to the objective function value. The components of matrix W are ranked according to the objective function. The W'_j matrix is shown as an array of the W matrix components (14) which was discussed earlier. This discussion is also correct for set K''_j (15). In this step, the price of the object function for W'_1 is chosen, ultimately, as the optimal answer (17).

$$F^{best}_{m} = \begin{bmatrix} F^{best}_{w_{1,k''_1}} \\ \cdot \\ \cdot \\ F^{best}_{w_{m,k''_m}} \end{bmatrix} \quad \forall m \in \Omega^m \tag{12}$$

$$F^{best\_sort} = \begin{bmatrix} F^{best}_{w'_1 \to k''_1} \\ \cdot \\ \cdot \\ F^{best}_{w'_m \to k''_m} \end{bmatrix} \tag{13}$$

$$w'_j = [w'_1, \ldots, w'_m] \quad \forall m \in \Omega^m \tag{14}$$

$$k''_j = [k''_1, \ldots, k''_m] \quad \forall m \in \Omega^m \tag{15}$$

$$F = F^{best}_{w'_1 \to k''_1} \tag{16}$$

Step 2: The new KT (KT^{new}_r) matrix is obtained at this stage. First of all, the W_j matrix is updated based on (17) with the W'_j matrix components. As the W'_1 is the best option in the earlier iteration, W'_2 as stated in (17) initializes this step. $K1^{new}_j$ is described by removing the k''_j and w'_j components from the K_j matrix (18). The new KT^{new}_r component (same as (11)), is generated from all these possible sets as a result of substituting each component of W_j with a component of $K1^{new}_j$. In KT^{new}_r and w'_j, the combination of sets is represented as ψ_r where r is between 1 and $m-j$, in which j is the number of iteration and m is a constant value, referring to the matrix length of W in the first step, as described by (19). For each member of ψ_r, the objective value is computed and the optimal result of the objective function ($F1^{Best}$) and the associated component is stored as (20) and (21) respectively in matrix ψ_r (ψ^{Best}). The matrix K is modified by ψ^{Best} in (22) for each iteration as defined in (23).

$$W_j = w'_{j+1} \quad \forall j \in \Omega^j \tag{17}$$

$$K1^{new}_j = \left\{ x \,\middle|\, x \in K_j, x \neq k''_j, x \neq w'_j \right\} \quad \forall j \in \Omega^j \tag{18}$$

$$\psi_r = KT^{new}_r \cup w'_j \tag{19}$$

$$r = \{1, 2, \ldots, m-j\}$$

$$F1_r = f(\psi_r) \tag{20}$$

$$F_j = F1^{Best} \quad \forall j \in \Omega^j \tag{21}$$

$$K_j = \psi^{Best} \quad \forall j \in \Omega^j \tag{22}$$

$$P = [p_1, \ldots\ldots, p_N] \tag{8}$$

$$K = [k_1, \ldots\ldots, k_n] \tag{9}$$

$$W = [w_1, \ldots\ldots, w_m] \tag{10}$$

$$KT = \begin{bmatrix} \not{k}_1 = k'_1 & & & \not{k}_1 = k'_1 \\ \uparrow & & & \uparrow \\ w_1 \quad k_2 \ldots k_n & & & w_m \quad k_2 \ldots k_n \\ \not{k}_2 = k'_2 & & & \cdot \\ k_1 \quad w_1 \ldots k_n & \} H_{w_1} \ldots & & \cdot \quad\quad\quad \} H_{w_m} \\ \not{k}_n = k'_n & & & \not{k}_n = k'_n \\ k_2 \quad k_2 \ldots w_1 & & & \uparrow \\ & & & k_1 \quad k_2 \ldots w_m \\ \downarrow & & & \downarrow \\ F(H_{w_1}) = F^{best}_{w_{1,k''_1}} & & & F(H_{w_m}) = F^{best}_{w_{m,k''_m}} \end{bmatrix},$$

$$H_{w_i} = \left[H_{w_1}, H_{w_2}, \ldots, H_{w_m}\right] \forall i \in \Omega^i$$

$$k''_M = [k'_1, k'_2, \ldots, k'_n] \forall M \in \Omega^M \tag{11}$$

Step 3: The last component in each iteration is chosen as the optimal one among the others.

$$F^{best\_total} = F^{Best} \tag{23}$$

Figure 3 summarizes the flowchart of the suggested optimization algorithm.

III. PROPOSED PEER-TO-PEER ENERGY TRADING FORMULATION

As mentioned before, hackers tend to disorganize the energy market for the sake of gaining more economic benefits. In the view of the fact, the online data pertaining to the energy market is usually indicated with the use of data estimator and the market operator transfers the data to the estimator by using the communication channels [44]. For this reason, these channels may increase the risk of cyber-attack in the energy market.

In other words, if a malicious hacker can intrude to the communication channels, the data taken by the estimator and consequently the results of the energy market will be affected. But, this situation can be grossly more vulnerable in the energy market based on the peer to peer structure compared to the centralized one owing to more communication ways [45]. To overcome this issue, we want to develop the effective IPS-RL method based detection scheme for the energy market, carrying out on the peer to peer framework. Hence, it is required to present the proposed peer to peer energy trading structure in this paper. Let us assume that the three microgrids, consisting of the different renewable energy resources, i.e. wind turbine (WT), photovoltaic (PV), tidal system, fuel cell unit and storage unit, tend to exchange their energies each other in order to maximize their economic benefits. To this end, this paper investigates and formulates an appropriate RCI method based peer to peer energy trading scheme for three microgrids connected in form of peer to peer structure. To make it clear that how the RCI method works, let us first provide the centralized structure of the proposed problem.

A. PROBLEM FORMULATION DEFINITION BASED ON CENTRALIZED STRUCTURE

In this section, we intend to introduce and formulate the infrastructure of the proposed model, consisting of three microgrids in such a way that each microgrid can exchange its energy with others for gaining more economic benefit. The first microgrid includes a PV unit, two TWs, a tidal system, storage unit and some loads satisfied by the generation units. Also, the other microgrids to supply their loads employ some renewable energy resources, i.e. two WTs, a fuel cell unit, two tidal system and battery unit related to the second microgrid and a fuel cell system, three PVs and storage unite for the third microgrid [46]. Let us assume that the communication ways among microgrids are assigned in order to transfer the energy. Also, a central operator is considered aiming to manage the power transaction among microgrids. Keeping this discussion

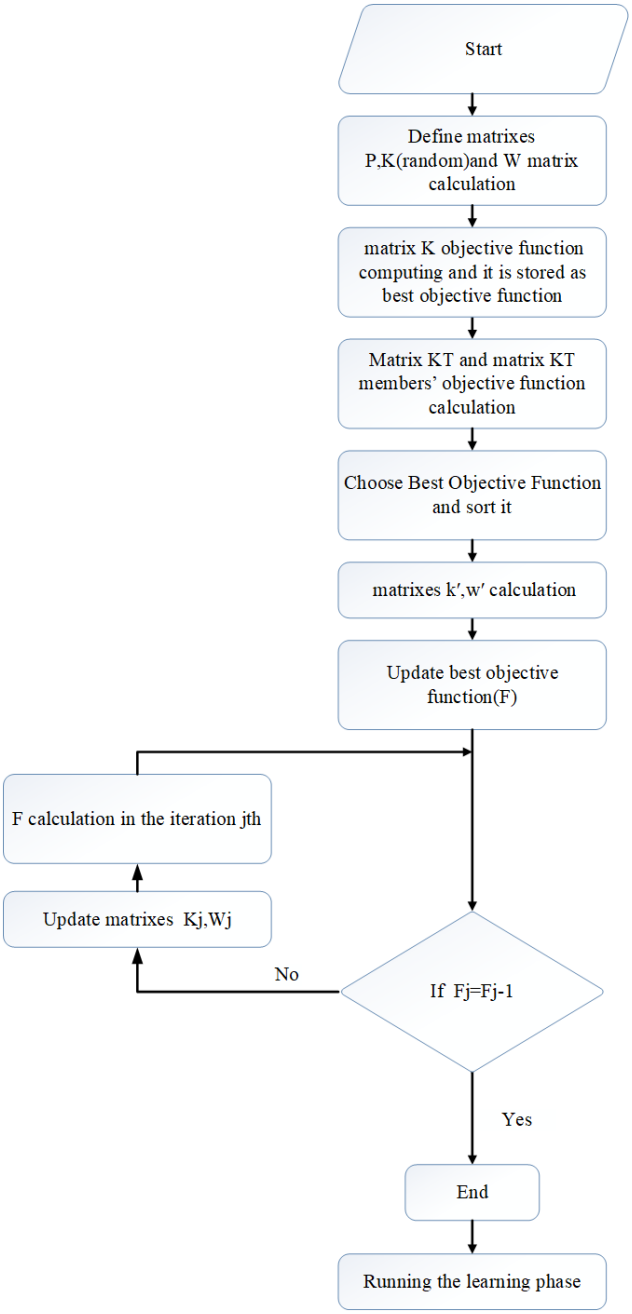

FIGURE 3. The flowchart of the proposed IPS algorithm.

in mind, the formulation of each microgrid can be explained as follows:

1) MULTI-MICROGRID FORMULATION

Technically, the objective function of each microgrid is aimed to minimize the cost of self-generation units with the use of the energy exchanging with the other microgrids as shown in (24)-(26). To clarify the cost function of microgrid, it is needed to describe some explanations here. The total power generation of microgrid includes sum of power produced by the energy units. Keeping this argument in mind, the cost function of each microgrid comprises of two main parts.

The first part is related to the maintenance and investment costs of each renewable energy unit deployed into microgrid structure which is conformed to reference [45]. The cost of trading power which is supplied by these the renewable energy units, makes the second part of the cost function. The last term of equation (24) follows the relevant power transaction cost to microgrid *2* and microgrid *3*. By focusing on (24), the positive values of P^{12} and P^{13} imply to transfer and consequently purchase the power from microgrids 2 and 3 to microgrid 1 and vice versa. Similar to the explanation related to microgrid 1, the objective functions of microgrid *2, 3* are delineated by (25)-(26). From the above-mentioned considerations, the diverse renewable resources, i.e. WT, PV, fuel cell, tidal turbine and storage units are employed in the system to bring the needed power of load demands. The power generation limits for WT, tidal unit and PV are defined by (27)-(29). Also, the output power of fuel cell unit is modeled by using the current and voltage of the connected power electronic device into the fuel cell unit, as shown in (30) and (31). Based on (27), the WT can generate power in compliance with wind speed such that the power value will be zero if the wind speed is less than a particular range (called cut-in speed value). Similar to the WT power, the power generation of the tidal system depends on the tidal current as indicated in (28) [47]–[50]. Equation (29) describes the PV power generation regarding to the solar radiation. The limits related to the charging/discharging of storage unite can be followed by (31)-(35). It is well accepted that the energy management of each microgrid is mainly to provide the power balance between its generation units, power transaction and load to get into the objective function, as shown in (36)–(38).

$$mic^1 = min \sum_{t\in\Omega^T} CTI_t^1 TI_t^1 + CPV_t^1 PV_t^1 + CB_t^1 PB_t^1 + \sum_{i=1}^{nw} CW_{t,i}^1 PW_{t,i}^1 + C1P_t^{12} + C2P_t^{13} \tag{24}$$

$$mic^2 = min \sum_{t\in\Omega^T} \sum_{i=1}^{nt} CTI_{t,i}^2 TI_{t,i}^2 + CFC_t^2 FC_t^2 + CB_t^2 PB_t^2 + \sum_{i=1}^{nw} CW_{t,i}^2 PW_{t,i}^2 - C3P_t^{12} + C4P_t^{23} \tag{25}$$

$$mic^3 = min \sum_{t\in\Omega^T} CFC_t^3 FC_t^3 + CB_t^3 PB_t^3 + \sum_{i=1}^{nv} CPV_{t,i}^3 PV_{t,i}^3 - C5P_t^{13} - C6P_t^{23} \tag{26}$$

$$PW_t = \begin{cases} 0 & 0 \le S^W \le S^W_{rated} \\ \varphi(S_t^W) & S^W_{cutin} \le S^W \le S^W_{rated} \\ & \forall t \in \Omega^T \\ PW_{rated} & S^W_{rated} \le S^W \end{cases} \tag{27}$$

$$TI_t = \begin{cases} 0 & 0 \le T_t^V \le T^V_{rated} \\ 0.5P\gamma\lambda\left(T_t^V\right)^3 & T^V_{cutin} \le T_t^V \le T^V_{rated} \\ & \forall t \in \Omega^T \\ TI_{rated} T^V_{rated} & \le T_t^V \end{cases} \tag{28}$$

$$PV_t = \frac{Q \times U_t}{Z} \times (1 - R^{loss}) \quad \forall t \in \Omega^T \tag{29}$$

$$P_{FC,t} = V_t^{fc} I_t^{fc} \quad \forall t \in \Omega^T \tag{30}$$

$$FC_t = V_t^{fc} I_t^{fc} + R(I_t^{fc})^2 \quad \forall t \in \Omega^T \tag{31}$$

$$VB_t = VB_{t-1} + PB_t \Delta_t \eta^{Bat} \quad \forall t \in \Omega^T \tag{32}$$

$$PB_t = PB_t^{ch} - PB_t^{dis} \quad \forall t \in \Omega^T \tag{33}$$

$$P^{\min} \le PB_t \le P^{\max} \quad \forall t \in \Omega^T \tag{34}$$

$$V^{\min} \le VB_t \le V^{\max} \quad \forall t \in \Omega^T \tag{35}$$

$$TI_t^1 + \sum_{i=1}^{nw} PW_{t,i}^1 + PV_t^1 + PB_t^1 + P_t^{13} + P_t^{12} = P_t^{load1} \quad \forall t \in \Omega^T \tag{36}$$

$$\sum_{i=1}^{nt} CTI_{t,i}^2 TI_{t,i}^2 + \sum_{i=1}^{nw} PW_{t,i}^2 + PB_t^2 + FC_t^2 + P_t^{23} = P_t^{load2} + P_t^{12} \quad \forall t \in \Omega^T \tag{37}$$

$$PB_t^3 + FC_t^3 + PV_t^3 = P_t^{load3} + P_t^{13} + P_t^{23} \quad \forall t \in \Omega^T \tag{38}$$

It is needed to say that the power transaction variables, which are P^{12} and P^{13} and P^{23}, should be only deployed in either generation or demand side of the power balance for each microgrid. According to the balance equation of microgrid 1, the variable P^{12} is assigned to the demand side of the power balance of the microgrid 2. This means that the power is exchanged from microgrid 2 to microgrid 1 if the value of P^{12} is positive and consequently it is shown with negative indication in the objective function of microgrid 2 (see equation (27)). This explanation can mainly be expanded for the power transaction between microgrids 2 and 3.

B. RCI BASED PEER TO PEER ENERGY TRADING FRAMEWORK

In the literature, the RCI based p2p trading has been presented in order to only determine the trading power in energy market. But, according to the growing occurrence of malicious attacks, there is needed to develop the p2p based energy trading framework in such a way that the relevant data should be secured to prevent the probable threats. In other words, Since the energy exchange based on the peer to peer structure and without a safe decision center is accomplished, participates (each microgrid) need not only to get into an acceptable agreement but also their information related to energy transaction are broadcasted in a secure environment. In this regard, the main goal of providing this paper is development of an effective framework to guarantee the

energy transaction trust in the peer to peer energy trading. To do this, we tried to develop a RCI based secured algorithm in order to cover both the data security and energy trading. Let us assume that the microgrids are connected to each other in the form of the peer to peer structure. The proposed RCI algorithm can guarantee to get into an acceptable power/price transaction among microgrids in such a way that the objective function of each microgrid is optimality satisfied.

In the RCI method, the master problem is solved by using two sub-problems similar to the dual approach [47]. The solution of each sub-problem should be converged to get into the global solution of the main problem. To make an effective agreement among the participants, the RCI method is developed to solve the problem by considering the Karuch-Kuhn-Tucker (KKT) conditions. Comparing this method with the dual ascent approach, a gradient function is added to the objective function of the problem to improve the solving procedure. On the other hand, all participants can make an appropriate agreement for both the power and price transactions in the RCI structure, carrying out a direct method to converge the sub-problems [47]. In addition, the Lagrangian Relaxation is used in order to limit the power boundary in the RCI method. Keeping the above argument in the mind, the objective function of the RCI algorithm in accordance with the proposed multi-microgrids structure can be developed as follows:

$$min \sum_{j=1}^{m} mic^{j} + R_t^{jj'} \left(P_t^{jj'}\right) - P_t^{jj'^{T}} \beta_t^{jj'} + \bar{H}_t^{j} \left(P_{j,t} - \overline{P}_j\right) - \underline{H}_t^{j} \left(\underline{P_j} - P_{j,t}\right) \quad (39)$$

$$(27) - (38) \quad (40)$$

$$P_t^{jj'} \geq 0, P_t^{jj'} \leq 0, \quad (41)$$

$$\beta_t^{jj'(k+1)} = \beta_t^{jj'(k)} - X^k (\beta_t^{jj'(k)} - \beta_t^{j'j(k)})\_\kappa^k \times (P_t^{jj'(k)} + P_t^{j'j(k)}) \quad \forall t \in \Omega^T \quad (42)$$

$$\bar{H}_t^{j(k+1)} = \max\left(0, \bar{H}_t^{j(k)} + \xi^k \left(P_{j,t} - \overline{P}_j\right)\right) \quad \forall t \in \Omega^T \quad (43)$$

$$\underline{H}_t^{j(k+1)} = \max(0, \underline{H}_t^{j(k)} + \xi^k \left(\underline{P_j} - P_{j,t}\right)) \quad \forall t \in \Omega^T \quad (44)$$

$$PS_{j,t}^{k+1} = \frac{-b_j + \beta_t^j - \bar{H}_t^j - \underline{H}_t^j}{a_j} \quad \forall t \in \Omega^T \quad (45)$$

It is important to first mention that as it can be shown, Equation (39) shows the total objective function of the RCI algorithm that the first part of this equation describes the objective function of each microgrid (mic^j) in which j indicates a microgrid in the proposed p2p framework. Also, the exchanging cost for each microgrid j is defined based on the second/third terms. In this regard, $P_t^{jj'}$ and $\beta_t^{jj'}$ donate the power/price transactions from microgrid j to microgrid j', respectively. The updating trend of the relevant problem variables in the RCI method is served with the use of the relaxed largrangian function and KKT conditions. To do so, the last term of the objective function is assigned to the slackness function to satisfy the condition related to the updating procedure. Equation (40) demonstrates the operation constraints of three microgrids mentioned in the previous section. Also, equation (41) shows that $P_t^{jj'}$ can take both positive and negative values. The price exchanging among microgrids is updated based on the $\mathcal{X}^k/\kappa^k$ coefficients as defined in (42). It is needed to say that the power transaction value is notably efficient on the updating trend of price. For this reason, the appropriate value of κ^k coefficient can help to converge process as much as possible. Based on (43) and (44), the slackness variables are calculated regarding the limitation of the power transaction.

To update the power transaction for each microgrid j, it is needed to first define a power set point based on the Lagrangian function of the relaxed problem and the inverse gradient. With doing this, the power set point of each microgrid j is determined by (45). By focusing on (46), the updating trend of the power exchanging among microgrids would be developed and defined in (44) in which $R_t^{jj'(k)}$ coefficient is calculated using (47).

$$P_t^{jj'(k+1)} = P_t^{jj'(k)} + R_t^{jj'(k)} \left(PS_{j_t}^{k+1} - P_{j,t}^k\right) \forall t \in \Omega^T \quad (46)$$

$$R_t^{j(k)} = \frac{\left|P_t^{jj'}\right| + \gamma^k}{\left|P_{jn}\right| + \gamma^k} \forall t \in \Omega^T \quad (47)$$

It is significant to say that the RCI algorithm has converged when iterative process is stopped. To this end, the terminating condition needs to be determined for the RCI algorithm that is represented as below:

$$\beta_t^{jj'(k+1)} - \beta_t^{jj'(k)} < \varepsilon \quad (48)$$

$$P_t^{jj'(k+1)} - P_t^{jj'(k)} < \gamma \quad (49)$$

$$H_t^{j(k+1)} - H_t^{j(k)} < \tau \quad (50)$$

As mentioned already, the proposed p2p framework is made of microgrids, each which has the different generation unit for supplying load demands. This means that each microgrid regarding type of generation unit needs to bring its power set point for getting an optimal power transaction in the p2p algorithm. Hence, behave of each microgrid considering the generation unit differentiation can be effective and significant into the converging procedure of the proposed p2p algorithm.

Note that this work considers the objection function and the constraints of generation units including the power balance and generation limitation related to each microgrid in the p2p energy trading process (see equations (39) and (40)). This means that the operator of each microgrid can execute its system operation in decision making process simultaneously. In addition, the multi-microgrid structure is designed in such a way that each of microgrid is able to balance and supply the power generation and load demand without getting involved in the p2p energy trading framework. All to all, given the peer to peer energy trading based on the RCI algorithm, it is needed to guarantee the security of data exchanging between microgrids with the IPS-RL based detection scheme against the malicious attacks as shown in Fig. 4.

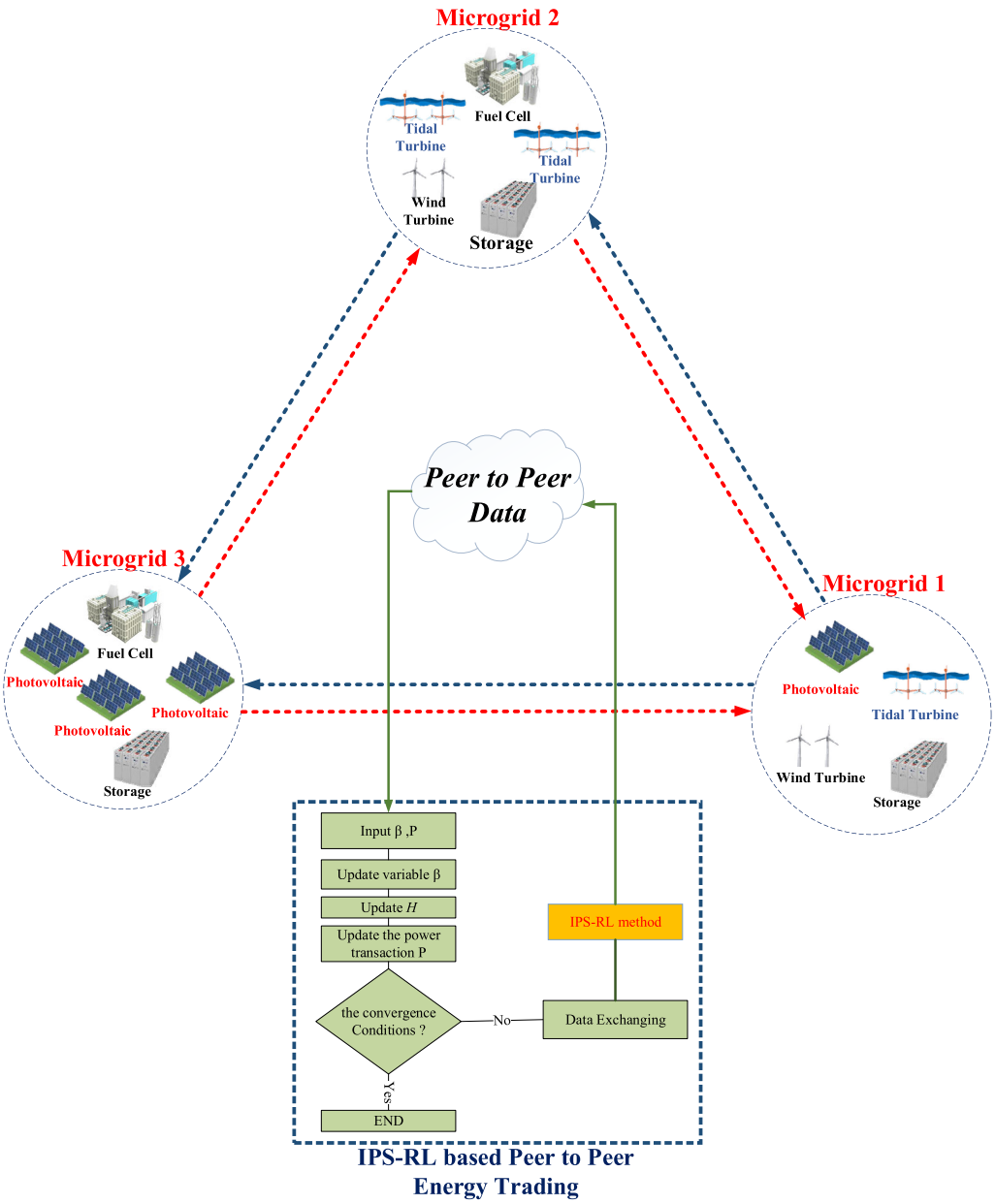

FIGURE 4. The IPS-RL based the RCI algorithm.

IV. UNCERTAINTY MODEL BASED ON UNSCENTED TRANSFORM METHOD

According to the uncertain output of the renewable energy resources, it is significant to investigate a close look at their effects on the energy trading process. To this end, this section aims to model the uncertainty effects by using UT method. It is important to say that the proposed model can model correlation among the uncertainty parameters, which are the solar radiation, wind speed, tidal current and loads. The UT model is defined by $U = \hat{f}(R)$ through $2p+1$ different sample points. Such method uses the normal distributed function in order to model each variable regarding the mean and standard deviation values related to variable which is depicted by m and σ. The UT method process can be described through steps (1) to (3):

Step 1: $2p + 1$ points can be computed by (51)-(53) as follows:

$$R^0 = m \tag{51}$$

$$R^k = m + \left(\sqrt{\frac{p}{1 - W^0}A_{aa}}\right)_k \quad k = 1, 2, \ldots, p \tag{52}$$

$$R^{k+p} = m - \left(\sqrt{\frac{p}{1 - W^0}A_{aa}}\right)_k \quad k = 1, 2, \ldots, p \tag{53}$$

where A_{aa} shows the covariance matrix and $\bar{R} = m$.

Step 2: Weight of points calculated by (52):

$$W^k = \frac{1 - W^0}{2c} \quad k = 1, 2, \ldots, 2c \tag{54}$$

Note that the sum of the weights should be equal to 1.

Step 3: By inserting the points calculated by step 1 into the nonlinear function $U^k = \hat{f}(R^k)$, the output values are determined by:

$$\overline{U} = \sum_{k=0}^{2p} W^k U^k \tag{55}$$

$$P_{FF} = \sum_{k=1}^{2p} W^k \left(U^k - \overline{U}\right)\left(U^k - \overline{U}\right)^T \tag{56}$$

V. PERFORMANCE EVALUATION

This section aims to assess and validate the online anomaly detection scheme based on the proposed IPS-RL method for a P2P based energy management structure against malicious attacks. To this end, we try to first implement an RCI approach based energy trading structure for three microgrids connected in form of the peer to peer framework. Then, an attack of FDIA type is launched to the peer to peer energy trading to get into the malicious goals of hacker. Also, we check the security of the proposed RCI algorithm equipped by the IPS-RL scheme for bringing an effective agreement among microgrids against the FDIA attack. In this paper, to accurately obtain the relevant results, we used the experimental sample data (false and correct data) related to the renewable resources which are collected and analyzed in reference [51]. As described before, the three microgrids proposed in this paper contain the renewable energy resources, i.e. the wind turbine, photovoltaic unit, tidal system, fuel cell unit as well as storage unit, aiming to supply the demand loads located in the areas far from the main grid [52]–[56].

It is needed to say that all the simulations are performed in GAMS and MATLAB software and solved on 3.4-GHz windows-based PC with 32 Gbytes of RAM. The above problem based on proposed method is solved and overall mixed integer linear problem (MILP) is obtained by using CPLEX solver. To make the performance of the proposed model clear, the results are exanimated based on different case studies as follows:

Case I: Validating the IPS-RL based online anomaly detection method

Case II: Assessing the IPS-RL based peer to peer energy trading structure under attack condition

Case III: Analyzing the effect of uncertainty on the proposed RCI method

Each case is presented and discussed in detail in the following sections.

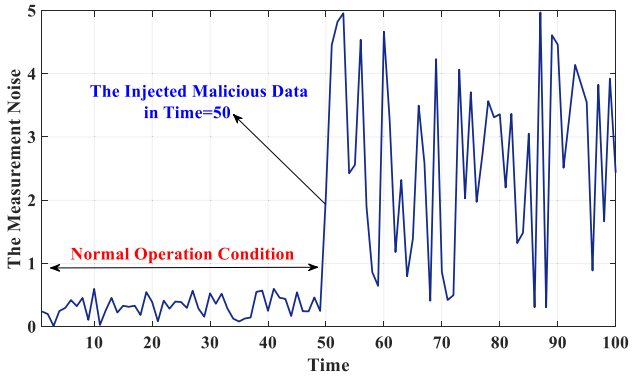

FIGURE 5. The measurement noise under attack condition.

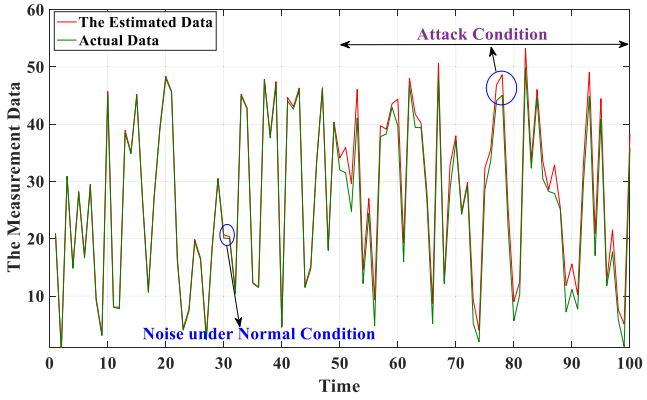

FIGURE 6. The measurement data under attack condition.

A. VALIDATING THE IPS-RL BASED ONLINE ANOMALY DETECTION METHOD

It is significant to first present the validation of the proposed anomaly detection method against the malicious attacks. In this regard, this section concentrates on assessing the IPS-RL based attack detection scheme with the occurrence of an attack of FDIA type. To this end, we model and launch the FDIA attack in the first place and then provide the IPS-RL approach in order to detect the attack. Let us assume that the hacker injected the false data into the system at time $t = 50$ as indicated in Figs. 5 and 6. By focusing on Fig. 5, it can be seen that the measurement noise has a high fluctuation at time $t = 50$. This change can be eminently seen in the estimated measurement data compared with the actual data as demonstrated in Fig. 6. In the case of lack of an attack detection system, the hacker can inject the false data and get into its malicious goals at subsequent times (t>50). To overcome this problem, we implement the proposed detection system based on the IPS-RL method and evaluate the system under attack condition. Fig. 7 shows the noise value related to the measurement device equipped by the proposed detection system when the hacker injected the compromised data into the system at time $t = 50$. The significant point is to check whether the proposed method could satisfy the main goals including the detection delay reduction and attack alarm. To make a clear assessment of

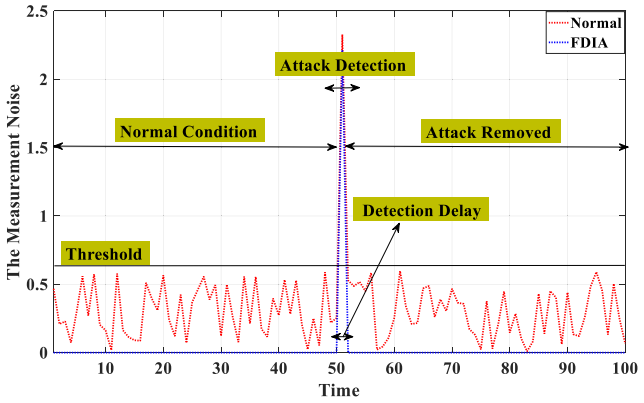

FIGURE 7. The IPS-RL based the RCI algorithm.

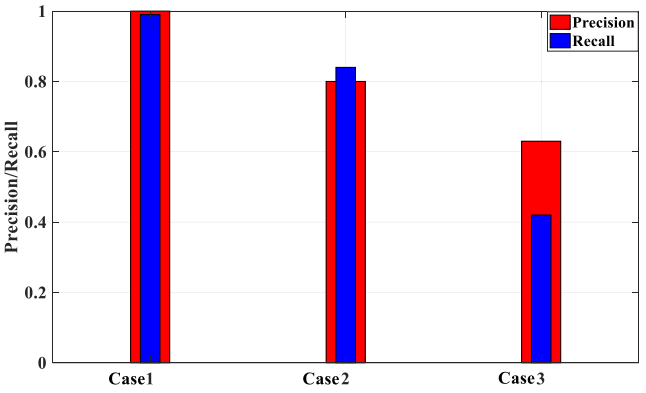

FIGURE 8. The precision/recall of different cases: case1: the proposed model, case2: the RL model, case3: SVM model.

the model, the measurement noise can be indicated in three conditions of normal condition, attack detection condition and removing condition. In Fig. 7, the measurement device provided the normal noise from time $t = 1$ to $t = 49$. After launching attack in time 50, the proposed system could detect the attack at time $t = 51$. By removing attack, the measurement noise is in the normal condition. This result can prove that the FDIA attack is detected and alarmed by the IPS-RL method with a slight delay, which is almost 1(s).

As mentioned already, one of the main goal of this paper is development of a p2p based energy trading framework with the use of making the energy transaction trust of the decentralized structure based system. Hence, there is needed to prove effectiveness and high efficiency of this model in security issue.

To validate this method, we try to compare the proposed model with the other well-known and successful detection models, i.e. the support vector machine (SVM) and the reinforcement learning (RL). Also, the IPS based optimization method used to improve the detection model is compared with the particle swarm optimization (PSO) and genetic algorithm (GA) methods named as PSO-RL and GA-RL. To this end, we computed and provided the precision and recall of 5000 trails for different cases. In this regard, Fig. 8 shows the precision versus and recall curves based on equations (57) and (58) for different cases, including the proposed model, SVM and RL. According to the results, the precision/recall values related to the proposed model are almost close to 1 while these values for the RL/SVM models are 0.8, 0.84 and 0.63, 0.42, respectively. In addition, the F-score value based on (59) is computed for different models such as the IPS-RL, SVM, RL, PSO-RL and GA-RL under 10000 and 5000 trails as shown in Table 3. Given the result of the F-score, the proposed model is more sensitive to distinguish the attack than the other models.

$$Recall = \frac{True\ Positive}{True\ Positive + False\ negative} \tag{57}$$

$$Precision = \frac{True\ Positive}{True\ Positive + False\ pasitive} \tag{58}$$

$$F - score = \frac{2(Precision * Recall)}{Precision + Recall} \tag{59}$$

TABLE 3. The F-score for different models.

		IPS-RL	RL	VSM	PSO-RL	GA-RL
F-Score	Number of Trail=10000	0.9994	0.843	0.572	0.934	0.922
	Number of Trail=5000	0.9997	0.8195	0.5040	0.943	0.9136

B. ASSESSING THE IPS-RL-BASED PEER TO PEER ENERGY TRADING STRUCTURE UNDER ATTACK CONDITION

One of the significant goals of this paper is to preserve the security of the data exchanging in the peer to peer energy system. Hence, this section aims to suggest and evaluate the RCI based secured energy trading with the use of the IPS-RL method, detecting the malicious activities (refer to Fig. 4). To do so, let us first provide the RCI algorithm performance and then follow the security of the energy trading against the FDIA. To better realize the false information injection in the system, it is needed to first express some explanations here. According to the performance of reinforcement learning designed based on two learning and detection phases, the accuracy and optimum of the proposed detection method depends on the number and type of the Trails and experiments trained by the first phase. Hence, to improve the results, we used the experimental sample data related to the renewable resources collected by reference [29]. We execute the RCI method for three microgrids to get into an appropriate agreement and represent the relevant results in Figs. 9-14. Based on Fig. 9, the converging trend between microgrids 2 and 3 is executed in three stages, including high and low fluctuations and steady. In the first stage, the energy trading procedure is continued with a high fluctuating trend because of not being an appropriate power set point for each microgrid. After determining the power set point, the power transaction takes a low fluctuation from iteration 40 to 80. As the last stage, the power exchanging between microgrid 2 and 3 is converged on an accepted power, which is 23.05 kW at time $t = 4$. According to the equations (44) and (53), the positive value of power implies to receive the power from the relevant microgrid and vice versa. This explanation can be followed

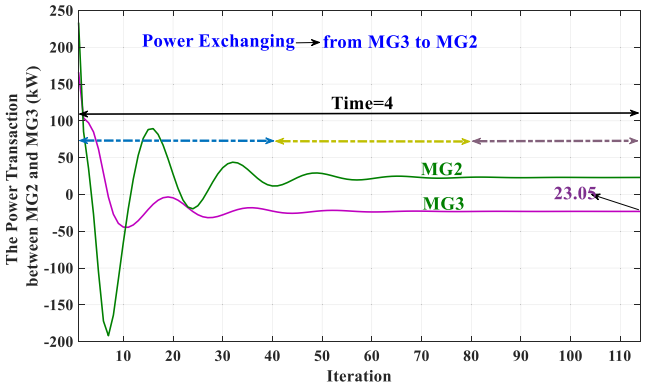

FIGURE 9. The power transaction between microgrids 2 and 3.

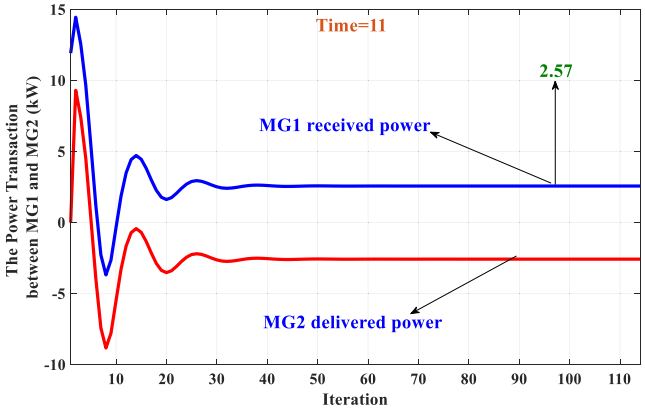

FIGURE 10. The power transaction between microgrids 1 and 2.

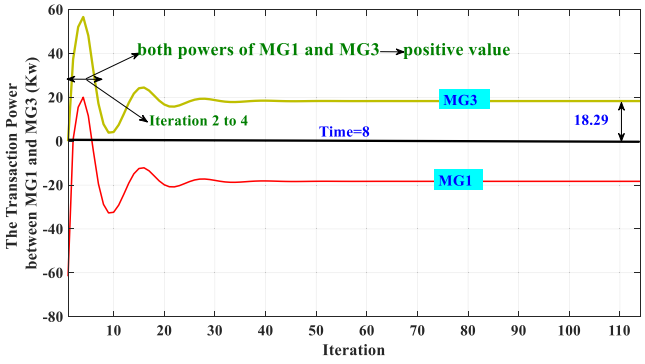

FIGURE 11. The power transaction between microgrids 1 and 3.

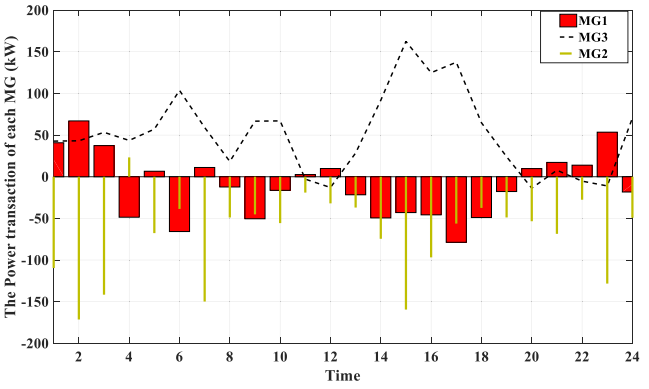

FIGURE 12. The power transaction for microgrids 1 to 3.

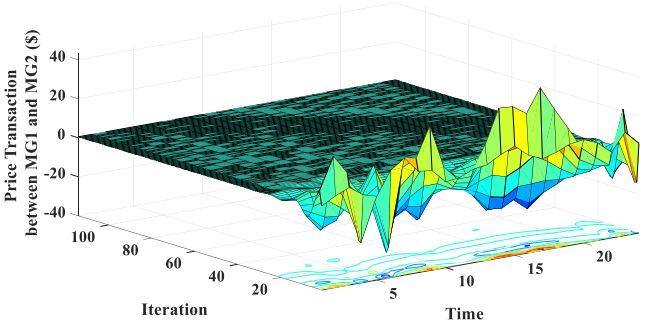

FIGURE 13. The price transaction between microgrids 1 and 2.

for power exchanging between microgrids 1 and 2 as shown in Fig. 10. Based on Fig. 11, the microgrids 1 and 3 settle down on an effective agreement in order to transfer the optimal power, which is 18.29 at time $t = 8$. With regards to the trading process in the primary iteration, it is possible that the power transaction can take the positive value for both microgrids 1 and 3 due to the incompatible power set point. Generally, the power transaction for each microgrid is indicated in Fig. 12 during the 24 hours. As mentioned before, the proposed consensus algorithm is able to converge the trading price among the microgrids, getting into an optimal operation. For instance, let us to report the price exchanging between microgrids 1 and 2, which is approximately obtained 0.49 $. It is important to say that According to equations (24)-(26), the last term of cost function related to each microgrid includes the energy exchanged with the other microgrids by considering the self-energy price. On the other hand, the proposed p2p framework is able to make not only the power transaction but also can calculate the trading price between two microgrids at each time. In this regard, each microgrid can transfer its energy to one which has more suitable energy price than other microgrids with aim of bringing the optimal energy management and cost reduction. Moreover, the converging process of the total operation cost corresponded to the power transaction curves takes 0.14×10^6 after the high fluctuations in iteration 114.

After the RCI algorithm description, it is important to consider a close look at the effects of attack launching in energy trading based on the proposed consensus method. To this end, we launch an attack of FDIA type to the peer to peer energy trading structure, which is equipped by an IPS-RL based security platform, in order to manipulate the power transaction between microgrids 1 and 2 and microgrids 1 and 3 at times $t = 10$ and $t = 13$. The relevant results are demonstrated in Figs. 15 and 16. By focusing on Fig. 15, the hacker injected false data in a given iteration that it causes to disturb the converging procedure of power transaction for microgrids 1 and 3. As it can be shown, the IPS-RL based security platform detected and alarmed the FDIA with a slight detection delay in the next iteration [57]–[59]. To ensure the proposed method performance,

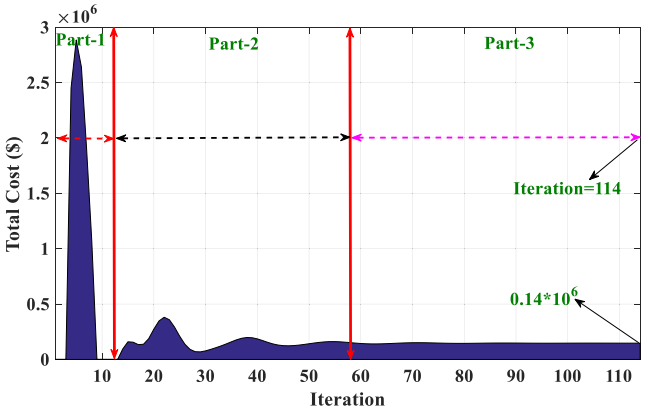

FIGURE 14. The total operation cost.

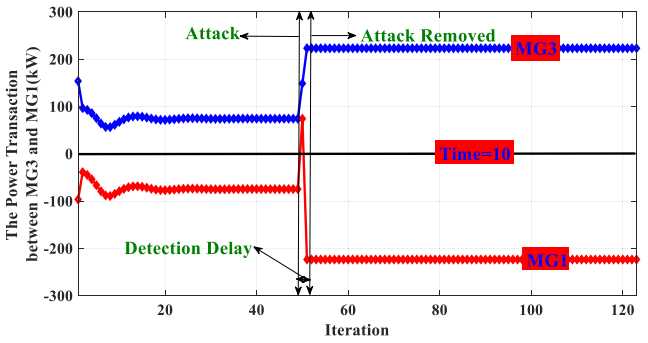

FIGURE 15. The power transaction between microgrids 1 and 3 under attack condition.

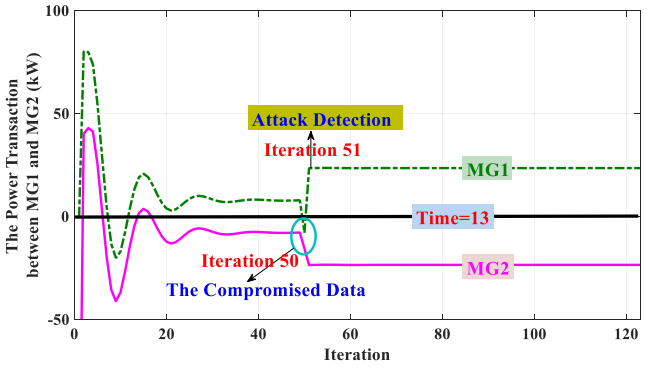

FIGURE 16. The power transaction between microgrids 1 and 2 under attack condition.

the result related to the energy exchanging between the microgrids 1 and 2 under attack condition is reported in Fig. 16. Another goal of this paper is development of a p2p based energy trading framework getting into a nearby global solution based on p2p energy training compared with the centralized. To do this, we valid and compare the proposed energy trading structure to the centralized form of the system in terms of the computing time, iteration number, energy trading efficiency and the variable number as shown in Table 4.

As mentioned before, increasing the cost pertaining to each microgrid is considered as the main goal of hackers by using injection of false data. On the other hand, the part of

TABLE 4. Computation time for proposed analysis.

	Variable Number	Computation Time (sec)	Number of Iteration	Total cost
Centralized method	3601	2148	-	0.112×10^6
Proposed method	3546	1521	114	0.14×10^6

cost function of each microgrid includes the cost of energy transaction determined by the energy trading framework. In this regard, attackers could manipulate data such that the power transferred among microgrids takes an increasing trend which led to rise in the transaction cost for the targeted microgrid. By focusing on these results, it may be concluded that the proposed attack detection scheme can be considered as appropriate and affective detection software, assuring the energy market based on the peer to peer structure against the malicious anomalies. Besides, in Table 4 is shown computational time and number of iteration for the proposed methods. According to Table 4, the total computing time of the proposed method is almost %29 less than another one which means that this method takes an acceptable value in computational efficiency. In addition, the last row in Table 4 indicates comparison of both the centralized and proposed frameworks of this work. According to this Table, the centralized and proposed methods obtained the total operation cost of the studied system as 0.112×10^6 and 0.14×10^6, which are nearly equal. This proves the effectiveness, validity and accuracy of the proposed model in providing a proper P2P based energy trading framework.

C. ANALYZING THE EFFECT OF UNCERTAINTY ON THE PROPOSED RCI METHOD

This part tries to investigate whether the uncertain output of renewable energy resources can change the energy trading performance or not. Hence, this section examinants the P2P energy trading trend in uncertainty condition and highlights the effects of uncertainty on the power transaction among microgrids compared with the normal condition. To this end, we implement UT model on the proposed consensus algorithm and see the consequence related to the operation cost of each microgrid and the total operation cost for both the deterministic and stochastic conditions as indicated in Figs. 17 and 18. As it is mentioned, each microgrid should be responsible for supplying its load demands in operation process. Since the load power of microgrid 2 is more than the other microgrids, it is clear that this microgrid needs to get more power generation through the energy units and the power transaction to other microgrids. This work leads to increase the cost of microgrid 2 (see Fig. 17). It is possible that the uncertainty effect makes an increase in the operation cost of each microgrid compared to the normal condition. For instance, with regards to Fig. 17, the operation cost of microgrid 2 has an increasing change from $\$1.2 \times 10^5$ to $\$2.13 \times 10^5$ due to the uncertain output of the renewable energy resources and load demand fluctuation

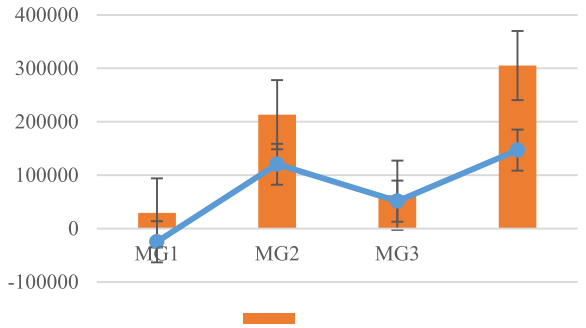

FIGURE 17. The operation cost of each microgrid for both deterministic and stochastic conditions.

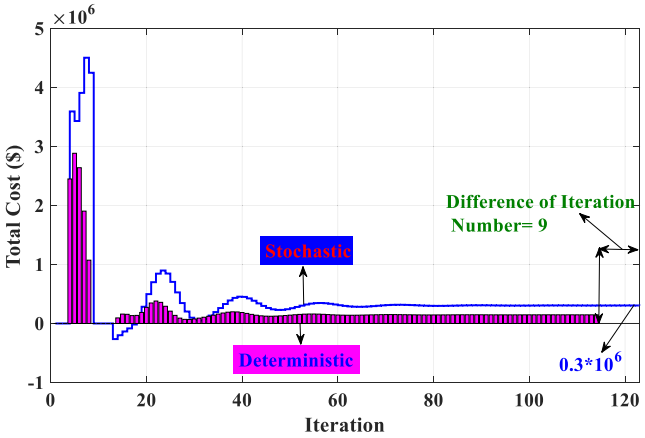

FIGURE 18. The total operation cost for both deterministic and stochastic conditions.

in the microgrid 2. Similar to the microgrid 2, this situation is expanded for the operation cost of the other microgrids. It is significant to say that the stochastic condition may alter the converging process of the consensus algorithm as shown in Fig. 18. It can be indicated that the iteration number and the total cost under uncertainty condition are approximately increased by 7.14% and 53% in comparison with the normal operation.

VI. CONCLUSION

One of the key aspects of the peer to peer based energy management is the issue of energy trading under attack condition. The main topic of this research is to remove the obstacles including the cyber-attacks for the realization of a secured peer-to-peer energy market. The most important impediment, which is a very significant and common cyber-attack, is the FDIA which can disrupt the proper functioning of the system, severely. The simulations results include various sections, which show the accuracy of the proposed method from different aspects. In the first part, a false data injection attack (FDIA) is applied to the peer-to-peer energy trading system among the microgrids, aiming to reach an appropriate consensus based on the RCI approach. Also, the proposed anomaly detection method based on adjusting the α coefficient detects the amount of deviation of the injected incorrect data with the aim of minimizing the detection delay in the trading procedure. In the other part, the improved detection method was compared with other methods such as SVM, RL, PSO-RL and GA-RL, and the time of detecting incorrect data intrusion by the proposed method reinforced the claim that the online data intrusion can be prevented online. In order to bring the simulation closer to the reality, the load and production uncertainty are considered which the UT method is used to simulate the uncertainty. As a result, it becomes much more difficult to detect FDIA in the uncertain environment. This makes it necessary for the proposed method to be robust under stochastic condition against FDIA. The obtained results clearly show the accuracy of the proposed method. However, the result of this study does not cover all smart city sections such as transportation or energy hub systems, as well online and offline training can be combined to improve the convergence. Future studies on the current topic are therefore recommended.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group number RG-1436-040.

REFERENCES

[1] C. Zhang, J. Wu, C. Long, and M. Cheng, "Review of existing peer-to-peer energy trading projects," *Energy Procedia*, vol. 105, pp. 2563–2568, May 2017.
[2] O. Utility. *A Glimpes into the Future of Britain's Energy Economy*. Accessed: May 2021. [Online]. Available: https://piclo.uk
[3] M. Daneshvar, S. Asadi, B. Mohammadi-Ivatloo, M. Daneshvar, S. Asadi, and B. Mohammadi-Ivatloo, "Energy trading possibilities in the modern multi-carrier energy networks," in *Power System*. New York, NY, USA: Springer, 2021, pp. 175–214.
[4] T. Morstyn, A. Teytelboym, and M. D. Mcculloch, "Bilateral contract networks for peer-to-peer energy trading," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2026–2035, Mar. 2019.
[5] W. Tushar, C. Yuen, H. Mohsenian-Rad, T. Saha, H. V. Poor, and K. L. Wood, "Transforming energy networks via peer-to-peer energy trading: The potential of game-theoretic approaches," *IEEE Signal Process. Mag.*, vol. 35, no. 4, pp. 90–111, Jul. 2018.
[6] B. P. Hayes, S. Thakur, and J. G. Breslin, "Co-simulation of electricity distribution networks and peer to peer energy trading platforms," *Int. J. Electr. Power Energy Syst.*, vol. 115, Feb. 2020, Art. no. 105419.
[7] M. Daneshvar, B. Mohammadi-Ivatloo, and M. Abapour, "The possibility of using blockchain based cryptocurrency in transactive energy markets: Ongoing activities and opportunities ahead," in *Proc. 4th Int. Energy Manage. Technol. Conf.*, 2018, pp. 1–5.
[8] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. Syst. Secur. (TISSEC)*, vol. 14, no. 1, p. 13, 2011.
[9] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, Art. no. 31533158.
[10] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Proc. 1st Workshop Secure Control Syst.*, 2010, pp. 1–6.
[11] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.
[12] A. Lima, F. Rocha, M. Volp, and P. Esteves-Veríssimo, "Towards safe and secure autonomous and cooperative vehicle ecosystems," in *Proc. 2nd ACM Workshop Cyber-Phys. Syst. Secur. Privacy*, 2016, pp. 59–70.
[13] S. Wang, A. F. Taha, J. Wang, K. Kvaternik, and A. Hahn, "Energy crowdsourcing and Peer-to-Peer energy trading in blockchain-enabled smart grids," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1612–1623, Aug. 2019.

[14] 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.

[15] A. Ahmadi, M. Nabipour, B. Mohammadi-Ivatloo, and V. Vahidinasab, "Ensemble learning-based dynamic line rating forecasting under cyber-attacks," *IEEE Trans. Power Del.*, early access, Feb. 1. 2021, doi: 10.1109/TPWRD.2021.3056055.

[16] K. C. Sou, H. Sandberg, and K. H. Johansson, "Detection and identification of data attacks in power system," in *Proc. Amer. Control Conf. (ACC)*, Jun. 2012, pp. 3651–3656.

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

[18] M. Giannini, "Improving cyber-security of power system state estimators," M.S. thesis, School Elect. Eng., KTH, Stockholm, Sweden, Feb. 2014.

[19] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proc. IEEE Conf. Decis. Control Eur. Control Conf.*, Orlando, FL, USA, Dec. 2011, pp. 4054–4059.

[20] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Brussels, Belgium, Oct. 2011, pp. 244–248.

[21] M. A. Rahman, E. Al-Shaer, and R. Kavasseri, "Impact analysis of topology poisoning attacks on economic operation of the smart power grid," in *Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst.*, Madrid, Spain, Jun. 2014, pp. 649–659.

[22] D.-H. Choi and L. Xie, "Impact analysis of locational marginal price subject to power system topology errors," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Vancouver, BC, Canada, Oct. 2013, pp. 55–60.

[23] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[24] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

[25] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Proc. IEEE/ACM 3rd Int. Conf. Cyber-Phys. Syst.*, Apr. 2012, pp. 183–192.

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

[27] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.

[28] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2435–2443, Sep. 2015.

[29] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[30] Y. Chakhchoukh and H. Ishii, "Cyber attacks scenarios on the measurement function of power state estimation," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2015, pp. 3676–3681.

[31] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Trans. Signal Inf. Process. over Netw.*, vol. 4, no. 1, pp. 48–59, Mar. 2018.

[32] B. Kailkhura, S. Brahma, and P. K. Varshney, "Data falsification attacks on consensus-based detection systems," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 3, no. 1, pp. 145–158, Mar. 2017.

[33] M. Ashrafuzzaman, Y. Chakhchoukh, A. A. Jillepalli, P. T. Tosic, D. C. de Leon, F. T. Sheldon, and B. K. Johnson, "Detecting stealthy false data injection attacks in power grids using deep learning," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018.

[34] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[35] H. Zou, J. Tao, S. K. Elsayed, E. E. Elattar, A. Almalaq, and M. A. Mohamed, "Stochastic multi-carrier energy management in the smart islands using reinforcement learning and unscented transform," *Int. J. Electr. Power Energy Syst.*, vol. 130, Sep. 2021, Art. no. 106988.

[36] M. A. Mohamed, H. M. Abdullah, M. A. El-Meligy, M. Sharaf, A. T. Soliman, and A. Hajjiah, "A novel fuzzy cloud stochastic framework for energy management of renewable microgrids based on maximum deployment of electric vehicles," *Int. J. Electr. Power Energy Syst.*, vol. 129, Jul. 2021, Art. no. 106845.

[37] L. Min, K. A. Alnowibet, A. F. Alrasheedi, F. Moazzen, E. M. Awwad, and M. A. Mohamed, "A stochastic machine learning based approach for observability enhancement of automated smart grids," *Sustain. Cities Soc.*, vol. 72, Sep. 2021, Art. no. 103071.

[38] A. K. Singh and B. C. Pal, "Decentralized dynamic state estimation in power systems using unscented transformation," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 794–804, Mar. 2014.

[39] Y. Xu, W. Zhang, W. Liu, and F. Ferrese, "Multiagent-based reinforcement learning for optimal reactive power dispatch," *IEEE Trans. Syst., Man, Cybern., C, Appl. Rev.*, vol. 42, no. 6, pp. 1742–1751, Nov. 2012.

[40] L. Zeng, T. Xia, S. K. Elsayed, M. Ahmed, M. Rezaei, K. Jermsittiparsert, U. Dampage, and M. A. Mohamed, "A novel machine learning-based framework for optimal and secure operation of static VAR compensators in EAFs," *Sustainability*, vol. 13, no. 11, p. 5777, May 2021.

[41] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[42] S. Mashayekh, M. Stadler, G. Cardoso, M. Heleno, S. C. Madathil, H. Nagarajan, R. Bent, M. Mueller-Stoffels, X. Lu, and J. Wang, "Security-constrained design of isolated multi-energy microgrids," *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 2452–2462, May 2018.

[43] M. A. Mohamed, A. Almalaq, H. M. Abdullah, K. A. Alnowibet, A. F. Alrasheedi, and M. S. A. Zaindin, "A distributed stochastic energy management framework based-fuzzy-PDMM for smart grids considering wind park and energy storage systems," *IEEE Access*, vol. 9, pp. 46674–46685, 2021.

[44] H. Chabok, M. Roustaei, M. Sheikh, and A. Kavousi-Fard, "On the assessment of the impact of a price-maker energy storage unit on the operation of power system: The ISO point of view," *Energy*, vol. 190, Jan. 2020, Art. no. 116224.

[45] A. Letafat, M. Rafiei, M. Ardeshiri, M. Sheikh, M. Banaei, J. Boudjadar, and M. H. Khooban, "An efficient and cost-effective power scheduling in zero-emission ferry ships," *Complexity*, vol. 2020, Apr. 2020, Art. no. 6487873.

[46] E. Sorin, L. Bobo, and P. Pinson, "Consensus-based approach to peer-to-peer electricity markets with product differentiation," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 994–1004, Mar. 2019.

[47] M. A. Mohamed, T. Jin, and W. Su, "An effective stochastic framework for smart coordinated operation of wind park and energy storage unit," *Appl. Energy*, vol. 272, Aug. 2020, Art. no. 115228.

[48] T. Lan, K. Jermsittiparsert, S. T. Alrashood, M. Rezaei, L. Al-Ghussain, and M. A. Mohamed, "An advanced machine learning based energy management of renewable microgrids considering hybrid electric vehicles' charging demand," *Energies*, vol. 14, no. 3, p. 569, Jan. 2021.

[49] M. A. Mohamed, T. Jin, and W. Su, "Multi-agent energy management of smart islands using primal-dual method of multipliers," *Energy*, vol. 208, Oct. 2020, Art. no. 118306.

[50] J. Yang, "Blockchain for peer-to-peer energy trading," Nanyang Technol. Univ., Singapore, Tech. Rep., 2020, doi: 10.32657/10356/139944.

[51] S. Ding, Y. Cao, M. Vosoogh, M. Sheikh, and A. Almagrabi, "A directed acyclic graph based architecture for optimal operation and management of reconfigurable distribution systems with PEVs," *IEEE Trans. Ind. Appl.*, early access, Jul. 14, 2020, doi: 10.1109/TIA.2020.3009050.

[52] L. Al-Ghussain, A. D. Ahmad, A. M. Abubaker, and M. A. Mohamed, "An integrated photovoltaic/wind/biomass and hybrid energy storage systems towards 100% renewable energy microgrids in university campuses," *Sustain. Energy Technol. Assessments*, vol. 46, Aug. 2021, Art. no. 101273.

[53] F. Yin, A. Hajjiah, K. Jermsittiparsert, A. S. Al-Sumaiti, S. K. Elsayed, S. S. Ghoneim, and M. A. Mohamed, "A secured social-economic framework based on PEM-blockchain for optimal scheduling of reconfigurable interconnected microgrids," *IEEE Access*, vol. 9, pp. 40797–40810, 2021.

[54] P. Wang, D. Wang, C. Zhu, Y. Yang, H. M. Abdullah, and M. A. Mohamed, "Stochastic management of hybrid AC/DC microgrids considering electric vehicles charging demands," *Energy Rep.*, vol. 6, pp. 1338–1352, Nov. 2020.

[55] X. Gong, F. Dong, M. A. Mohamed, O. M. Abdalla, and Z. M. Ali, "A secured energy management architecture for smart hybrid microgrids considering PEM-fuel cell and electric vehicles," *IEEE Access*, vol. 8, pp. 47807–47823, 2020.
[56] X. Gong, F. Dong, M. A. Mohamed, E. M. Awwad, H. M. Abdullah, and Z. M. Ali, "Towards distributed based energy transaction in a clean smart island," *J. Cleaner Prod.*, vol. 273, Nov. 2020, Art. no. 122768.
[57] M. Khorasany, Y. Mishra, and G. Ledwich, "A decentralized bilateral energy trading system for Peer-to-Peer electricity markets," *IEEE Trans. Ind. Electron.*, vol. 67, no. 6, pp. 4646–4657, Jun. 2020.
[58] N. Liu, X. Yu, C. Wang, C. Li, L. Ma, and J. Lei, "Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3569–3583, Sep. 2017.
[59] S. Cui, Y.-W. Wang, and J.-W. Xiao, "Peer-to-peer energy sharing among smart energy buildings by distributed transaction," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6491–6501, Nov. 2019.

MOHAMED A. MOHAMED (Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from Minia University, Minia, Egypt, in 2006 and 2010, respectively, and the Ph.D. degree in electrical engineering from King Saud University, Riyadh, Saudi Arabia, in 2016. He joined the College of Electrical Engineering and Automation, Fuzhou University, China, as a Postdoctoral Research Fellow, in 2018. He has been a Faculty Member with the Department of Electrical Engineering, College of Engineering, Minia University, since 2008. His research interests include power system analysis, renewable energy integration, energy management, power electronics, electrical vehicles, optimization, smart islands, smart cities, and smart grids. He has supervised multiple M.Sc. and Ph.D. thesis. He worked on a number of technical projects and published in various articles and books. He has also joined the editorial board of some scientific journals and the steering committees of many international conferences.

ALI HAJJIAH received the B.Sc. degree in electrical engineering from Oklahoma State University, USA, in 1998, and the M.Sc. and Ph.D. degrees from Virginia Tech, USA, in 2003 and 2009, respectively. He was the Director of the Semiconductor Laboratory, Kuwait University, from 2011 to 2012, and the Director of the Engineering Training and Alumni Center (ETAC), College of Engineering and Petroleum, from 2015 to 2017. From January 2014 to August 2014, he was working as an Industrial Fellow with IMEC Belgium, where he working on enhancing the conversion efficiency of n-type PERT crystalline silicon solar cells. As a Visiting Scholar, he joined the Virginia Polytechnic Institute and State University (Virginia Tech), USA, in 2013 and subsequently the Catholic University of Leuven (KU Leuven), Belgium, from 2015 to 2017. He is currently working as an Associate Professor with Kuwait University, where he held a key positions. He is also working on efficiency improvement and device physics of Perovskite/Si tandem solar cells. His research interests include processing and fabrication of Si and III-V semiconductor lasers and thin film solar cells. He has been a member of several honor societies, such as the Golden Key National Honor Society, since 1995, the Tau Beta Pi Honor Society-Gamma Chapter, since 1997, the Eta Kappa Nu Honor Association-Omega Chapter, since 1997, and the Phi Sigma Theta National Honor Society, since 2002.

KHALID ABDULAZIZ ALNOWIBET received the B.Sc. degree in operations research from the College of Sciences, King Saud University (KSU), Saudi Arabia, in 1992, the M.Sc. degree in operations research from the School of Engineering and Applied Sciences, George Washington University, Washington DC, USA, in 1994, and the Ph.D. degree in operations research from the School of Engineering, North Carolina State University, NC, USA, in 2004. He joined as a Faculty Member of the College of Science, KSU, for more than 15 years. During his service in KSU, he was appointed to several key administrative. He is currently an Associate Professor with the Statistics and Operations Research Department, KSU. He published several articles in wide range of applications, such as performance evaluation using stochastic modeling, queueing networks applications, queueing theory and applications, stochastic processes theory and applications, and modeling communication networks.

ADEL FAHAD ALRASHEEDI received the B.Sc. degree in mathematics and the M.Sc. degree in operations research from King Saud University and the Ph.D. degree in operations research from the University of Edinburgh, U.K. He is currently working as an Assistant Professor and the Department Chairman with the Department of Statistics and Operations Research, College of Science, King Saud University. His research portfolio encompasses a broad range of applications and a variety of research methodologies in optimization, inventory management, stochastic modeling, stochastic inventory control, production planning and scheduling, and optimal control.

EMAD MAHROUS AWWAD is currently pursuing the Ph.D. degree with the Electrical Engineering Department, King Saud University. He was a Teaching Assistant with the Industrial Electronics and Control Engineering Department, Faculty of Electronic Engineering, Menofia University, Egypt. He developed his researches in the field of design, control, and implementation of autonomous mobile robot. He is interested in modeling, optimization, observer design, and MPC controller of vehicle dynamics under the wheel-terrain interaction slippage phenomenon. He is also interested in artificial intelligence, machine learning, and deep learning related to the field of robotics and image processing.

S. M. MUYEEN (Senior Member, IEEE) received the B.Sc.Eng. degree in electrical and electronic engineering from the Rajshahi University of Engineering and Technology (RUET) (currently, Rajshahi Institute of Technology), Bangladesh, in 2000, and the M.Eng. and Ph.D. degrees in electrical and electronic engineering from the Kitami Institute of Technology, Japan, in 2005 and 2008, respectively. He is currently working as an Associate Professor with the School of Electrical Engineering Computing and Mathematical Sciences, Curtin University, Australia. His research interests are power system stability and control, electrical machine, FACTS, energy storage systems (ESSs), renewable energy, and HVDC systems. He has been a keynote speaker and an invited speaker at many international conferences, workshops, and universities. He has published more than 225 articles in different journals and international conferences. He has published seven books as an author or editor. He is serving as Editor/Associate Editor for many prestigious journals from IEEE, IET, and other publishers, including IEEE TRANSACTIONS ON SUSTAINABLE ENERGY, IEEE TRANSACTIONS ON ENERGY CONVERSION, IEEE POWER ENGINEERING LETTERS, *IET Renewable Power Generation*, and *IET Generation, Transmission and Distribution*. He is a Fellow of Engineers Australia.