Effective Management of Energy Internet in Renewable Hybrid Microgrids: A Secured Data Driven Resilient Architecture

Effective Management of Energy Internet in Renewable Hybrid Microgrids: A Secured Data Driven Resilient Architecture

Mojtaba Mohammadi, Abdollah Kavousi-Fard, *Senior IEEE*, Morteza Dabbaghjamanesh, *Senior IEEE,* Amir Farughian, Abbas Khosravi, *member IEEE*

Abstract—This paper proposes a two-layer in-depth secured management architecture for the optimal operation of energy internet in hybrid microgrids. In the cyber layer of the proposed architecture, a two-level intrusion detection system (IDS) is proposed to detect various cyber-attacks (i.e. Sybil attacks, spoofing attacks, false data injection attacks) on wireless-based advanced metering infrastructures. The sequential probability ratio testing (SPRT) approach is utilized in both levels of the proposed IDS to detect cyber-attacks based on a sequence of anomalies rather than only one piece of evidence. The process of making a decision in the proposed IDS is a random walk that starts from a point between two thresholds and moves toward one of them concerning received data samples. The feasibility and performance of the proposed architecture are examined on the IEEE 33-bus test system and the results are provided for both islanded and grid-connected operation modes.

Index Terms— Advanced metering infrastructure, data security, hybrid microgrid, energy internet, energy management, architecture.

M. Mohammadi and A. Kavousi-Fard are with the Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran (e-mail: mojtabamohammadi303@gmail.com, and kavousi@sutech.ac.ir).

M. Dabbaghjamanesh is with the Department of Mechanical Engineering, The University of Texas at Dallas, Richardson, TX 75080 USA (e-mail: dabaghmanesh.morteza@gmail.com).

A. Farughian is with the Department of Electrical Engineering and Energy Technology, University of Vaasa, P.O. Box 700, FI-65101 Vaasa, Finland (e-mail: amir.farughian@uva.fi)

A. Khosravi is with the Institute for Intelligent Systems Research and Innovation, Deakin University, Geelong, VIC 3220, Australia (e-mail: abbas.khosravi@deakin.edu.au).

NOMENCLATURE

B_{Gi}^t	Cost of the i^{th} DGU at interval t
B_{Grid}^t	Cost of the upstream grid at interval t
DR_i/UR_i	Ramp down/up rate of the i^{th} DGU
$f(S\|H)$	Conditional mass function
$h(X)$	Cost objective function
m	Number of observations with type H_1 in a sample set
n	Sample set size
N_i	Number of time intervals
N_d/ $N_{d\text{-}dc}$/ $N_{d\text{-}ac}$	Number of DGU in the MG/dc sub-grid/ac sub-grid
$N_{Load\text{-}dc}$	Number of loads in dc sub-grid
N_b	number of buses
N_{Load}	Number of loads in the MG
$P_{Grid,min}^t$/ $P_{Grid,max}^t$	Min/max power of the upstream grid
$P_{load\text{-}dc}$	The load in the dc sub-grid
$P^{inj,t}{}_j$/ $Q^{inj,t}{}_j$	Active/reactive power injected to the j^{th} bus at interval t
P_{Gi}^{min}/ P_{Gi}^{max}	Min/max output power of the i^{th} DGU
P_{conv}^{min}/ P_{conv}^{max}	Min/max power of the ac-dc converter
$P_{i,max}^{line,t}$	maximum capacity of the i^{th} feeder
P_{lm}^i/P_{lf}^i	Measured/forecasted load value of the i^{th} bus
P_{Grid}^t	Power purchased/sold from/to utility at interval t

$P_{Loss\text{-}dc}$	Power loss in dc-sub-grid
RES^t	The spinning reserve at interval t
S_{Gi}^{on}/S_{Gi}^{off}	Startup/shutdown cost of the i^{th} DGU
S_{rss}^i/S_l^i	Binary sample of the i^{th} smart meter related to the first/second level of the IDS
$S_{SPRT,k}^i$	K^{th} Input sample of the SPRT method related to i^{th} smart meter
u_i^t	ON/OFF Status of the i^{th} DGU
UE^i/LE^i	Upper/lower forecasting error bounds
U^i/L^i	Upper/lower bound of the SPRT
V_{min}^i/V_{max}^i	Min/max voltage of the i^{th} bus
V/δ	Magnitude/phase of the voltage
X	Control variables
Y/Θ	Magnitude/phase of the line impedance
σ_i/μ_i	Standard deviation/mean value of the signal strength data set related to i^{th} smart meter
α_i	User-selected false positive value
β_i	User-selected false negative value

I. INTRODUCTION

The concept of the smart grid was first introduced as a digitalization scheme for legacy centralized power grids. This digitalization process was performed by placing digital metering devices and sensors in the grid to provide real-time data related to the status of the system. Afterward, the idea of creating an interactive energy-information-oriented grid, which allows consumers to generate and share green energy, was discussed by corporations like IBM and EPRI. This idea which nowadays is known as the energy internet (EI), is considered the third industrial revolution [1]. According to a report from the KEMA, it is demonstrated that investing $16 billion on the EI can cause $64 billion worth of projects and directly create more than 28,000 jobs in the United States in only four years [1]. In this regard, many countries such as United States, Germany,

Japan, China, etc. have allocated huge funds in this area [2-4]. The idea of EI brings many benefits to the grid. This paper addresses some of the problems in energy management and cybersecurity of EIs. Technically, MGs can be classified into three different categories: ac, dc, and hybrid [5]. The concept of hybrid microgrid (HMG) is proposed to make benefit from both ac and dc MGs at the same time. Generally, in comparison with ac, and dc MGs, which are well-studied topics, hybrid MGs have more challenges. Implementation of advanced metering infrastructure (AMI), which is one of the key technologies in modern power systems, creates bidirectional communication between consumers and electricity provider companies.

The main issue for the economic and efficient operation of MGs is the management and optimal scheduling of DGUs main grid, and loads [6]. In [7], the authors suggested a stochastic management framework for the optimal scheduling of HMGs. In that paper, various kinds of renewable energy sources, batteries, and DGUs are considered and unscented transform is employed to model the uncertainties of the system. To tackle the management problem in renewable MGs, a probabilistic management scheme based on the *2m* point estimation approach is presented in [8]. In [9], a secured energy management scheme for HMGs is introduced. In that paper, the complete model of PEM-fuel cells, which includes optimal hydrogen production strategy and thermal recovery, as well as electric vehicles, reconfigurable structure, and several renewable energy sources are considered. Authors in [10] introduced a novel cloud-fog-based architecture for energy management in networked MGs considering dynamic line rating and reconfigurable structure. A cyber-attack resilient optimal scheduling framework is proposed in [11] for industrial internet of things-based microgrids. In [12] authors utilized the software-defined networking approach to improve cybersecurity in the energy management of distribution networks. Reference [13] proposed an energy management scheme for EIs in which a deep-reinforcement learning algorithm is used to solve the operation problem. A game-theory-based energy management framework for EIs is introduced in [14], [15].

Due to an increase in the number of cyber-attack incidents involving power utilities in recent years, data security has attracted the attention of researchers in this area. Authors in [16] proposed a machine-learning-based anomaly detection scheme to detect cyber-attacks in the AMIs. In that paper, a novel modified

symbiotic organisms search-based approach is employed to improve lower and upper bound estimation training by accurate adjusting of the parameters. A novel SAE deep-learning-based method is introduced in [17] to detect cyber-attacks in smart grids. This paper also proposes a two-stage model to describe cyber-attacks within smart grids. In [4], a secured management framework for HMGs considering identity-based cyber-attacks is proposed.

In this paper, a novel two-level intrusion detection system (IDS) is proposed to enhance the security in-depth within the system's cyber level. The proposed IDS includes two levels: 1) identity level, 2) integrity level. At the identity level, we use the received signal strength (RSS) of data packets to detect identity-based cyber-attacks (i.e. Sybil attack and spoofing attack) on loads' smart metering devices. The second level of the proposed IDS makes use of the forecasted load demand of the consumers, which central control uses for one-day ahead optimal scheduling, to detect integrity attacks. Sequential probability ratio testing (SPRT), which is implemented in both levels separately, computes a test statistic based on the collected information and statistical data and uses these test statistics to observe the sequence of samples and decide whether the system is under attack or not. It is worth noting that the proposed IDS has several advantages over traditional detection methods. For instance, since the SPRT, which is utilized in both levels separately, is a statistical sequential decision-making method, the proposed IDS makes decisions based on a sequence of samples rather than only one piece of evidence. This sequential behavior can result in more trustworthy detections. Another advantage of the proposed method is its ability to build a sequence of statistics where each step builds on the prior steps. Also, in contrast with deep-learning-based methods, which require high computation power to train, the proposed method is highly effective from computation power standpoint. Additionally, the proposed IDS can detect various cyber-attacks (i.e. Sybil attack, Spoofing attack, false data injection attack (FDIA)) at the same time. Our test system, which is constructed based on the IEEE 33-bus system, includes three WTs, two PVs, two MTs, and one fuel cell unit. To summarize, the main contributions of this work can be named as below:

- Developing a secured data-driven architecture for the optimal operation of HMGs.

- Developing a novel two-layer IDS based on SHT to detect integrity-based and identity-based cyber-attacks in AMIs.
- Simulating FDIA on an IEEE test system-based case study and analyzing the results.

The rest of this paper is organized as follows: Section II focuses on the proposed management architecture and presents the model. In this section, an energy management scheme for the system's physical operation, possible cyber-attack scenarios, network model, and the proposed SPRT based IDS are explained in detail. Section III is devoted to the simulation results and the main conclusion of the paper can be found in section IV.

II. PROPOSED TWO-LAYER MANAGEMENT ARCHITECTURE

EI, which can be considered as a new way of thinking about the development of sustainable energy systems, is one of the most promising structures for future energy grids. The EI provides the info-energy infrastructure required by smart cities in which smart homes, factories, utilities, electric vehicles, etc. can easily generate green energy and exchange energy and information. Generally, EI includes three main levels 1) technology level: this level, which is also known as the physical level, is the main core of the EI that includes physical components such as loads, generation units, physical devices, etc. 2) market level: market level mainly reflects the commercial side of the EI, and 3) cyber level: this level is related to the data flow in different levels of the system.

A. Physical layer: Hybrid ac-dc Microgrid operation

A.1 Problem Formulation & Constraints

The cost objective function of the HMG incorporates the cost of all components within the system as follows:

$$Min \quad h(X) = \sum_{t=1}^{N_t} \Big(\sum_{i=1}^{N_d} [u_i^t P_{Gi}^t B_{Gi}^t + S_{Gi}^{on} \max\{0, u_i^t - u_i^{t-1}\} + S_{Gi}^{off} \max\{0, u_i^{t-1} - u_i^t\}] + P_{Grid}^t B_{Grid}^t \Big) \tag{1}$$

In (1), *h(X)* denotes the overall cost of the HMG, and *X* contains the active power purchased/sold from/to the main grid, output power of DGUs, and their ON/OFF status as follows:

$$\begin{aligned} &X=[P_g,U_g]_{1\times(2\times n\times Ni)} \quad , \quad n=N_d+1 \quad ; \quad \forall t\in N_i \\ &P_g{}^t=[P_G^t,P_{Grid}^t] \quad ; \quad P_G^t=[P_{G1}^t,P_{G2}^t,...,P_{GN_d}^t] \\ &U_g^t=[u_1^t,u_2^t,...,u_{N_d}^t] \quad , \quad u_k^t\in\{0,1\} \\ &P_{Grid}^t=[P_{Grid}^t] \end{aligned} \tag{2}$$

The above cost objective function must be optimized considering several technical constraints in both ac and dc sub-grids.

$$\sum_{i=1}^{N_{d-DC}} P_{Gi}^t+P_{conv}^t=\sum_{k=1}^{N_{Load-DC}} P_{Load-DC}^t+P_{Loss-DC} \tag{3}$$

Equation (3), indicates the balance between power consumption and generation in the dc sub-grid:

$$P_j^{inj,t}=\sum_{n=1}^{N_b} V_j^t V_n^t Y_{jn}\cos(\theta_{jn}+\delta_j-\delta_n) \tag{4}$$

$$Q_j^{inj,t}=\sum_{n=1}^{N_b} V_j^t V_n^t Y_{jn}\sin(\theta_{jn}+\delta_j-\delta_n) \tag{5}$$

The rest of the constraints are presented as follows:

- Converter, upstream grid, and DGUs' capacity limit:

$$\begin{aligned} &P_{Gi,\min}^t\le P_{Gi}^t\le P_{Gi,\max}^t \\ &P_{conv,\min}^t\le P_{conv}^t\le P_{conv,\max}^t \\ &P_{Grid,\min}^t\le P_{Grid}^t\le P_{Grid,\max}^t \end{aligned} \tag{6}$$

- spinning reserve:

$$\sum_{i=1}^{N_d} u_i^t P_{Gi,\max}^t+P_{Grid,\max}^t\ge\sum_{k=1}^{N_{Load}} P_{Load,k}^t+P_{loss}^t+\mathrm{Re}s^t \tag{7}$$

- feeder capacity limit:

$$|P_i^{Line,t}|\le P_{i,\max}^{Line} \tag{8}$$

- bus voltage limit:

$$V_m^{\min}\le V_m^t\le V_m^{\max} \tag{9}$$

- ramp-rate constraint:

$$| P_{Gi}^{t} - P_{Gi}^{t-1} | < UR_i, DR_i \quad (10)$$

B. Cyber layer

In the proposed architecture, smart metering devices are assumed as immobile wireless-based devices which communicate with MGCC through wireless networks. Each bus is equipped with a smart meter that measures the load value and reports it to the MGCC at regular time intervals. The AMI system operates based on IEC 62559 standard and DLMS/COSEM protocol, which are designed for metering applications. According to IEC 62559 standard [22] and DLMS/COSEM protocol [23], the IP address of the source and target of any data packet within AMI networks must be attached to the data itself. Also, the MGCC is aware of the IP address of all nodes within the network, and signal receivers in the system are equipped with an antenna that measures the RSS of received signals and sends these values along with data packets to the MGCC.

In this work, two types of cyber-attacks are addressed:

1) *Integrity attack:* integrity attack is one of the most common cyber-attacks in wireless-based systems. In this type of attack, hacker tends to change the content of data packets in the location of the meter or the communication path. There are various scenarios for such attacks such as FDIA. Reference [24] investigated the effects of FDIAs on critical infrastructures and also presented a comprehensive overview of the existing countermeasures to defend against such attacks.
2) *Identity-based attacks:* Second class of cyber-attacks are identity-based attacks. In this class of cyber-attacks, the adversary forges the identity of nodes in the system. These attacks are usually carried out in two ways: *Sybil attack and spoofing attack*. Sybil attack is a type of attack in which the adversary hacks a legitimate node and uses that node to impersonate the identity of other nodes and gain control of the network. In a spoofing attack, the hacker individually forges the identity of nodes on the network and uses their identity to launch the attack.

B.1 The Proposed SPRT Based Intrusion Detection System

In this section, a two-level IDS is proposed in which each level detects one of the above cyber-attacks.

B.1.1 Identity Level

The RSS of an immobile transmitter in wireless networks is relatively constant and has a predictable distribution [18]. RSS is strongly influenced by the distance between the transmitter and receiver and the communication path. Therefore, in stationary networks, RSSs can be considered as a unique fingerprint to distinguish different signal sources. To this end, in this section, the RSS values are employed to develop an IDS. For each smart meter, during the operation time, the corresponding RSS values related to each smart meter are saved in the MGCC to form a historical data set for each specific meter. In order to evaluate the authenticity of a signal transmitter, a normal distribution function is fitted to the preceding historical data set of that specific meter. Regarding the obtained distribution function, for every received data packet a binary sample is computed as follows:

$$S_{rss}{}^{i} = \begin{cases} 0 & RSS_i \in [\mu_i - 2\sigma_i, \mu_i + 2\sigma_i] \\ 1 & o.w \end{cases} \qquad (11)$$

where μ_i and σ_i present the mean value and standard deviation of the historical data set. equation (11) indicates that if the RSS value of the received data, which is related to i^{th} smart meter, lies out of the range, the MGCC will suspect the signal source. Since there are several uncertainties associated with the RSS (e.g. weather condition, air temperature, etc.), it is not reasonable to decide about the authenticity of the signal source by considering only one signal sample. To overcome this problem, the SPRT approach, which is explained in the next section in detail, is employed to decide based on the sequence of signals rather than only one sample. In the first level of the IDS, the input of the SPRT is S_{rss} and the output is a binary decision that determines if an identity attack has occurred.

B.1.2 Integrity Level

The integrity level is responsible to examine the contents of the data packet, which is the load value measured by smart meters. This process is carried out by comparing the measured load value with the

corresponding value forecasted in MGCC. For each data packet received by MGCC, the following binary sample (S_l^i) is computed:

$$e_{l,i} = | P_{l,m}{}^{i} - P_{l,f}^{i} | \tag{12}$$

$$S_l^i = \begin{cases} 0 & 0 < e_l^i < LE^i \times P_{l,f}^i \\ 1 & LE^i \times P_{l,f}^i \leq e_l^i \leq UE^i \times P_{l,f}^i \end{cases} \tag{13}$$

B.1.3 Sequential Probability Ratio Test

SPRT, which is also known as sequential hypothesis testing, is a statistical decision-making process that is introduced by Wald. A [19]. This method can be considered as a random walk with an upper (U^i) bound and lower (L^i) bound. In this method, the first two hypotheses called the null hypothesis (H_0) and the alternative hypothesis (H_1) are defined in such a way that the null and alternative hypotheses are associated with the lower and upper bounds respectively. These hypotheses are defined as below:

- H_1: The smart meter is under attack.
- H_0: The smart meter has a normal operation.

During the decision-making process, concerning each new sample, a test-statistic is calculated. The process will continue until the test statistic reaches or exceeds one of the thresholds. Thresholds are defined based on user-selected false positive and false negative rates. Although it is desirable to have zero false positive and false negative rates, but there is a tradeoff between these values and the number of samples required by the process to reach a decision. In other words, decreasing false positive and false negative values increases the number of samples required by the process to reach a decision. For simplicity, from now on, each input sample is considered as an observation and a sample set is defined as a finite number of observations (i.e. $S_{SPRT,1}$, $S_{SPRT,2}$…., $S_{SPRT,n}$). According to the (iid), the likelihood ratio of a sample set of size n is calculated as follows [19]:

$$PR_T^{\,i} = \ln\left(\prod_{k=1}^{n} \frac{f(S_{SPRT,k}{}^{i} | H_1)}{f(S_{SPRT,k}{}^{i} | H_0)}\right) = \sum_{k=1}^{n} PR_k{}^{i} = m * \ln\left(\frac{P_1^i}{P_0^i}\right) + (n-m) * \ln\left(\frac{1-P_1^i}{1-P_0^i}\right) \tag{14}$$

where $P_0^i=PR_k^i(S_{SPRT,k}^i=1|H_0)$ and $P_1^i=PR_k^i(S_{SPRT,k}^i=1|H_1)$. At each step of the process when a new sample is received and added to the sample set, the likelihood ratio of the new sample set (PR_T^i) is computed. If $PR_T^i \le Ln(L^i)$, the null hypothesis is accepted, if $Ln(U^i) \le PR_T^i$, the alternative hypothesis is accepted, and if $Ln(L^i) \le PR_T^i \le Ln(U^i)$, no decision is made and the process waits for the next observation. After a decision is made, the process is restarted, meaning that the current sample set is cleared and a new blank sample set is generated. According to [19], the thresholds are obtained as follows:

$$U^i = ((1-\beta^i)/\alpha^i) \tag{15}$$

$$L^i = (\beta^i / (1-\alpha^i)) \tag{16}$$

Let λ^i denotes the ratio of the number of observations with type H_1 ($S_{SPRT}^i=1$) to the number of total observations in a sample set with size n that SPRT accepts the alternative hypothesis if the sample set includes at least $\lambda^i \times n$ ones. According to (14), if we neglect the surplus of the likelihood ratio over thresholds, the λ^i is obtained as follows:

$$\lambda^i = \frac{\ln(\frac{1-\beta^i}{\alpha^i}) - n \times \ln(\frac{1-P_1^i}{1-P_0^i})}{n \times (\ln(\frac{P_1^i}{P_0^i}) - \ln(\frac{1-P_1^i}{1-P_0^i}))} \tag{17}$$

Since the number of observations (N^i) required by the SPRT to reach a decision is not predetermined, the expected value of N^i can be calculated as follows [19]:

$$E(N^i \mid H_0) = \frac{(1-\alpha^i) \times \ln(L^i) + \alpha^i \times \ln(U^i)}{P_0^i \times \ln(\frac{P_1^i}{P_0^i}) + (1-P_0^i) \ln(\frac{1-p_1^i}{1-p_0^i})} \tag{18}$$

When the decision is made to accept H_0, and by:

$$E(N^i \mid H_1) = \frac{\beta^i \times \ln(L^i) + (1-\beta^i) \times \ln(U^i)}{P_1^i \times \ln(\frac{P_1^i}{P_0^i}) + (1-P_1^i) \ln(\frac{1-p_1^i}{1-p_0^i})} \tag{19}$$

When the decision is made to accept H_0.

Table I Characteristics of DGUs and ac-dc converter

Type	Min Power (kW)	Max Power (kW)	Bid ($/kWh)	Startup/ shutdown cost ($)	Ramp Up/Down Rate	Bus Number
Micro-turbine 2	100	1300	0.475	75	185	12
Micro-turbine 3	90	1100	0.475	70	150	25
Wind-turbine 2	0	550	1.073	0	-	30
Wind-turbine 3	0	450	1.073	0	-	21
Photovoltaic 2	0	400	2.584	0	-	16
AC-DC converter	-1500	1500	-	-	-	18
Fuel cell	50	700	0.494	38.5	110	DC MG
Wind-turbine 1	0	200	1.073	0	-	DC MG
Micro-turbine 1	35	300	0.48	60	60	DC MG
Photovoltaic 1	0	250	2.584	0	-	DC MG

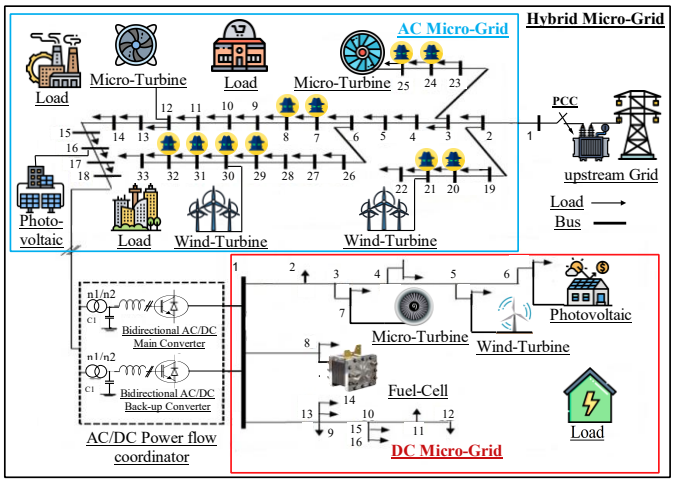

Fig. 1 schematic illustration of the test system and attack points

III. SIMULATION RESULTS

In this section, the optimal scheduling of the HMG, operation of HMG under cyber-attack, and performance analysis of the proposed SPRT based IDS are presented. The test system includes three WTs, two PVs, one fuel cell unit, and two MTs. Table I shows the characteristics of DGUs and converter and Fig. 1 presents the schematic illustration of the test system. Complete data related to the market price, dc sub-grid load demand, generation pattern of WTs and PVs, and ac sub-grid load factor is presented can be found in [8] and Fig. 2. The ac and dc sub-grids are connected through ac-dc converters on bus 18 and the voltage levels in the ac and dc sub-grids are 12.66 kV and 1kV respectively. All renewable energy sources (i.e. WTs and PVs) have

the same generation pattern as Fig. 2 but with different capacities. In order to achieve more realistic results, the ramp-up/down rate of DGUs is considered. In our architecture, MGCC schedules the loads and DGUs for a day ahead based on system characteristics and forecasted values. Then in the operation moment, it uses the real-time data collected by smart meters to provide a balance between consumption and generation in the system. It is worth noting that in simulations, the cost objective function of the HMG is minimized using heuristic method [20].

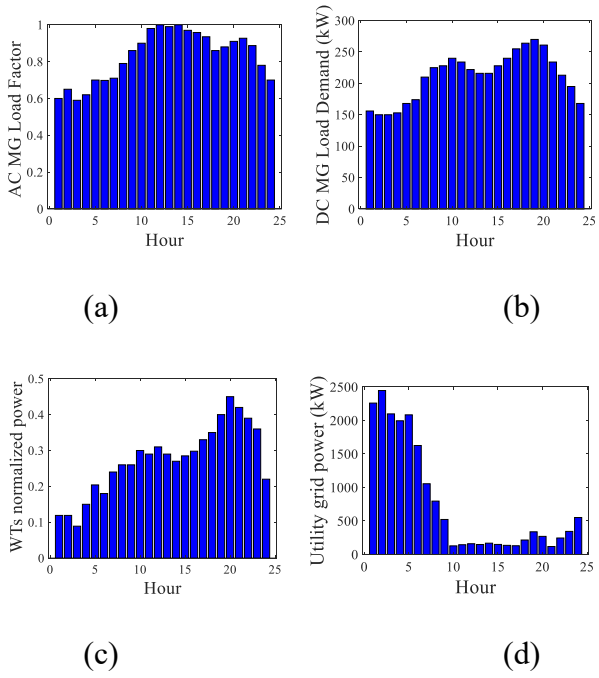

Fig. 2 (a) ac MG load factor, (b) dc sub-grid load demand, (c) WT and (d) utility grid power [4]

A. HMG optimal scheduling

In this section, we focus on the optimal scheduling of HMGs. The scheduling is carried out for 24 hours considering both grid-connected and islanded operation modes.

A.1 Grid-Connected Mode

Table II shows the optimal output power of DGUs and the converter in the grid-connected operation mode. As can be seen from Table I and Fig. 2, the power generation price for different DGUs as well as the energy market price at different hours of the day are different. Therefore, it is more efficient to turn off expensive units during the hours when the market price is lower than DGUs' generation price. According to Table IV,

by comparing the operation cost of the system in grid-connected mode with the operation cost of islanded mode, in which HMG is not connected to the utility grid and all of the loads are supplied by DGUs, it can be seen that this is a beneficial policy to decrease the operation cost of the system. As can be seen from Table IV, in grid-connected mode, the maximum voltage deviation constraint (i.e. 0.1pu) is satisfied.

Table II Optimal output power of DGUs in grid-connected mode

PV1	WT1	Fuel Cell	MT1	AC-DC Converter	MT2	MT3	WT2	WT3	PV2
0	24	0	35	97.2	0	0	65.45	53.6	0
0	24	50	0	76.2	0	0	65.45	53.6	0
0	18	0	0	132.2	0	94.8	48.95	40.1	0
0	30	0	0	123	0	244.8	82.5	67.5	0
0	41	0	0	127.2	0	393.5	112.2	91.8	0
0	36	110	35.02	-6.9761	184.7	500.8	99	81	0
27.3	48	219.3	95.02	-179.56	369.4	650.5	132	108	44
62.5	52	329.1	155.02	-373.65	554.4	800.4	143	117	100
85	52	439.1	215.01	-563.14	738.7	950.4	143	117	136
97.5	60	549.1	275.01	-741.64	922.6	1099	165	135	156
117	58	657.9	299.87	-898.81	1073	1100	159.5	131	187
118	62	691.1	297.21	-945.77	1231	950	170.5	140	188
115	58	700	300	-957.25	1300	857.2	159.5	131	184
125	54	628.9	287.89	-879.74	1300	974.5	148.5	122	200
118	57	519	271.04	-736.54	1300	1007	156.8	128	188
87.5	60	611.6	292.28	-810.93	1300	923.6	163.9	134	140
65	66	538	232.28	-646.32	1300	911.6	181.5	149	104
47.5	70	428.3	271.83	-553.59	1300	761.6	192.5	158	76
10	80	321.1	223.68	-364.74	1300	611.6	220	180	16
0	90	211.1	164.03	-204.09	1296	662.1	247.5	203	0
0	84	312.9	224.03	-386.95	1297	731.1	231	189	0
0	78	218.6	176.4	-259.99	1115	581.1	214.5	176	0
0	72	108.6	119.25	-104.84	945.4	431.8	198	162	0
0	44	0	59.366	64.634	1003	282.2	121	99	0

Table III Optimal output power of DGUs in islanded mode

PV1	WT1	Fuel Cell	MT1	AC-DC Converter	MT2	MT3	WT2	WT3	PV2
0	24	680.3	157.2	-705.27	310.6	1094	65.45	53.6	0
0	24	698.8	209.24	-781.84	495.6	1027	65.45	53.6	0
0	18	665.2	149.24	-682.21	439.9	981.7	48.95	40.1	0
0	30	696.6	171.82	-745.38	456.3	955.6	82.5	67.5	0
0	41	691.2	228.95	-792.96	612	1003	112.2	91.8	0
0	36	685.3	172.79	-720.07	650.9	1050	99	81	0
27.3	48	581.2	215.14	-661.58	766.1	935.1	132	108	44
62.5	52	621.1	266.75	-777.36	951.1	877.1	143	117	100
85	52	663.6	257.54	-830.09	1044	969.8	143	117	136
97.5	60	617.8	235.32	-770.65	1229	939.5	165	135	156
117	58	649.8	253.02	-843.81	1300	1090	159.5	131	187
118	62	640	295.4	-892.88	1300	1100	170.5	140	188
115	58	645.6	274.41	-877.23	1300	1100	159.5	131	184
125	54	700	264.15	-927.15	1300	1100	148.5	122	200
118	57	590.2	258.02	-794.7	1300	1100	156.8	128	188
87.5	60	639.2	231.98	-778.3	1300	1100	163.9	134	140
65	66	532.2	274.67	-682.85	1300	1100	181.5	149	104
47.5	70	422.2	214.67	-490.35	1240	1058	192.5	158	76
10	80	419.4	274.67	-514.1	1300	1059	220	180	16
0	90	528.8	298.22	-656.01	1298	1006	247.5	203	0
0	84	610.8	298.83	-759.63	1300	1004	231	189	0
0	78	664.1	265.12	-794.26	1300	854.4	214.5	176	0
0	72	583.8	235.5	-696.3	1163	704.4	198	162	0
0	44	581.9	287.92	-745.83	1111	554.4	121	99	0

A.2 Islanded Mode

The simulation results related to the optimal scheduling of HMG in islanded mode are presented in Table III. As can be seen from Table IV, the operation cost in the islanded mode is higher than the grid-connected mode. This is due to the absence of a utility grid that can provide cheap energy in some hours. According to Table III, at peak load hours (i.e. middle of the day) most DGUs operate near their maximum generation capacity, and also it can be seen that in the scheduling the priority is given to the cheaper DGUs. Since the power generation capacity of DGUs in the ac sub-grid is lower than demand, at all hours of the day DGUs in the dc sub-grid inject power to the ac sub-grid. According to Table IV, similar to the grid-connected mode, the maximum voltage deviation constraint (i.e. 0.1pu) is satisfied in the islanded mode. Also, it can be seen from that table that power loss is reduced in the islanded mode which is the result of local load supply.

B. Operation of HMG Under Cyber-Attack

In order to investigate the effect of cyber-attacks on the operation of HMGs in steady-state, in this section FDIA with 35% severity is launched against the measured load demand values of the buses 7, 8, 20, 21, 24, 25, 29, 30, 31, and 32 as illustrated in Fig. 1. It is worth noting that these buses are the most loaded buses in the grid which contain a total load of 2100 kW. The attack is performed in the 12th hour of the day, which is the peak load hour. It is assumed that the attacker manipulates the data packet either in the location of the meter or on the communication path and reduces the measured load demand value of these buses by 35% of their actual demand. The analyses are provided for both islanded and grid-connected operation modes. It is worth noting that in this work, the dynamic effects of FDIA on the operation of the system are neglected, and also the energy not supplied penalty factor is considered as the maximum market price in the operation day (i.e. 4 $/kWh).

Table IV Power loss, operation cost, and maximum voltage deviation of different cases

Operation Mode	Case	Power Loss (kW)	Total Cost ($)	Maximum Voltage Deviation (pu)
Grid-Connected	No attack	2825.7	46499	0.059
Islanded operation mode	No attack	2615.6	48802	0.068
	%35 Attack	2460.3	54140	0.041

B.1 Grid-Connected Mode

In the grid-connected operation mode, when the hacker decreases the measured load value data, the MGCC decides to decrease the output power of DGUs. The moment DGUs reduce their power generation, the upstream grid (bus1) acts as a slack bus, and by injecting more power into the network does not allow the balance between generation and consumption to be disturbed. The MGCC that observes the real-time value of power exchanged with the upstream grid, increases the output power of dispatchable units to avoid purchasing expensive power from the upstream grid.

B.2 Islanded mode

Table V shows the output power of DGUs when an integrity attack with 35% severity is carried out. In this scenario when the attacker decreases the measured load value of buses, the MGCC sees 735 kW additional power in the system. At this moment, MGCC tends to reduce the power generation of DGUs to restore the power balance in the system. But due to the ramp rate limit of DGUs, their power generation can be decreased by a certain amount. In the case where an attack with %35 severity is carried out at the 12th hour, if all DGUs reduce their power output concerning the ramp-rate constraints, still 227.43 kW additional power will remain in the system. At this point, MGCC, which does not have any other plans to restore the balance, sends the emergency shutdown command to the fuel cell unit. Note that MGCC makes all of these decisions based on the false data received from meters. The moment the fuel cell turns off, the actual balance in the system is lost. At this moment, the only choice for MGCC to keep frequency in the range is to cut off some loads. After the shutdown-startup period of the fuel cell, which is neglected in this work, has passed, it turns on again. But due to its ramp rate limitation, it should start from its minimum capacity and increase its output step by step. In order to reduce load shedding in the system, all DGUs increase their output as much as they can. Tables V shows the output power of DGUs and hourly load shedding in the grid. As can be seen from Table IV, due to energy not supplied penalty cost, the operation cost of the system has increased 5,338$. Therefore, according to Tables V and IV, a successful attack can affect the performance of the system for hours and highly increase the operation cost of the system. Also, this kind of attack by preventing consumers from being supplied causes social damages as well.

Table V Hourly load shedding and output power of DGUs and converter in the islanded mode when integrity attack with %35 severity is carried out

PV1	WT1	Fuel Cell	MT1	AC-DC Converter	MT2	MT3	Load Shedding
0	24	680.3	157.2	-705.3	310.6	1094	0
0	24	698.8	209.24	-781.8	495.6	1027	0
0	18	665.2	149.24	-682.2	439.9	981.7	0

0	30	696.6	171.82	-745.4	456.3	955.6	0
0	41	691.2	228.95	-793	612	1003	0
0	36	685.3	172.79	-720.1	650.9	1050	0
27.3	48	581.2	215.14	-661.6	766.1	935.1	0
62.5	52	621.1	266.75	-777.4	951.1	877.1	0
85	52	663.6	257.54	-830.1	1044	969.8	0
97.5	60	617.8	235.32	-770.7	1229	939.5	0
117	58	649.8	253.02	-843.8	1300	1090	0
118	62	50	300	-307.5	1300	1100	528.862
115	58	160	300	-417.3	1300	1100	412.945
125	54	270	300	-533	1300	1100	350.097
118	57	380	300	-626.5	1300	1100	149.482
87.5	60	490	300	-697.1	1300	1100	72.1813
65	66	532.2	274.67	-682.9	1300	1100	0
47.5	70	422.2	214.67	-490.4	1240	1058	0
10	80	419.4	274.67	-514.1	1300	1059	0
0	90	528.8	298.22	-656	1298	1006	0
0	84	610.8	298.83	-759.6	1300	1004	0
0	78	664.1	265.12	-794.3	1300	854.4	0
0	72	583.8	235.5	-696.3	1163	704.4	0
0	44	581.9	287.92	-745.8	1111	554.4	0

C. SPRT-Based Intrusion Detection System Performance Analysis

In this section, we analyze the performance of the SPRT based IDS. Regarding (17), in order to investigate the effects of different parameters of the SPRT on λ^i, a sensitivity analysis considering two scenarios is considered. In the scenario, the false-negative value is fixed and the λ^i-n diagram is plotted for different values of α^i. Note that in Fig. 3, it is assumed that $P_1{}^i$=0.85 and $P_0{}^i$=0.1. As can be seen from Fig. 3, there is a reverse relation between λ^i and n, meaning that the fraction of observations with type H_1 required for the IDS to accept the alternative hypothesis decreases when the sample set size goes up. Fig. 3 indicates that for a fixed sample set size (n), decreasing α^i increases the λ^i which is what we expected. In general, it can be concluded that however lower false positive and false negative rates result in a more accurate model, but on the other hand, it slows down the detection process. Therefore, there is a trade-off between the model accuracy and decision-making speed.

Let N^i denote the size of the sample set in which the SPRT decides to accept a hypothesis. Since $S_{SPRT}{}^i$ is a random variable and also according to (18) and (19), the expected values for N^i are functions of four parameters (i.e. $P_1{}^i$, $P_0{}^i$, α^i, β^i), with these variable specified we can calculate the expected values. To this end, Fig. 4 shows the relation between the $P_1{}^i$ and the expected N^i in which the SPRT hits the upper threshold

(i.e. $E(N^i|H1_1)$). In Fig. 4 $\alpha^i=\beta^i=0.01$. This diagram is plotted considering three different values for P_0^i. As can be seen, increasing P_1^i decreases the $E(N^i|H1_1)$ and in contrast, increasing P_0^i when P_1^i is fixed increases the expected value. It can be concluded that increasing P_1^i, as well as decreasing P_0^i, results in a faster detection process.

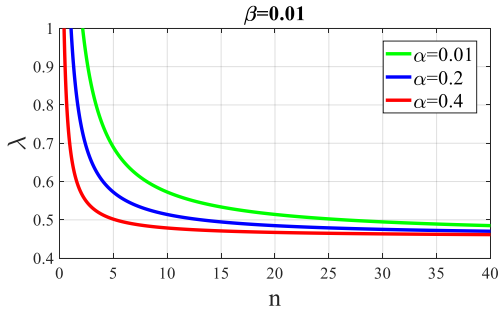

Fig. 3: λ^i vs n, when β^i is constant

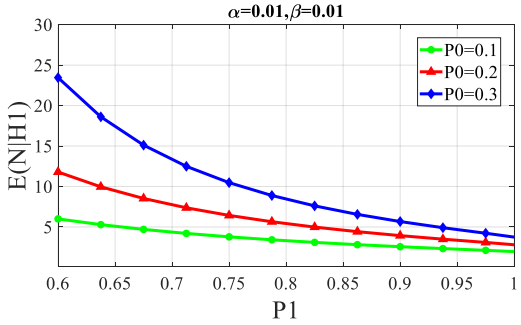

Fig. 4 $E(N^i|H1_1)$ vs P_1^i

In order to evaluate the performance of the proposed IDS, a scenario consisting of two cyber-attacks (i.e. FDIA and spoofing attack) is launched against the test system. In the attack scenario, the hacker penetrates the system at the 5th hour of the day and individually forges the IP address and identity information of the smart meter of bus 9, and sends false data to the central control. Since the hacker and the legitimate node have different geographical locations, their signal communication path, and RSS values are different. According to [21], the mean value and standard deviation of the RSS historical data set for the legitimate node are considered as μ_i=-89.4 dBm and σ_i=3.09 and for the adversary is considered as μ_i=-69.4 dBm, σ_i=5.69. It is worth noting that the RSS data are generated using the random normal distribution. Also, the hacked measured power data are generated using a uniform normal distribution such that their deviation from

the corresponding forecasted values is in the range of [0.08× $P_{l,f}^{j}$, 0.2× $P_{l,f}^{j}$]. Note that since the received data with a deviation of more than 0.2× $P_{l,f}^{j}$ are directly considered as the attack, data with deviation out of [0.08× $P_{l,f}^{j}$, 0.2× $P_{l,f}^{j}$] range is not generated.

Table VI and Table VII show the performance of the proposed IDS. In the following results, parameters of the integrity level are UE^{i}=0.2, LE^{i}=0.8, P_1^{i}=0.95, P_0^{i}=0.1, α^{i}=0.01, and β^{i}=0.02 and parameters of the identity level are P_1^{i}=0.96, P_0^{i}=0.05, α^{i}=0.01, and β^{i}=0.02. As can be seen from Table VI and Table VII, the identity level has detected the spoofing attack with two samples and the integrity level has detected FDIA with three samples. Note that during the process, after a decision was made in any of the levels, the probability ratio related to that level becomes zero. In the case of Sybil attacks, since the RSS value of the Sybil node is different from other nodes, when the Sybil node impersonated the identity of other nodes and sends information to the hybrid MGCC, the proposed IDS can easily detect the anomaly and detect the attack.

Table VI Performance of the integrity level

Hour	RRS of the legitimate node	RSS of adversary node	Probability ratio vs thresholds	Decision
1	-87.73	-	$Ln(L_{rss}^{i})<-3.16<ln(U_{rss}^{i})$	No decision
2	-90.15	-	$-6.33<ln(L_{rss}^{i})$	No attack
3	-89.48	-	$Ln(L_{rss}^{i})<-3.16<ln(U_{rss}^{i})$	No decision
4	-91.72	-	$-6.33<ln(L_{rss}^{i})$	No attack
5	-92.39	-64.68	$Ln(L_{rss}^{i})<+2.95<ln(U_{rss}^{i})$	No decision
6	-90.99	-76.54	$Ln(U_{rss}^{i})<+5.90$	Attack
7	-88.42	-69.41	-	-
8	-88.73	-78.71	-	-
9	-91.94	-69.78	-	-

Table VII Performance of the identity level

Hour	Forecasted load of bus 9	received data	Probability ratio vs thresholds	Decision
1	58	58	$Ln(L_l^{i})<-2.89<ln(U_l^{i})$	No decision
2	58.5	58.5	$-5.78<ln(L_l^{i})$	No attack
3	53.1	53.1	$Ln(L_l^{i})<-2.89<ln(U_l^{i})$	No decision
4	55.8	55.8	$-5.78<ln(L_l^{i})$	No attack

5	63	68.29	$Ln(L_l^i)<+2.25<ln(U_l^i)$	No decision
6	62.82	70.93	$Ln(L_l^i)<+4.50<ln(U_l^i)$	No decision
7	63.9	76.13	$Ln(U^i)<6.75$	Attack
8	71.1	76.88	-	-
9	77.4	89.55	-	-

IV. Conclusion

This paper proposed an in-depth secured management architecture for optimal operation of EI HMGs. The proposed architecture consists of two layers: the physical layer and the cyber layer. Results showed the good performance of the proposed optimal scheduling method in minimizing the operation cost of the system by optimally adjusting the output power of DGUs and energy storage. Also, the performance of the proposed IDS was examined using a test case. The results of this part showed the good performance of the proposed IDS in detecting cyber-attacks. Additionally, in order to investigate the effect of cyber-attacks on the HMGs, FDIA with 35% severity executed on the test system. The results showed that a successful cyber-attack can highly damage the grid and cause economical losses and load shedding.

References

[1] Rifkin J. The third industrial revolution: how lateral power is transforming energy, the economy, and the world. Macmillan; 2011 Sep 27.

[2] Hong, Bowen, et al. "Energy-Internet-oriented microgrid energy management system architecture and its application in China." *Applied Energy* 228 (2018): 2153-2164.

[3] Hussain, S. M., et al. "The emerging energy internet: Architecture, benefits, challenges, and future prospects." *Electronics* 8.9 (2019): 1037.

[4] Lei, Ming, and Mojtaba Mohammadi. "Hybrid machine learning based energy policy and management in the renewable-based microgrids considering hybrid electric vehicle charging demand." International Journal of Electrical Power & Energy Systems 128: 106702.

[5] Cheng, T., Zhu, X., Gu, X., Yang, F. and Mohammadi, M., 2021. Stochastic Energy Management and Scheduling of Microgrids in Correlated Environment: A Deep Learning-Oriented approach. *Sustainable Cities and Society*, p.102856.

[6] Tajalli, Seyede Zahra, et al. "A secure distributed cloud-fog based framework for economic operation of microgrids." *2019 IEEE Texas Power and Energy Conference (TPEC)*. IEEE, 2019.

[7] Papari, Behnaz, et al. "Effective energy management of hybrid ac–dc microgrids with storage devices." *IEEE transactions on smart grid* 10.1 (2017): 193-203.

[8] Baziar, A., & Kavousi-Fard, A. (2013). Considering uncertainty in the optimal energy management of renewable micro-grids including storage devices. *Renewable Energy*, *59*, 158-166.

[9] Gong, Xuan, et al. "A secured energy management architecture for smart hybrid microgrids considering PEM-fuel cell and electric vehicles." *IEEE Access* 8 (2020): 47807-47823.

[10] Dabbaghjamanesh, M., Kavousi-Fard, A., & Dong, Z. (2020). A novel distributed cloud-fog based framework for energy management of networked microgrids. *IEEE Transactions on Power Systems*.

[11] Tajalli, S.Z., Mardaneh, M., Taherian-Fard, E., Izadian, A., Kavousi-Fard, A., Dabbaghjamanesh, M. and Niknam, T., 2020. DoS-resilient distributed optimal scheduling in a fog supporting IIoT-based smart microgrid. *IEEE Transactions on Industry Applications*, *56*(3), pp.2968-2977.

[12] Li, Z., Shahidehpour, M., & Liu, X. (2018). Cyber-secure decentralized energy management for IoT-enabled active distribution networks. *Journal of Modern Power Systems and Clean Energy*, *6*(5), 900-917.

[13] Zhang, Huaguang, et al. "Distributed optimal energy management for energy internet." *IEEE Transactions on Industrial Informatics* 13.6 (2017): 3081-3097.

[14] Hua, Haochen, et al. "Optimal energy management strategies for energy Internet via deep reinforcement learning approach." *Applied Energy* 239 (2019): 598-609.

[15]Tabar, Vahid Sohrabi, Saeid Ghassemzadeh, and Sajjad Tohidi. "Energy management in hybrid microgrid with considering multiple power market and real time demand response." *Energy* 174 (2019): 10-23.

[16]Abdollah, K.F., Su, W. and Jin, T., 2020. A Machine Learning Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids. *IEEE Transactions on Industrial Informatics*.

[17]Wang, Huaizhi, et al. "Deep learning-based interval state estimation of ac smart grids against sparse cyber attacks." *IEEE Transactions on Industrial Informatics* 14.11 (2018): 4766-4778.

[18]Tang, Zhanyong, et al. "Exploiting wireless received signal strength indicators to detect evil-twin attacks in smart homes." *Mobile Information Systems* 2017 (2017).

[19]Wald, A., 2004. *Sequential analysis*. Courier Corporation.

[20]Rao, R. V., Savsani, V. J., & Vakharia, D. P. (2011). Teaching–learning-based optimization: a novel method for constrained mechanical design optimization problems. *Computer-Aided Design*, *43*(3), 303-315.

[21]Le, N. T., & Benjapolakul, W. (2019). Received signal strength data of ZigBee technology for on-street environment at 2.4 GHz band and the interruption of vehicle to link quality. *Data in brief*, *22*, 1036-1043.

[22]Gottschalk, Marion, Mathias Uslar, and Christina Delfs. *The Use Case and Smart Grid Architecture Model Approach: The IEC 62559-2 Use Case Template and the SGAM Applied in Various Domains*. Springer, 2017.

[23]Štruklec, Gordan, and Joško Maršić. "Implementing DLMS/COSEM in smart meters." *2011 8th International Conference on the European Energy Market (EEM)*. IEEE, 2011.

[24]Ahmed, M. and Pathan, A.S.K., 2020. False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling*, *8*, pp.1-14.

Mojtaba Mohammadi received his B.Sc. degree in Control engineering from Shiraz University of Technology, Iran, in 2019. He is currently pursuing his M.Sc. degree in Electrical engineering at Shiraz University of Technology, Iran. His current research interests include machine/deep learning, management and operation of smart grids and microgrids, power system cyber security, Blockchain, and Bitcoin. Mojtaba Mohammadi is reviewer of IEEE transactions on industry applications, international journal of electrical power & energy systems (Elsevier), sustainable cities and society (Elsevier), and Iranian journal of science and technology (Springer).

Abdollah Kavousi-Fard (M'15, SM'19) received the B.Sc. degree from Shiraz University of Technology, Shiraz, Iran, in 2009; the M.Sc. degree from Shiraz University, Shiraz, in 2011; and the Ph.D. degree from Shiraz University of Technology, Shiraz, Iran, in 2016, all in electrical engineering. He was a Postdoctoral Research Assistant at the University of Michigan, Mi, USA from 2016-2018. Dr. Kavousi-Fard was a researcher with the University of Denver, Denver, CO, USA from 2015 to 2016 conducting research on microgrids. His current 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.

Morteza Dabbaghjamanesh (SM’19) received the M.Sc. degree in electrical engineering from Northern Illinois University, DeKalb, IL, USA, in 2014, and the Ph.D. degree in electrical and computer engineer ing form Louisiana State University, Baton Rouge, LA, USA in 2019. Currently, he is a Research Associate in the Design and Optimization of Energy Systems (DOES) Laboratory at the University of Texas at Dallas, Richardson, TX, USA. His current research interests include power system operation and planning, reliability, resiliency, renewable energy sources, cybersecurity analysis, machine/deep learning, smart grids, and microgrids.

Amir Farughian received his B.Sc. degree in Electrical Engineering from Shiraz University of Technology, Iran, 2010 and the M.Sc. degree in Smart Grids from Tampere University of Technology, Finland in 2015. He is currently pursuing the Ph.D. degree at University of Vaasa, Finland. His research interest includes earth fault location in medium voltage distribution networks. He was involved in several research projects as a project researcher from 2015 to 2019. Mr. Farughian is a member of FREESI smart grid laboratory which is a member of DERlab, an international network of leading research laboratories focusing on distributed energy resources.

Abbas Khosravi (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2002, the M.Sc. degree in electrical engineering from the Amirkabir University of Technology, Tehran, in 2005, and the Ph.D. degree from Deakin University, Australia, in 2010. He is currently an associate professor at IISRI of Deakin University. His research interests include artificial intelligence, data mining, optimization, and their applications in different fields of science and engineering