Reinforcing Data Integrity in Renewable Hybrid AC-DC Microgrids from Social-Economic Perspectives

Author(s): Mohammadi, Mojtaba; Kavousi-Fard, Abdollah; Dehghani, Moslem; Karimi, Mazaher; Loia, Vincenzo; Haes Alhelou, Hassan; Siano, Pierluigi

Title: Reinforcing Data Integrity in Renewable Hybrid AC-DC Microgrids from Social-Economic Perspectives

Year: 2022

Version: Accepted manuscript

Mohammadi, M., Kavousi-Fard, A., Dehghani, M., Karimi, M., Loia, V., Haes Alhelou, H. & Siano, P. (2022). Reinforcing Data Integrity in Renewable Hybrid AC-DC Microgrids from Social-Economic Perspectives. *ACM Transactions on Sensor Networks*. https://doi.org/10.1145/3512891

Reinforcing Data Integrity in Renewable Hybrid AC-DC Microgrids from Social-Economic Perspectives

Mojtaba Mohammadi

Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran,

Abdollah Kavousi-Fard *

Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran,

Moslem Dehghani

Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran,

Mazaher Karimi

School of Technology and Innovations, University of Vaasa, Wolffintie 34, 65200 Vaasa, Finland,

Vincenzo Loia

Department of Management and Innovation Systems, University of Salerno, Salerno, Italy

Hassan Haes Alhelou *

Department of Electrical Power Engineering, Tishreen University, Lattakia, Syria,

Pierluigi Siano

Department of Management and Innovation Systems, University of Salerno, Salerno, Italy

The microgrid (MG) is a complicated cyber-physical system that operates based on interactions between physical processes and computational components, which make it vulnerable to varied cyber-attacks. In this paper, the impact of data integrity attack (DIA) has been considered, as one of the most dangerous cyber threats to MGs, on the steady-state operation of hybrid MGs (HMGs). Additionally, a novel method based on sequential hypothesis testing (SHT) approach, is proposed to detect DIA on the renewable energy sources' metering infrastructure and improve the data security within the HMGs. The proposed method generates a binary sample, which is used to compute a test statistic that is further used against two thresholds to decide among three alternatives. The performance of the suggested method is examined using an IEEE standard test system. The results illustrated the acceptable performance of the proposed methodology in detection of DIAs. Also, to evaluate the effect of DIA on the operation of the HMGs, DIAs with different severities are launched on the measured power generation of renewable energy resources (RESs) like wind turbine (WT). The results of this part showed that a successful DIA on renewable units can severely affect the operation of electric grids and cause serious damages.

CCS CONCEPTS • Security and privacy → Intrusion/anomaly detection and malware mitigation • Security and privacy → Systems security • Computer systems organization → Embedded and cyber-physical systems

Keywords: Advanced Metering Infrastructure, Data Integrity, Hybrid Microgrids, Renewable Energy Sources, Sequential Hypothesis Testing.

ACM Reference Format:

Mojtaba Mohammadi, Abdollah Kavousi-fard, Moslem Dehghani, Mazaher Karimi, Vincenzo Loia, Hassan Haes Alhelou, Pierluigi Siano. 2021. Reinforcing Data Integrity in Renewable Hybrid AC-DC Microgrids from Social-Economic Perspectives.

1 INTRODUCTION

Microgrid (MG) is a combination of controllable loads, distributed generation (DG) units, and energy storage devices, which acts as an individual controllable unit and can operate in islanded or grid-connected mode. The concept of MG brings many benefits to both power generation companies and electricity consumers. From the consumer's point of view, the MG can increase reliability, reduce greenhouse gas emissions, improve power quality, and from power generation companies’ point of view, it can eliminate peak consumption points, reduce power loss, reduce operation costs, etc. [1-4]. Moreover, the development of MG is able to aid to supply remote loads when the proper distributions or transmission infrastructure are not available. It is expected that the installation of MG capacity in the United States (US) will reach more than 30% increase by 2020 [5].

In terms of voltage types, MGs is able to be categorized into three different categories of AC, DC, and hybrid AC-DC [6]. In AC MGs, all DG agents and loads have been coupled to the AC busses. Therefore, the DC sources have been connected to the grid using DC-AC converters and DC loads can be supplied using AC-DC inverters. DC MGs use rectifiers to connect AC generation agents to the system and HMGs make usage of advantages in both DC and AC MGs through incorporating both kinds of technologies and busses [7]. In this way, the use of advanced communication and information technology by MGs to provide an infrastructure for the exchange of information such as advanced metering infrastructure (AMI), improves the dynamics and operation of MGs. However, it makes MGs vulnerable to cyber-attacks at the same time. Therefore, the health of data transmission and measuring devices (AMI in short) must be taken into consideration to increase MG security [8].

Regarding the growth of the MGs in modern power systems, serious concerns about cyber-attacks have appeared. Pursuant to the recent reports from the US department of homeland security, 224 attacks on electrical companies were reported from 2013 to 2014. The malicious cyber-attack of Stuxnet worm to the SCADA system in 2010 could damage the industrial electrical systems severely [9, 10]. Therefore, concerns have been raised about cyber-attacks on MG’s vulnerable points in the power system. In [11,12], a machine learning based DIA detection scheme on the basis of upper and lower bound estimation way and symbiotic organisms search algorithm is proposed to detect anomaly in MGs’ AMI. The results in that paper showed the proposed evolutionary method over genetic algorithm and other methods. the main drawback of the proposed method in [12] is the reverse relation between the attack severity and detection rate. Authors in [13] presented a review of cyber-attacks in power systems, their impacts on economic aspects of the system, and describe possible attack scenarios and some defense strategies. A sequential false data injection detection scheme is investigated in [14]. The results of that paper showed the good performance of the proposed methodology in attack detection. In [15], hybrid model based on SHT is proposed to detect several attacks. the results of that paper showed the high accuracy and performance of the SHT in detection of identity-based attacks. Authors in [16] developed a method to identify the false data injection attacks in MGs. The main drawback of the proposed method in that paper is the high rate of false negative. In [17] the authors used a hierarchical framework to detect cyber attacks and a decision tree algorithm to eliminate the cyber-attacks targeting PMUs. The mentioned hybrid framework was able to detect most of FDI and DoS attacks. A deep learning regression method can be used to boost the accuracy of the mentioned method instead of decision tree. Authors in [18] focused on the Sybil attacks and proposed a detection model. The results of that paper illustrated the vulnerability of MGs against such attacks. They also introduced various models of flooding attack and malware installation attack on AMI. Authors in [19-21] introduced two types of false data injection attacks against power system economic dispatch and analyzed their impact on optimality and stability of the system. Table 1 displays a summary of some of the well-known cyber-attacks on the power grid in recent years [12]. In [22], an SHT based detection method is introduced to identify Sybil attack in wireless sensor networks. In this method, each node uses the identity and location of neighboring nodes to detect Sybil nodes in wireless sensor networks. Once the Sybil node was identified, all neighboring nodes cut off communication with it and the malicious node will be isolated. Reference [23] investigated the denial of service (DOS) cyber-attack on static VAR compensator (SVC) and its impacts on the smart grid. In that paper, two kinds of delays are modeled, exponentially distributed delay and fixed delay. The results show that such attacks on SVC can strongly affect voltage stability of the system and in some cases even cause voltage collapse. Wavelet transform is applied to detect false data injection attacks in AC smart grids [24]. Authors in [25] proposed a detection scheme using the statistical model to predict automatic generation control operation and also to consider the impact of DIAs from the electricity market and power system frequency perspectives. References [26-28] proposed blockchain technology as an intrusion prevention system to improve the security of data transactions.

Table 1: A review of most well-known cyber-attacks in recent years [12]

Attack type	Impact	Attack point
DOS attack	Disconnecting 30 substations for about three hours and outage of more than 230000 people	SCADA system, Ukraine, 2015
Slammer Worm	Disabling safety alert system	Ohio Nuclear Power Plant, USA, 2002
Stuxnet worm	Disrupting industrial components	SCADA System, Iran, 2010
Havex malware	Disruption and damage to ICS (Industrial Control Systems)	ICS United States and Europe, 2014

As each of the mentioned studies has addressed an aspect of cyber-attacks in modern power systems, none of them has considered the cyber-attack issues in the HMGs. In fact, the widespread penetration of AMI technology in modern power systems brings many security issues. The intelligent operation of MGs has been endeavored with the secured monitoring and control of local power generation units and consumers. In this way, DIAs can interrupt MGs operation by injecting false data instead of healthy data reported through smart meters. Such attacks can silently manipulate legitimate data and lead MG central control (MGCC) to make wrong decisions and give commands based on incorrect data and cause problems in dynamic and steady-state operation of MGs.

This paper is focused on the DIA on the RESs' metering interfaces and its effects on HMGs' steady-state operation. To investigate the effects of such attacks, the DIA is executed with different severities on a practical HMG. In the simulation section, a hybrid AC-DC MGs has been analyzed based on IEEE standard test system that includes five RESs in AC and DC sub-grids. It has been assumed that an adversary suddenly increases the measured output power of these RESs by 35%, 50%, and 65% of their maximum capacity. The performance of the system and the effects of this cyber-attack from both social and economic point of views is analyzed in detail. A new and relatively simple method to detect DIA is considered based on Wald's procedure [29]. The SHT is a widespread approach to identify defect items in manufacturing industries.

Unlike conventional hypothesis testing techniques, SHT does not reach the decision with fixed-size samples, and also it aims to minimize the decision error. Experimental outcomes display that sequential sampling requires fewer instances than fixed-size sampling [30].

Generally, there are several advantages associated with the proposed method over traditional detection methods. For instance, the proposed SHT-based method is a sequential decision making approach, meaning that this method makes decisions based on the sequence of samples rather than only one sample. Therefore, this method is more trustworthy than non-sequential based methods. Another advantage of the proposed method is its ability to build a sequence of statistics where each step builds on the prior steps. In contrast with machine/deep learning-based detection methods, which require high computational power to train, this method can detect anomalies using only several simple operations. Therefore, the proposed method has a highly effective performance from computation point of view. In order to investigate the performance of the proposed method, its performance is examined using a case study. It is worth noting that this paper is the first work addressing impact of cyber-attacks on the scheduling of hybrid microgrids.

The main contribution of this paper is summarized as follow: 1) Investigating the cyber security in hybrid microgrids as a cyber-physical system; 2) Developing a SHT-based cyber-attack detection method; 3) Simulating data integrity attack against measured output power of renewable energy resources.

The rest of the study has been formed as follows: Part 2 has been explained cyber security in MGs and descries the cyber-attack pattern. The system layout and assumptions have been expressed in part 3. In part 4, an efficient anomaly detection model has been proposed based on the SHT procedure to diagnose and stop DIA in HMGs. In this part, the formulation of the suggested technique and analysis of its performance are presented. In section 5, DIA with different severities executed on a HMG and feasibility and proficiency of the suggested technique is investigated. The main conclusion of this paper is explained in Section 6.

2 CYBER SECURITY IN MGS WITH DIA

This part is focused on the cyber security of MGs, defines MGs as a cyber-physical system (CPS), and explains the model of cyber-attacks.

2.1 Cyber security in MGs as a CPS

According to the United States' national science foundation, CPS is defined as "systems that are built from, and depend upon, the integrated physical components and computational algorithms." MGs generally consist of two infrastructures: the cyber layer and the physical layer. The physical layer contains DG units, controllable loads, substations, etc., and the cyber layer mainly includes MGCC, metering devices, and communication platforms and makes decisions based on data obtained from the physical layer using AMI. Extensive interaction between the two layers makes MG a complex cyber-physical system that is a great target for hackers to cause damages to the grid. Therefore, appropriate measures should be taken to increase the system's cyber security. AMI is the main key layer producing a two-way communication channel among the automated physical layer and MGCC. AMI is responsible for gathering data from the physical layer and communicating between system components, which makes real-time decision making in both the consumption and production side possible.

Generally, information security is characterized by three main principles, confidentiality, integrity, and availability together known as "CIA triad" [31]. A cyber-attack can be defined as any unauthorized action in the cyber layer that targets at least one of these indices. For instance, a DOS attack is an attack targeting the availability of data in the system. Integrity in AMI is defined as preventing varies to data as it is gained from metering devices and deterring unauthorized commands to be transmitted through the AMI system. figure 1 displays the schematic framework of MG incorporating the AMI. Also through AMI, all DGs are scheduled at optimal operation point and consumers are able to make informed choices about energy usage based on market price. Due to the great penetration and impact of intelligent devices on modern power systems, various security mechanisms such as encryption, signatures, alarms, detection schemes, identifiers, etc. should be implemented to ensure secure and reliable operation.

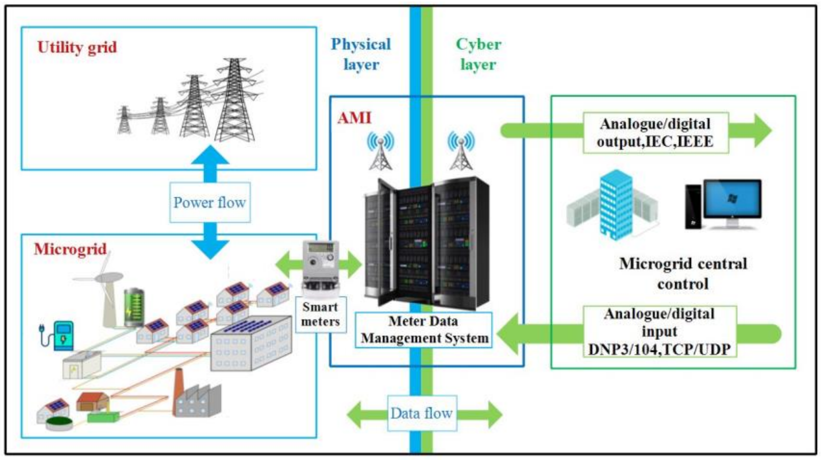
Utility grid
Physical layer
Cyber layer
AMI
Analogue/digital output,IEC,IEEE
Power flow
Microgrid
Smart meters
Meter Data Management System
Microgrid central control
Analogue/digital input DNP3/104,TCP/UDP
Data flow

Figure 1: Illustration of MG structure as a cyber-physical system

2.2 Cyber-attack

One of AMI's main goals is to gather data from consumers and DG agents and transfer it to the MGCC to provide the real-time information needed by central control for proper scheduling of loads and generation units. AMI can also reduce MG operation costs and avoid feeder congestion by shifting peak load hours using demand response technology. Benefits associated with AMI deployment depend on the accuracy and validity of the real-time data collected by smart meters. As using AMI brings a variety of benefits to the power grid, new security challenges arise at the same time. As described above, MGs are able to operate in islanding or non-islanding mode. The cyber-attack on AMI in grid-connected mode can increase operating costs and power loss and cause voltage collapse but in islanding mode, due to the lack of a high-powered grid, a cyber-attack can cause more damages such as losing the balance between generation and load demand, load shedding, blackouts, etc. MGCC optimizes the power dispatch based on loads and power generation capacity and decides to buy or sell power to the main grid based on electricity market price.

As one of the significant sources of energy in modern power systems, RESs play an important role in MG operation, so that any mismatch between measured power reported to the MGCC and actual power of RESs can lead MGCC to dispatch based on false data and cause problems in dynamic and steady-state operation of MGs. An attack that injects false data to the operation center or controllers of the grid is denoted as a DIA. In this paper, DIA has been analyzed on RESs measured data such that the adversary manipulates the measured power generation of the RESs either in the location of smart metering devices or in the communication path. This scenario has been investigated with different severities. An SHT based detection model is also offered to identify the cyber-attack activities in the HMG that has been described comprehensive in the following sections. The suggested anomaly detection scheme makes usage of the forecasted power generation of RESs, which MGCC uses for a day-ahead optimal economical dispatch.

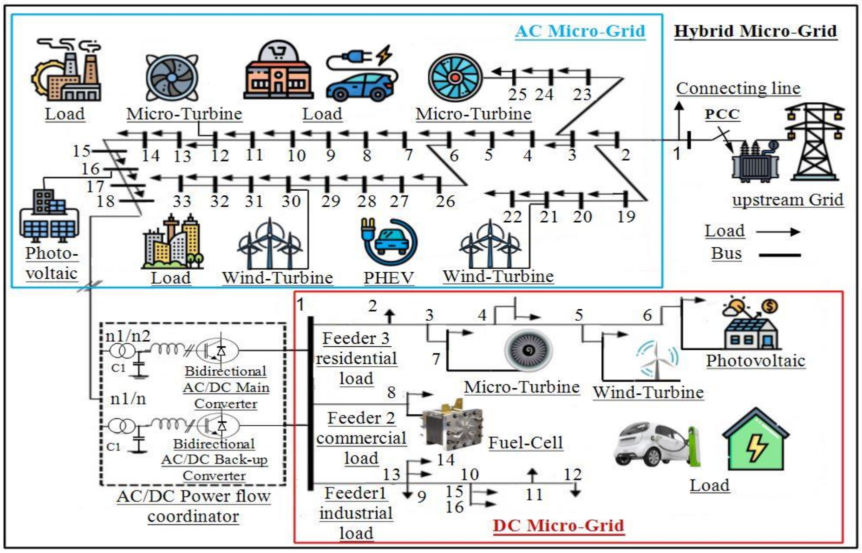

Figure 2: conceptual illustration of HMG system

3 SYSTEM MODEL AND ASSUMPTIONS

Figure 2 shows a conceptual illustration of HMGs in which different DC and AC loads and power agents are connected to the corresponding DC and AC busses. Also, HMG central control (HMGCC) is able to decide to buy/sell energy to the main grid and work in the islanding or non-islanding mode at different time intervals. To support the idea of RESs, photovoltaic (PV) and WT resources have been supposed as non-dispatchable units. In the day-ahead optimal dispatch, HMGCC schedules the DGs at their optimal point based on the system's information, load forecasted data, RESs forecasted data, and market price.

In this paper, it has been assumed that the forecasted power generation of the units is equal to the power provided in the operation moment and also stable and equal current sharing between parallel sources or power converters has been provided. In the operation moment, HMGCC uses the real-time data gathered by AMI in regular time intervals to provide a balance among power production and consumption in the grid. In this work, smart meters communicate with HMGCC once every hour. To achieve more reliable and realistic results, power generation units' ramp up/down rates are considered.

4 PROPOSED DIA DETECTION METHOD BASED ON THE SHT

HMGCC communicates with RESs' local smart metering devices in regular time intervals and monitors their real-time output power. Due to the lack of a suitable algorithm to check the validity of the received data, an adversary can disrupt the performance of the system by manipulating the data measured by smart meters. The SHT is adapted to tackle this problem.

SHT, also known as the sequential probability ratio test, is a statistical decision-making process that was presented and expanded via Wald [29]. SHT can be considered as a one-dimensional random walk with upper and lower thresholds. In SHT, first, two hypotheses have been described in such a way that the alternative hypothesis is related to the upper threshold, and the null hypothesis is related to the lower threshold. The process of making a decision, which it has been considered as a random walk, begins from a point among two thresholds and moves toward the upper or lower threshold concerning each observation. Once the random walk reaches/exceeds the upper threshold, the SHT admits the alternative hypothesis. In contrast, when the random walk reaches/exceeds the lower threshold, SHT admits the null hypothesis. Upper and lower thresholds are defined based on user-configured false negative and false positive rates in such a way that decision of false positive and false negative rates will not exceed these values, respectively.

4.1 Formulation

In order to formulate the SHT, two hypotheses have been considered:

- H_1 (alternative hypothesis): The sequence of data measured by the RES's metering device is corrupted.
- H_0 (null hypothesis): The sequence of data measured by the RES's metering device is legitimate.

For each RES, during the hypothesis testing process, X_k^i considers as a random variable and a hypothesis concerning is tested the integrity of data measured by the ith RES's smart meter. The process of determining the value of the random variable X_k^i, which is known as the observation, is based on comparing any data received from the smart meter with the corresponding value predicted by the HMGCC. Since the result of each observation does not affect the subsequence observations and all of the observations have equal distributions, then the probability of the random variables X^i is independent and identically distributed (iid) and is able to be collected as follows:

$$e_{ij} = | P_{ij}^{m} - P_{ij}^{f} | \tag{1}$$

$$X_k^{i} = \begin{cases} 0 & 0 \le e_{ij} \le 0.08 \times P_{ij}^{f} \\ 1 & 0.08 \times P_{ij}^{f} < e_{ij} \le 0.2 \times P_{ij}^{f} \end{cases} \tag{2}$$

Due to the unusual difference between measured and forecasted data, in a case where e_{ij} is greater than $0.2 \times P_{ij}^f$, we have been accepted the alternative hypothesis without calculating X_{k+1}^i and continuing the process. It is worth noting that considered $X_k^i=1$ and $X_k^i=0$ as an observation with type H_1 and observation with type H_0 respectively. The decision to reject or accept the hypothesis is always made based on finite observations. A set of finite observations is called a sample and the number of observations contained in the sample is called the sample size. In this way, the successive observations has been denoted by $X_1^i,\ldots,X_n^i$. For any positive value n, the probability that sample $X_1^i,\ldots, X_n^i$ is obtained so far is given by:

$$Y_{1n}^i = f(X_1^i | H_1)' \; f(X_2^i | H_1)....f(X_n^i | H_1) \tag{3}$$

when H_1 is true, and by:

$$Y_{0n}^i = f(X_1^i | H_0)' \; f(X_2^i | H_0)....f(X_n^i | H_0) \tag{4}$$

when H_0 is true.

At each step of the process (at nth observation), the value of the probability ratio is computed by $\ln(\frac{Y_{1n}^i}{Y_{0n}^i}) = \ln(\prod_{k=1}^{n} \frac{f(X_k^i|H_1)}{f(X_n^i|H_0)})$. The probability ratio can be simplified as follows:

$$\mathrm{Pr}_k^{i} = \ln(\frac{f(X_k^i | H_1)}{f(X_n^i | H_0)}) = \begin{cases} \ln(\frac{P_1^i}{P_0^i}) & X_k^i=1 \\ \ln(\frac{1-P_1^i}{1-P_0^i}) & X_k^i=0 \end{cases} \tag{5}$$

$$\ln(\prod_{k=1}^{n} \frac{f(X_k^i|H_1)}{f(X_k^i|H_0)}) = \sum_{k=1}^{n} \mathrm{Pr}_k^i = m * \ln(\frac{P_1^i}{P_0^i}) + (n-m) * \ln(\frac{1-P_1^i}{1-P_0^i}) \tag{6}$$

At each step of the process, if $\sum_{k=1}^{n} \Pr_k{}^i \leq \ln(L^i)$, the process is terminated with the acceptance of H0. If $\ln(U^i) \leq \sum_{k=1}^{n} \Pr_k{}^i$, the process is terminated with the acceptance of H1 and if $\ln(L^i) < \sum_{k=1}^{n} \Pr_k{}^i < \ln(U^i)$ the process moves forward by taking an additional observation. According to (5), in the next observation, if the X_{n+1} is an observation with type H_0, the constant $\ln((1\text{-}P_1{}^i)/(1\text{-}P_0{}^i))$ is added to the preceding value of (6) and if the observation is an observation with type H_1, the constant $\ln(P_1{}^i/P_0{}^i)$ is added to the preceding value of (6). This process will continue until the probability ratio reaches one of the thresholds. The constants Ui and Li must be determined in such a way that the test has the desired strength (α^i, β^i). For this purpose, based on [29], it should be considered U_i and L_i as below:

$$\begin{cases} L^i = \left(b^i/\left(1\text{-}\ a^i\right)\right) \\ U^i = ((1\text{-}\ b^i)/a^i) \end{cases} \tag{7}$$

It is worth noting that $(1\text{-}\beta^i)$ and $(1\text{-}\alpha^i)$ denote the detection rate and true negative rate respectively. Figure 3 displays the flowchart of the suggested SHT based method.

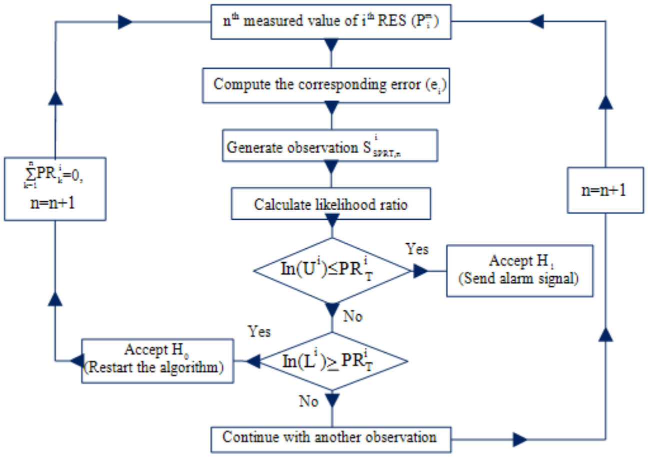
nth measured value of ith RES (P_i^n)
Compute the corresponding error (e_i)
Generate observation $S^i_{SPRT,n}$
Calculate likelihood ratio
$\ln(U^i) \leq PR^i_T$
Yes
Accept H_1
(Send alarm signal)
No
$\ln(L^i) \geq PR^i_T$
Yes
Accept H_0
(Restart the algorithm)
No
Continue with another observation
$\sum_{k=1}^{n} PR_k^i = 0,$
n=n+1
n=n+1

Figure 3: Flowchart of the suggested SHT based method

4.2 Analysis

Let λ^i (γ^i) denotes the ratio of the number of the observations with type H_1 (H_0) to the number of total observations in a sample with size n that HMGCC considers the sequence of data originated from ith RES as an adversary (legitimate) if sample $X_1{}^i,\ldots,X_n{}^i$ includes at least $\lambda^i \times n$ ($\gamma^i \times n$) ones (zeroes). According to (6), if the excess of probability ratio is neglected over the thresholds, λ^i and γ^i are able to be computed like below:

$$\lambda^i = \frac{\ln(\frac{1-\beta^i}{\alpha^i}) - n \times \ln(\frac{1-P^i{}_1}{1-P_0^i})}{n \times (\ln(\frac{P_1^i}{P_0^i}) - \ln(\frac{1-P_1^i}{1-P_0^i}))} \tag{8}$$

$$\gamma^i = \frac{\ln(\frac{\beta^i}{1-\alpha^i}) - n \times \ln(\frac{P_1^i}{P_0^i})}{n \times (\ln(\frac{1-P_1^i}{1-P_0^i}) - \ln(\frac{P_1^i}{P_0^i}))} \tag{9}$$

To explore how changing the n, α^i, and β^i affect the λ^i and γ^i, according to (8) and (9), λ^i-n and γ^i-n diagrams are plotted considering two scenarios. In the first (second) scenario, the λ^i-n(γ^i-n) diagram is plotted considering different values of α^i(β^i). It is worth noting that in Figure 4 and Figure 5, it is assumed that $P1^i$=0.85 and $P0^i$=0.1. As can be seen, in both cases λ^i and γ^i gradually decrease when n increases. Figure 4 indicates that this method requires a lower fraction of observations with type H1 to detect DIA when the size of the sample increases. Similarly, Figure 5 indicates that this method requires a lower fraction of observations with type H_0 to consider a sequence of data originated from corresponding RES as legitimate when the size of the sample increases.

Generally, it is desirable for us to minimize α^i and β^i. In this regard, as can be seen from Figure 5 that decreasing β^i significantly increases γ^i. Generally, it can be concluded that although decreasing either α^i or β^i makes our model more accurate, it slows down the decision-making process at the same time. The bottom line is that there is a trade-off between minimizing the α^i and β^i and the speed of the decision making process.

Let N^i denote the observation number at which the probability ratio of the ith RES first hits either upper threshold ln(U^i) or lower threshold ln(L^i). Since X^i is a random variable and the number of observations required for a decision to be made is not predetermined, it should be denoted the expected value of N^i by E(N^i|H_1) when the decision is made to accept alternative hypothesis and by E(N^i|H_0) when the decision is made to accept the null hypothesis. If it has been neglected the excess of ($Y_{1n}{}^i$/ $Y_{0n}{}^i$) over the boundaries U^i and L^i, for a decision to be made, the probability ratio can take only the values ln(U^i) or ln(L^i) with the probability (1-W^i(H_s)), s=0,1 and W^i(H_s) respectively. Therefore, the expected value of E($X_1{}^i$,…,$X_n{}^i$) can be calculated by (9). In this way the conditional expected value of N_i is able to be obtained like below:

$$E(X_1^i,...,X_n^i) = W^i(H_s)\times\ln(L^i) + (1-W^i(H_s))\times\ln(U^i) \tag{10}$$

$$E(N^i \mid H_0) = \frac{(1-\alpha^i)\times\ln(L^i) + \alpha^i \times \ln(U^i)}{P_0^i \times \ln(\frac{P_1^i}{P_0^i}) + (1-P_0^i)\ln(\frac{1-p_1{}^i}{1-p_0{}^i})} \tag{11}$$

$$E(N^i \mid H_1) = \frac{\beta^i \times\ln(L^i) + (1-\beta^i)\times\ln(U^i)}{P_1^i \times \ln(\frac{P_1^i}{P_0^i}) + (1-P_1^i)\ln(\frac{1-p_1{}^i}{1-p_0{}^i})} \tag{12}$$

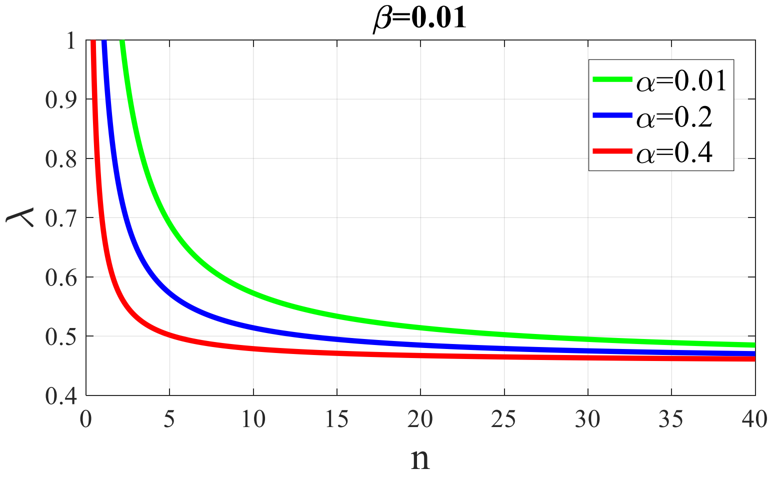

Figure 4. The effect of n on λi by considering different values for αi.

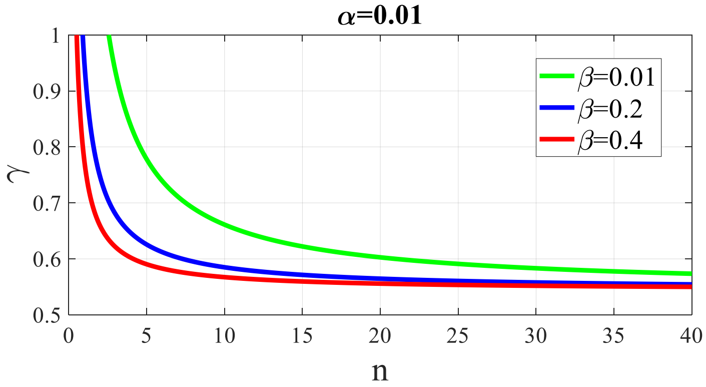

Figure 5. The effects of n on γ^i by considering different values for β^i.

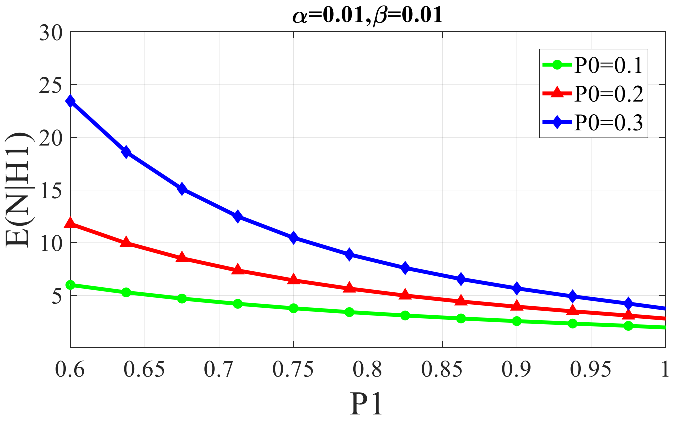

Figure 6. $E[N^i|H_1]$ vs. P_1^i when β^i =0.01 and α^i=0.01

As shown in (11) and (12), $E(N^i|H_0)$ and $E(N^i|H_1)$ are functions of four parameters P_1^i, P_0^i, α^i, and β^i. With these values set, it can estimate the average number of observations needed by the process to reach a decision. Figure 6 shows how $E(N|H_1)$ changes as P_1 increases. With α^i=0.01, β^i=0.01, and P_0^i=0.3, $E(N^i|H_1)$ is 4.22 when P_1^i=0.97, and it increases to 18.6 when P_1^i=0.63. According to Figure 6, by increasing P_1^i, the average number of observations needed via the technique to admit H_1 decreases, and by increasing P_0^i, this number increases. On the other hand, as can be seen from Figure 7, which presents the $E[N^i|H_0]$ vs. P_0i diagram, the values of the $E(N^i|H_0)$ and P_0 have direct relation. Note that in Figure 7 α^i=0.01 and β^i=0.01. Additionally, it can be seen from Figure 7 that $E(N^i|H_1)$ is highly sensitive to the value of P_1 such that when P_0=0.37, by increasing P_1 from 0.7 to 0.9, the value of $E(N^i|H_0)$ goes from 5.46 to 19.8. It is worth noting that this sensitivity decreases when lower values for P_0 are considered.

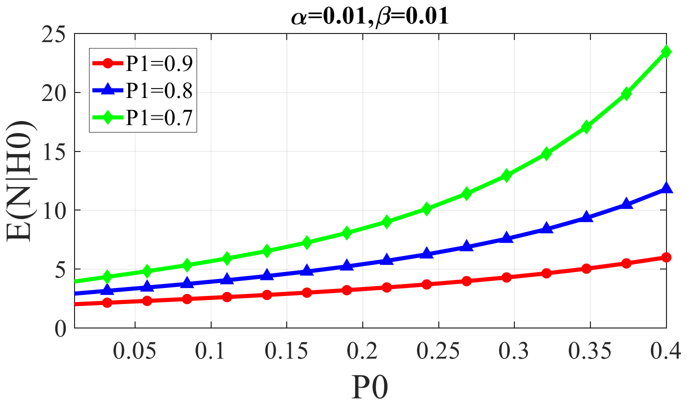

Figure 7. $E[N^i|H_0]$ vs. P_0^i when β^i =0.01 and α^i=0.01

5 NUMERICAL SIMULATIONS

5.1 Operation of the HMG under cyber-attack

The following part has been devoted to the numerical simulation result on a practical HMG, which is constructed based on the IEEE 33-bus standard test system, to investigate the effects of DIA on the steady-state operation. In the HMG, the IEEE 33-bus system is considered as the AC grid with an interconnected DC grid on the 18th bus. Figure 2 displays the schematic diagram of the HMG. The voltage level of the system in the AC part is 12.66 kV and the DC and AC parts have been coupled using AC-DC converters. As shown in Figure 2, five RESs (three WTs and two PVs) with the same pattern as shown in Figure 8 are connected to the system and three micro-turbines (MTs) are installed on busses 25, 18, and 12. The complete data of the DGs and converter can be found in Table 2. The AC MG load factor and DC MG load demand are also available in Figure 8. In the simulation, the resistance of the lines in the DC section has been neglected and bus 1 is assumed as an infinite bus. Power generation of RESs and loads are recorded on an hourly basis by smart meters installed in the location of loads and RESs.

The attack scenario is that the hacker penetrates the AMI and increases the value of recorded data related to RESs by 35%, 50%, and 65% of the RESs' maximum capacity in the 12th hour. To make a deep comparison, the analysis is simulated for 24 hours and in two different modes of islanded and grid-connected. As has been shown in Table 2, the energy production cost is various for different kinds of resources. Thus, HMGCC optimizes the operation of the loads and DGs to minimize the cost. For this purpose, the teacher learning algorithm has been used as a powerful tool for optimizing the cost and managing the energy in the grid. Note that in this work, the energy not supplied penalty factor is considered as the maximum market price value in the operation day (i.e. 5 $/kWh), while the dynamic effect of DIAs on the system is neglected and considered as the future work.

5.1.1 Islanded Mode

In this section, the effects of the DIA has been investigated on the islanded HMG operation. Technically, the HMG can decide to operate in either islanding or non-islanding modes depending on the situation. In the islanding mode, the main grid is modeled as a slack bus and controls the frequency of the system. In this operating mode, due to the presence of an infinite bus in the system, the HMG is resistant to frequency changes, which means that the upstream grid can generate or consume as much power as it needs to keep the frequency in the desired range. But in the islanded operation mode, due to the lack of the slack bus, it is the responsibility of the DGs to keep the frequency constant. Therefore, if unanticipated changes in the load or generation of the DGs exceeds the total ramp rate of the DGs, the frequency of the system cannot remain at the desired value. Table 3 displays the optimal power dispatch of the units in the islanded mode when no attack has been carried out. According to Table 3, when the system is not hacked, there is a balance between generation and consumption in both DC and AC sections, and the system operates normally.

Tables 4, 5, and 6 show the grid's hourly cost and the output power of generation units when an attacks with 35%, 50%, and 65% severity are launched against the RESs measured data. In these scenarios, the moment system has faced the cyber-attack, the adversary suddenly increases the data measured by smart meters dramatically. At this point, the HMGCC, based on incorrect data, observes excess power in the grid and decides to reduce the output power of other DGs. If the excess power is greater than the total ramp-down rate of the generation units, to balance between generation and consumption, the HMGCC will inevitably send an emergency shutdown command to at least one unit. As soon as the unit is switched off, due to the lack of power in the system, the balance among generation and consumption is lost and the frequency deviates from the desirable level. To adjust the frequency, HMGCC commands other units to increase their generation again.

Table 2: Characteristics of the converter and DG units

Type	Min Power (KW)	Max Power (KW)	Bid ($/KWh)	Startup/ shutdown cost ($)	Ramp Up/Down Rate
MT2	100	1300	0.475	75	185
MT3	90	1100	0.475	70	150
WT2	0	550	1.073	0	-
WT3	0	450	1.073	0	-
PV2	0	400	2.584	0	-
AC-DC converter	-1500	1500	-	-	-
Fuel cell	50	700	0.194	38.5	110
WT1	0	200	1.073	0	-
MT1	35	300	0.18	60	60
PV1	0	250	2.584	0	-

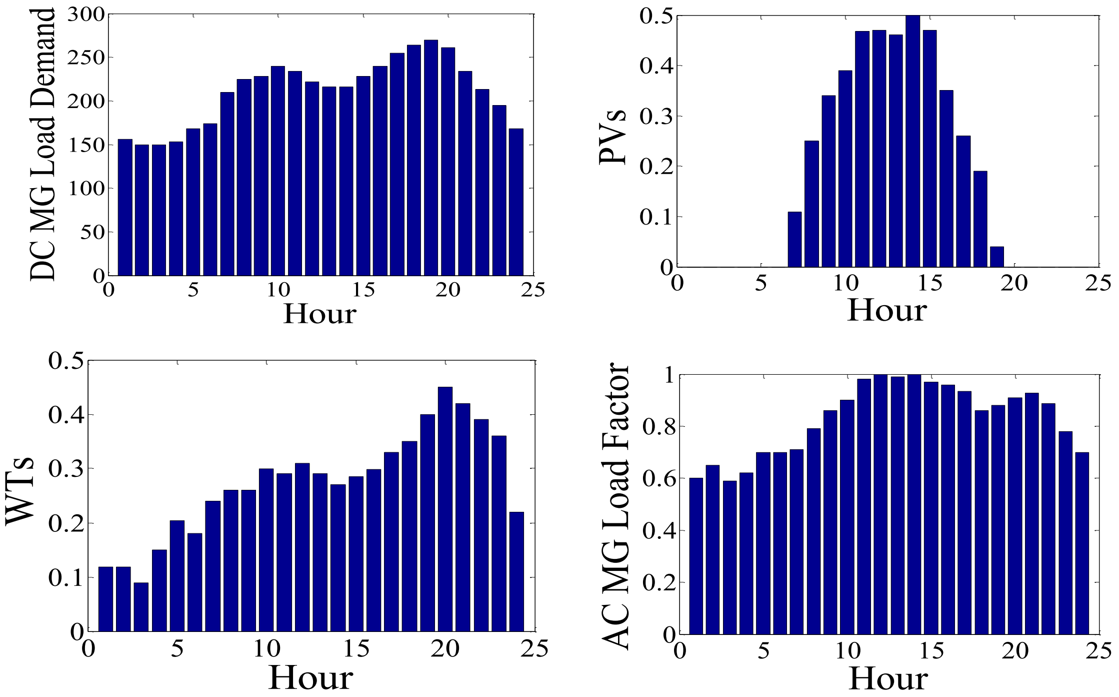

Figure 8 forecasted values of DC MG load demand, AC MG load factor and normalized output of WT and PV power units

Table 3: Output Power and Hourly Cost of Units When No Attack Has Been Carried Out (Islanded mode)

Time	PV1	WT1	MT1	Fuel cell	AC-DC Converter	MT2	MT3	WT2	WT3	PV2	Hourly cost
1	0	23.8	269.29	287.28	-424.38	1300	403.37	65.45	53.55	0	890.56
2	0	23.8	364.29	231.42	-469.511	1300	545.597	65.45	53.55	0	950.365
3	0	17.8	254.726	174.637	-297.164	1300	514.373	48.95	40.05	0	870.743
4	0	30	361.653	221.518	-460.172	1267	443.614	82.5	67.5	0	937.423
5	0	40.8	414.188	237.608	-524.597	1300	593.614	112.2	91.8	0	1087.61
6	0	36	323.533	196.259	-381.792	1300	742.245	99	81	0	1089.23
7	27.25	48	306.486	171.782	-343.519	1281.28	738.294	132	108	43.6	1333.69
8	62.5	52	415.671	220.092	-525.264	1249.36	824.594	143	117	100	1644.35
9	85	52	525.403	251.958	-686.362	1200.58	951.681	143	117	136	1849.71
10	97.5	60	586.587	299.977	-804.064	1108.57	1022.77	165	135	156	1996.64
11	117	58	679.297	239.99	-860.288	1273.12	1100	159.5	130.5	187.2	2210.77

12	117.5	62	659.946	277.466	-894.913	1298.07	1100	170.5	139.5	188	2252.62
13	115.2	58	641.718	294.468	-893.436	1300	1085.68	159.5	130.5	184.4	2206.99
14	125	54	700	264.152	-927.152	1300	1100	148.5	121.5	200	2256.79
15	117.5	57	605.489	242.713	-794.702	1300	1100	156.7	128.2	188	2205.42
16	87.5	59.6	655.68	248.368	-811.149	1300	1070.62	163.9	134.1	140	2019.34
17	65	66	595.339	225.629	-696.969	1300	1087.18	181.5	148.5	104	1901
18	47.5	70	487.431	165.993	-506.925	1179.85	1100	192.5	157.5	76	1739.42
19	10	80	538.497	225.87	-584.368	1234.84	1055.91	220	180	16	1575.61
20	0	90	559.58	218.383	-606.964	1300	1049.52	247.5	202.5	0	1597.16
21	0	84	613.757	255.815	-719.573	1300	1040.74	231	189	0	1571.41
22	0	78	503.757	205.277	-574.035	1292.11	1062.41	214.5	175.5	0	1509.71
23	0	72	412.696	152.745	-442.442	1186.35	915.992	198	162	0	1351.21
24	0	44	346.57	97.7466	-320.317	1001.35	1054.68	121	99	0	1132.18

Once the other units reach their ramp-up rate limit, if the power shortage is not compensated, HMGCC has no choice but to cut off some loads. After the period of shutdown and startup of the off unit, which is neglected in this work, is passed; it will turn on again but due to the limitation on its ramp-up rate, it must start from the minimum value and increase its output power step by step. For instance, in the second scenario, wherein an attack with 50% severity has been carried out, the HMGCC that observes 925 kW excess power at the 12th hour, which is 420 kW more than the total ramp-down rate of dispatchable DGs, sends an emergency shutdown command to both fuel-cell and MT1. The shutdown of these two units reduces the total generation of the DGs by 937.4 kW.

Table 4: output power and hourly cost of units when attack with 35% severity has been carried out (Islanded mode)

Time	PV1	WT1	MT1	Fuel cell	AC-DC Converter	MT2	MT3	WT2	WT3	PV2	Hourly cost
1	0	23.8	269.296	287.289	-424.385	1300	403.379	65.45	53.55	0	890.561
2	0	23.8	364.29	231.42	-469.51	1300	545.597	65.45	53.55	0	950.365
3	0	17.8	254.726	174.637	-297.163	1300	514.373	48.95	40.05	0	870.743
4	0	30	361.653	221.518	-460.172	1267	443.614	82.5	67.5	0	937.423
5	0	40.8	414.188	237.608	-524.597	1300	593.614	112.2	91.8	0	1087.61
6	0	36	323.533	196.258	-381.792	1300	742.245	99	81	0	1089.23
7	27.25	48	306.486	171.782	-343.518	1281.28	738.294	132	108	43.6	1333.69
8	62.5	52	415.671	220.092	-525.264	1249.36	824.594	143	117	100	1644.35
9	85	52	525.403	251.958	-686.36	1200.58	951.681	143	117	136	1849.71
10	97.5	60	586.587	299.977	-804.064	1108.57	1022.77	165	135	156	1996.64

11	117	58	679.297	239.99	-860.287	1273.12	1100	159.5	130.5	187.2	2210.77
12	117.5	62	50	299.99	-307.49	1300	1100	170.5	139.5	188	4795.62
13	115.2	58	160	300	-417.25	1300	1100	159.5	130.5	184.4	4194.26
14	125	54	270	300	-533	1300	1100	148.5	121.5	200	3938.91
15	117.5	57	380	300	-626.5	1300	1100	156.7	128.2	188	2923.9
16	87.5	59.6	490	300	-697.1	1300	1100	163.9	134.1	140	2371.73
17	65	66	595.339	240	-711.339	1286.19	1087.18	181.5	148.5	104	1898.41
18	47.5	70	487.431	180	-520.931	1166.23	1100	192.5	157.5	76	1736.83
19	10	80	538.497	225.87	-584.36	1234.84	1055.91	220	180	16	1575.61
20	0	90	559.58	218.383	-606.964	1300	1049.52	247.5	202.5	0	1597.16
21	0	84	613.757	255.815	-719.572	1300	1040.74	231	189	0	1571.41
22	0	78	503.757	205.277	-574.035	1292.11	1062.41	214.5	175.5	0	1509.71
23	0	72	412.696	152.745	-442.441	1186.35	915.991	198	162	0	1351.21
24	0	44	346.57	97.7466	-320.316	1001.35	1054.68	121	99	0	1132.18

Table 5: output power and hourly cost of units when attack with 50% severity has been carried out (Islanded mode)

Time	PV1	WT1	MT1	Fuel cell	AC-DC Converter	MT2	MT3	WT2	WT3	PV2	Hourly cost
1	0	23.8	269.296	287.289	-424.385	1300	403.379	65.45	53.55	0	890.561
2	0	23.8	364.29	231.42	-469.51	1300	545.597	65.45	53.55	0	950.365
3	0	17.8	254.726	174.637	-297.163	1300	514.373	48.95	40.05	0	870.743
4	0	30	361.653	221.518	-460.172	1267	443.614	82.5	67.5	0	937.423
5	0	40.8	414.188	237.608	-524.597	1300	593.614	112.2	91.8	0	1087.61
6	0	36	323.533	196.258	-381.792	1300	742.245	99	81	0	1089.23
7	27.25	48	306.486	171.782	-343.518	1281.28	738.294	132	108	43.6	1333.69
8	62.5	52	415.671	220.092	-525.264	1249.36	824.594	143	117	100	1644.35
9	85	52	525.403	251.958	-686.36	1200.58	951.681	143	117	136	1849.71
10	97.5	60	586.587	299.977	-804.064	1108.57	1022.77	165	135	156	1996.64
11	117	58	679.297	239.99	-860.287	1273.12	1100	159.5	130.5	187.2	2210.77
12	117.5	62	50	35	-42.5	1300	1100	170.5	139.5	188	6013.17
13	115.2	58	160	95	-212.25	1300	1100	159.5	130.5	184.4	5117.44
14	125	54	270	155	-388	1300	1100	148.5	121.5	200	4578.74

15	117.5	57	380	215	-541.5	1300	1100	156.7	128.2	188	3292.23
16	87.5	59.6	490	275	-672.1	1300	1100	163.9	134.1	140	2479.06
17	65	66	595.339	225.629	-696.968	1300	1087.18	181.5	148.5	104	1901
18	47.5	70	487.431	165.993	-506.925	1179.85	1100	192.5	157.5	76	1739.42
19	10	80	538.497	225.87	-584.367	1234.84	1055.91	220	180	16	1575.61
20	0	90	559.58	218.383	-606.964	1300	1049.52	247.5	202.5	0	1597.16
21	0	84	613.757	255.815	-719.572	1300	1040.74	231	189	0	1571.41
22	0	78	503.757	205.277	-574.035	1292.11	1062.41	214.5	175.5	0	1509.71
23	0	72	412.696	152.745	-442.441	1186.35	915.991	198	162	0	1351.21
24	0	44	346.57	97.7466	-320.316	1001.35	1054.68	121	99	0	1132.18

After these two units turned back on again and the rest of the units increased their generation as much as they could, there is still a power shortage in the grid. In order to restore the balance between generation and consumption, HMGCC has to cut off 781.92 kW of loads. Grid's hourly load shedding (LS) in all three scenarios is available in Table 8. As can be seen from the results, due to the non-optimal operation of the DGs and failure to supply loads (ENS penalty cost), the operation cost of the grid has greatly increased. For instance, according to table 3 and table 4, in the 12th hour, when an attack with 65% severity has been carried out, the cost of the system has increased to 6682.41$ comparing to the case that no attack has been carried out. Also as shown in the results, in addition to the time of the attack, the system will be damaged both economically and socially in the next hours.

Table 6: output power and hourly cost of units when attack with 65% severity has been carried out (Islanded mode)

Time	PV1	WT1	MT1	Fuel cell	AC-DC Converter	MT2	MT3	WT2	WT3	PV2	Hourly cost
1	0	23.8	269.296	287.289	-424.385	1300	403.379	65.45	53.55	0	890.561
2	0	23.8	364.29	231.42	-469.51	1300	545.597	65.45	53.55	0	950.365
3	0	17.8	254.726	174.637	-297.163	1300	514.373	48.95	40.05	0	870.743
4	0	30	361.653	221.518	-460.172	1267	443.619	82.5	67.5	0	937.423
5	0	40.8	414.188	237.608	-524.597	1300	593.614	112.2	91.8	0	1087.61
6	0	36	323.533	196.258	-381.792	1300	742.245	99	81	0	1089.23
7	27.25	48	306.486	171.782	-343.518	1281.28	738.294	132	108	43.6	1333.69
8	62.5	52	415.671	220.092	-525.264	1249.36	824.594	143	117	100	1644.35
9	85	52	525.403	251.958	-686.361	1200.58	951.681	143	117	136	1849.71
10	97.5	60	586.587	299.977	-804.064	1108.57	1022.77	165	135	156	1996.64
11	117	58	679.297	239.99	-860.287	1273.12	1100	159.5	130.5	187.2	2210.77
12	117.5	62	700	299.99	-957.49	1300	90	170.5	139.5	188	6682.41

13	115.2	58	700	300	-957.25	1300	240	159.5	130.5	184.4	5863.18
14	125	54	700	300	-963	1300	390	148.5	121.5	200	5391.67
15	117.5	57	700	300	-946.5	1300	540	156.7	128.2	188	4149.19
16	87.5	59.6	700	300	-907.1	1300	690	163.9	134.1	140	3364.4
17	65	66	700	300	-876	1300	840	181.5	148.5	104	2271.47
18	47.5	70	597.431	240	-690.931	1117.15	990	192.5	157.5	76	1707.11
19	10	80	538.497	225.87	-584.364	1234.84	1055.91	220	180	16	1575.61
20	0	90	559.58	218.383	-606.964	1300	1049.52	247.5	202.5	0	1597.16
21	0	84	613.757	255.815	-719.572	1300	1040.74	231	189	0	1571.41
22	0	78	503.757	205.277	-574.035	1292.11	1062.41	214.5	175.5	0	1509.71
23	0	72	412.696	152.745	-442.441	1186.35	915.992	198	162	0	1351.21
24	0	44	346.57	97.7466	-320.316	1001.35	1054.68	121	99	0	1132.18

Table 7: output power and hourly cost of units (Grid-connected mode)

Time	PV1	WT1	MT1	Fuel cell	AC-DC Converter	MT2	MT3	WT2	WT3	PV2	Hourly cost
1	0	23.8	50	35	47.2	0	0	65.45	53.55	0	680.1259
2	0	23.8	0	0	126.2	0	0	65.45	53.55	0	704.6611
3	0	17.8	0	0	132.2	0	0	48.95	40.05	0	429.8804
4	0	30	50.3447	0	72.65531	0	0	82.5	67.5	0	564.6907
5	0	40.8	50	0	77.2	185	150	112.2	91.8	0	776.8465
6	0	36	158.507	60	-80.5071	337.286	286.536	99	81	0	1004.389
7	27.25	48	268.507	120	-253.757	522.286	426.512	132	108	43.6	1213.097
8	62.5	52	378.507	180	-448.007	707.286	576.305	143	117	100	1569.593
9	85	52	488.319	240	-637.319	892.286	726.305	143	117	136	1898.961
10	97.5	60	597.824	299.07	-814.394	1077.16	875.693	165	135	156	2094.948
11	117	58	553.831	296.196	-791.027	1261.94	1022.33	159.5	130.5	187.2	2199.036
12	117.5	62	533.935	236.196	-727.631	1300	1100	170.5	139.5	188	2261.439
13	115.2	58	622.446	291.652	-871.348	1143.71	1100	159.5	130.5	184.4	2223.685
14	125	54	698.473	240.879	-902.352	1152.41	1099.83	148.5	121.5	200	2263.273
15	117.5	57	643.79	198.035	-788.325	1300	953.814	156.7	128.2	188	2203.602
16	87.5	59.6	590.732	138.035	-635.867	1300	1100	163.9	134.1	140	1982.149

17	65	66	640.343	198.035	-714.378	1122.91	956.32	181.5	148.5	104	2065.795
18	47.5	70	698.424	138.035	-689.958	943.338	814.947	192.5	157.5	76	1769.06
19	10	80	632.277	180.255	-632.532	762.397	872.295	220	180	16	1462.595
20	0	90	700	240.255	-769.255	694.025	726.353	247.5	202.5	0	1583.322
21	0	84	700	300.255	-850.255	524.041	576.353	231	189	0	1580.967
22	0	78	700	243.163	-808.163	339.041	458.344	214.5	175.5	0	1528.648
23	0	72	590	183.163	-650.163	157.453	320.029	198	162	0	1303.25
24	0	44	480.86	139.452	-496.312	0	214.603	121	99	0	989.4464

Table 8: hourly load shedding of the grid due to attacks

Time (Hour)	9	10	11	12	13	14	15	16	17	18
35% scenario	0	0	0	528.87	412.95	350.1	149.48	72.181	0	0
50% scenario	0	0	0	781.92	604.96	483.28	226.21	94.548	0	0
65% scenario	0	0	0	959.36	792.44	678.93	425.4	294.16	86.315	0

5.1.2 Grid-Connected Mode

In the islanding mode, when a hacker increases the measured data of RESs, based on units' production cost and upstream grid market price in the twelfth hour, HMGCC decides to reduce the power generation of DGs and also reduce the power received from the upstream grid. At this moment, the upstream grid (bus 1) acts as a slack bus, and by increasing the power injected to the HMG does not allow the frequency to be changed. On the other hand, the HMGCC, which observes an increase in the power received from the upstream grid, orders DGs to increase their power production again to prevent the economic loss caused via the purchase of expensive power from the upstream grid. Therefore, due to the negligence of the dynamic effect of DIA on the operation of the HMG, it can be concluded that this type of attack does not affect the performance of the grid-connected HMGs in the steady-state. Table 7 presents the hourly cost and output power of units in grid-connected mode.

5.2 SHT based DIA detection method efficiency evaluation

In this part, the performance and efficiency of the suggested SHT based DIA detection method is examined in a case study. To this end, a scenario is considered in such a way that the received data (i.e. the measured output power that is received in the HMGCC) related to the first PV unit (i.e. PV1) in the test system is hacked. In this scenario, the adversary penetrates to the system in the 5th hour of the day and hacks the measured output power of the PV1. The hacked data are generated using a random uniform distribution in such a way that their deviation from the corresponding forecasted value is in the range [0.08*P_{ij}^f, 0.2*P_{ij}^f]. Note that, since the errors higher than 0.2*P_{ij}^f are directly considered as the cyber-attack and are not imported to the detection method, data with a deviation of more than 0.2*P_{ij}^f are not generated. Complete data related to the forecasted values and hacked data of the case study can be found in Table 9. In order to detect DIA on the measured output power of the PV1, an SHT based detection agent with parameters P_1^i=0.95, P_0^i=0.1, α^i=0.01, and β^i=0.02 is considered. According to (7), the upper and lower thresholds are ln(U^i)=4.5850 and ln(L^i)=-3.9020 respectively. Note that in the process after a decision is made, the value of the probability ratio becomes zero. As it can be seen from Table

9, in the fourth hour, the probability ratio is lower than the lower threshold and the null hypothesis is accepted. In the next hour wherein the data is hacked, the value of $\ln(P_1=0.95/P_0=0.1)=2.25$ is added to the preceding probability ratio (which is zero after a decision is made in the previous hour). But since the probability ratio has not reached one of the thresholds, no decision has been made. This process is repeated until at the 7th hour the probability ratio passes the upper threshold, and the model detects the attack.

6 CONCLUSION

The secure operation of electrical power grids is very critical to the economy and security of the nations. However, the integration of intelligent technologies applied in modern power systems makes these systems vulnerable to cyber-attacks. DIA can damage the management and operation of HMGs by misleading the HMGCC to dispatch the units based on false data. This can result in not only increasing the operation cost of the grid by making DGs operate in the non-optimal point but also can force HMGCC to cut-off loads. Therefore, in addition to causing economic damages, this kind of attack can also damage social welfare. To address this problem, this paper proposed an efficient detection method based on SHT to detect such attacks. The performance and sensitivity of this method analyzed in detail. The simulation result on a practical HMG constructed based on IEEE standard system, revealed that DIA on RESs, unlike the grid-connected mode, which does not have much effects on the system, in the islanded-mode can have destructive effects. The bottom line is that grid's security must be guaranteed to achieve a reliable, efficient, and stable system. As the future work, the proposed method can be combined with machine learning algorithms like convolutional neural network or long short term memory. Also the proposed method can be utilized for loads' smart meters for detection purposes. The proposed method can be extended to detect even other types of attacks like identity-based cyber-attacks. However, there are several limitations associated with the proposed methodology specifically its vulnerability to stealthy long term attacks and false positive alarm in the event of sudden unusual load changes.

Table 9 performance of the proposed method on a case study

Hour	Forecasted value	Hacked data	Probability ratio vs thresholds	Decision
1	29.75	29.75	$\mathrm{Ln}(L^i)<-2.89<\ln(U^i)$	No decision
2	29.75	29.75	$-5.78<\ln(L^i)$	No attack
3	22.25	22.25	$\mathrm{Ln}(L^i)<-2.89<\ln(U^i)$	No decision
4	37.5	37.5	$-5.78<\ln(L^i)$	No attack
5	51	55.7517	$\mathrm{Ln}(L^i)<+2.25<\ln(U^i)$	No decision
6	45	53.7102	$\mathrm{Ln}(L^i)<+4.50<\ln(U^i)$	No decision
7	60	53.0285	$\mathrm{Ln}(U^i)<6.75$	Attack
8	65	73.3235	$\mathrm{Ln}(Li)<+2.25<\ln(Ui)$	-
9	65	56.8597	$\mathrm{Ln}(Li)<+4.50<\ln(Ui)$	-

REFERENCES

[1] Kavousi-Fard, Abdollah, Mojtaba Mohammadi, and A. S. Al-Sumaiti. "Effective Strategies of Flexibility in Modern Distribution Systems: Reconfiguration, Renewable Sources and Plug-in Electric Vehicles." Flexibility in Electric Power Distribution Networks. CRC Press, 2021. 95-119.

[2] S. Z. Tajalli, S. A. Mohammad Tajalli, A. Kavousi-Fard, T. Niknam, M. Dabbaghjamanesh and S. Mehraeen, "A Secure Distributed Cloud-Fog Based Framework for Economic Operation of Microgrids," 2019 IEEE Texas Power and Energy Conference (TPEC), 2019, pp. 1-6, doi: 10.1109/TPEC.2019.8662201.

[3] Mobtahej, M., Esapour, K., Tajalli, S.Z., Mohammadi, M.: Effective demand response and GANs for optimal constraint unit commitment in solar-tidal based microgrids. IET Renew. Power Gener. 1–11 (2021). https://doi.org/10.1049/rpg2.12331

[4] Duan, Pengfei, Hamid Soleimani, Arezoo Ghazanfari, and Moslem Dehghani. "Distributed Energy Management in Smart Grids Based on Cloud-Fog Layer Architecture Considering PHEVs." IEEE Transactions on Industry Applications (2020).

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

[6] Dabbaghjamanesh, Morteza, Abdollah Kavousi-Fard, Shahab Mehraeen, Jie Zhang, and Zhao Yang Dong. "Sensitivity analysis of renewable energy integration on stochastic energy management of automated reconfigurable hybrid AC–DC microgrid considering DLR security constraint." IEEE Transactions on Industrial Informatics 16, no. 1 (2019): 120-131.

[7] Papari, Behnaz, Chris S. Edrington, Indranil Bhattacharya, and Ghadir Radman. "Effective energy management of hybrid AC–DC microgrids with storage devices." IEEE transactions on smart grid 10, no. 1 (2017): 193-203.

[8] Masaud, Tarek Medalel, Jonathan Warner, and Ehab Fahmy El-Saadany. "A Blockchain-Enabled Decentralized Energy Trading Mechanism for Islanded Networked Microgrids." IEEE Access 8 (2020): 211291-211302.

[9] Aflaki, Arshia, Mohsen Gitizadeh, and Burak Kantarci. "Accuracy Improvement of Electrical Load Forecasting Against New Cyber-Attack Architectures." Sustainable Cities and Society (2021): 103523.

[10] Langner, Ralph. "Stuxnet: Dissecting a cyberwarfare weapon." IEEE Security & Privacy 9, no. 3 (2011): 49-51.

[11] Cui, Hao, Xiaorui Dong, Hongyan Deng, Moslem Dehghani, Khalid Alsubhi, and Hani Moaiteq Abdullah Aljahdali. "Cyber Attack Detection Process in Sensor of DC Micro-Grids Under Electric Vehicle based on Hilbert-Huang Transform and Deep Learning." IEEE Sensors Journal (2020).

[12] Abdollah, Kavous-Fard, Wencong Su, and Tao Jin. "A Machine Learning Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids." IEEE Transactions on Industrial Informatics (2020).

[13] Liu, Xuan, and Zuyi Li. "False data attack models, impact analyses and defense strategies in the electricity grid." The Electricity Journal 30, no. 4 (2017): 35-42.

[14] Li, Shang, Yasin Yılmaz, and Xiaodong Wang. "Quickest detection of false data injection attack in wide-area smart grids." IEEE Transactions on Smart Grid 6, no. 6 (2014): 2725-2735.

[15] M. Mohammadi, A. Kavousi-Fard, M. Dabbaghjamanesh, A. Farughian and A. Khosravi, "Effective Management of Energy Internet in Renewable Hybrid Microgrids: A Secured Data Driven Resilient Architecture," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2021.3081683.

[16] 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, 69, p.102856. https://doi.org/10.1016/j.scs.2021.102856

[17] Aflaki, Arshia, Mohsen Gitizadeh, Roozbeh Razavi-Far, Vasile Palade, and Ali Akbar Ghasemi. "A hybrid framework for detecting and eliminating cyber-attacks in power grids." Energies 14, no. 18 (2021): 5823.

[18] 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 (2021): 106702. https://doi.org/10.1016/j.ijepes.2020.106702

[19] Zeng, Wente, Yuan Zhang, and Mo-Yuen Chow. "Resilient distributed energy management subject to unexpected misbehaving generation units." IEEE Transactions on Industrial Informatics 13, no. 1 (2015): 208-216.

[20] Dehghani, Moslem, Mohammad Ghiasi, Taher Niknam, Abdollah Kavousi-Fard, and Sanjeevikumar Padmanaban. "False data injection attack Detection based on Hilbert-Huang Transform in AC Smart Islands." IEEE Access 8 (2020): 179002-179017.

[21] Wu, Kehe, Jiawei Li, Bo Zhang, Zongchao Yu, and Xuan Liu. "Preventive Dispatch Strategy Against FDIA Induced Overloads in Power Systems With High Wind Penetration." IEEE Access 8 (2020): 210452-210461.

[22] Vamsi, P.R. and Kant, K., 2014, July. Sybil attack detection using sequential hypothesis testing in wireless sensor networks. In 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014) (pp. 698-702). IEEE.

[23] Chen, Bo, Karen L. Butler-Purry, Sruti Nuthalapati, and Deepa Kundur. "Network delay caused by cyber attacks on SVC and its impact on transient stability of smart grids." In 2014 IEEE PES General Meeting| Conference & Exposition, pp. 1-5. IEEE, 2014.

[24] Dehghani, Moslem, Mohammad Ghiasi, Taher Niknam, Abdollah Kavousi-Fard, Elham Tajik, Sanjeevikumar Padmanaban, Hamdulah Aliev. "Cyber Attack Detection based on Wavelet Singular Entropy in AC Smart Islands: False data injection attack." IEEE Access 9 (2021).

[25] S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for automatic generation control,” IEEE Transactions on Smart Grid, vol. 5, no. 2, pp. 580–591, 2014.

[26] Dehghani, Moslem, Mohammad Ghiasi, Taher Niknam, Abdollah Kavousi-Fard, Mokhtar Shasadeghi, Noradin Ghadimi, and Farhad Taghizadeh-Hesary. "Blockchain-Based Securing of Data Exchange in a Power Transmission System Considering Congestion Management and Social Welfare." Sustainability 13, no. 1 (2021): 90.

[27] J. Lee, "Blockchain Technologies: Blockchain Use Cases for Consumer Electronics," in IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 53-54, July 2018, doi: 10.1109/MCE.2018.2816278.

[28] Puthal, Deepak, et al. "The blockchain as a decentralized security framework [future directions]." IEEE Consumer Electronics Magazine 7.2 (2018): 18-21.

[29] Wald, A., 2004. Sequential analysis. Courier Corporation.

[30] Pele, O. and Werman, M., 2008. Robust real-time pattern matching using bayesian sequential hypothesis testing. IEEE transactions on pattern analysis and machine intelligence, 30(8), pp.1427-1443.

[31] Song, H., Fink, G. and Jeschke, S., 2017. Security and Privacy in Cyber-Physical Systems. Wiley-IEEE Press.