IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 29, 2021, accepted February 10, 2021. Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2021.3059042

Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform

MOHAMMAD GHIASI[1], MOSLEM DEHGHANI[1], TAHER NIKNAM[1], (Member, IEEE), ABDOLLAH KAVOUSI-FARD[1], (Member, IEEE), PIERLUIGI SIANO[2], (Senior Member, IEEE), AND HASSAN HAES ALHELOU[3,4], (Senior Member, IEEE)

[1]Department of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz 71555-313, Iran
[2]Department of Management and Innovation Systems, University of Salerno, 84084 Salerno, Italy
[3]School of Electrical and Electronic Engineering, University College Dublin, 04 Dublin, Ireland
[4]Department of Electrical Power Engineering, Tishreen University, Lattakia 2230, Syria

Corresponding authors: Hassan Haes Alhelou (alhelou@ieee.org) and Taher Niknam (niknam@sutech.ac.ir)

This publication has emanated from research supported in part by Science Foundation Ireland (SFI) under the SFI Strategic Partnership Programme Grant Number SFI/15/SPP/E3125 and additional funding provided by the UCD Energy Institute. The opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Science Foundation Ireland.

ABSTRACT Due to the simultaneous development of DC-microgrids (DC-MGs) and the use of intelligent control, monitoring and operation methods, as well as their structure, these networks can be threatened by various cyber-attacks. Overall, a typical smart DC-MG includes battery, supercapacitors and power electronic devices, fuel cell, solar Photovoltaic (PV) systems, and loads such as smart homes, plug-in hybrid electrical vehicle (PHEV), smart sensors and network communication like fiber cable or wireless to send and receive data. Given these issues, cyber-attack detection and securing data exchanged in smart DC-MGs like CPS has been considered by experts as a significant subject in recent years. In this study, in order to detect false data injection attacks (FDIAs) in a MG system, Hilbert-Huang transform methodology along with blockchain-based ledger technology is used for enhancing the security in the smart DC-MGs with analyzing the voltage and current signals in smart sensors and controllers by extracting the signal details. Results of simulation on the different cases are considered with the objective of verifying the efficacy of the proposed model. The results offer that the suggested model can provide a more precise and robust detection mechanism against FDIA and improve the security of data exchanging in a smart DC-MG.

INDEX TERMS Smart DC-microgrid, Hilbert-Huang Transform, false data injection attack, data exchanging, blockchain.

I. INTRODUCTION

Due to the significant advantages of smart microgrids (MGs), attention to this structure is increasing today. MGs are mainly sorted into three categories which include hybrid MG, DC-MG, and AC-MG. MG consists of different parts such as interlinked loads and distributed energy resources (DERs) owning coordinated control which improves the sustainability, reliability, and performance of such recent electrical power systems. The advent of DC-MG idea arises from growing access to renewable energy resources. Clearly, DC-MG includes energy storage systems, RERs, and electric vehicles (EVs). Besides, DC-MG usually consists of a wide range of consumer electronic devices and components with various communication links, sensors, and detectors [1], [2]. Smart DC-MGs incorporate complex interactions among computational and physical procedures which make them as cyber-physical systems (CPSs), with vulnerability to cyber-attacks [3]–[5]. Connecting MGs and sources of energy and loads to each other and exchanging information between them in order to improve the controller efficiency of converters and load sharing and coordination causes cyber-malicious attack points.

Using effective methods based on artificial intelligence, signal processing, neural networks, deep learning and blockchain-based techniques to detect cyber-attacks can make the power network more secure against these types of attacks, as well as improving the stability of CPS. So in this

The associate editor coordinating the review of this manuscript and approving it for publication was Zhehan Yi.

research, a combination of blockchain technique and a signal processing method is used to secure smart DC-MG data.

A. BACKGROUND

In 2008, Distributed blockchain technology was presented to support the cryptocurrency Bitcoin and was named Satoshi Nakamoto, and in 2009, the Bitcoin network was initiated [6], [7]. After that, Bitcoin slowly came into the financial industry and became the most effective cryptocurrency. The blockchain technology behind Bitcoin turns to be a game-variable novelty for the entire world, and there are various industries which will be disrupted through blockchain technology, like life services, financial sciences, legal industry, cybersecurity, health care, private transport, supply chain management, and cloud storage, ride-sharing, voting, charity, public benefits, government, retail, energy management, and real estate between others [8]. The blockchain technology applies in distributed generation resources, renewable energy resources, and data security of power systems against cyber-attacks [9] efficiency.

So, using a smart DC-MG requires to be modified with the aim of taking benefit of the novel technology, and the aim of this study is to survey how a huge industrial user is able to greatest handle under such a novel blockchain on the basis of data exchanging among distributed generations agents, loads like smart homes and, plug-in hybrid electrical vehicle (PHEV), smart metering (sensors) and control units) are able to be safe versus cyber-attacks like false data injection attack (FDIA). Expansion of the cyber-physical energy systems, and the usage of developed information technology (IT) like communication, control, conception, and computation results in inchmeal releasing networking, intelligentisation, and informatisation by the power system [10], [11]. Potential security risks are increased by interface terminals due to promote real-time analysis, scientific decision-making, and effective placement of electrical grids, open communication networks [12]. In comparison with the partly robust power primitive system, the research into security enhancement of the electrical power data system is in its infancy, with many security vulnerabilities undetected. Given the importance and great transmissibility of the electrical grid, after attack, a significant effect on energy security, industrial production, and livelihood of people will be engendered, which has attracted a lot of attention. [13]. In the role of a novel attack process for essential industrial facilities, a threat to the stable and safe operation of electrical networks can be considered as the cyber-attack, that its attack and defense method needs more investigation [9], [14].

Pursuant to attack points, the cyber-attacks versus electrical systems are able to be categorized into taking down the availability, confidentiality, and integrity of data. The availability demolition can be obtained in inaccessible data causing by communication interruption, that its generic procedures include various attacks like black hole, denial-of-service (DoS), and varying network topology attacks. The totality destruction can be obtained in false data causing by FDI, that its generic procedures include FDIA, replay attack, and man-in-the-middle attack. The confidentiality attack can be obtained in data leakage and illegal use that its general procedures include brute force password cracking, utilization of malware, and internal employee attack [15], [16]. In the role of a typical state with the aim of destroying information integrity, the analysis outcomes of state estimation can be disrupted by the FDA, so result in misleading the control center decision. Nowadays, blockchain [17] has been promoted in the role of an efficient and safe technology for the online financial operations by the communication merely among transaction network peers and without the third party's involvement. Through applying blockchain, the datum is able to be saved in the distributed partly small databases instead of saving the whole datum in a central datum center. The security of the all-cloud system might be increased due to the majority of the attack damages on likewise databases is able to be simply locally limited. So, different areas such as the financial sector and the Internet of Things (IoT) are able to utilize blockchain with success. For enhancing the scope of reliability, security of the system has a growingly significant role in order to keep unbiased coordination between the resources because the technological aspects have straightly affected by it on the basis of penalties precisely assigned for poor efficiency metrics [18], [19]. Cyber-attacks consider as some possible ways with the aim of violating security measures that usually consists of FDIAs [8], DoS [20], replay attacks [21], and so on. These attacks have skills to disrupt the system stability and also control mechanisms.

B. LITERATURE REVIEW

Some cases have been reported before, which considered fundamental trouble for the central control units [22], [23]. FDIAs change the system mode through injecting incorrect data into each of the in-danger sensors or actuators. An instance of the implementation of these attacks has been given in the reference [24]. For analyzing the effect of these attacks, more study has been done with the aim of assessing its effects on the economic load dispatch that can figure out in a cooperative kind [25]. That's why the system with the attack reached a consensus phase that is not favorable. Widely, due to these attacks interrupt the function of observers that can be considered as a naive criterion for detection, reduction, and detection of ordinary attacks is already well categorized in the literature. Nonetheless, according to the research done, generalized FDIAs which are usually known as stealth attacks [26], which are able to simply attack in networked systems with no change of the system observability. Such attacks are able to be particularly categorized as coordinated intelligent attacks that include coordinated attack vectors in variable points with the aim of nullifying system dynamics. Therefore, at the time of a malicious cyber-attack, system operators were unaware of this attack. Earlier, an incorrect growth in the magnitude of attack vectors could be caused by the attacker that might result in shutting down the system depending on the attack severity. In addition, at the time the

attacker has gained a previous knowledge of system applying proper system monitoring, it might result in having easier implementation for these attacks [27].

An additional example of coordinated attacks has been provided on electrical power systems and its vulnerability evaluation. Accordingly, risk evaluation alongside with control vulnerabilities is essential, because the modeling of coordinated attacks for MGs is able to be simpler due to their small size of the system with no important security measures [28]. An artificial intelligence (a special kind of recurrent neural network) was offered to estimate DC currents/voltages to detect cyber-attacks in DC-MG, furthermore, the attacked DER unit has been identified in the reference [29]. The FDI attack's effect in DC MGs has also been discussed which contains parallel DC/DC converters. The converters have been controlled with a droop-based control method to retain the eligible voltage level. In addition, a method on the basis of artificial neural networks to track references has been suggested to eliminate the FDIAs in DC-MG in paper [30]. The various statistical Spatio-temporal methods were applied to detect FDIAs in smart grid. The procedures are leveraged the datum co-linearity which occur in the AMI measurements of the electrical power grid to prepare anticipation for the AMI observations of the grid, attaining to rapidly diagnose the presence of ''bad data''; besides, a plan for FDIAs with several adversaries and an alone smart grid defender were presented in reference [31]. Two-game schemes have been investigated to consider the interplays among the attackers and the defender. Firstly, a Stackelberg game is offered in which the defender operates as a leader that is able to estimate the movements of the adversaries, which operate as followers, before determining which measurements to protect. Secondly, the defender is not able to estimate the operations of the adversaries. So, a hybrid euphoria equilibrium-Nash equilibrium game has been presented in reference [13].

A two-layer energy trading system has been proposed on the basis of multi-agent and blockchain with the aim of facilitating the P2P market in paper [32]. In electric vehicles (EVs), a consortium blockchain for local aggregators with the aim of auditing and validating electricity trading between PHEVs, and also a novel energy blockchain with the aim of enabling electrical vehicles have been proposed in references [33], [34]. In addition, the consortium blockchain way to generic energy blockchain transactions has been extended with the aim of credit-based payment and transaction security in paper [35].

An adept system layer was considered with blockchain in [36]. The adept system operates by applying a neural network as the conclusion tool. The terminal and server with an internet connection aid the user to access the system. The entire system was performed as a smart contract. The proposed approach provided a system to make an open energy market for user's society. A system has been applied on the basis of IoT for energy flow accountancy. Blockchain was applied to remove the need for a central control being through keeping to pursue distributed energy transactions. Both methods were applied to build an energy dealing market that the market contributors have predetermined targets. Also, this pattern was contained for EVs. The P2P electricity dealing pattern has been presented for PHEV on the basis of blockchain technology in [37]. This scheme acts on demand response and absorbs the users to take part in it by giving them motivations. The electricity supply and demand have been balanced to gain the maximum motivations by any contributor take part in the system.

C. MOTIVATION AND MAIN CONTRIBUTION

This study presents an FDI attack detection strategy and blockchain technology to secure exchanging data for smart DC microgrid with loads, battery, supercapacitor, fuel cell, and PV. In summary, these study contributions are:

- FDI attack detection in smart DC-MGs based on the spectral energy of Hilbert-Huang transform
- Using blockchain technology to secure data exchanging among agents
- Security enhancement in smart sensors, smart homes, control units, and wireless or fiber cable networks

D. PAPER STRUCTURE

The rest of the paper is classified as follows: basic concepts of Hilbert-Huang transform (HHT), blockchain technology, and FDI attacks are presented in Section II. The system model and offered technique are defined in Part III. Simulation results of FDI attack detection on the basis of HHT and security enhancement based on blockchain technology are considered in Section IV. Discussion is provided in Part V. Finally, the main conclusion is described in Part VI.

II. BASIC CONCEPT

A. HUANG-HILBERT TRANSFORM

The HHT is a term for determining the combination of experimental mode decomposition (EMD) with Hilbert spectral assessment (HSA). The main component of HHT is the EMD approach that can be used to decompose any complex data set into a limited number of often limited and insignificant components, named intrinsic state functions (IMFs).

The IMF has been designated as any function which has the similar or various at most by one number of zero-crossing and extrema; besides and it has equiponderant envelopes designated via the local maximum and minimum. With the HHT, the IMF's efficiency instantaneous frequencies work as functions of time to identify embedded structures. The EMD decomposes each type of signal into intrinsic state functions shows in continues: for every defined discrete signal s(t), μ_1 defines the mean value of the more and fewer envelope curves of the local maximum and minimum. The first archetype member η_1 is assessed using equation (1).

$$\eta_1 = s(t) - \mu_1 \tag{1}$$

In the second sifting procedure, η_1 is also behaved as the data, and μ_{11} is the mean of η_1's more and fewer envelopes,

as follows:

$$\eta_{11} = \eta_1 - \mu_{11} \tag{2}$$

This sifting process should be repeated k times until η_{1k} is an IMF, which is given as follows:

$$\eta_1 (k-1) - \mu_{1k} = \eta_{1k} \tag{3}$$

If this member convinces the stopping proof for the IMF sieving η_1, therefore, it will be the first IMF. In this way, the remnant signal is defined as equation (4).

$$r(t) = s(t) - \eta_1 \tag{4}$$

If r (t) convinces the stopping proof for EMD, afterward, it will be the final remnant signal, and the EMD procedure will be ended. The IMF sieving technique overrides the ride waves and makes archetype IMFs more symmetric based on zero. When a stopping criterion is met mathematically, the sifting procedure approach finishes. Such proof serves to take a fair to decompose analysis without loss of data. The most prevalent stopping pattern is designated through Cauchy and operates when the standard aberration among two IMFs attains a determined value.

In the set, the number of functions should depend on the principal signal and also the threshold value utilized through the stopping scale.

The instantaneous frequency is able to be calculated via the HHT; every actual valued function g (t) of Lp class is able to be transformed into an analytic function by adding a complicated segment, h (t), which is given by equation (5).

$$h(t) = \frac{1}{\pi} \cdot \mathrm{p} \cdot \int_{-\infty}^{\infty} \frac{g(\alpha)}{t-\alpha} .d \propto \tag{5}$$

where p provides the main value of the singular integral. Hence, by the HHT, the analytic function can be calculated by:

$$z(t) = g(t) + j \cdot h(t) = \beta(t) \cdot e^{j\phi(t)} \tag{6}$$

$$\beta(t) = \sqrt{g^2 + h^2}; \phi(t) = arctg(\frac{h}{g}) \tag{7}$$

where β gives the instantaneous amplitude, ϕ represents the phase function. Therefore, the instantaneous frequency can also be simply defined as follows:

$$\phi = -\frac{d\omega}{dt} \tag{8}$$

This equation provides the best local fit of a variable phase and amplitude of a trigonometric function up to g(t). However, HHT is only able to generate physically significant outcomes for so-named single-component signals [9].

The below Equation is defined the signal spectral energy:

$$\mathrm{SE} = (\beta(t))^2 \tag{9}$$

B. BLOCKCHAIN-BASED TECHNIQUE

Blockchain is defined as a distributed public ledger in which dealings are registered publicly and chronologically. These transactions are registered in blocks, and the blocks are spread to the distributed P2P network of the nodes of blockchain. The mechanism which enables the nodes to attain an agreement on the subsequent authentic block is introduced as a consensus mechanism. After an authentic block is detected, it is enhanced to the blockchain, and it is transferred to the nodes network. A node is a computer linked to the blockchain network applying client software that does the duty of relaying and validating dealings. Everyone is able to link a common blockchain network only by implementing a client on a local computer while a validated invitation is needed for joining a consortium or a private one. After the node links to the network, it gains a copy of the whole blockchain. For a great short definition of the blockchain protocol, the user is recourse to reference [6].

There are specific benefits as well as special shortcoming in applying a private or public blockchain. In this research, a private (permissioned consortium) blockchain network for the following major proofs is considered.

- The blockchain is acted through independent market contributors, who are formed a consortium. This means that it is not a general blockchain. It is able to consider as a consortium blockchain [38], a private blockchain which is not controlling centrally.
- The energy-web foundation is a universal non-profit organization which is researching and studying the blockchain's potential in the energy section, applies Proof-of-Authority consensus workmanships to confront the energy usage issue of the blockchain topic [39]. It is extensively admitted which consortium blockchains applying proof-of-authority consensus workmanships veritably propose enhanced dealing throughput and diminished energy usage. Proof-of-Authority is removed the rivalry between validators who compete each other to construct blocks, which is the significant sake lying after extensive energy usage of blockchains.
- Because of their nature, consortium blockchains are more confident which means the nodes that produce new blocks are specified and trusted through the network makers and members link the network only through invitation.
- Electrical power networks trust on the functions of modifiers. Hence, some centralization is someway innate in suchlike grids. Role of the regulator requires to be revised when blockchain technology is consisted of in the subsequent-production power grid actions however they will ever act their intensive duty, indirectly or directly, partially or entirely.

It is very acceptable that consortium blockchain networks do restrict, in other words, decentralization. Nonetheless,

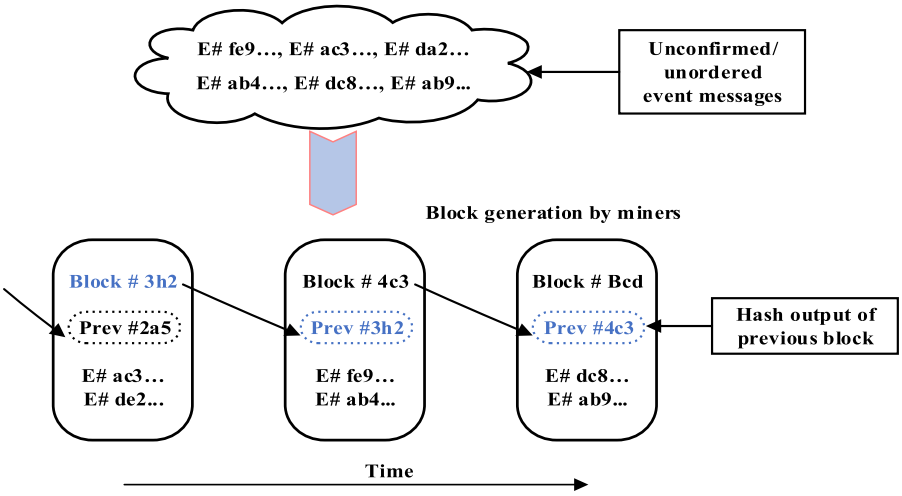


FIGURE 1. The blockchain production from unconfirmed event messages.

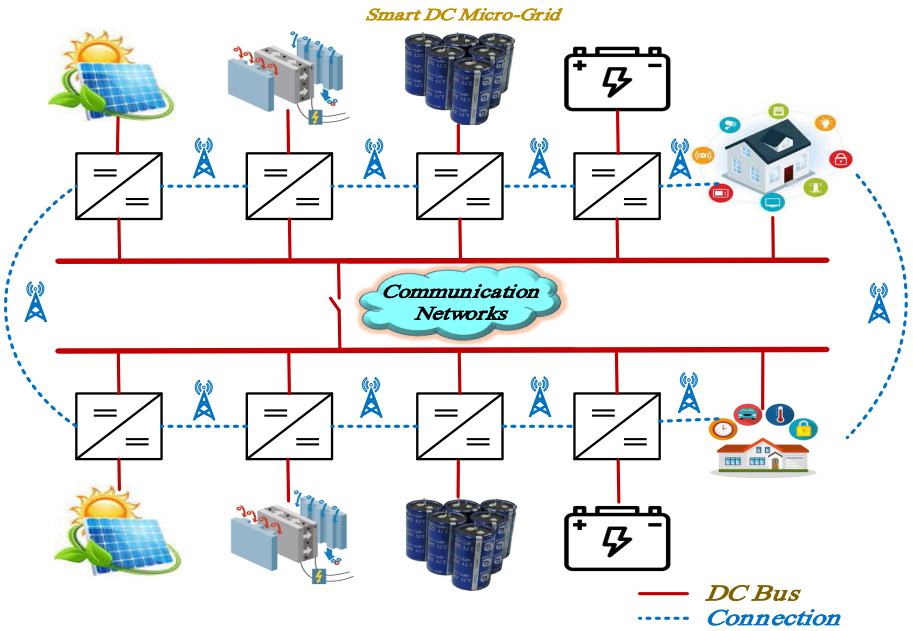


FIGURE 2. System architecture.

this cannot consider as a shortcoming when illustrated for electrical grids because these grids generally act under the lead of centralized modifiers. The Linux Foundations Hyperledger Fabric can be considered as an instance of an allowed blockchain frame performance as is the Microsoft's Azure frame, along with some others. In this implementation, Ethereum consortium blockchains is mainly considered for their wide users' community and their current large admission. Ethereum is defined as a blockchain with a built-in Turing-complete programming language that makes it possible to write smart agreements, where laws for acquisition, dealing molds and functions of state transition might be determined [40].

C. BLOCKCHAIN SCHEME IN EXCHANGING DATA AMONGST ISO AND UNDER-OPERATING AGENTS

In this study, a novel kind of blockchain with the aim of solving the topics relevant to reliable message broadcast in exchanging data among distributed generation Agents and smart loads/sensors is proposed. The method is novel as the content of invariable distributed public database for secure message broadcast in exchanging data among distributed generation Agents and smart loads/sensors, where each node is able to achievement the information, is used. Plus, each country is able to maintain it independently.

Recently, the presentation of blockchain has made it to become practical. However, the essence of the issue is various

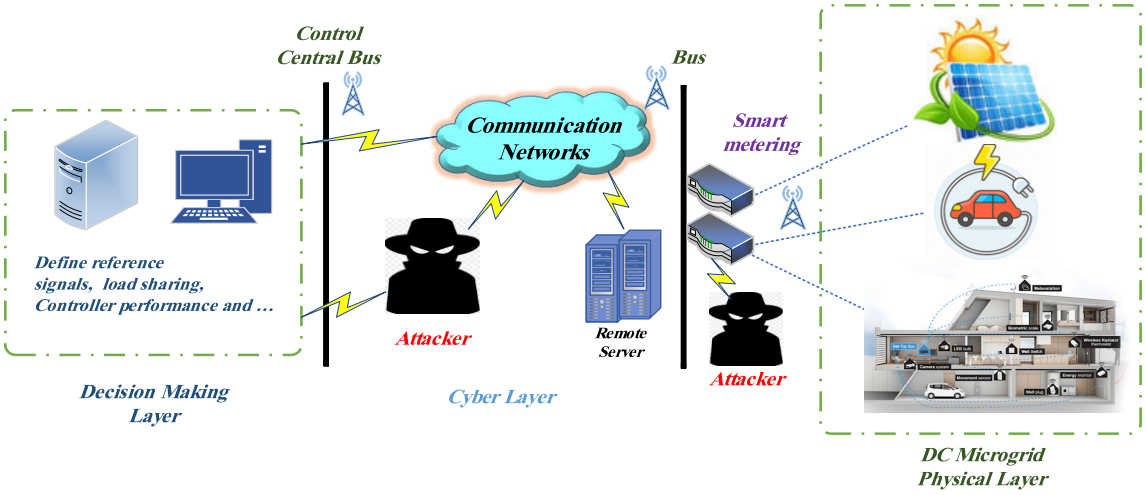


FIGURE 3. Block diagram of the cyber-physical layer of a single MG.

from the bitcoin blockchain-based methods because everyone trades in event messages more than cryptocurrency transactions.

D. ASSUMPTIONS

Distributed generation agents (DGAs) and smart loads/sensors communications are assumed and they are able to link to the internet impressively. It is assumed that entire the agents have needed devices such as sensors, global positioning system (GPS) and on-board units. It is assumed that the agents have wide calculating power and a wide reliance level are attended as complete node agents that are able to take part in the extraction procedures while another node are usual nodes that aids in message forwarding and confirmation. It is assumed that the acute event messages are published through an interest region in a special geographical place. It is also assumed that the acute messages are not hided thus that those messages are able to be accessible to each close agent.

E. PROPOSED BLOCKCHAIN IN SENDING DATA AMONGST ISO AND UNDER-OPERATING AGENTS

In this research, a new type of blockchain is proposed since easy assumption of available blockchain-based method is not appropriate for this case. The traditional blockchain-based technique trades with cryptocurrency, whereas this blockchain trades with event messages without applying any form of crypto coins. This proposed blockchain is suitable for confidence of security messages in vehicular ad hoc network that pertains to the true real world. Additionally, the event message history along with device dependency levels in a reliable, unchangeable, and distributed manner are managed and stored using this blockchain method. In each country, region or area, an individual blockchain will be existed and that is maintained and managed in an independent way with the aim of recording device information. Whole agents distribute their statuses via beacon messages. A position certificate is used, which is a digital affirmation that an agent is seated at a special position at a specific time [9].

Whole agent location requires having a position certificate to affirm their place at a certain time. A legitimate side unit provides a location certificate. The side unit exports a location certificate to the demanding agent applying its private key and own public pair.

This location validates functions as position proofs for agents which help identifying event messages in a specific geographic area. Existing blockchains have timely and scalable problems that might not be suitable for real-time operating applications. In this design, all events are considered to be local, for example, event messages are limited to an agent in a specific geographic region. In the common traditional blockchain, the new multiplicative block is distributed throughout the world.

However, in this plan, the messages of the agents do not need to cross the borders of one country. It is because the traffic and accident data of one country are not related to the agents who are based in another country. Therefore, new form of blockchain content that is different from the common traditional blockchain is required.

In every standalone blockchain, generally all extractors and miners extract the new block based on event messages, and then send the new block to another local blockchain network.

Blockchain as a real international structure can act to confirm the reliability of the node in different countries, which means that any factor can check the level of reliability in the blockchain at any time. Then, new blocks are created by collecting unverified event message tables from the message pool. Figure 1 shows how the mixtures of each block are sequentially chained to form the blockchain. After production, new blocks are distributed and all components in the blockchain network update and verify their blockchain.

III. SYSTEM LAYOUT AND PROPOSED METHOD

In this research paper, the considered strategy includes 2 various DC-MGs that can be connected to each other. Every MG contains a PV resource; a fuel cell employed polymer

TABLE 1. Smart DC-MG parameters.

Units	Parameters	DC MG_1 & DC MG-2
Fuel cell	Nominal power	4 kW
PV	Maximum power	4 kW_p
	Voltage & current at maximum power	72 V, 56.64 A
Supercapacitor	Capacity	208.3 F
	Nominal voltage	72 V
Battery	Capacity	240 Ah
	Nominal voltage	72 V
Bidirectional converter	Voltage ration	36/110 V
Boost converter	Voltage ration	45/110 V
Bus voltage	Nominal voltage	110 V
DC loads	Constant	2 kW
	Variable	5 kW

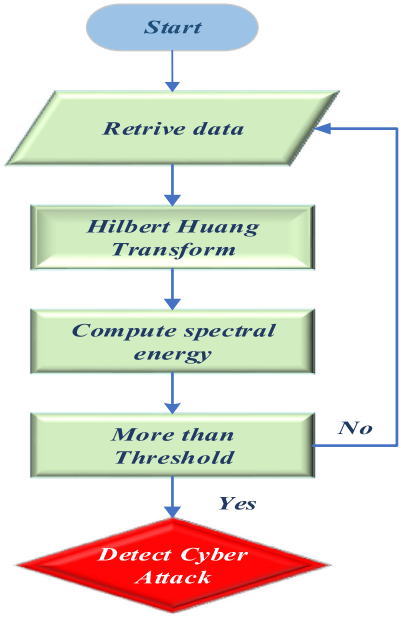


FIGURE 4. FDIAs detection flowchart based on Hilbert Huang transforms.

electrolyte membrane, the battery storage as well as superconductor that stores hybrid power with different controllable loads and converters. The hybrid energy storage system supports stability by storing energy and retrieval that facilitates the conditions of MG operating. In our assumed system, the battery storage has a high-power density so that it is able to supply or absorb less energy for a lengthier duration and the superconductor has also a high energy density that can produce a lot of power for a shorter period of time.

Fuel cell and PV components are coupled to the bus using a boost converter, while battery storage and also supercapacitor is interfaced with the bus via a bi-directional DC to DC converter. Our presented system consists of a centralized control unit, local and manual operational controllers along with a cloud method; where the datum from our system is transmitted to the cloud server. The cloud framework analysis retrieved data of the system and transmits adequate energy sources to local controllers. The framework of the presented system is displayed in Figure 2. These characteristics of the generation units and loads of our system are given in Table 1. The flowchart of the cyber-physical layer in a standalone MG including RERs, converters, and loads is depicted in Figure 3.

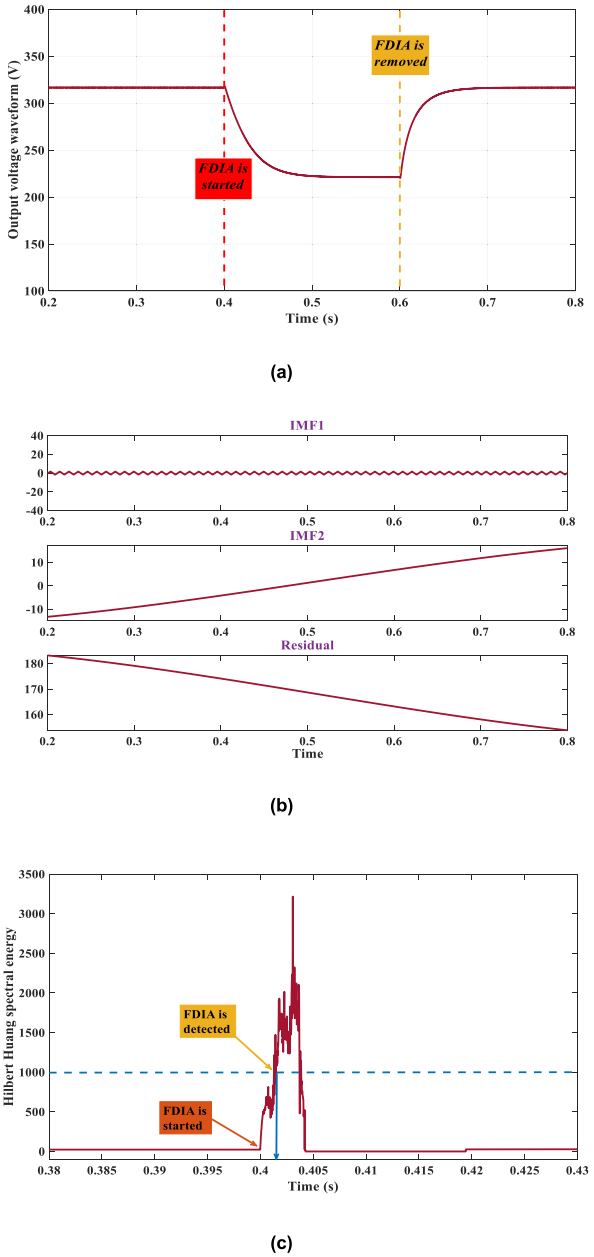


FIGURE 5. FDIA according to increasing the voltage reference signal's amplitude: a) voltage Waveform, b) Empirical mode decomposition, c) Hilbert-Huang spectral energy.

For increasing the cyber-security of a smart DC-MG, this presented strategy in this paper is that malicious FDI attacks on system sensors and controllers are detected by signal processing techniques. Also, in this article, the data sent between units and sensors and other equipment in smart DC-MG is sent by blockchain technology, which increases the security of the transmitted data, which prevents having easy access to this data.

IV. SIMULATION RESULTS

In order to verify the efficiency of the suggested FDIAs detection strategy and security enhancement based on blockchain technology for smart DC-MG, the FDI attack model is

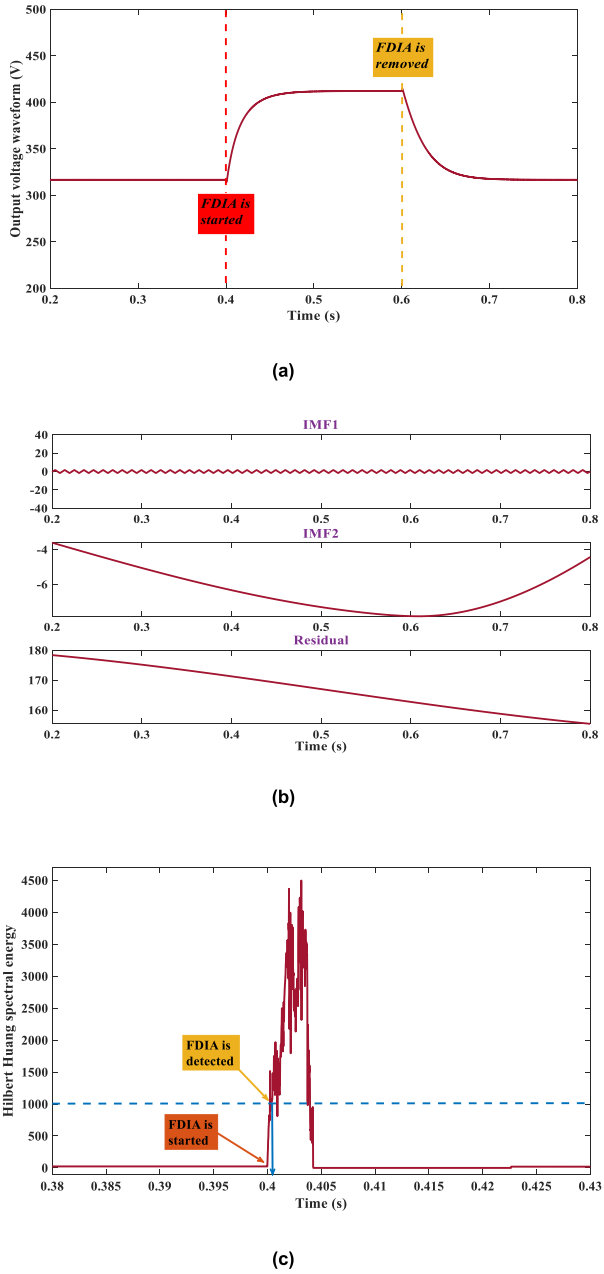


FIGURE 6. FDIA according to increasing the amplitude of voltage signal in the smart sensor: a) Voltage Waveform, b) Empirical mode decomposition, c) Hilbert-Huang spectral energy.

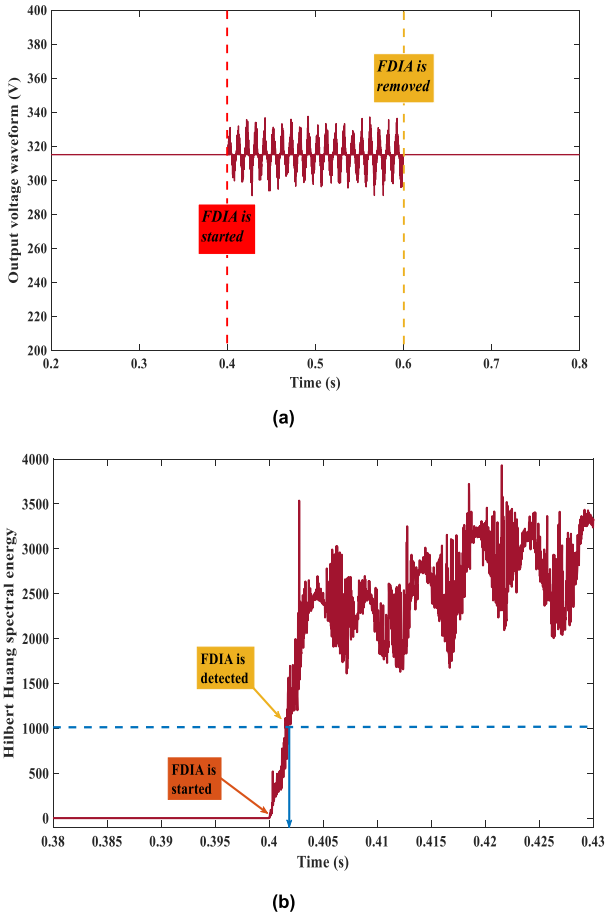


FIGURE 7. FDIA according to the pulsing a noise to the voltage waveform in the smart sensor: a) Voltage waveform, b) Hilbert-Huang spectral energy.

applied to the case study. It should be mentioned that each event in the mentioned cases has been divided by a given time-gap with the objective of making a better understanding the issue; which means that in the simulation, attacks in all scenarios start from 0.4 seconds after the simulation, and end in 0.6 seconds. The results of this work will examine the effectiveness of the proposed detecting attacks method, and will illustrate how sensitive the proposed method is to attacks and can detect them. The FDIAs detection flowchart based on HHT is displayed in Figure 4. In this work, the input to HHT technique consists of 200 patterns. HHT is completely sensitive to the signal magnitude changing and the Empirical mode decomposition of HHT has been used to compute the spectral energy based on equation (9). The spectral energy of HHT can detect various FDI attack and diagnose changing of loads by FDI attacks.

Case A: In this case of study, the hacker is attacked based on FDIA on the voltage reference signal in the controller of the agent II. A model of this FDI attack kind investigates in the smart DC-MG to analyze the behavior of the signal. FDIA is started and dispelled at time t=0.4 and t=0.6 (sec), respectively. The amplitude of the voltage reference signal is varied (decreased by 30%).

Figure 5 exposes the simulation results of this part. Figure 5 (a) is the voltage of the smart DC-MG that the FDI attack has reported on time. The HHT under varied IMFs with residual value is shown in Figure 5 (b). The Hilbert-Huang spectral energy that diagnoses the FDIA through determining a threshold as 1000 is shown in Figure 5 (c). The offered method can detect the FDIA less than 5ms from the cyber-attack inception.

Case B: In this case study, the hacker is attacked based on FDIA on the smart sensor of voltage in agent V. A model

TABLE 2. Transaction blockchain explanation.

Block Index	Block Information			
Index	1			Explanation
Time	1			
Transaction Data	Sender	Receiver	Load of MG1 (KW)	
	Loads	DGs	5.7	
Prior HA	fc8fdb29501a6289b7bc8b0bdd8155df			
Self HA	84f5ddd735176becc72c3b1ff424149e			
Index	2			Explanation
Time	2			
Transaction Data	Sender	Receiver	Voltage (V)	
	Sensor of PV in the MG2	Fuel Cell of the MG2	110	
Prior HA	84f5ddd735176becc72c3b1ff424149e			
Self HA	5f93f983524def3dca464469d2cf9f3e			
Index	4			Explanation
Time	4			
Transaction Data	Sender	Receiver	Voltage (V)	
	Control unit	Controller of Battery in the MG1	110	
Prior HA	e44436592c2daabbd3d797f8967245a3			
Self HA	5f93f983524def3dca464469d2cf9f3e			
Index	5			Explanation
Time	4			
Transaction Data	Sender	Receiver	Voltage (V)	FDIA is occurred
	Control unit	Controller of Battery in the MG1	150	
Prior HA	e44436592c2daabbd3d797f8967245a3			
Self HA	7ef605fc8dba5425d6965fbd4c8fbe1f			
Index	6			Explanation
Time	5			
Transaction Data	Sender	Receiver	Current (A)	
	Current of the Loads	Controller	36	
Prior HA	5f93f983524def3dca464469d2cf9f3e			
Self HA	19ca14e7ea6328a42e0eb13d585e4c22			
Index	7			Explanation
Time	5			
Transaction Data	Sender	Receiver	Current (A)	FDIA is occurred
	Current of the Loads	Controller	28	
Prior HA	5f93f983524def3dca464469d2cf9f3e			
Self HA	33e75ff09dd601bbe69f351039152189			

of this FDI attack kind investigates in the smart DC-MG to analyze the signal behavior. FDIA is started and dispelled at time t=0.4 and t=0.6 (sec), respectively. The amplitude of the signal is varied (decreased by 30%). Figure 6 exposes the simulation results of this part. Figure 6 (a) is the voltage of the smart DC-MG that the FDI attack has reported on time. The HHT under varied IMFs with residual value is shown in Figure 6 (b). The Hilbert-Huang spectral energy that diagnoses the FDIA through determining a threshold as 1000 is shown in Figure 6 (c). The offered method can detect the FDIA less than 5ms from the cyber-attack inception.

Case C: In this case study, the hacker is attacked based on FDIA on the smart sensor of voltage in agent VII. A model of this FDI attack kind investigates the smart DC-MG behavior. FDIA is started and dispelled at time t=0.4 and t=0.6 (sec), respectively. The grid voltage waveform is changed by adding noise. Figure 7 exposes the simulation results of this part.

Figure 7 (a) is the voltage of the smart DC-MG that the FDI attack has reported on time. The HHT under varied IMFs with residual value are shown in Figure 7 (b). The Hilbert-Huang spectral energy that diagnoses the FDIA through determining

TABLE 3. Confusion rate matrix of the introduced detection scheme.

		Actual Value	
		Pos	Neg
Detection scheme Response	Pos	Hit Rate True Pos (TP)	False Alarm Rate False Pos (FP)
	Neg	Miss Rate False Neg (FN)	Correct Rejection Rate True Neg (TN)

TABLE 4. Confusion result matrix of the introduced detection scheme.

	Method	Actual Value	Pos	Neg
Detection scheme Response	Spectral energy of HHT	Pos	96.51 %	3.92 %
		Neg	3.49 %	96.08 %
	Shallow Model	Pos	90.79 %	8.58 %
		Neg	9.21 %	91.42 %
	HHT and DNN [15]	Pos	93.75%	4.77 %
		Neg	6.25 %	95.23 %

	Method	Spectral energy of HHT	HHT and DNN [15]
Response Time	Average Detection Time	5 ms	5 ms
	DNN Training Time	-	2713.2 s

a threshold as 1000 is shown in Figure 7 (c). The offered method can detect the FDIA less than 5ms from the cyber-attack inception.

Case D: In this case study, blockchain-based technology is implemented to Secure data exchanging between renewable resources (such as PV, fuel cell), smart metering, smart loads (like smart homes), and PHEVs. It has been assumed that the transaction processing capacity maximum is between 1 and 3 transactions per second.

In this regard, the measured data of agents in the context of blockchain technology is exchanged between agents and after confirming the validity of the transmitted data and not the malicious attack of information such as FDIAs, the converter controller uses the received data of loads and other units and produces the optimal amount of voltage and current to minimize losses in the smart DC-MG and the amount of production and consumption are the same and a stable voltage is established throughout the system, which allows the information of sensors, loads and other production units to be sent safely and detect any cyber-attack on the transmitted data so that the smart DC-MG with the least losses, optimally and balance between consumption and production is established. Table 2 shows examples of data sent in the smart DC-MG based on blockchain technology.

V. DISCUSSION

Figures 5 to 7 expose the simulations results of FDIA based on the spectral energy of Hilbert-Huang. Figs. 5 (a), 6 (a), and 7 (a) are the voltage of the smart DC-MG that the FDI attack has reported on time. The HHT under various IMFs with residual value is shown in Figures 5 (b), 6 (b), and 7 (b). The Hilbert-Huang spectral energy that diagnoses the FDIA through determining a threshold as 1000 is shown in Figures 5 (c), 6 (c) and 7 (c).

In general, it is considered that when a subject is investigated as a cyber-activity, it will be named as a positive (Pos) decision. On the contrary, it will be a negative (Neg) decision whenever the type of anomaly detection identifies as a usual matter. The true decision will be made until the specimen of uncommon diagnosing is corrected. Therefore, it is clear that an incorrect decision illustrates a false response from the cyber-attack diagnosing type. According to this concept, it is resulted that a proper form for detection anomalies will be a form with a low false rate. Based on these definitions, four various types namely false alarm rate (FAR), miss rate (MR), correct reject rate (CRR) and hit rate (HR) are defined. For providing better concept of these issues, Table 3 represents the confusion matrix. Consequently, in order to confirm the effectiveness and validation of presented HHT in FDIA detection, various test cases are applied. The efficiency of the suggested detection plan is evaluated through applying it into a FDIA scheme where the evaluation outcomes are illustrated. The performance of presented detection plan is investigated by using the FDIA scheme and the evaluation outcomes are presented in Table 4. Furthermore, to demonstrate the sufficiency of suggested cyber-attack detection model, it compares with HHT and deep neural network (DNN) presented in the reference [15]. Table 4 is able to remark that the offered method can detect the FDIA less than 5ms from the cyber-attack inception in different scenarios with more than 96 % accuracy from 1259 samples.

As can be seen, Table 2 shows the public blockchain linked to the smart DC-MG, where the data has been matched with the private blockchain of the smart DC-MG. The procedure is able to aid with the aim of retrieving the information in the presence of a cyber-attack or package drop off in two of private and public blockchain. Although it is noteworthy that the agents' generation output current and voltage and others data, also the production power of distributed generation units, smart metering and loads of agent, is not accessible in the blockchain, that is able to raise the privacy and the security of the network and messages. The transaction blocks are presented in Table 2 . Pursuant to the table, for example, at t = 1, DGs gets a message from loads. In addition, the table shows the loads power, and also the amount of power in kilowatt. Like the private blockchain, any block comprises the HA (hash algorithm) function recognized in the role of the self HA, that is able to chain to the prior block through applying the prior HA. Also, if a hacker attacks the data (see index 5 and 7), the HA is altered and the HA is not similar, therefore the multi-plate data is defined.

The detection accuracy based on HHT as input of DNN is able to detect FDIAs over 95 % and the DNN training time is 2713.2 s where average detection time is 5 ms; and the accuracy of detection according to Shallow Model can detect FDIAs over 90.5 % but in the suggested method, the average detection time is 5 ms with more than 96 % accuracy and without the training time and complexity of DNN (The volume and computational time of the deep learning method are high, so the feasibility of implementing the proposed method in today's digital processors and relays is questionable.), so,

it displays the sufficiency of the introduced detection plan to detect the FDIAs.

VI. CONCLUSION

FDIA interrupts the consensus protocols applied in cyber-physical smart DC-MGs. FDIA detection way is introduced based on Hilbert-Huang transform to detect malicious attacks in the sensors and controller. The offered technique can detect various FDIA in voltage and current sensors and controller of the converters be defining a threshold.

In addition, a sound and effective data-exchanging layout on the basis of blockchain and a community detection framework is presented. According to the previous assumption, warrantying data security, the suggested layout produces extra fine-grained data-exchanging services through categorizing clients applying label data. For achieving secure and effective data sharing, four phases are introduced, involving initialization, identity authentication, signature/verification, and information exchanging phases. The community detection server considers as the key to the information exchanging layout. In the layout, the community detection server gets and analyses the label datum of whole clients, diagnoses the community via cosine resemblance. By securing the data exchanged between agents in the smart DC-microgrid, the attacker is not able to penetrate to the systems and make the system more reliable and stable. The outcomes of the simulation on a test system show the high efficiency and benefit of the suggested way, particularly in the existence of cyber-attack wherein the information is not available for unauthorized members out of the system. The chief reason is that the HAs are altered in any iteration.

REFERENCES

[1] M. Ghiasi, "Detailed study, multi-objective optimization, and design of an AC-DC smart microgrid with hybrid renewable energy resources," *Energy*, vol. 169, pp. 496–507, Feb. 2019.

[2] P. Duan, H. Soleimani, A. Ghazanfari, and M. Dehghani, "Distributed energy management in smart grids based on cloud-fog layer architecture considering PHEVs," *IEEE Trans. Ind. Appl.*, early access, Jul. 21, 2020, doi: 10.1109/TIA.2020.3010899.

[3] M. Fathi and M. Ghiasi, "Optimal DG placement to find optimal voltage profile considering minimum DG investment cost in smart neighborhood," *Smart Cities*, vol. 2, no. 2, pp. 328–344, Jun. 2019.

[4] M. Ghiasi, "Technical and economic evaluation of power quality performance using FACTS devices considering renewable generations," *Renew. Energy Focus*, vol. 29, pp. 49–62, Jun. 2019.

[5] M. Dehghani, A. Kavousi-Fard, T. Niknam, and O. Avatefipour, "A robust voltage and current controller of parallel inverters in smart island: A novel approach," *Energy*, vol. 214, Jan. 2021, Art. no. 118879.

[6] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. Manubot, 2019. [Online]. Available: https://git.dhimmel.com/bitcoin-whitepaper/

[7] G. Chapron, "The environment needs cryptogovernance," *Nature*, vol. 545, no. 7655, pp. 403–405, May 2017.

[8] M. Dehghani, A. Kavousi-Fard, M. Dabbaghjamanesh, and O. Avatefipour, "Deep learning based method for false data injection attack detection in AC smart islands," *IET Gener., Transmiss. Distrib.*, vol. 14, no. 24, pp. 5756–5765, Dec. 2020.

[9] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, and S. Padmanaban, "False data injection attack detection based on Hilbert-huang transform in AC smart islands," *IEEE Access*, vol. 8, pp. 179002–179017, 2020.

[10] A. Afshari, M. Karrari, H. R. Baghaee, and G. B. Gharehpetian, "Resilient synchronization of voltage/frequency in AC microgrids under deception attacks," *IEEE Syst. J.*, early access, May 29, 2020, doi: 10.1109/JSYST.2020.2992309.

[11] M. Ghiasi, "A comparative study on common power flow techniques in the power distribution system of the tehran metro," *Tehnički glasnik*, vol. 12, no. 4, pp. 244–250, Dec. 2018.

[12] H. Karimipour and H. Leung, "Relaxation-based anomaly detection in cyber-physical systems using ensemble Kalman filter," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 1, pp. 49–58, Mar. 2020.

[13] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2038–2049, Jul. 2016.

[14] M. Ghiasi, M. Dehghani, T. Niknam, and A. Kavousi-Fard, "Investigating overall structure of cyber-attacks on smart-grid control systems to improve cyber resilience in power system," *IEEE Smart Grid Newslett.*, Mar. 2020. [Online]. Available: https://smartgrid.ieee.org/newsletters/march-2020/investigating-overall-structure-of-cyber-attacks-on-smart-grid-control-systems-to-improve-cyber-resilience-in-power-system

[15] H. Cui, X. Dong, H. Deng, M. Dehghani, K. Alsubhi, and H. M. A. Aljahdali, "Cyber attack detection process in sensor of DC micro-grids under electric vehicle based on Hilbert-Huang transform and deep learning," *IEEE Sensors J.*, early access, Sep. 29, 2020, doi: 10.1109/JSEN.2020.3027778.

[16] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, E. Tajik, S. Padmanaban, and H. Aliev, "Cyber attack detection based on wavelet singular entropy in AC smart islands: False data injection attack," *IEEE Access*, vol. 9, pp. 16488–16507, 2021.

[17] A. Ometov, Y. Bardinova, A. Afanasyeva, P. Masek, K. Zhidanov, S. Vanurin, M. Sayfullin, V. Shubina, M. Komarov, and S. Bezzateev, "An overview on blockchain for smartphones: State-of-the-art, consensus, implementation, challenges and future trends," *IEEE Access*, vol. 8, pp. 103994–104015, 2020.

[18] J. E. Stamp, C. K. Veitch, J. M. Henry, D. H. Hart, and B. Richardson, *Microgrid Cyber Security Reference Architecture (V2)*. Albuquerque, NM, USA: Sandia National Lab.(SNL-NM), 2015.

[19] M. Ghiasi, "A detailed study for load flow analysis in distributed power system," *Int. J. Ind. Electron., Control Optim.*, vol. 1, pp. 159–160, Sep. 2018.

[20] W. Chen, D. Ding, H. Dong, and G. Wei, "Distributed resilient filtering for power systems subject to denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1688–1697, Aug. 2019.

[21] H. M. AlBuflasa, "Detecting replay attacks in power systems: A data-driven approach," in *Proc. Adv. Comput. Methods Energy, Power, Electr. Vehicles, Their Integr., Int. Conf. Life Syst. Modeling Simulation, LSMS Int. Conf. Intell. Comput. Sustain. Energy Environ., ICSEE*, Nanjing, China, Sep. 2017, p. 450.

[22] H. Khaloie, A. Abdollahi, M. Shafie-khah, A. Anvari-Moghaddam, S. Nojavan, P. Siano, and J. P. S. Catalão, "Coordinated wind-thermal-energy storage offering strategy in energy and spinning reserve markets using a multi-stage model," *Appl. Energy*, vol. 259, Feb. 2020, Art. no. 114168.

[23] M. K. Arpanahi, M. Kordi, R. Torkzadeh, H. H. Alhelou, and P. Siano, "An augmented prony method for power system oscillation analysis using synchrophasor data," *Energies*, vol. 12, no. 7, p. 1267, Apr. 2019.

[24] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021.

[25] W. Zhang and X. He, "Stealthy attack detection and solution strategy for consensus-based distributed economic dispatch problem," *Int. J. Electr. Power Energy Syst.*, vol. 103, pp. 233–246, Dec. 2018.

[26] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, Sep. 2018.

[27] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, Dec. 2010, pp. 5991–5998.

[28] M. El-Hendawi and Z. Wang, "An ensemble method of full wavelet packet transform and neural network for short term electrical load forecasting," *Electr. Power Syst. Res.*, vol. 182, May 2020, Art. no. 106265.

[29] M. R. Habibi, H. R. Baghaee, T. Dragicevic, and F. Blaabjerg, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE J. Emerg. Sel. Topics Power Electron.*, early access, Jan. 20, 2020, doi: 10.1109/JESTPE.2020.2968243.

[30] M. R. Habibi, H. R. Baghaee, T. Dragicevic, and F. Blaabjerg, "False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 2, pp. 717–721, Feb. 2021.
[31] N. Bayati, H. R. Baghaee, A. Hajizadeh, and M. Soltani, "Localized protection of radial DC microgrids with high penetration of constant power loads," *IEEE Syst. J.*, early access, Jun. 8, 2020, doi: 10.1109/JSYST.2020.2998059.
[32] B. P. Hayes, S. Thakur, and J. G. Breslin, "Co-simulation of electricity distribution networks and peer to peer energy trading platforms," *Int. J. Electr. Power Energy Syst.*, vol. 115, Feb. 2020, Art. no. 105419.
[33] S. Wang, A. F. Taha, J. Wang, K. Kvaternik, and A. Hahn, "Energy crowdsourcing and Peer-to-Peer energy trading in blockchain-enabled smart grids," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1612–1623, Aug. 2019.
[34] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.
[35] E. S. Kang, S. J. Pee, J. G. Song, and J. W. Jang, "A blockchain-based energy trading platform for smart homes in a microgrid," in *Proc. 3rd Int. Conf. Comput. Commun. Syst. (ICCCS)*, Apr. 2018, pp. 472–476.
[36] R. Carreño, V. Aguilar, D. Pacheco, M. A. Acevedo, W. Yu, and M. E. Acevedo, "An IoT expert system shell in block-chain technology with ELM as inference engine," *Int. J. Inf. Technol. Decis. Making*, vol. 18, no. 1, pp. 87–104, Jan. 2019.
[37] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.
[38] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019.
[39] M. Foti and M. Vavalis, "Blockchain based uniform price double auctions for energy markets," *Appl. Energy*, vol. 254, Nov. 2019, Art. no. 113604.
[40] W. Ethereum, "A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

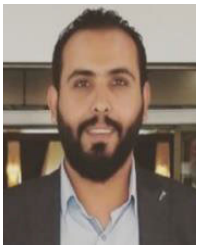
MOHAMMAD GHIASI received the B.S. and M.S. degrees in electrical power engineering, in 2012 and 2016, respectively. He is currently a Research Assistant with the Shiraz University of Technology, Shiraz, Iran. He has two Hot Articles and one Highly-Cited article, based on SciVal and Web of Science statistics. His research interests include modeling, simulation and optimization of power systems, integration and control of hybrid and distributed renewable energy resources, smart grids, as well as cyber-physical resilience in power systems has led to multiple publications in these fields. He is also a Reviewer of several IEEE, IET, Elsevier, Springer, Wiley, Sage and Taylor & Francis journals and conferences.

MOSLEM DEHGHANI was born in Shiraz, Iran, in 1990. He received the B.S. and M.S. degrees in electrical engineering from Islamic Azad University-Kazerun Branch, in 2012 and 2014, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with the Shiraz University of Technology, Shiraz, Iran. His current research interests include power electronic, control, and cyber security analysis of smart grids, microgrid, smart city, HVDC systems as well as protection of power systems, fuzzy logic, and signal processing.

TAHER NIKNAM (Member, IEEE) was born in Shiraz, Iran. He received the B.S. degree from Shiraz University, Shiraz, Iran, in 1998, and the M.S. and Ph.D. degrees from the Sharif University of Technology, Tehran, Iran, in 2000 and 2005, respectively, all in power electrical engineering. He is a Faculty Member with the Department of Electrical Engineering, Shiraz University of Technology. His research interests include power system restructuring, impact of distributed generations on power systems, optimization methods, and evolutionary algorithms.

ABDOLLAH KAVOUSI-FARD (Member, IEEE) received the B.Sc. degree in electrical engineering from the Shiraz University of Technology, Shiraz, Iran, in 2009, the M.Sc. degree in electrical engineering from Shiraz University, Shiraz, in 2011, and the Ph.D. degree in electrical engineering from the Shiraz University of Technology, in 2016. He was a Postdoctoral Research Assistant with the University of Michigan, Ann Arbor, MI, USA, from 2016 to 2018. He was a Researcher with the University of Denver, Denver, CO, USA, from 2015 to 2016, conducting research on microgrids. He is currently an Assistant Professor with the Shiraz University of Technology. 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. He is an Editor in Springer, and ISTE and ISI journal.

PIERLUIGI SIANO (Senior Member, IEEE) received the M.Sc. degree in electronic engineering and the Ph.D. degree in information and electrical engineering from the University of Salerno, Fisciano, Italy, in 2001 and 2006, respectively. He is currently an Associate Professor with accreditation for a Full Professor of Electrical Energy Engineering with the Department of Industrial Engineering, University of Salerno. His research interests include demand response, integration of distributed energy resources in smart grids and planning, and management of power systems.



HASSAN HAES ALHELOU (Senior Member, IEEE) is currently a Faculty Member with Tishreen University, Latakia, Syria. He has published more than 100 research papers in the high quality peer-reviewed journals and international conferences. He has also performed more than 600 reviews for high prestigious journals, including IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, ENERGY CONVERSION AND MANAGEMENT, *Applied Energy*, and *International Journal of Electrical Power and Energy Systems*. He has participated in more than 15 industrial projects. His major research interests include power systems, power system dynamics, power system operation and control, dynamic state estimation, frequency control, smart grids, micro-grids, demand response, load shedding, and power system protection. He is included in the 2018 and 2019 Publons list of the Top 1% Best Reviewer and Researcher in the field of engineering. He was a recipient of the Outstanding Reviewer Award from the *Energy Conversion and Management Journal*, in 2016, *ISA Transactions Journal*, in 2018, *Applied Energy Journal*, in 2019, and many other Awards, and the Best Young Researcher Award from the Arab Student Forum Creative among 61 researchers from 16 countries at Alexandria University, Egypt, in 2011.