This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2022.3142755, IEEE Transactions on Industrial Informatics

A Proof-of-Authority Blockchain Based Distributed Control System for Islanded Microgrids

Jiawei Yang, *Member*, IEEE, Jiahong Dai, *Student Member*, IEEE, Hoay Beng Gooi, *Life Senior Member*, IEEE, Hung Dinh Nguyen, *Member*, IEEE, Amrit Paudel, *Member*, IEEE

***Abstract*—Control systems are significant to the microgrid as they regulate performance parameters such as frequency, active power, and voltage. Distributed control systems allow direct communication between the secondary controllers and controls the parameters efficiently. To secure each distributed control process and ensure a good quality of control results, a Proof-of-Authority private blockchain is applied in this study to defend the distributed control system against various types of cyber-attacks such as false data injection. A four-DG islanded microgrid is tested with the implementation of the blockchain. Smart contracts are created to calculate the control feedback and return the value to corresponding secondary controllers. All of the four nodes are initially assigned as the authority nodes to share the mining burden, but according to the Proof-of-Authority consensus protocol, the authority role could be excluded if the node behaves illegally and causes damage to the control system. In addition, different attacking scenarios are categorized and analyzed with their respective solutions. Finally, a case study is introduced to verify the corresponding solutions and proves that the proposed method is able to secure the distributed control system while ensuring the control quality. Numerical results show the effectiveness and feasibility of the proposed approach.**

***Index Terms*—Distributed control, private blockchain, cyber-security, smart grid, proof-of-authority**

I. Introduction

With the development of distributed generation within microgrids, the requirement for ensuring a solid control system for locally distributed generators becomes a significant task, especially for the secondary control system. Nowadays, reliable energy supply is fundamentally supported by modern cyber-physical power systems. The paradigm of cyber-physical power systems involves the interface of all electrical supplies, including conventional power plants and new add-ons such as smart meters, phasor measurement units, communication infrastructures and distributed generations . Cyber-physical power systems are vulnerable to cyber attacks that threaten its pervasive application of communication and information technologies, leading to further attacks on physical systems. In a networked control system, the exchange of measurement data and control commands via the unprotected network is exposed to the malicious attackers and likely to be corrupted by energy theft or false data injection. Currently, blockchain technology is mostly utilized in the power system operation for energy trading due to its cryptographic mechanism and distributed ledger feature, which could protect transactions against any cyber-attacks. Therefore, the application of blockchain technology to ensure the security of control systems is extremely promising and needs to be explored.

A. Related Work

The research works on cyber-security in modern cyber-physical power systems provide different methods to achieve the data protection of control systems. In [1], the mechanism and categories of false data injection (FDI) are introduced. In addition, some defensive strategies are listed in this study. Specifically, in [2], the authors survey the attacks to state estimation of power systems. The detailed mathematical and theoretical depths on false data attacks and defense are proposed. The investigation on the attacks against networked control systems is provided in [3], in which a Kalman filter-based networked predictive output tracking control scheme is designed to protect both feedback and forward channels. Another work studying state estimation protection [4] presents the process of the test system setup and also proposes a method of bad data detection, which is experimented with different attacking scenarios. The authors in [5] propose a joint-transformation detection method of data integrity attacks. This method increases the detection probability by transforming the measurement variation. Deep learning [6] and deep neural network [7] techniques are used to recognize the behavior patterns of false data injection attacks by using the historical measurement data. These methods also detect recent attacks patterns with incomplete power network information. Furthermore, other ideas such as colored Gaussian noise [8] and incomplete information [9] are applied as detection-based approaches in power systems. According to the methods mentioned above to safeguard power systems, some of the previous studies only focus on detection and identification [4–9] of the cyber-attacks without an effective protection approach. And the protection-based approach design of other works is only effective to a few specific attacks [2, 3] or their problem setting is based on random or benign attacks [6, 7]. The objective of this paper is to propose a comprehensive protection method for power systems.

Blockchain is considered an effective tool to secure information exchange comprehensively because of its unique cryptographic mechanism and verification process [10]. Information is packed into each block by using the cryptographic method of blockchain after being validated by the other nodes. But this advantage is not realized fully in the power system. Due to the capability of securing and storing data, blockchain is currently only applied as a framework with various pricing mechanisms to safeguard energy transactions in the power system domain, including iterative methods [11], game theory [12] and double auction [13]. According to the previous researches, various types of consensus protocols are adopted such as Proof-of-Work (PoW), Proof-of-Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT). But in the control system of microgrids, the usage of blockchain is rarely adopted. The responsibility of distributed control in the power system is to sense the electrical parameters (frequency, voltage, active and reactive power) of the microgrid and adjust them to the respective reference value to maintain a normal operation of the whole power system [14]. It relies on the communication and data transmission among the primary and secondary hardware controllers [15]. The authors in [16] propose an auditable access control system for private data in service-centric IoT environments. This ensures private data security for real application scenarios in IoT environments. Similarly, in [17], the authors design a blockchain-based access control protocol in the IoT-enabled smart grid system. Their proposed blockchain records the profile of power generation and transmission and manages energy trading. The authors in [18] present a theoretical control-model formulation of the founding Satoshi Nakamoto blockchain with PoW, which is generic of every honest ledger-maintainer's local operations on a blockchain network. Current studies on access control systems with IoT are mainly focused on privacy data security rather than data transmission security [16, 17, 19]. And the concept of their control systems is completely different from the control system existing in power systems. In addition, their proposed blockchain model works separately with the control system, which means the blockchain is only able to protect the attacks outside the system but cannot provide protection if any nodes within the blockchain become malicious [20]. The other related work only proposed a theoretical idea in which the blockchain enables the protection of distributed control without a feasible implementation [21]. Therefore their conclusion is unreliable. More significantly, none of the blockchain models in the previous work could match the sampling rate of the power system control. To maintain a stable power system, the control system samples the electrical parameters more than 10,000 times per second [22, 23]. This means the mining rate should equal the sampling rate and generate 10,000 blocks per second. The complex mining mechanism and huge gas consumption needed for PoW and PoS make the such required mining rate impossible.

Overall, the research gaps are concluded as follows:

- Except blockchain, other methods can only detect and identify FDI attacks without providing a comprehensive protection method.
- For the blockchain-based control system, previous works cannot defend the FDI attacks aimed at data transmission.
- The security is not completely ensured when the internal nodes become malicious.
- Theoretical assumption without the support from actual implementation.
- The block production rate cannot match the sampling rate of distributed control in power systems.

B. Motivation and Contribution

In this paper, the main focus is to design a blockchain-based comprehensive protection method against various cyber-attacks for the secondary control layer of the islanded microgrid. It enables a secure and efficient communication environment for the neighboring local distributed generation (DG) controllers. The proposed blockchain model could support controllers to exchange information with one another, and thus, the application of blockchain in power systems can be expanded to control systems. The adoption of blockchain prevents malicious attacks such as FDI. In the proposed model, the functions of blockchain engaged in the control operation directly as the designed smart contracts are responsible for the exchange of the input and feedback control signals of DG controllers instead of money and products for transactions. The penetration of the proposed blockchain applications into the control system is deep enough to protect both external and internal attacks. Therefore, the quality and security of the control from the secondary control layer are ensured. In the proposed model, a Proof-of-Authority (PoA) based private blockchain is applied to secure the secondary frequency control of islanded microgrids. To achieve the synchronization to the fast sampling rate, the gRPC technique is applied to further enhance the mining rate of the proposed blockchain. In this context, the contributions of this paper are:

- A PoA based private blockchain is proposed to provide comprehensive protection for the distributed control system (DCS) of the microgrid, in which the data transmission between the microgrid and the DCS is secured.
- Different cyber-attacks such as FDI against secondary control for a four-DG islanded microgrid are defended by the deep penetration of the proposed blockchain application, including the external attacks and internal injections.
- The implementation of the proposed blockchain model is specifically demonstrated with the creation of smart contracts to prove the feasibility and effectiveness of the proposed method, which requires low energy consumption.
- The gRPC technique is utilized to enhance the mining rate of the proposed blockchain. Therefore, the block production speed can match the sampling rate and ensure the quality of the DCS outcomes.

The remaining of this study is organized as follows: Section II presents a distributed secondary control system for frequency regulation. Section III introduces the Ethereum based PoA private blockchain for securing the frequency regulation of a four-DG islanded microgrid with smart contracts creation. Different attacking scenarios are analyzed in Section IV, with corresponding solutions offered by the proposed blockchain model. A case study and the implementation process of the proposed method are shown in Section V. The evaluation of the proposed method is discussed in Section VI. Finally, Section VII includes the conclusion of the study and future works.

II. Distributed Secondary Frequency Control for Microgrids

Secondary control removes the steady-state frequency deviations produced from the primary droop control. The conventional secondary control layer is based on a microgrid central controller (MGCC) as a central agent responsible for collecting information from each local DG and sending the control commands back to them. This control method requires a huge computation and communication burden on the central agent, leading to poor control dynamics and potential single-point failures. Therefore, distributed control strategy has been invented to regulate the frequency value. Under the distributed control strategy, each local controller could communicate with its neighboring controllers and adjust their frequency to the reference values. In this scenario, both secondary controllers and primary controllers are locally distributed to each DG unit. Fig. 1 illustrates the structure of a distributed secondary control system.

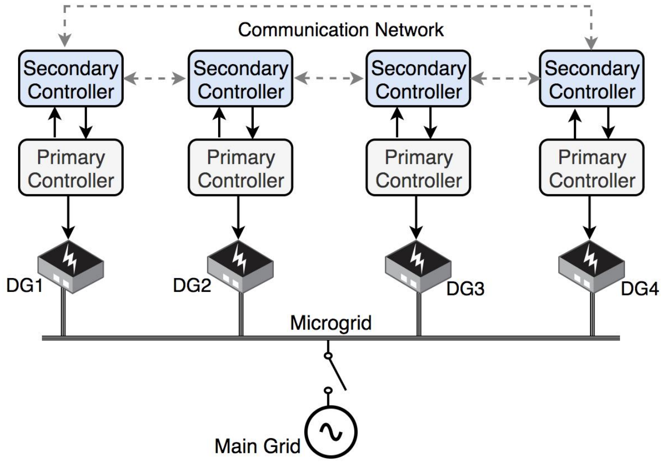


Fig. 1. Distributed control system for microgrids

From Fig. 1, the secondary controllers of DG units collect the measurements (such as frequency) of the microgrid via the communication network supported by the PoA private blockchain, which will be proposed in Section III. The communication network of DG units could be described by a weighted adjacency matrix A. According to Fig. 1, A is shown as:

$$A = \begin{bmatrix} 0 & a_{12} & 0 & a_{14} \\ a_{21} & 0 & a_{23} & 0 \\ 0 & a_{32} & 0 & a_{34} \\ a_{41} & 0 & a_{43} & 0 \end{bmatrix} \tag{1}$$

where elements $a_{ij} > 0$ refer to the direct information exchange between controllers of DG_i and DG_j.

The distributed control feedback of frequency U_w sent by secondary controllers could be calculated as:

$$U_w = K_w \times [(A - D) \times F + G \times (F^* - F)] \tag{2}$$

$$F = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix} \tag{3}$$

$$D = \begin{bmatrix} a_{12}+a_{14} & 0 & 0 & 0 \\ 0 & a_{21}+a_{23} & 0 & 0 \\ 0 & 0 & a_{32}+a_{34} & 0 \\ 0 & 0 & 0 & a_{41}+a_{43} \end{bmatrix} \tag{4}$$

where G is the weighted matrix and F^* is the reference frequency matrix, in which w_1-w_4 are the reference frequency values of the four DG units. K_w refers to the positive control gain. For each controller, the diagonal elements in D refer to the other controllers that could be communicated with according to A.

The frequency of the proposed distributed secondary frequency controllers and its targeted frequency are calculated as:

$$w_i = w_i^* - k_{wi}P + \delta w_i \tag{5}$$

$$\lim_{t \to \infty} w_i(t) = w_i^* \tag{6}$$

where w_i^* is the reference frequency value for DG_i. k_{wi} is the droop coefficients and δw_i is the secondary control signal sent to the primary control level. Equation (5) implies that the final goal of the DCS is to adjust the electrical parameters to the reference value.

III. Blockchain and Smart Contracts Implementation for DCS

After the introduction of DCS, this section first identifies the blockchain features that most applicable for the proposed DCS and control algorithms proposed in Section II. In addition to the security requirement of DCS, the proposed blockchain type should also adequately match the frequency of DCS sampling, in which each round of input and control commands exchange is extremely fast. A short block production period is required for the selection of blockchain types.

From the working mechanism of blockchain, the information of data exchange (control signals or transactions) proposed by the participants are packed by validators, who use a cryptographic method called hash function to encode and secure the information. The blockchain types are determined by their consensus protocols, which define the agreement rules among all the participants. Before the data package, the information should be verified and authenticated by the participants of the blockchain according to the rules of agreement offered by the consensus protocol. In the blockchain applications for the power system domain, Ethereum and Hyperledger Fabric are the two most popular blockchain platforms that are widely used in the previous studies. Table I compares the performance of a four-node microgrid by using different blockchain types from different platforms.

TABLE I
THE COMPARISON OF PERFORMANCES OF ETHEREUM AND HYPERLEDGER BLOCKCHAIN

Platform	Ethereum	Ethereum	Hyperledger Fabric
Blockchain type	Public	Private	Private
Nodes quantity	4	4	4
Consensus	PoW/PoS	PoA	PBFT
Setup tool	EVM	Geth	Fabric
Authority	Decentralised	Consortium	Centralised
Block production	$> 5mins$	$< 10^{-2}second$	$< 10^{-2}second$
Smart contracts	Solidity	Solidity	Chaincode
Gas	Required	Required	Not required
Mining difficulty	$> 10^{12}$	1	$> 3 * 10$

According to Table I, compared to the public chains, the private blockchain does not require high-performance hardware due to its lower mining difficulty and much shorter period for each block production. The interval time of block production is more predictable, and it has been proved that a private blockchain is able to mine 20,000 transactions per second [24]. Such a high mining rate is able to match the DCS sampling rate. Besides, a longer time of block production results in more frequent calls of the smart contract functions. This leads to enormous gas costs because every control process requires the execution from the smart contract. The disadvantages of public blockchain also include heavy computation burden and huge energy consumption. For the comparison between different platforms, nodes of Hyperledger Fabric have different roles and cannot be switched [25]. This feature conflicts with the distributed secondary controllers which share the same communication burden in the microgrid. But in the Ethereum based blockchain, it is flexible to adjust the roles of nodes [26]. According to the PoA consensus protocol, only authority nodes are able to mine the blocks. The selection of the authority nodes is decided on the legitimacy of the contributions made by the nodes of the blockchain, such as validating information legally without injecting false data maliciously. In this study, to maintain the decentralised structure of the blockchain system, all of the four DG controllers are assigned as authority nodes to validate the blockchain and share the mining and communication burden.

Based on the aforementioned advantages, the Ethereum based PoA private blockchain is selected for securing the four-DG islanded microgrid. The specific introduction of the proposed PoA blockchain system is provided in the next section.

A. PoA Blockchain Implementation for DCS

The integration and implementation of PoA blockchain with DCS models includes four modules, which are demonstrated in Fig. 2. Module I, corresponding to DCS simulation, is set up by the RT-Lab [27] is supported by a real-time simulation machine. Module II is the server interface for real-time data transmission between the DCS and the PoA blockchain system, including four data channels for the four secondary controllers respectively. Real-time data such as frequency is first transferred from RT-LAB to the Socket interface via a user datagram protocol (UDP). The data items are then packed and categorized for further transmission to the proposed blockchain system by using Remote Procedure Calls (gRPC) which provides services such as authentication and bidirectional streaming.

Model III refers to the proposed PoA blockchain system, in which four node-accounts representing the four secondary DG controllers are created with different addresses and private keys. After receiving the information from the server interface, the Web3 Python-written scripts call the functions of the smart contracts to calculate Equation (2) and pass the calculation results to Module IV. The communication network is set up by connecting those four nodes via a Bootnode channel which is a service provided by the proposed PoA blockchain. Finally, Module IV sends the control commands back to the server interface to achieve the results of DCS.

According to Module III shown in Fig. 2, the input data is packed by the four miner nodes to form a new block added to the blockchain. The packing method is achieved by using a crypto-graphic method called hash function, which translates the practical measurements to a set of hash code. This hash code is extremely difficult to be traced and thus the data of DCS is secured by the blockchain system. The hash function in the proposed PoA blockchain is defined as:

$$Code(n) = H(< f, P >, Contrs, Time, Code(n-1)) \quad (7)$$

where f, P refers to the measurement data and $Contrs$ is the deployed smart contracts. $Code(n-1)$ refers to the hash code of the previous block.

In Equation (6), the hash code of previous blocks is taken into the hash code calculation of the later block. This feature constructs the connection among every block. A slight change happened in one block will crash the 'chain' of the blockchain so that any malicious attack could be easily detected and then becomes invalid. The specific attacks in different scenarios and the corresponding solutions provided by the PoA blockchain will be analysed in Section IV.

A disadvantage of blockchain technology needs to be noted. The mining duration is not a stable period, which means each mining process could not only match one but multiple DCS sampling processes. During each block production T_b, the number of DCS processes n mined in each block could be defined as:

$$n = \frac{T_b}{T_s} \quad (8)$$

where T_s refers to each sampling time.

The solution for this problem is provided by blockchain itself, which is called Merkle tree mining structure (MTMS). By using the MTMS, miners first calculate n sets of hash codes for the corresponding n DCS processes. Then, they form these hash codes to groups and continually hash each hash code group until a final hash code is generated to represent all of the n DCS processes. Fig. 3 illustrates the mechanism of MTMS, in which $HashCode(1 + 2 + ... + n)$ represents the n DCS processes during a block production.

B. Smart Contracts Creation for DCS

Smart contracts in blockchain are responsible for executing data exchange automatically. In this paper, the functions in the smart contracts for data exchange are designed respectively for the four secondary controllers. After receiving the measurements from the other controllers, smart contracts calculate U_w and return this value to each controller. Since smart contracts are designed for efficient calculation, they cannot afford complex computation so that the integrated computation related to Equation (5) and (6) are calculated in Module IV of Fig. 2. The working mechanism of smart contracts in the proposed blockchain model is shown in the algorithm below.

It should be noted that the last step of Algorithm 1 removes the previous data of the four controllers. Because after each block production, new measurements of the four controllers will be transferred from Module I to Module III and the removal of previous measurements helps to relive the storage burden of smart contracts and prevent any latency that may

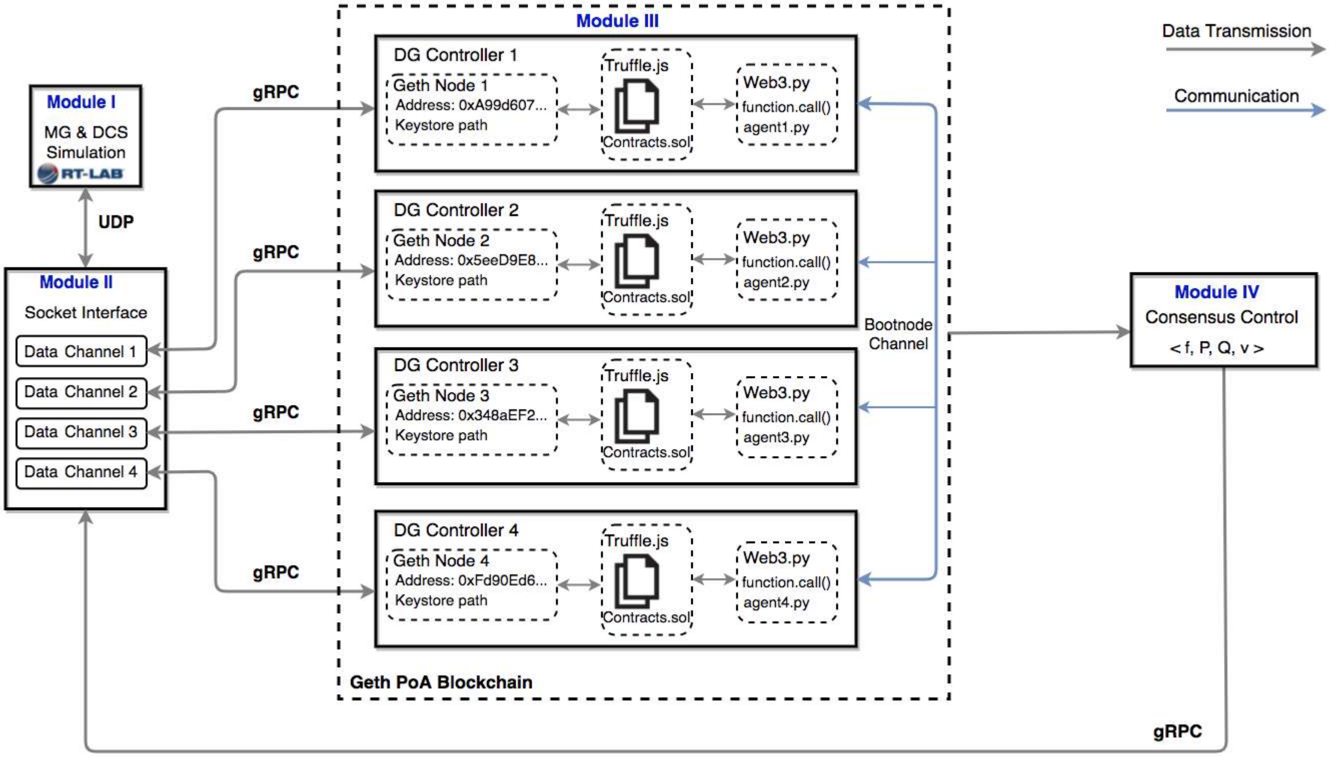


Fig. 2. Schematic diagram for the PoA blockchain system based microgrid. Module I: RT-LAB simulation; Module II: Socket interface; Module III: The PoA blockchain implementation; and Module IV: Control signals delivery to Module II.

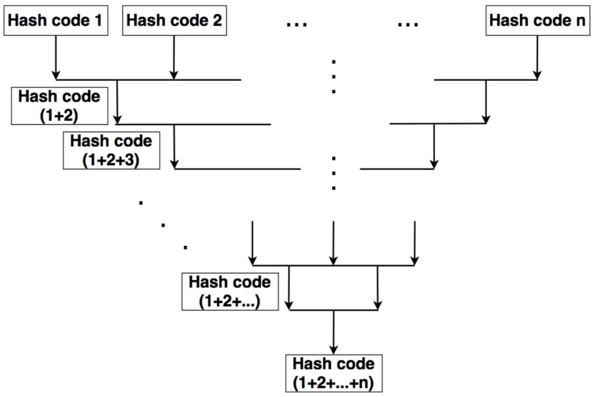


Fig. 3. MTMS mechanism of hash process

cause unpredictable time of mining. By using smart contracts for the DCS execution, the control structure of the four-DG microgrid is slightly changed, which is shown in Fig. 4.

IV. Attack Analysis for PoA Blockchain Based DCS

To attack the proposed PoA blockchain process, the attackers aims to inject a false measurement to mislead the DCS process. The capability of defending the DCS by a blockchain is positively proportional to the number of blocks. Although blockchain is vulnerable when it only contains few blocks, the block production of the private chain is extremely fast, and thousands of blocks could be mined per second. Therefore, the scenarios of different attacks are based on the rational

Algorithm 1 DCS execution of smart contract

```
for each $smartcontract_i \in [block_i]$ do
    Establish structure of each node:
$< address[account], uint[id], int[f, P, Q, v] >$
    Receive data:
Register nodes $< address, id, [f, P, Q, v] >$;
    Calculation:
Function I: feedback calculation for $Node_1$;
Function II: feedback calculation for $Node_2$;
Function III: feedback calculation for $Node_3$;
Function IV: feedback calculation for $Node_4$;
    Return values to four nodes:
$< address[account], uint[id], int[f, P, Q, v] >$;
    Delete nodes information;
end for;
```

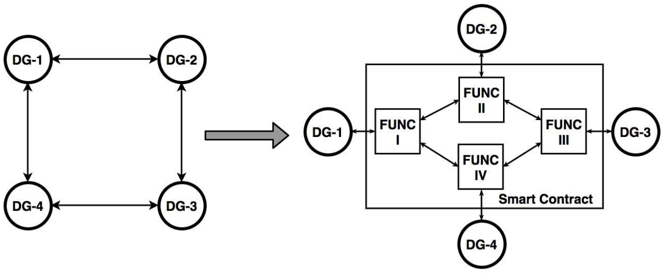


Fig. 4. Transformation of distributed control structure caused by smart contracts deployment

assumption that there are already adequate number of blocks generated and the smart contracts have already been deployed to the blockchain before the execution of the malicious attack. Since the DCS has already been protected by the PoA private blockchain, the attacking scenarios are categorized as three types against the blockchain based DCS process:

- The attacker is outside of the microgrid.
- The attacker is one of the controller nodes or it manages to control one of the controller nodes.
- The attacker aims to overwrite the smart contract.

Furthermore, another problem called Double-feedback Sending (DfS) is also analysed in this section.

A. Attacks Outside Microgrid

Blockchain technology is effective to solve the attacks out of the network. To inject information or overwrite the content of any block of the blockchain maliciously, the attacker needs to decode the hash codes. According to Equation (7), each hash code set is related to that of the other block. Once the content of a block has been changed, its original hash codes becomes invalid. However, the blockchain only recognizes the longest chain and thus, the attacker is required to decode all of the blocks behind the attacked block and meanwhile re-mine a new blockchain whose length and mining speed must overpass those of the original blockchain to legalize his attack.

In addition, in some of the blocks, the data has been hashed multiple times by the MTMS mechanism illustrated in Fig. 3. The attacker needs to decode at least one branch of the merkle tree successfully to get only part of the DCS measurements. This enormous workload for attackers outside the microgrid is theoretically impossible to be completed. The energy and gas consumption of this type of attack are quantified in Section V.

B. Attacks Within Microgrid

Unlike other blockchain service in which the identities of validators are anonymous or pseudo-anonymous, the authority nodes (validators) need to confirm their true identities to establish a valid and trustworthy mining environment for the PoA private blockchain. According to the PoA consensus protocol, only the authority nodes are able to pack the DCS measurements, which means the attacker must pre-authenticated to become the authority nodes so that the probability of a successful false data injection could be realised. This requirement exposes the identity of the attacker to the whole network and increases the chances to detect the attacks. If the authority node is unavailable or behaves maliciously, it will be excluded from the list of authority nodes.

In the worst case, if 1) the attacker passes the pre-authentication of the proposed blockchain system and 2) it is able to control $Node1$ controller from the x^{th} DCS process and 3) send false data which is also not detected by the verification process from the other three nodes, it could read the measurements transmitted through the feedback and forward channels and modify them arbitrarily. As all the four DG secondary controllers are assigned as authority nodes, the role matrix of the microgrid is defined as:

$$A^T = \begin{bmatrix} A_1 & A_2 & A_3 & A_4 \end{bmatrix} \tag{9}$$

During each DCS process, the input of the attacker $Node_1$ is defined as:

$$I_1^T = \begin{bmatrix} M_1 & M_2 & 0 & M_4 \end{bmatrix} \tag{10}$$

where M_i is the input from the $Node_i$ controller.

After receiving the input, the attacker overwrites the elements of the input to achieve a false calculation result of the smart contract as:

$$U_{ow1} = K[(M^* - M_{f1}) + (M_{f2} - M_{f1}) + (M_{f3} - M_{f1})] \tag{11}$$

$$U_{ow1} = U + \alpha_{ow1} \tag{12}$$

where M_{fi} is the element that probably be modified by the attacker and α_{ow1} refers to the deviation between thr corrected U and the false U_{ow1}.

Then, for the DCS process of $Node_2$ controller, the input received by it could be defined as:

$$I_2^T = \begin{bmatrix} M_{f1} & M_2 & M_3 & 0 \end{bmatrix} \tag{13}$$

where M_{f1} is the false input from $Node_1$ controller.

Its feedback value U_2 is also influenced by the false M_{f1} injection as:

$$U_{ow2} = K[(M^* - M_2) + (M_{f1} - M_2) + (M_3 - M_2)] \tag{14}$$

The false feedback provided by the attacker $Node_1$ will progressively influence the inputs for all the other controller nodes as well as that of the next DCS process which are shown in Equation (15) and (16) respectively.

$$I(x) = \begin{bmatrix} M_1 & M_{f1} & 0 & M_{f1} \\ M_2 & M_2 & M_{f2} & 0 \\ 0 & M_3 & M_3 & M_{f3} \\ M_4 & 0 & M_4 & M_4 \end{bmatrix} \tag{15}$$

$$I(x+1) = \begin{bmatrix} M_{f1} & M_{f1} & 0 & M_{f1} \\ M_{f2} & M_{f2} & M_{f2} & 0 \\ 0 & M_3 & M_{f3} & M_{f3} \\ M_{f4} & 0 & M_{f4} & M_{f4} \end{bmatrix} \tag{16}$$

According to Equation (16), all the input measurements are false data which are injected into the DCS, and once the system becomes unstable, the proposal for re-selection of authority nodes will be raised. As all of the nodes are unwilling to be excluded from the authority nodes listthe input matrix will be traced and verified by them and after the voting mechanism provided by PoA consensus protocol, the new agreement is the achieved by removing the attacker $Node1$ from the authority nodes list as:

$$A = \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ A_2 \\ A_3 \\ A_4 \end{bmatrix} \tag{17}$$

where 0 refers to false and 1 refers to true.

After the removal of $Node_1$ from the authority nodes list, the attacker node becomes a common node who has no access to the DCS measurements. The opportunity for the attacker, with no access to the DCS data, to attack the proposed blockchain based DCS is introduced in Section IV.A.

C. Attacks against Smart Contracts

In the blockchain system, the procedures of smart contracts deployment are similar to the mining mechanism for transactions. The authority nodes mine the smart contract to the blockchain which means the smart contracts are also protected by hash functions. After being deployed to the blockchain system, the method to overwrite the content of the smart contracts equals to the attacking scenarios introduced in Section IV.A, which requires enormous energy and gas consumption. Before the deployment, only the owner of the private blockchain could change the content of the smart contracts. Adversely, all the nodes within the microgrid are not allowed to modify smart contracts, including the authority nodes.

D. Other Possible Attacking Scenarios

Another attack against the PoA blockchain based DCS is DfS. The rationale of DfS is similar to the mechanism of double-spending problem. In this scenario, the malicious node within the microgrid sends multiple different input values to other nodes in a DCS process. If these false inputs are not sent simultaneously, only the firstly sent input would be confirmed for the blockchain system and then verified to the subsequent block but the other inputs will be recognized as invalid. If these different false data inputs are sent simultaneously, the input with highest number of confirmations verified by the other nodes is selected to be mined and the other inputs will be discarded. In both conditions, the malicious node cannot escape from the removal of its authority role because the false input will be detected by using the solution introduced in Section IV.B.

Regardless of the advantages mentioned in Section III, this section shows the tolerance to malicious nodes of the proposed PoA blockchain based DCS, as long as 2/3 of the nodes are not compromised. Overall, the proposed PoA private blockchain is able to guarantee the DCS's integrity and reliability.

V. Case Study

In this section, the simulation of the control system is performed in RT-LAB and MATLAB software. The simulation model of the four-DG islanded microgrid is established and shown in Fig. 5 and Table II shows the electrical and control parameters for the microgrid.

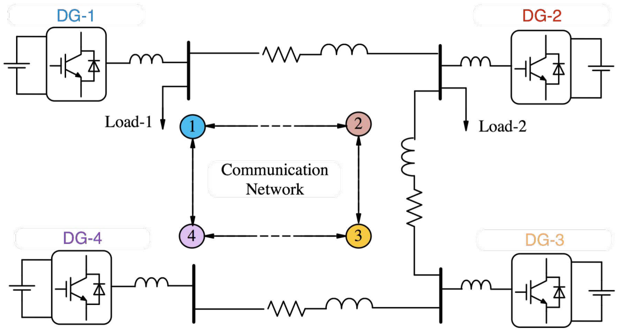


Fig. 5. Microgrid simulation model

TABLE II
Parameters of DCS

Parameter	Value
Line Impedance (1,2)	R_{12}=0.8 Ω, $L_{12} = 3.6mH$
Line Impedance (2,3)	R_{23}=0.4 Ω, $L_{23} = 1.8mH$
Line Impedance (3,4)	R_{34}=0.7 Ω, $L_{12} = 1.7mH$
$Load_1$	P_1= 18 kW, Q_1= 6 kVar
$load_2$	P_2= 12 kW, Q_2= 4 kVar
Reference Value	w^*= 50 Hz, V^*= $230\sqrt{2}V$
DG Impedance	R= 0.1 Ω, $L = 4.8mH$
$DG_{1,2}$ Capacity	$k_P = 2e^{-4}$, $k_Q = 4e^{-3}$
$DG_{3,4}$ Capacity	$k_P = e^{-4}$, $k_Q = 2e^{-3}$

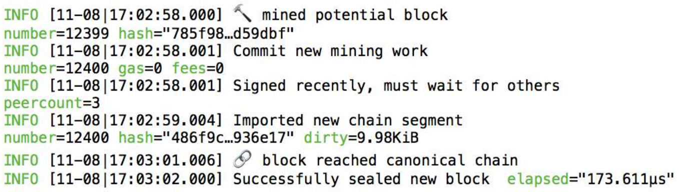
A. Blockchain Implementation

The hardware and software used for the blockchain setup is clarified in Table III.

TABLE III
Instruments information for blockchain setup

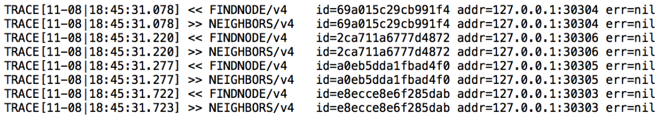
Name	Version
Geth	1.10.6
Node.js	6.14.6
Truffle.js	5.1.49
Web3.py	5.12.0
Solidity smart contracts	>= 0.4.22 < 0.7.0
Raspberry Pi	4 Model B
RT-LAB	11.3.1.34

The communication within the microgrid is supported by the *Bootnode* service. The interval time of each block production is controlled from 101.203µs to 451.487µs. The mining process of the proposed blockchain is shown in Fig. 6 and the nodes communication channel as well as the smart contracts deployment are shown in Fig. 7 and Fig. 8 respectively.



```
INFO [11-08|17:02:58.000] 🔨 mined potential block
number=12399 hash="785f98…d59dbf"
INFO [11-08|17:02:58.001] Commit new mining work
number=12400 gas=0 fees=0
INFO [11-08|17:02:58.001] Signed recently, must wait for others
peercount=3
INFO [11-08|17:02:59.004] Imported new chain segment
number=12400 hash="486f9c…936e17" dirty=9.98KiB
INFO [11-08|17:03:01.006] 🔗 block reached canonical chain
INFO [11-08|17:03:02.000] Successfully sealed new block  elapsed="173.611µs"
```

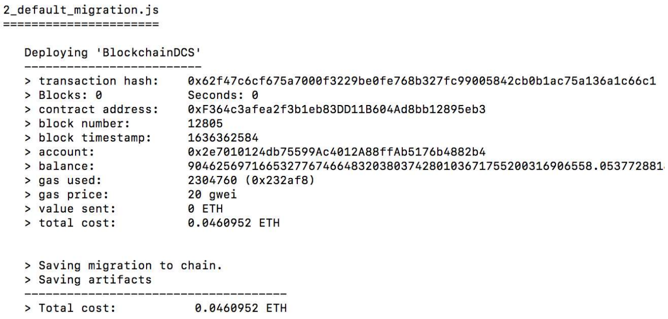
Fig. 6. Mining process of the PoA blockchain



```
TRACE[11-08|18:45:31.078] << FINDNODE/v4    id=69a015c29cb991f4 addr=127.0.0.1:30304 err=nil
TRACE[11-08|18:45:31.078] >> NEIGHBORS/v4   id=69a015c29cb991f4 addr=127.0.0.1:30304 err=nil
TRACE[11-08|18:45:31.220] << FINDNODE/v4    id=2ca711a6777d4872 addr=127.0.0.1:30306 err=nil
TRACE[11-08|18:45:31.220] >> NEIGHBORS/v4   id=2ca711a6777d4872 addr=127.0.0.1:30306 err=nil
TRACE[11-08|18:45:31.277] << FINDNODE/v4    id=a0eb5dda1fbad4f0 addr=127.0.0.1:30305 err=nil
TRACE[11-08|18:45:31.277] >> NEIGHBORS/v4   id=a0eb5dda1fbad4f0 addr=127.0.0.1:30305 err=nil
TRACE[11-08|18:45:31.722] << FINDNODE/v4    id=e8ecce8e6f285dab addr=127.0.0.1:30303 err=nil
TRACE[11-08|18:45:31.723] >> NEIGHBORS/v4   id=e8ecce8e6f285dab addr=127.0.0.1:30303 err=nil
```

Fig. 7. Communication channel service for the blockchain network supported by Bootnode

Fig. 6 shows the mining process of one block, including the block number, block size, hash codes and production time. According to Fig. 7, the blockchain is mined by the four authority nodes in rotation, in which 30303 to 30306 are the respective communication channels of the four controller nodes. Shown in Fig. 8, the smart contract for DCS calculation is deployed to the blockchain. In addition, the information



```
2_default_migration.js
======================

   Deploying 'BlockchainDCS'
   -------------------------
   > transaction hash:    0x62f47c6cf675a7000f3229be0fe768b327fc99005842cb0b1ac75a136a1c66c1
   > Blocks: 0            Seconds: 0
   > contract address:    0xF364c3afea2f3b1eb83DD11B604Ad8bb12895eb3
   > block number:        12805
   > block timestamp:     1636362584
   > account:             0x2e7010124db75599Ac4012A88ffAb5176b4882b4
   > balance:             904625697166532776746648320380374280103671755200316906558.053772881
   > gas used:            2304760 (0x232af8)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.0460952 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.0460952 ETH
```

Fig. 8. Deployment interface of Smart contract achieved by Truffle.js

of the smart contracts address, miner address and the gas costs of the deployment are also demonstrated. These types of information are valuable as they are used in $Web3.py$ based scripts to realize the function offered by smart contracts.

B. Results of Blockchain based DCS

The frequency regulation results of DCS with and without the implementation of the proposed PoA blockchain are compared in Fig. 9, according to which the control result of the blockchain based DCS (B-DCS) is synchronized to that of the DCS. In Fig. 9, P1-P4 and f1-f4 are the respective active power and frequency of the four DG controllers.

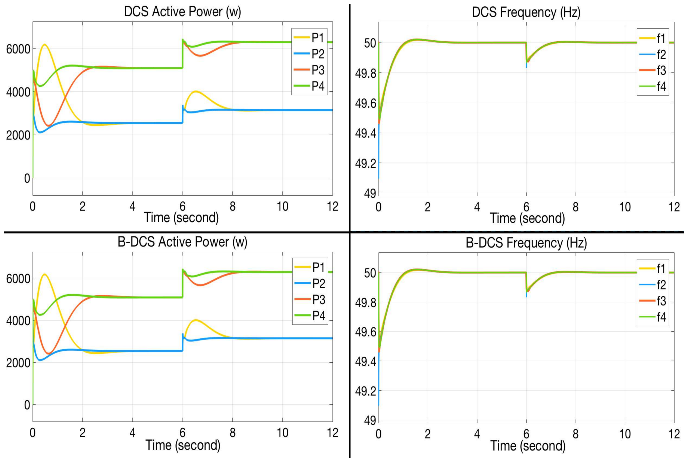


Fig. 9. Control results of the four-DG microgrid without blockchain (DCS) and with blockchain (B-DCS) implementation.

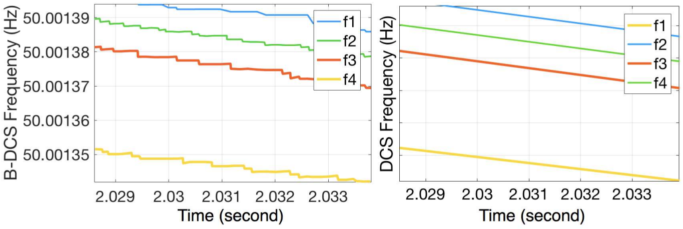


Fig. 10. Frequency regulation of B-DCS and DCS based microgrid (f1-f4 are the frequency of the four DG controllers)

However, there is still a slight difference between the control results of DCS and B-DCS when enlarging the frequency result from Fig. 9 to Fig. 10. The reason for this difference is because multiple sampling processes of DCS are mined in each block, which slightly delays feedback sent to the DCS controllers. The number of the processes mined in each block is positively proportional to the duration of the latency caused. Therefore, the interval time of each block production is required to be constrained in a predictable scope. The number of DCS processes mined in each block in this study is shown Fig. 11 (d).

The comparison shown in Fig. 9 proves that the proposed PoA blockchain for the DCS would not negatively influence the DCS when it is implemented. Therefore, the quality of the control process is ensured. For the attack outside the microgrid, Fig. 11 presents the energy and gas consumption as well as the re-mining rate of the attacker compared with the original blockchain operation, where the $Decoding$ and $Re-mining$ refers to the malicious attack and $Mining$ refers to the proposed blockchain operation. Additionally, the number of DCS processes mined in each block of the proposed blockchain is also shown.

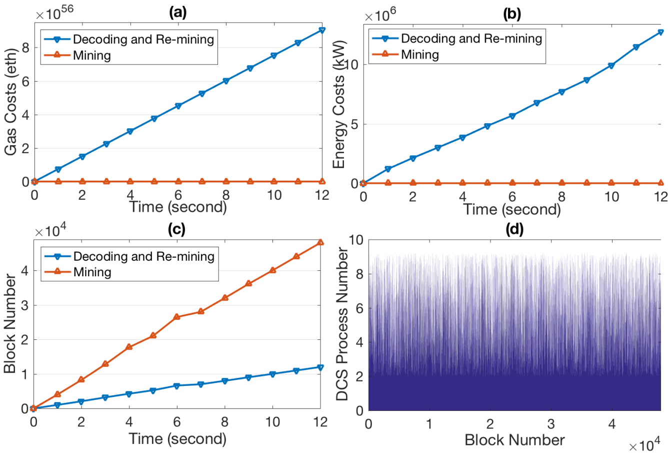
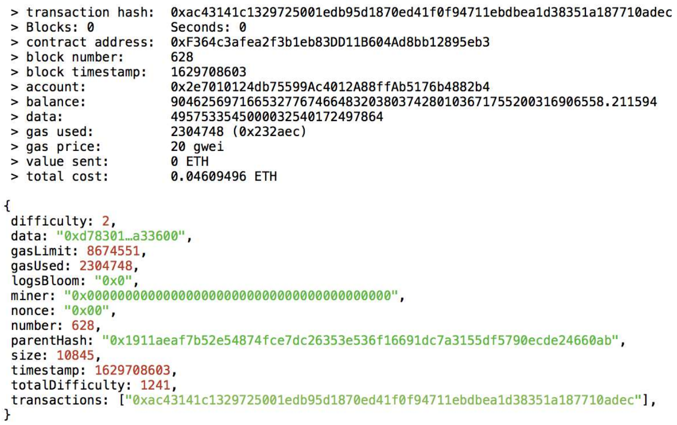


Fig. 11. The comparison of (a) gas costs, (b) energy consumption and (c) mining rate between the attacker and the authority nodes. (d) the number of DCS processes mined in each block.

Depending on Fig. 11 (a), (b) and (c), the extremely huge amount of gas and energy consumption required for a malicious attack is unaffordable for the attackers. More desperately, the existing fast mining rate of the proposed private blockchain is also difficult to surpass. According to Fig. 11 (d), 480,027 blocks are totally mined during the 12 seconds and the number of DCS processes mined in each block is restrained below 10.

For the attacker within the microgrid, once it has been detected by the proposed blockchain system, it is excluded from the authority nodes list and it loses the data access of mining blocks. In this case study, $Node_1$ is set as a malicious node and it has been detected after 627 blocks (0.157 seconds) were mined. Therefore, $Node_1$ cannot check the data for the rest of the blockchain since it is defined as a common node. Fig. 12 demonstrates the practical content of block No. 628 (at the top, black) compared to the content that a common node could check (at the bottom, green).

According to the green content presented in the bottom of Fig. 12, the common node is forbidden to check the DCS data but only able to check the hash codes and mining difficulty. The valuable data is replaced by $0xd783...0$ in the block



```
> transaction hash:  0xac43141c1329725001edb95d1870ed41f0f94711ebdbea1d38351a187710adec
> Blocks: 0          Seconds: 0
> contract address:  0xF364c3afea2f3b1eb83DD11B604Ad8bb12895eb3
> block number:      628
> block timestamp:   1629708603
> account:           0x2e7010124db75599Ac4012A88ffAb5176b4882b4
> balance:           904625697166532776746648320380374280103671755200316906558.211594
> data:              4957533545000032540172497864
> gas used:          2304748 (0x232aec)
> gas price:         20 gwei
> value sent:        0 ETH
> total cost:        0.04609496 ETH
```

```
{
 difficulty: 2,
 data: "0xd78301…a33600",
 gasLimit: 8674551,
 gasUsed: 2304748,
 logsBloom: "0x0",
 miner: "0x0000000000000000000000000000000000000000",
 nonce: "0x00",
 number: 628,
 parentHash: "0x1911aeaf7b52e54874fce7dc26353e536f16691dc7a3155df5790ecde24660ab",
 size: 10845,
 timestamp: 1629708603,
 totalDifficulty: 1241,
 transactions: ["0xac43141c1329725001edb95d1870ed41f0f94711ebdbea1d38351a187710adec"],
}
```

Fig. 12. The respective DCS data that could be checked by authority nodes (upper) and common nodes (bottom).

structure and thus the DCS is secured. The actual valuable information is presented at the upper part of Fig. 12, including the smart contract address, the miner account as well as its balance and the DCS data, in which the input measurements are $< 49.5753Hz, 3454w, 325.4017V, 249.7864Val >$. Because the input and output of smart contracts can only be presented in integers, the DCS data is covered in $data$: $4957533545000032540172497864$.

Based on the results of the case study, the proposed PoA private blockchain based DCS is effective to defend the control system against all of the mentioned attacking scenarios. It provides no opportunity for the attackers outside the network while reducing the risks of selecting questionable authority nodes and incentivizing a long-term commitment.

VI. Discussion

In this paper, the proposed PoA blockchain is utilized to secure each control process of DCS and smart contracts are written to calculate the feedback for each input instead of transaction execution. The results of the case study prove the effectiveness and feasibility of the proposed method. In other words, this study shows the potential of applying blockchain into securing technical operations in power system domain in addition to its usage for P2P energy trading. The distributed structure features for both DCS and blockchain are combined perfectly and the operation of DCS is secured by the PoA private blockchain without any negative performance. Although, the control results presented by the proposed method is slightly different to those without blockchain implementation, it could be addressed by increasing the mining rate to match each sampling time if more advanced facilities could be used according to [24]. The proposed method is also efficient in energy consumption. As a private chain requires neither high-performance hardware nor high mining difficulty value for operation, the mining rate is fast but predictable with low energy and gas consumption.

Unlike other types of blockchain services that pseudo-anonymity or anonymity is used to hide customers' privacy, the PoA consensus protocol requires real identities from the authority nodes. This feature coincidentally becomes an advantage when it is applied in the DCS as it reduces the risks of selecting malicious authority nodes. In PoA consensus protocol, the roles of nodes are not constant. Each node could earn the reputation from the microgrid to pass the pre-authentication or could be excluded from the authority nodes list due to its illegal behaviours. In addition, it also provides a flexible mining environment for the microgrid network because the performance parameters could be adjusted according to the specific DCS requirement, including the upper limits of block number mined, the value of mining difficulty and gas price.

VII. Conclusion

In conclusion, this paper proposed PoA private blockchain based DCS for a four-DG islanded microgrid, which breaks through the bottleneck of blockchain applications in the power system domain. The process of DCS is presented for the frequency regulation and the blockchain is set up based on Ethereum platform. The fast mining rate and low energy consumption of the proposed private blockchain match each DCS process efficiently. Various attacking scenarios against the proposed model are analyzed and the designed blockchain model provides corresponding solutions in each scenario and thereby becoming a solid tool for safeguarding the DCS. In the case study section, the blockchain implementation and smart contracts creation for the four-DG islanded microgrid is specifically demonstrated. Four Raspberry Pi 4Bs are used for the node communication of the four secondary controllers. Numerical results prove the effectiveness and feasibility of the proposed method as it is able to secure the DCS while maintaining the quality of the control process.

The extension work would be expanding the microgrid size and testing the performance of the proposed PoA blockchain. Since the malicious node needs to control at least 2/3 of the nodes within the microgrid to achieve a successful attack, a larger microgrid size with more DG units and secondary controllers could theoretically provide a more resilient network structure against various cyber-attacks.

References

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

[2] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—attacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, 2017.

[3] Z.-H. Pang, G.-P. Liu, D. Zhou, F. Hou, and D. Sun, "Two-channel false data injection attacks against output tracking control of networked systems," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 5, pp. 3242–3251, 2016.

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

[5] S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, and A. Joshi, "Joint-transformation-based detection of false data injection attacks in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 1, pp. 89–97, 2018.

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

[7] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271–3280, 2018.

[8] B. Tang, J. Yan, S. Kay, and H. He, "Detection of false data injection attacks in smart grid under colored gaussian noise," in *2016 IEEE Conference on Communications and Network Security (CNS)*, 2016, pp. 172–179.

[9] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *2012 IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 3153–3158.

[10] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.

[11] J. Yang, A. Paudel, and H. B. Gooi, "Compensation for power loss by a proof-of-stake consortium blockchain microgrid," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3253–3262, 2021.

[12] Y. Jiang, K. Zhou, X. Lu, and S. Yang, "Electricity trading pricing among prosumers with game theory-based model in energy blockchain environment," *Applied Energy*, vol. 271, p. 115239, 2020.

[13] S. Zhang, M. Pu, B. Wang, and B. Dong, "A privacy protection scheme of microgrid direct electricity transaction based on consortium blockchain and continuous double auction," *IEEE Access*, vol. 7, pp. 151 746–151 753, 2019.

[14] F. Guo, C. Wen, J. Mao, and Y.-D. Song, "Distributed secondary voltage and frequency restoration control of droop-controlled inverter-based microgrids," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 7, pp. 4355–4364, 2015.

[15] Z. Li, C. Zang, P. Zeng, H. Yu, and S. Li, "Fully distributed hierarchical control of parallel grid-supporting inverters in islanded ac microgrids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 679–690, 2018.

[16] D. Han, Y. Zhu, D. Li, W. Liang, A. Souri, and K.-C. Li, "A blockchain-based auditable access control system for private data in service-centric iot environments," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2021.

[17] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in iot-enabled smart-grid system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744–5761, 2021.

[18] K. T. Seow, "Supervisory control of blockchain networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 159–171, 2020.

[19] Z. Li, J. Hao, J. Liu, H. Wang, and M. Xian, "An iot-applicable access control model under double-layer blockchain," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 6, pp. 2102–2106, 2021.

[20] J. J. Mendoza and F. Núñez, "Blockchain-driven on-demand control loops over iot environments," *IEEE Access*, vol. 7, pp. 157 524–157 534, 2019.

[21] A. Stanciu, "Blockchain based distributed control system for edge computing," in *2017 21st International Conference on Control Systems and Computer Science (CSCS)*. IEEE, 2017, pp. 667–671.

[22] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 11, pp. 7025–7038, 2015.

[23] M. A. Shahab, B. Mozafari, S. Soleymani, N. M. Dehkordi, H. M. Shourkaei, and J. M. Guerrero, "Distributed consensus-based fault tolerant control of islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 37–47, 2020.

[24] C. Gorenflo, S. Lee, L. Golab, and S. Keshav, "Fastfabric: Scaling hyperledger fabric to 20 000 transactions per second," *International Journal of Network Management*, vol. 30, no. 5, p. e2099, 2020.

[25] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[26] M. Valenta and P. Sandner, "Comparison of ethereum, hyperledger fabric and corda," *ebook] Frankfurt School, Blockchain Center*, 2017.

[27] C. Dufour, S. Abourida, and J. Belanger, "Hardware-in-the-loop simulation of power drives with rt-lab," in *2005 International conference on power electronics and drives systems*, vol. 2. IEEE, 2005, pp. 1646–1651.

Jiawei Yang (Member, IEEE) received the B.E. degree in electrical engineering and automation from Wuhan University, China in 2018 and the M.E. degree in electrical and electronic engineering from Nanyang Technological University, Singapore in 2020. He is currently working as a Ph.D. candidate in electrical engineering at Nanyang Technological University, Singapore. His current research interest includes peer-to-peer energy trading and blockchain application in power system.

Jiahong Dai (Student Member, IEEE) received his B.Eng. degree in Smart Grid Information Engineering from Hefei University of Technology, China, in 2017. He is currently working toward the Ph.D. degree with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include communication system in smart grids, simulation and validation of cyber-physical systems and cybersecurity of microgrids.

Hoay Beng Gooi (Life Senior Member, IEEE) received the B.S. degree from National Taiwan University in 1978; the M.S. degree from University of New Brunswick in 1980; and the Ph.D. degree from Ohio State University in 1983, all in electrical engineering. He is an associate professor at School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His current research interests include microgrid energy management systems dealing with storage, electricity market, and spinning reserve.

Hung Dinh Nguyen (Member, IEEE) received the Ph.D. degree in electric power engineering from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2017. He is a 2017 Siebel Scholar in energy science. Currently, he is an Assistant Professor in Electrical and Electronic Engineering at Nanyang Technological University, Singapore. His research interests include power system operation and control with machine learning, the nonlinearity, dynamics and stability of large scale power systems; dynamic security assessment (DSA)/energy management system (EMS) and smart grids.

Amrit Paudel (Member, IEEE) received the B.E. degree in electrical and electronic engineering from Pokhara University, Nepal, in 2012, the M.E. degree in energy engineering from the Asian Institute of Technology, Bangkok, Thailand, in 2016, and the Ph.D. degree in electrical and electronic engineering from Nanyang Technological University, Singapore, in 2020. He is a recipient of the Singapore International Graduate Award (SINGA). He is currently a Postdoctoral Associate in the Schulich School of Engineering, Department of Electrical and Software Engineering at the University of Calgary, Canada. His current research interests include cyber-physical power systems, transactive energy systems, peer-to-peer (P2P) energy trading, distribution level electricity market, blockchain applications in power systems, and electrified transportation systems.