Decentralized Consensus Decision-Making for Cybersecurity Protection in Multimicrogrid Systems

Bowen Hu, Chunjie Zhou, Yu-Chu Tian, *Senior Member, IEEE*,
Xiaoya Hu, *Senior Member, IEEE*, and Xinjue Junping

***Abstract*—Multimicrogrid (MMG) systems play an increasingly important role in the smart grid. They come with various potential cyberattacks, which may cause power supply interruption or even human casualties. Therefore, decision-making for timely mitigation of cyberattack risks is highly desirable in the security protection of power systems. However, there is a lack of effective decentralized decision-making strategies that are able to deal with MMG scenarios through distributed consensus. To address this issue, a decentralized consensus decision-making (DCDM) approach is proposed in this article for the security of MMG systems. It achieves decentralized consensus without the need of a trusted authority or central server, making it distinct from existing consensus methods. Meanwhile, it guarantees the consistency and nonrepudiability of consensus results, which are stored on the blockchain in sequence. In each of the distributed agents, the approach consists of a fuzzy static Bayesian game model (FSB-GM) to determine the optimal security strategy and a hybrid consensus algorithm to achieve consensus. The FSB-GM considers the fuzzy preferences of different types of attackers and defenders. The hybrid consensus algorithm is implemented by the fusion improvement of two consensus mechanisms in the blockchain. The effectiveness of the presented approach is demonstrated through a case study on an MMG system.**

***Index Terms*—Blockchain, cybersecurity, Decentralized consensus decision-making (DCDM), fuzzy static Bayesian game model (FSB-GM), multimicrogrid (MMG).**

Manuscript received November 29, 2019; revised June 9, 2020; accepted August 15, 2020. Date of publication September 17, 2020; date of current version March 17, 2021. The work of Chunjie Zhou was supported in part by the National Natural Science Foundation of China under Grant 61873103 and Grant 61433006; and in part by the National Key Research and Development Program of China under Grant 2019YFB2006300. The work of Yu-Chu Tian was supported by the Australian Research Council through the Discovery Project Scheme under Grant DP170103305. This article was recommended by Associate Editor Y.-J. Liu. *(Corresponding author: Chunjie Zhou.)*

Bowen Hu, Chunjie Zhou, and Xiaoya Hu are with the Key Laboratory of Image Processing and Intelligent Control, Ministry of Education, School of Artificial Intelligence and Automation, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: hubowen@hust.edu.cn; cjiezhou@hust.edu.cn; huxy@hust.edu.cn).

Yu-Chu Tian is with the School of Computer Science, Queensland University of Technology, Brisbane, QLD 4001, Australia (e-mail: y.tian@qut.edu.au).

Xinjue Junping is with the School of China-EU Institute for Clean and Renewable Energy, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: jpxj95@hust.edu.cn).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSMC.2020.3019272

I. Introduction

With the integration of renewable energy sources, modern power systems show significant increases in both size and complexity. As a result, centralized management of power systems becomes more difficult and less flexible. It is also exposed in an environment with a potential single-point of failure (SPoF). The massive deployment of distributed renewable energy generation under distributed control is transforming conventional power systems into multimicrogrid (MMG) systems [1], [2]. MMG systems can be operated in either grid-connected or islanded modes [3], [4]. A typical mesh type of MMG structure is shown in Fig. 1.

However, MMG systems suffer from various cyberattacks. A cyberattack to power systems has caused the Ukraine blackout in 2015, plunging approximately 225 000 customers into darkness. Therefore, ensuring the security of MMG systems is an issue of great significance.

Due to the tight integration of both cyber and physical components in MMG systems [5], a failure of the cyber layer may affect the operation of the physical layer. This may further lead to a cascade of blackout catastrophe. Hence, it is important to develop an appropriate security strategy for timely mitigation of cyberattack risks [6]. Among multiple distributed agents of MMG systems, decision-making through consensus is a feasible way for cybersecurity protection of MMG systems. While consensus decision-making (CDM) can be either centralized [7] or decentralized [8], decentralized methods are more suitable for MMG systems because of the advantages of flexibility, scalability, and robustness [9]. Meanwhile, decentralized methods would not crop up problems, such as calculation bottleneck or SPoF in centralized methods. Encouraged by these recommendations, the researchers have focused on decentralized control approaches for multiagent systems [10]–[12].

Recently, decentralized consensus has been investigated [13]. A fully distributed peer-to-peer architecture, Overgrid, is designed to control and implement distributed demand response [14]. A fully distributed scheduling methodology is also proposed based on discrete-time optimal control and consensus networks [15], to alleviate the need of a central node. Nevertheless, focusing more on strategic coordination in consensus, these methods have not considered the credibility and trust of distributed nodes. The survey [16] also points out that the reliability and accuracy of each response action is highly demand, more so in the absence of a centralized trusted authority.

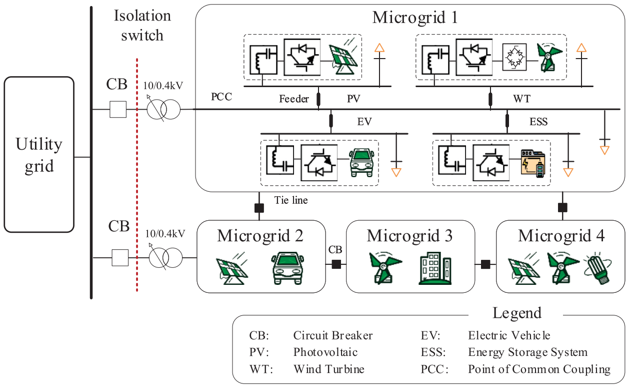


Fig. 1. Typical structure of MMG system.

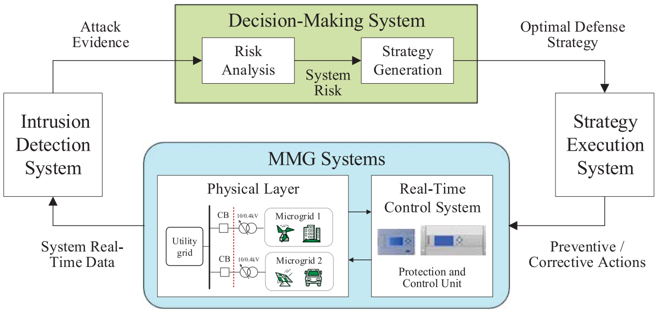


Fig. 2. Cybersecurity protection architecture for MMG.

Some efforts have been made to address the problem of the reliability of each response action. For example, the credentials of the participant are either generated by using a central certification authority (CA) or certified among peers [17]. Each agent associates a trust metric to each of its neighbors. The trust metrics are taken into account in the filtering scheme. Therefore, the information transmitted from agents with low trust is disregarded [18]. In spite of these efforts, most existing methods use a central CA or trust mechanism among peers to guarantee the security countermeasures generated from a trusted participant. However, the trust mechanism tends to fall into the favor of high-reputation agents. Furthermore, a central CA is easy to become a bottleneck in computing and storage capacity as the number of participants increases.

Motivated by the results mentioned above, a decentralized CDM (DCDM) approach is proposed in this article for cybersecurity protection in MMG systems. Addressing various deficiencies of centralized methods, such as SPoF, it deals with the scenarios in which distributed nodes are attacked or untrustworthy. As a result, it ensures the reliability and immutability of decision results. In the DCDM approach, a fuzzy static Bayesian game model (FSB-GM) is designed to obtain the optimal security strategy in each of the distributed agents. It considers probabilistic variables and approximate values in realistic games. Employing the obtained security strategies, CDM is achieved based on a hybrid consensus mechanism derived from a blockchain. Then, the final consensus countermeasures are stored on each block in sequence.

Overall, the main contributions of this article include as follows.

1) Without the need of a trusted authority or central server, a DCDM approach is proposed for cybersecurity protection in MMG systems. It avoids SPoF problem of centralized methods, and guarantees the consistency and nonrepudiability of consensus results at the same time.
2) As part of the approach, an FSB-GM is designed to enhance the accuracy of decision-making in distributed agents. It considers the fuzzy preferences of different types of attackers and defenders when estimating the payoff matrix.
3) A hybrid algorithm of delegated proof of stake (DPoS) and proof of work (PoW) mechanisms in the blockchain is devised for consensus on the distributed decision results. It increases the transaction rate and overcomes the defect of one single richest member.

The remainder of this article is organized as follows. Section II reviews related work on cybersecurity protection architecture, fuzzy Bayesian game theory, and decentralized consensus mechanisms in blockchain. Section III designs our DCDM approach. The generation of a security strategy based on FSB-GM is analyzed in Section IV. This is followed by discussions on our consensus algorithm using blockchain in Section V. Experiments are conducted in Section VI to demonstrate our approach. Finally, Section VII concludes this article.

II. Background and Related Work

A. Cybersecurity Protection Architecture for MMG

The architecture of cybersecurity protection is shown in Fig. 2. It consists of four components: 1) MMG systems; 2) intrusion detection system; 3) decision-making system; and 4) strategy execution system. These four components altogether form an intrusion tolerance scheme with a closed loop [19]. The main idea of the architecture is to protect MMG systems in advance from being compromised.

First, various real-time data in cyber and physical layers are collected for basic security analysis and deep intrusion detection. Then, from the detected attack evidence, system risk is assessed and the optimal defense strategy is obtained to gain an acceptable risk for maintaining or regain operational status. After that, the optimal defense strategy is fed into the strategy execution system. It will be interpreted as a group of preventive or corrective actions to protect the system, perhaps at a degraded level of performance, stability, or security. Our decision-making strategy proposed in this article is able to deal with MMG scenarios through distributed consensus, which can be implemented in a decentralized system.

B. Fuzzy Bayesian Game Theory

Recently, most of the existing game-theoretic decision-making methods adopt a complete and crisp information game model [20], [21]. However, the stringent and unrealistic assumption [19] can not handle the ambiguity properly in real life games. To address the issue where the payoffs are probabilistic variables or approximate values, two types of game models are suitable [22].

The first type of game model is the Bayesian game. It is able to deal with the situation where both attacker and defender are not aware of each other's behavior. More specifically, the model classifies the types of players first. Each player only knows the probability of each type of opponent. Recently, a number of articles have been published on the incomplete information version of game theory [23]. With consideration of the uncertainty of attack behaviors, a security decision-making approach based on the stochastic game model is proposed in [24].

The second type of game model is fuzzy game. Because the vagueness of human judgment and uncertainty of objective things are still hard to characterize in many situations, there are mainly two types of fuzziness in games: 1) fuzzy preferences or strategies of players and 2) fuzzy evaluation of the payoffs [25]. Since the fuzzy set theory has been proposed, it has been well developed and applied in the problem of approximation. A noncooperative game model is developed in [26], where both payoffs and strategies of players are considered as fuzzy sets.

Thus, in order to estimate the payoff matrix accurately in Bayesian game, the types and fuzzy preferences of attackers and defenders are worthy to be considered.

C. Decentralized Consensus Mechanism in Blockchain

First of all, the entire MMG is divided into several regions with consideration of logical and physical connections so as to achieve decentralized consensus of security strategies [27]. There are overlapping areas between these partitions, i.e., redundancy between the divided regions. The overlapping areas can be used for mutual authentication to achieve consensus and enhance system security.

It is ingenious that the blockchain technology derived from Bitcoin [28] has raised the idea of decentralization to an unprecedented height [29]. Blockchains and smart contracts have been used for providing transaction security in decentralized smart grid energy trading [30]. Furthermore, with the blockchain technology, an architectural design for decentralized management of energy systems is presented in [31]. However, it does not depict process and implementation plan clearly.

Analogous to the fact that new block can be obtained by the behavior of mining in Bitcoin, the consensus of security strategies can also be reached by each microgrid region (MR). In order to verify the information added to the ledgers, the consensus mechanisms are widely used in cryptocurrency [32]. They can be classified into three classes: 1) PoW; 2) proof of stake (PoS); and 3) DPoS [33]. A comparison of these three classes is shown in Table I. As the earliest consensus mechanism in Bitcoin, PoW is highly decentralized, but requires a longer time to reach consensus. In contrast, the transaction rate of DPoS is relatively high. The advent of consensus mechanisms of blockchain provides a solution to the classic consistency problem of distributed systems. The problem is known as the Byzantine Generals Problem.

TABLE I
COMPARISON OF THE THREE CLASSES OF CONSENSUS MECHANISMS

	PoW	**PoS**	**DPoS**
Energy Consumption	High	Low	Very Low
Transaction Rate	Very Low	Low	High
Decentralization	High	High	Low
Application	Bitcoin [28]	Dash	EOS [34]

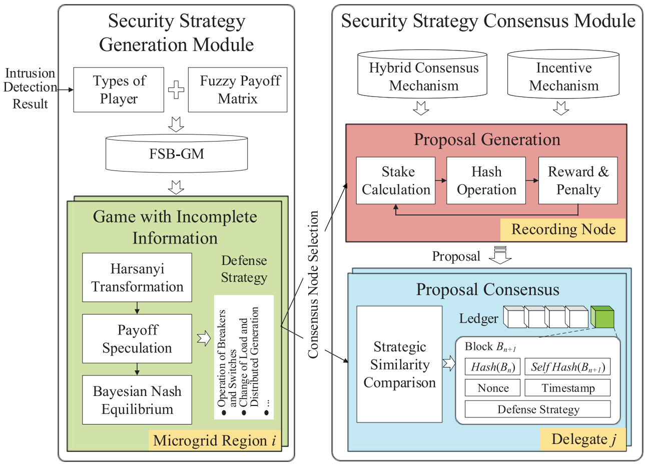


Fig. 3. Design of DCDM in MMG.

In summary, the fitness of the blockchain and decentralized system has motivated us to investigate the consensus mechanism for CDM, which addresses the problem of security and credibility in the data transmission process. Its performance can be improved by integrating the consensus mechanisms in the blockchain.

III. DESIGN OF DCDM

Our game-theoretic DCDM approach based on blockchain technology is shown in Fig. 3. The DCDM process consists of two stages in each of the distributed agent: 1) FSB-GM-based security strategy generation and 2) security strategy consensus by using a hybrid consensus mechanism in blockchain. Their functions are described below in detail.

In security strategy generation, each MR generates its optimal defense strategy independently according to its own information. From the type and fuzzy preference of attackers and defenders, the fuzzy payoff matrix is estimated and mapped into an FSB-GM. In order to solve the problem of the static game with incomplete information, the Harsanyi transformation is used to infer the Bayesian Nash equilibrium, i.e., mixed security strategy.

The security strategy consensus module realizes the consensus of decentralized security decision-making among MMGs. First, an improved hybrid algorithm based on DPoS and PoW is proposed for selecting the recording node and generating proposal. The content of proposal is the defense strategy seeking for consensus. Then, the node coupled with the recording node becomes the delegates. It judges the rationality and reliability of the proposal according to the comparison of strategic similarity. Finally, consensus-derived strategies are stored on blockchain, i.e., distributed ledger, in sequence to

TABLE II
DEFINITIONS OF GAME PARAMETERS

Parameters	**Description**
Players	$N = \{N^A, N^D\}$.
Attacker's type	$T^A = \{T_1^A, T_2^A, \ldots, T_V^A\}$.
Defender's type	$T^D = \{T_1^D, T_2^D, \ldots, T_W^D\}$.
Attacker's strategy	$S^A = \{S_1^A, S_2^A, \ldots, S_L^A\}$.
Defender's strategy	$S^D = \{S_1^D, S_2^D, \ldots, S_M^D\}$.
Attacker's belief	$P^A : P(T^D \mid T^A) \to [0,1]$.
Defender's belief	$P^D : P(T^A \mid T^D) \to [0,1]$.
Attacker's payoff	$U^A : U^A(S^A, S^D, T^A, T^D) \to \mathbb{R}$.
Defender's payoff	$U^D : U^D(S^A, S^D, T^A, T^D) \to \mathbb{R}$.

ensure its immutability and reliability. In addition, in order to ensure the active involvement of distributed nodes, incentive mechanism-based reward, and penalty are also considered.

IV. FSB-GM-Based Security Strategy Generation

This section solves the security decision-making problem of each MR from the game-theoretic perspective. It begins with an introduction to a two-person static Bayesian game model (SB-GM). Then, a solution to a static game with incomplete information is analyzed, expressing attack-defense game in the realistic process. After that, due to the difficulty of obtaining the precise payoff matrix, the fuzzy payoff is adopted instead of conventional Boolean two-valued logic. It considers three perspectives of strategic cost, system loss, and state stability.

A. Bayesian Game Model

As the impact of attacks is often different from the perspectives of attackers and defenders, a bimatrix game can be designed to solve a nonzero-sum attack-defense game. In a realistic attack-defense game, factors, such as the changes in the operating state and the occurrence of own faults may lead to uncertain results and random effects. Thus, a player may not know exactly the payoffs of the game or the types of their opponents. With consideration of these incomplete information, the classical types of attackers and defenders are improved in this article. Then, a two-person SB-GM $\mathcal{G}$ is formulated as a 9-tuple

$$\mathcal{G} = <N, T^A, T^D, S^A, S^D, P^A, P^D, U^A, U^D> \tag{1}$$

where all game parameters are explained in Table II.

In the SB-GM, N^A is the attacker, and N^D is the defender. The types of attacker (T^A) can be divided into two categories: 1) target-based and 2) benefit-based. The types of defender (T^D) include system loss-based and state stability-based. $P^A : P(T^D|T^A)$ represents the probability judgment on the type of defender T^D when the attacker's type is T^A. P^D represents defender's transcendental beliefs. Due to the different types of participants, their preferences and definitions of payoff (U) are also different. They are determined by $\{S^A, S^D, T^A, T^D\}$.

B. Solution to Static Game With Incomplete Information

In real life games, each player could not accurately grasp the opponent's type, specific strategies, and benefits. To solve this game problem with incomplete information, the Harsanyi transformation [35] is employed to convert this problem into a game with complete but imperfect information. This means that all players and payoffs are known to everyone. But they do not know the types of other players except the probability.

In this case, the defender (N^D) infers the attacker's types (T^A) according to its own particular type (T_j^D) and Bayes' theorem. Then, it develops its strategy (S^D). Corresponding U_{j-lm}^D and $U_{j'-lm}^A$ indicate the payoff of the defender and attacker when defense strategy S_m^D and attack strategy S_l^A are adopted, respectively. They are given by

$$\begin{cases} U_{j-lm}^D = \sum_{i=1}^{V} U^D\Big(S_l^A, S_m^D, T_i^A, T_j^D\Big) P\Big(T_i^A | T_j^D\Big) \\ U_{j'-lm}^A = \sum_{i=1}^{V} U^A\Big(S_l^A, S_m^D, T_i^A, T_j^D\Big) P\Big(T_i^A | T_j^D\Big). \end{cases} \tag{2}$$

Similarly, the universal payoff can also be obtained in the same way, thus forming the final payoff matrix from the perspective of the defender type T_j^D, as shown in (21) below

$$\begin{array}{cc} \begin{array}{cccc} S_1^D & S_2^D & \cdots & S_M^D \end{array} & \\ \begin{pmatrix} \Big(U_{j'-11}^A, U_{j-11}^D\Big) & \Big(U_{j'-12}^A, U_{j-12}^D\Big) & \cdots & \Big(U_{j'-1M}^A, U_{j-1M}^D\Big) \\ \Big(U_{j'-21}^A, U_{j-21}^D\Big) & \Big(U_{j'-22}^A, U_{j-22}^D\Big) & \cdots & \Big(U_{j'-2M}^A, U_{j-2M}^D\Big) \\ \vdots & \vdots & \ddots & \vdots \\ \Big(U_{j'-L1}^A, U_{j-L1}^D\Big) & \Big(U_{j'-L2}^A, U_{j-L2}^D\Big) & \cdots & \Big(U_{j'-LM}^A, U_{j-LM}^D\Big) \end{pmatrix} & \begin{array}{c} S_1^A \\ S_2^A \\ \vdots \\ S_L^A \end{array} \end{array}. \tag{3}$$

Assume that the selected attack strategy $\boldsymbol{p}^A = (p_1^A, p_2^A, \ldots, p_L^A)$ and protection strategy $\boldsymbol{p}^D = (p_1^D, p_2^D, \ldots, p_M^D)$ are mixed strategies. Then, the total payoff of the attacker and defender is defined as

$$\begin{cases} U^A\big(\boldsymbol{p}^A, \boldsymbol{p}^D\big) = \sum_{l=1}^{L} \sum_{m=1}^{M} p_l^A \, p_m^D \, U_{j'-lm}^A \\ U^D\big(\boldsymbol{p}^A, \boldsymbol{p}^D\big) = \sum_{l=1}^{L} \sum_{m=1}^{M} p_l^A \, p_m^D \, U_{j-lm}^D. \end{cases} \tag{4}$$

It is known that every finite game has a mixed strategy Nash equilibrium solution [36]. In a static game with incomplete information, a Bayesian Nash equilibrium is defined as a mixed strategy profile $(\boldsymbol{p}_*^A, \boldsymbol{p}_*^D)$

$$\begin{cases} \forall \boldsymbol{p}^A, \;\; U^A\big(\boldsymbol{p}^A, \boldsymbol{p}^D\big) \le U^A\big(\boldsymbol{p}_*^A, \boldsymbol{p}^D\big) \\ \forall \boldsymbol{p}^D, \;\; U^D\big(\boldsymbol{p}^A, \boldsymbol{p}^D\big) \le U^D\big(\boldsymbol{p}^A, \boldsymbol{p}_*^D\big). \end{cases} \tag{5}$$

It can be obtained from

$$\frac{\partial\, U^A\big(\boldsymbol{p}^A, \boldsymbol{p}^D\big)}{\partial p_l^A} = 0, \quad \frac{\partial\, U^D\big(\boldsymbol{p}^A, \boldsymbol{p}^D\big)}{\partial p_m^D} = 0 \tag{6}$$

with constraints $\sum_{l=1}^{L} p_l^A = 1$, $\sum_{m=1}^{M} p_m^D = 1$. Thus, there is no strategy that one player could choose to yield a higher payoff.

C. Attack-Defense Fuzzy Payoff Matrix

After solving the problem of incomplete information about the opponent, howbeit the subjective consciousness and preference of the players are still there and worth noting. It is difficult for the players to accurately estimate the payoff matrix of the game. Therefore, in this article, fuzzy payoffs ($\tilde{U}^A$, $\tilde{U}^D$) are adopted instead of conventional Boolean two-valued logic.

T^A mainly includes target-based and benefit-based. A target-based attacker focuses on the completion of the attack goal

TABLE III
DETAILED EXPLANATIONS OF OVERALL PAYOFF FACTORS

Category	Parameter Explanation
$\mathcal{C}(\boldsymbol{p}^A), \mathcal{C}(\boldsymbol{p}^D)$	represent the expense of enforcing the attack strategy $\boldsymbol{p}^A$ and defense strategy $\boldsymbol{p}^D$, respectively.
$\mathcal{L}(\boldsymbol{p}^A, \boldsymbol{p}^D)$	represents the system loss ($\sum k_a LS_a + \sum \Delta ls$) caused by attacks after enforcing the defense strategy $\boldsymbol{p}^D$ as attack strategy is $\boldsymbol{p}^A$, which mainly determined by the load shedding ($\sum k_a LS_a$) and line loss ($\sum \Delta ls$).
$\mathcal{S}(\boldsymbol{p}^A, \boldsymbol{p}^D)$	represents the change of state stability after implementing the defense strategy $\boldsymbol{p}^D$ as attack strategy is $\boldsymbol{p}^A$, which depends on responsive action of breakers and interconnection switches ($\sum (SW_{b,t} \bigoplus SW_{b,t+1})$).

and the damage caused to the system, regardless of the cost comparatively. Thus, its fuzzy preference parameter $\tilde{\beta}$ will be larger in the calculation formula of the $\tilde{U}^A$. Meanwhile, the coefficient $\tilde{\alpha}$ will be smaller

$$\tilde{U}^A = -\tilde{\alpha}\mathcal{C}\left(\boldsymbol{p}^A\right) + \tilde{\beta}\left\{\mathcal{L}'\left(\boldsymbol{p}^A, \boldsymbol{p}^D\right) + \mathcal{S}'\left(\boldsymbol{p}^A, \boldsymbol{p}^D\right)\right\}. \tag{7}$$

On the contrary, T^D is composed of two categories: 1) system loss-based and 2) state stability-based. $\tilde{U}^D$ can be defined as

$$\tilde{U}^D = -\mathcal{C}\left(\boldsymbol{p}^D\right) - \tilde{\gamma}\mathcal{L}'\left(\boldsymbol{p}^A, \boldsymbol{p}^D\right) - \tilde{\nu}\mathcal{S}'\left(\boldsymbol{p}^A, \boldsymbol{p}^D\right) \tag{8}$$

where fuzzy preference parameter $\tilde{\gamma}$ and $\tilde{\nu}$ vary depending on the type of defender (T^D).

More detailed explanations of these payoff factors are summarized in Table III. As the result dimensions derived from these factors are not uniform, the normalization process theory is adopted based on the concept of relative importance degree

$$\mathcal{L}' = \frac{\mathcal{L} - \mathcal{L}_{\min}}{\mathcal{L}_{\max} - \mathcal{L}_{\min}}, \quad \mathcal{S}' = \frac{\mathcal{S}}{\mathcal{S}_{\max}}. \tag{9}$$

Therefore, $\tilde{u}_{lm}$ indicates the element of payoff matrix under attack-defense strategy profile (p_l^A, p_m^D) after normalization. Assume that each element is a triangular fuzzy number (TFN) $\tilde{u}_{lm} = (\underline{u}_{lm}, u_{lm}, \overline{u}_{lm})$, and its membership function is given by

$$\mu_{\tilde{u}_{lm}}(x) = \begin{cases} \left(x - \underline{u}_{lm}\right)/\left(u_{lm} - \underline{u}_{lm}\right), & \underline{u}_{lm} \leq x \leq u_{lm} \\ \left(\overline{u}_{lm} - x\right)/\left(\overline{u}_{lm} - u_{lm}\right), & u_{lm} < x \leq \overline{u}_{lm} \\ 0, & x < \underline{u}_{lm} \text{ or } \overline{u}_{lm} < x \end{cases} \tag{10}$$

where $x \in \mathbb{R}$, $\underline{u}_{lm} \leq u_{lm} \leq \overline{u}_{lm}$, u_{lm} is the main value of the TFN ($\tilde{u}_{lm}$) and means the most likely value of this probability, $\underline{u}_{lm}$ and $\overline{u}_{lm}$ are the lower and the upper bounds, respectively.

In order to convert this fuzzy problem into a static game problem, we adopt a method based on fuzzy probability and its mean to achieve defuzzification of the payoff matrix.

Parameter N indicates the probability of main value (u_{lm}) is N times as much as the probability of lower bound ($\underline{u}_{lm}$) as actual payoff. The larger the value of N, the greater the degree of deviation ($u_{lm} - \underline{u}_{lm}$). Similarly, the probability of main value (u_{lm}) is M times the probability of the upper bound ($\overline{u}_{lm}$).

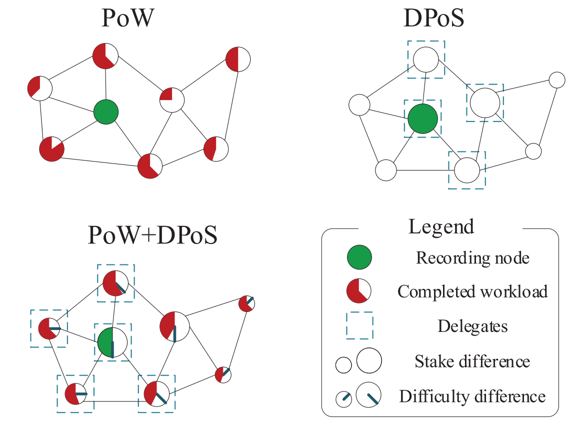


Fig. 4. Comparison of different consensus algorithms.

Then, the probability vector $[p_{\underline{u}_{lm}}, p_{u_{lm}}, p_{\overline{u}_{lm}}]$ of TFN $\tilde{u}_{lm}$ can be defined as

$$\begin{aligned} p_{\underline{u}_{lm}} &= \frac{1}{2(1+N)}, p_{u_{lm}} = \frac{N + 2NM + M}{2(1+N)(1+M)} \\ p_{\overline{u}_{lm}} &= \frac{1}{2(1+M)}. \end{aligned} \tag{11}$$

where the probability vector means the probability distribution of $\underline{u}$, u, and $\overline{u}$, which needs to satisfy that $p_{\underline{u}} + p_u + p_{\overline{u}} = 1$. The mean of TFN $\tilde{u}_{lm}$ is expressed as

$$M_{\tilde{u}_{lm}} = p_{\underline{u}_{lm}} \cdot \underline{u}_{lm} + p_{u_{lm}} \cdot u_{lm} + p_{\overline{u}_{lm}} \cdot \overline{u}_{lm}. \tag{12}$$

Thus, $\tilde{U}^A$ and $\tilde{U}^D$ can be obtained. The game is converted to a static game problem with incomplete information. The static game problem has already been solved in Section IV-B.

V. HYBRID ALGORITHM FOR SECURITY STRATEGY CONSENSUS

Based on the security strategy derived from each MR, a hybrid consensus algorithm is proposed to select the recording node and delegates. Therefore, a proposal for consensus and a new block storing result information can be generated. Then, Choquet integral and incentive mechanism are used separately for the implementation of strategy similarity comparison and reward. Finally, the DCDM is achieved with the consensus strategy information that stored in the new block.

A. Recording Node and Delegates Selection

To timely mitigate cyberattack risks, each energy management system (EMS) of the related region strives to propose its own defense strategy. Thus, it needs to choose a recording node first.

As mentioned in Table I, there are some consensus mechanisms giving the way of selecting recording node. PoW consensus mechanism means that the more work done by a participant, the greater the possibility of being selected as the recording node. In contrast, the DPoS consensus mechanism implies that the capability of a particular depends on the stake it owns, in addition, the consensus of results is between delegates not all of the distributed nodes.

If a hybrid consensus is used with the integration of both DPoS and PoW mechanisms, the energy consumption and processing time will become smaller in the process of reaching consensus. Consequently, the cost and difficulty of attacks will increase significantly. Therefore, an improved hybrid algorithm with both DPoS and PoW is proposed, as shown in Fig. 4. The size of the circle represents the stake of node. The blue line in the circle indicates the cutoff line for different difficulty work. The red sector that rotates counterclockwise means the amount of work that has been completed.

The main features of the hybrid algorithm are as follows.

1) Different from the way of the traditional DPoS in which the cyclic delegates generate blocks in sequence, the solution still needs to be obtained by mining so as to increase the degree of decentralization and the difficulty of attack. However, the difficulty of mining is related to the stake of the node itself, which is replaced by credibility in this article.
2) The MMG system is divided into a number of regions with mutual coupling relationship, which has been discussed in Section II-C. Each region is equivalent to a distributed node, and the delegates are selected by having the coupling relationship with the recording node.

The detailed steps of the hybrid algorithm are shown in Algorithm 1. In the pseudocode of the algorithm, *RN* indicates the selected recording node, $\boldsymbol{D}$ represents the selected delegates, and N means the total number of distributed nodes. First, the stake of each node $\mathrm{ST}(k)$ is calculated. It is multiplied by the product of the credibility $\mathrm{Cred}(k)$ and its duration $T(k)$. $T(k) \leq T_{\max} = 72$ (hours). Then, hash operations are performed on each node separately from

$$\mathrm{SHA256}\left(\mathrm{SHA256}\left(\mathrm{Hash}(k)'\right) + \mathrm{Timestamp} + \mathrm{Nonce} + \mathrm{Merkle\,Root}\right) < \mathrm{Target}(k) \quad (13)$$

where $\mathrm{Hash}(k)'$ means the hash value in the previous block of node k. The larger the stake $\mathrm{ST}(k)$ implements, the easier the inequality achieves. Because $\mathrm{ST}(k) \in [0, 72]$, $\mathrm{Target}(k)$ could be cut into 4 levels according to $\mathrm{Target}_{\max} \cdot 16^{\lfloor \mathrm{ST}(k)/18 \rfloor}$. To ensure real-time decision-making, $\mathrm{Target}_{\max}$ is set to $0 \times \mathrm{FFFF0000} \times 2^{4\times 56}$. Finally, only the node coupled with *RN* has the right to become the delegates and participate in the consensus process of generating new block. This is distinct from the traditional DPoS consensus mechanism, which elects determined 21 (EOS) or 101 (Bitshare) nodes as delegates [34].

B. Strategic Similarity Comparison

As mentioned in Section IV, each EMS of region has different fuzzy preferences and security strategies. When a consensus is made on the proposal proposed by one region, the delegates elected as representatives will review and judge the compliance and similarity of the content of proposal.

Different from the collaboration among detection results [37], the consensus of security decision-making will be a many-valued or fuzzy logic instead of a Boolean one. For MMG systems, defense measures mainly include operating breakers and interconnection switches, turning the distributed generation (DG) on or off, dynamically changing adjustable load, and replacing faulty equipment.

Algorithm 1 Hybrid Algorithm of Both DPoS and PoW

```
Require: The information of distributed nodes
Ensure: $RN, \boldsymbol{D}$
$RN \leftarrow 0, \boldsymbol{D} \leftarrow \varnothing$
$Target_{max} \leftarrow$ 0xFFFF0000 $\times 2^{4\times 56}$
$Hash_{max} \leftarrow$ 0xFFFF0000 $\times 2^{4\times 64}$
for all $k \in \{1, 2, \ldots, N\}$ do
    $Hash(k) \leftarrow Hash_{max}$
end for
while $Hash(k) < Target(k)$ do
    for all $k \in \{1, 2, \ldots, N\}$ do
        $ST(k) \leftarrow Cred(k) \cdot T(k)$
        $Target(k) \leftarrow Target_{max} \cdot 16^{\lfloor ST(k)/18 \rfloor}$
        $Hash(k) \leftarrow SHA256(SHA256(Hash(k)') + Timestamp + Nonce + Merkle\,Root)$
    end for
end while
$RN \leftarrow k$
$\boldsymbol{D} \leftarrow \{x|$ Coupling relationship between $x$ and $k\}$
```

In order to judge whether the security strategy in the proposal is reasonable and correct, it is first necessary to judge whether the strategy satisfies these basic constraints [38]–[40], which are discussed below.

1) Constraints of Supply-Demand Balance:

$$\sum P_{\mathrm{DG},j} \geq \sum P_{\mathrm{LS},i} + \sum P_{ls,l} \quad (14)$$

where $P_{\mathrm{DG},j}$ represents the upper bound of active power of DG_j, $P_{\mathrm{LS},i}$ is the load (LS_i) of the microgrid, and $P_{ls,l}$ indicates a loss on the line l.

2) Constraints of Nodal Voltage:

$$V_{i.\min} \leq V_i \leq V_{i.\max} \quad (15)$$

where $V_{i.\min}$ and $V_{i.\max}$ are, respectively, lower and upper limits of each nodal voltage V_i.

3) Constraints of Branch Capacity:

$$S_l \leq S_{l.\max} \quad (16)$$

where $S_{l.\max}$ indicates the maximum allowable apparent power of the branch l.

After that, cosine similarity is used to calculate the consistency of different defense strategies

$$\mathrm{sim}(\boldsymbol{x}, \boldsymbol{y}) = \frac{\boldsymbol{x} \cdot \boldsymbol{y}}{\|\boldsymbol{x}\| \|\boldsymbol{y}\|} = \frac{\sum_{i=1}^{n} x_i \times y_i}{\sqrt{\sum_{i=1}^{n} (x_i)^2} \times \sqrt{\sum_{i=1}^{n} (y_i)^2}} \quad (17)$$

where $\boldsymbol{x}$ and $\boldsymbol{y}$ indicate defense measures, which may include binary boolean vectors and continuous vectors.

There are often correlations between several types of defense measures, which are nonadditive properties. Therefore, we adopt Choquet integral to fuse different similarities, and the final similarity result is compared and judged with the threshold. Then, delegates will agree with the security strategy proposed by *RN* as the result exceeds the threshold.

A nonadditive measure μ on measurable space $\boldsymbol{X}$ is a set function μ: $\boldsymbol{X} \rightarrow [0, 1]$, satisfying the following axioms: 1) $\mu(\varnothing) = 0$; 2) $\mu(\boldsymbol{X}) = 1$; and 3) $\boldsymbol{A} \subseteq \boldsymbol{B} \rightarrow \mu(\boldsymbol{A}) \leq$

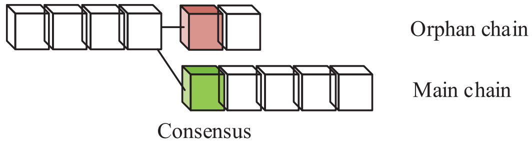


Fig. 5. Longest chain rule in blockchain.

$\mu(\boldsymbol{B})$. The discrete version of Choquet integral of measurable function f with respect to μ is expressed as

$$(C)\int f d\mu = \sum_{i=1}^{n}\big[f(x_i) - f(x_{i-1})\big]\mu(\boldsymbol{A_i}) \tag{18}$$

where $f(x_i)$ indicates that the indices have been permuted so that $0 \leq f(x_1) \leq \cdots \leq f(x_n) \leq 1$; $f(x_0) = 0$ and $\boldsymbol{A_i} = \{x_i, \ldots, x_n\}$.

C. Reward and Penalty

In Bitcoin, *RN* could get the corresponding digital currency as a reward through the process of mining. The incentive mechanism in blockchain is adopted into our scheme. This ensures the active involvement of distributed nodes in the process of CDM. The rewards are mainly divided into economic and noneconomic categories. Economic incentives are achieved by lowering electrovalency in the region. The reward range is proportional to $\mathrm{ST}(k)$. After being rewarded, the duration $T(k)$ is cleared and reset. Noneconomic incentives are implemented by adjusting the credibility of distributed node

$$\mathrm{Cred}'(k) = \max\left\{\mathrm{Cred}(k) + \mu\left(1 - \rho^{\frac{\mathrm{Cred}(k)\cdot T(k)}{T_{\max}}}\right), 1\right\} \tag{19}$$

where $\mathrm{Cred}'(k)$ means the credibility obtained after modification, reward factor μ represents the strength of reward that is proportional to the percentage of consensus, and ρ indicates the historical behavior of the node, i.e., the proportion of the punished action in all actions.

From the consensus mechanism and the longest chain rule in blockchain, the untrusted or wrong proposal could not get the approval from most representatives or reach consensus. Therefore, this block will not be added to the end of the chain by majority. It would become an orphan block and eventually be eliminated, as shown in Fig. 5. And the node that proposed the proposal is deemed to have been invaded or affected by the attack. Its credibility will decline. If a regarding node has long-term malicious behavior, its rate of reduction will become higher and higher. Furthermore, when $\mathrm{Cred}(k)$ is below a certain threshold, the node will not receive any economic benefit. Therefore, the penalty is shown as

$$\mathrm{Cred}'(k) = \min\left\{\mathrm{Cred}(k) - \lambda\rho^{\mathrm{Cred}(k)}, 0\right\} \tag{20}$$

where penalty factor λ represents the strength of penalty that is inversely proportional to the percentage of consensus.

VI. Experimental Studies

To demonstrate, this section implements and tests our DCDM approach on a typical MMG platform.

TABLE IV
Attack Strategy

Strategy	Description	Load Unserved	Cost
S_1^A	Manipulation on $Load_7$	20	500
S_2^A	Manipulation on $Load_8$	20	1,500
S_3^A	Destroy DG_6	40	3500
S_4^A	Manipulation on $Load_9$	20	500
S_5^A	Manipulation on $Load_{10}$	30	2,000
S_6^A	Destroy DG_7	15	2,000
S_7^A	Destroy DG_8	40	3,500
S_8^A	No operation	0	0

TABLE V
Defense Strategy of MR_5

Strategy	Description	Prevented Attacks	Cost
S_1^D	Open CB_{45}	S_1^A, S_2^A, S_3^A	-500
S_2^D	Cut $Load_1, Load_4$ and $Load_7$	S_3^A, S_7^A	0
S_3^D	Cut $Load_7$ and $Load_9$	S_3^A, S_7^A	2,000
S_4^D	$Load_5$ shedding	S_3^A, S_6^A, S_7^A	3,500
S_5^D	Reduce DG_3 and DG_8	$S_1^A, S_2^A, S_4^A, S_5^A$	1,000
S_6^D	Reduce DG_5 and DG_8	$S_1^A, S_2^A, S_4^A, S_5^A$	1,250
S_7^D	Increase DG_5 and DG_8	S_6^A	-1,500
S_8^D	No operation	S_8^A	0

A. Simulation Setup

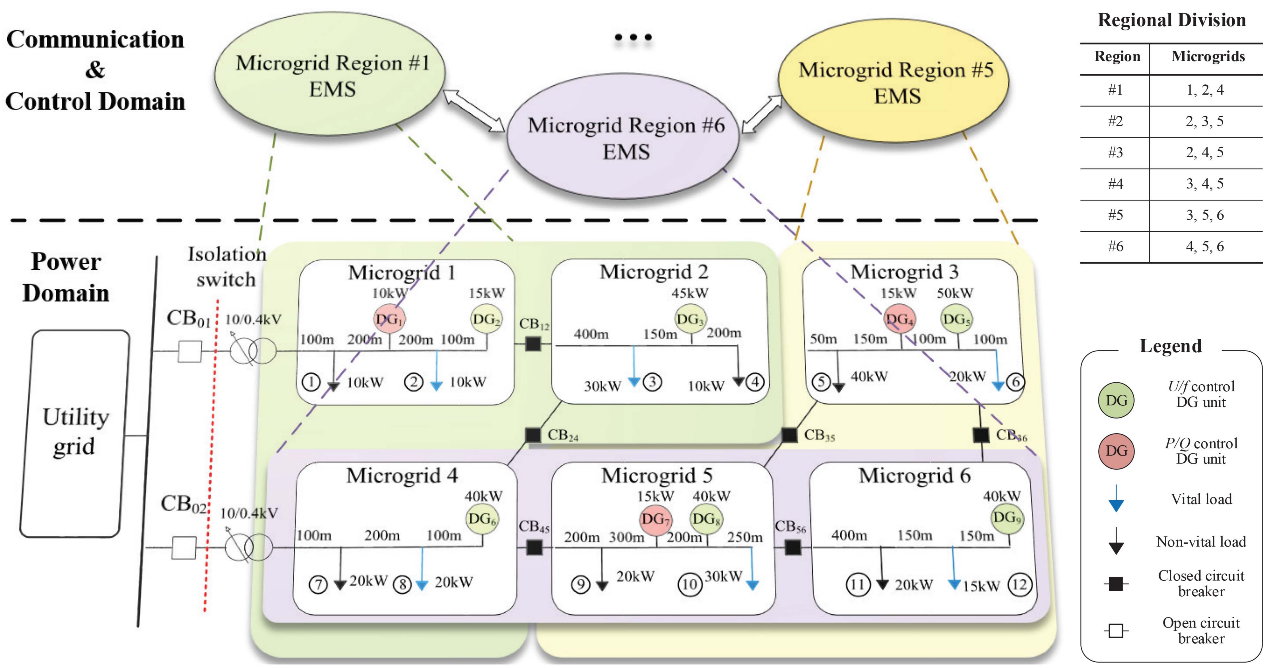
Fig. 6 depicts the architecture of the MMG simulation testbed. It is a typical decentralized scenario when the isolation switches (CB_{01}, CB_{02}) are open and the interconnected microgrids are running in island mode without the support of the utility grid. The green DG nodes adopt U/f control to guarantee the stability of the voltage and frequency in microgrid systems running in island mode. The red DG units adopt the way of P/Q control to achieve the designated control for active and reactive power. In each microgrid, two colored adjustable loads, blue and black, are used to represent vital load and nonvital load, respectively. The regional division indicates the correspondence between the power flow and the EMS. The transmissions of measurement information and operating instructions are via the wide area network (WAN) [41], [42].

According to the vulnerabilities of system, some attack scenarios are enumerated. They are assumed that the attacker has infiltrated the communication of MR_6 and a man-in-the-middle (MITM) attack is conducted by the modification of operating instructions on microgrids 4 or 5. So, the next available attack strategies are enumerated in Table IV.

In contrast to the attack actions, the strategies of defender MR_5 are listed in Table V. According to Tables IV and V, the available network game tree is drawn in Fig. 7. The defender needs to get the prior conviction of attackers' types through the analysis of historical data.

B. Simulation and Result Analysis

Two experiment scenarios are designed: 1) obtain the optimal attack/defense strategy profile based on our FSB-GM and 2) Use our hybrid algorithm to acquire the DCDM.



Regional Division

Region	Microgrids
#1	1, 2, 4
#2	2, 3, 5
#3	2, 4, 5
#4	3, 4, 5
#5	3, 5, 6
#6	4, 5, 6

Fig. 6. Typical decentralized MMG model.

1) Experiment 1—Security Strategy Generation: Let us focus on security decision-making in a single MR to demonstrate the effectiveness of the proposed FSB-GM. From the perspective of the system loss-based defender, defender (MR$_5$)'s transcendental beliefs of attacker's types are (target-based attacker, benefit-based attacker) = (0.6, 0.4), which are related to the analysis of historical attack scenarios. Different defenders may have different perceptions. The perceptions can be constantly updated and improved through the analysis of new attack scenarios. As the attacker belongs to target-based type, the fuzzy parameters $\tilde{\alpha}$ and $\tilde{\beta}$ in the formula (7) are set as (0.1, 0.2, 0.3) and (18 000, 20 000, 22 000), respectively. If the attacker is benefit-based type, parameters $\tilde{\alpha}$ and $\tilde{\beta}$ are (0.9, 1.0, 1.2) and (12 000, 14 000, 17 000), respectively. We combine the historical data to determine the empirical value in TFN, and estimate that the probability of occurrence of u_{lm} is twice that of $\underline{u}_{lm}$ and $\overline{u}_{lm}$. According to formula (11), $p_{\underline{u}_{lm}} = 1/6$, $p_{u_{lm}} = 4/6$, $p_{\overline{u}_{lm}} = 1/6$. From the calculation formula (7) and (8) of U^A and U^D, payoff matrix is obtained as

$$\begin{array}{cccc|c} S_1^D & S_2^D & \cdots & S_8^D & \\ (4,592,-5,765) & (10,966,-13,733) & \cdots & (5,406,-6,783) & S_1^A \\ (5,226,-6,908) & (17,209,-21,886) & \cdots & (6,042,-7,928) & S_2^A \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (-25,31) & (11,165,-13,956) & \cdots & (0,0) & S_8^A \end{array}.$$

Then, from (4) and (6), the Bayesian Nash equilibrium is obtained. The mixed optimal strategy profile $(\boldsymbol{p}_*^A, \boldsymbol{p}_*^D)$ is depicted as Fig. 8. This means that based on the defender's transcendental beliefs, the attacker is very likely to take the attack strategy S_3^A. The defender would take the defense strategy S_7^D with a higher probability.

2) Experiment 2—Security Strategy Consensus: In this experiment, facing with the conducted MITM attack on microgrids 4 or 5, all MRs associated with it propose their own defense strategy. In order to achieve consensus of security strategies, they will campaign for being *RN* first. After that, their proposals have a chance to be approved and accepted. The initial stake of each MR is set in Table VI. According to the hybrid consensus algorithm of DPoS and PoW (Section V-A), MR$_5$ is finally selected as *RN* after hash operations. The nodes with coupling relationship become delegates ($D = \{\mathrm{MR}_2, \mathrm{MR}_3, \mathrm{MR}_4, \mathrm{MR}_6\}$).

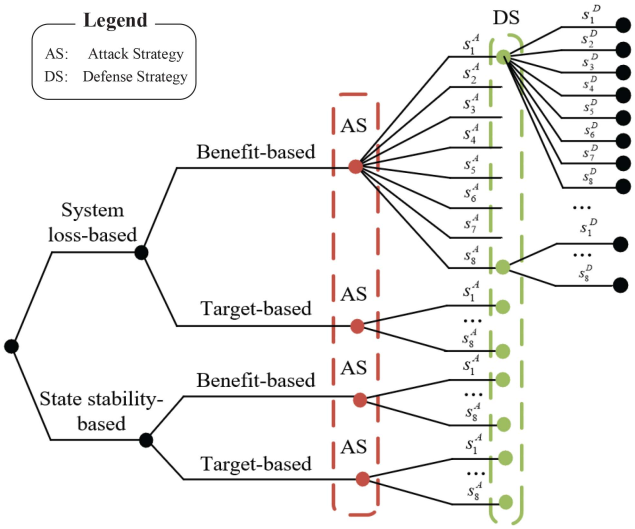


Fig. 7. Network game tree.

Then, with the mixed strategy profile $\boldsymbol{p}_*^D$ obtained in Experiment 1, MR$_5$ takes the defense strategy S_7^D and saves this result in the new Block B_n of its distributed ledger (Fig. 9).

However, this security strategy needs to get the approval and consensus from delegates, and let delegates record the new block on their own distributed ledger. To achieve this goal,

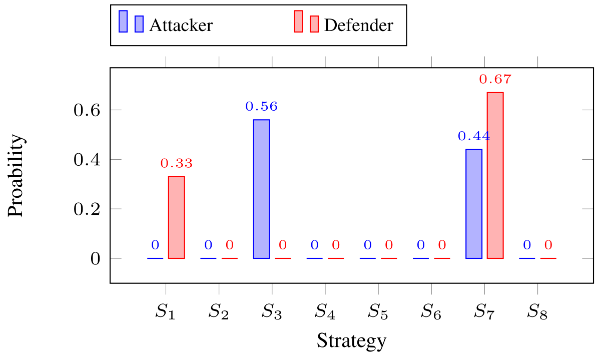


Fig. 8. Attacker and defender's optimal strategies.

TABLE VI
STAKE OF EACH MR

Factor	**MR$_1$**	**MR$_2$**	**MR$_3$**	**MR$_4$**	**MR$_5$**	**MR$_6$**
$Cred(k)$	0.5	0.4	0.6	0.4	0.7	0.65
$T(k)$	48	30	72	48	72	64
$ST(k)$	24	12	43.2	19.2	50.4	41.6
$Target(k)$	$T \cdot 16$	T	$T \cdot 16^2$	$T \cdot 16$	$T \cdot 16^3$	$T \cdot 16^2$

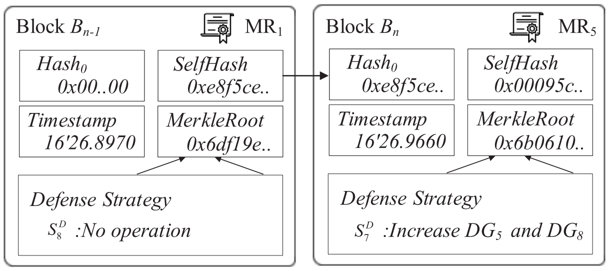


Fig. 9. Security strategy is stored in the block.

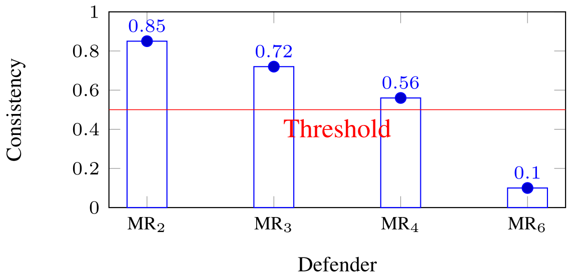


Fig. 10. Consistency of defense strategies.

each delegate should first judge whether the proposal of security strategy satisfies the basic constraints (14)–(16). Then, in the light of Choquet integral of measurable function (18), the consistency of different defense strategies is shown in Fig. 10. The value of threshold is determined with consideration of many factors, e.g., the types of defense strategies, the number of MGs, etc. The factor threshold is set as 0.5 after verification.

It is seen from Fig. 10 that only the strategy proposed by MR$_6$ has great dissimilarity. The other delegates accept the proposal and record the new block behind their distributed ledgers. Thus, the node MR$_6$ has likely been attacked. Its security strategy will be ignored to form a consensus.

Next, based on the incentive mechanism, the credibility of *RN* (MR$_5$) will get an upgrade from 0.7 according to (19) when $\mu = 0.375$ and $\rho = 0.3$

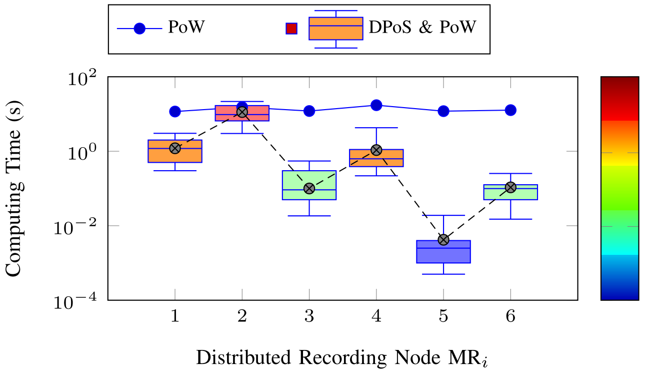


Fig. 11. Computing time of different recording nodes.

$$\mathrm{Cred}'(5) = \max\left\{\mathrm{Cred}(5) + \mu\left(1 - \rho^{\frac{\mathrm{Cred}(5)\cdot T(5)}{T_{\max}}}\right), 1\right\}$$
$$= 0.9318.$$

Finally, the real-time performance of our hybrid consensus algorithm is evaluated. It is compared with the conventional PoW mechanism. Thus, we plan to contrast the computing time when two consensus algorithms generate a new block (Fig. 11). Each of the simulation scenarios is conducted for 500 runs under the parameters given in Table VI. It is noted that the computing time mainly depends on the hash operations of each node. The level of *Target*(k) determines the difference of computing time. Therefore, the proposed hybrid consensus algorithm has advantages over the PoW mechanism in terms of real-time performance. Furthermore, the expression of the correlation between the influencing factors stake [ST(k) = Cred(k)·T(k)] and the computing time of generating a new block (CT) is shown in (21). This correlation indicates that with the increase of stake of MR$_k$, the computing time declines exponentially

$$\lg \mathrm{CT} \approx -1.1244\left\lfloor \frac{\mathrm{ST}(k)}{18} \right\rfloor + 1.1560. \tag{21}$$

C. Further Discussions

Through the above experiments, the proposed DCDM approach is shown to be able to efficiently make opportune defense strategy for MMGs. It also solves the consensus problem of strategies between decentralized nodes. Security strategy generation from our FSB-GM obtains the optimal defense strategy dynamically with a unified payoff quantification approach, which considers the incomplete information of realistic game and the fuzzy preferences of different types of attackers and defenders. Security strategy consensus based on our hybrid consensus mechanism and incentive mechanism achieves DCDM without the need of a trusted authority or central server, thus effectively avoiding SPoF problem. Consensus-derived security strategies are stored on blockchain in sequence, guaranteeing the consistency, and nonrepudiability of results.

Tables VII and VIII compare our proposed approach with some existing methods. Since the experiment environments

TABLE VII
COMPARISONS OF THE PROPOSED FSB-GM WITH EXISTING METHODS ON STRATEGY GENERATION

Approach	Non-zero-sum game	Information	Fuzzy preferences	Payoff	Attacker's types	Defender's types
[20]	×	Complete	×	Rotor speed of generator	×	×
[21]	√	Complete	×	Quantified physical impacts on shed load	Isolated and Coordinated	×
[43]	×	Complete	×	Incident probability and consequences	×	×
[22]	×	Incomplete	√	×	×	×
[23]	√	Incomplete	×	Combining counterattacks and successful rate	Risky and Conservative	First level, Second level and Third level
Ours	√	Incomplete	√	Strategic cost, system loss, and state stability	Target-based and Benefit-based	System loss-based and State stability-based

TABLE VIII
COMPARISON OF THE PROPOSED HYBRID CONSENSUS ALGORITHM WITH RELATED WORKS ON STRATEGY CONSENSUS

Approach	Scenario	Consensus approach	Decentralization	Operating rate	Participant safety	Without central CA or certified among peers	Incentive mechanism
[7]	Distribution Networks	Hierarchical integration model	×	–	×	–	–
[9]	DG Islanding	Multiagent system approaches	√	–	×	–	×
[17]	Peer-to-Peer networks	Self organizing trust model	√	–	√	×	×
[18]	Power system	Trust-based mechanism	√	–	√	×	√
[28]	Bitcoin	PoW	High	Slow	√	√	√
[34]	EOS	DPoS	Low	Fast	√	√	√
Ours	MMGs	Hybrid algorithm based on DPoS and PoW	High	Fast	√	√	√

Note: '–' means that the item was not mentioned and could not be inferred.

and the simulated attack scenarios are different, it is difficult to directly quantitatively compare the performance of the methods. Therefore, some qualitative metrics have been given in the two tables.

From Tables VII and VIII, it is observed the following.

1) *Strategy Generation:* The existing approaches somewhat overlooked the relationship between payoff matrix and the type of attackers and defenders. They assumed that both attacker and defender were aware of each other's behavior. Such an assumption is often unrealistic in practical systems.
2) *Strategy Consensus:* Most previous studies did not consider the problem of how to achieve consensus on security strategy when these assumptions of trust and security were relaxed. While central CA and trust mechanism among peers were developed, a central CA is a bottleneck for scalability and the trust mechanism could not prevent the malicious data transmitted by high-reputation participants.
3) *Hybrid Consensus Algorithm:* The superiority of hybrid consensus algorithm over existing methods is reflected in two aspects. On the one hand, compared with the PoW algorithm, the amount of calculation is reduced, and the transaction rate is increased. On the other hand, unlike the DPoS algorithm that sequentially generates blocks by delegates, our hybrid algorithm overcomes the defect of one single richest member.

Therefore, our approach is applicable to decentralized scenarios for solving the problem of CDM in MMG systems.

VII. CONCLUSION

In this article, a new DCDM approach has been proposed for protecting MMG systems by using consensus mechanisms in blockchain. It solves SPoF and other inaccurate decision issues without the need of a trusted authority or central server. Meanwhile, it guarantees the consistency and nonrepudiability of consensus results in the process of distributed data transmission. More specifically, we first detail the classification of attackers and defenders, and consider fuzzy preference in the process of payoff quantification, which mainly takes into account the strategic cost, system loss, and state stability. Then, in order to increase transaction rate and overcome the defect of one single richest member, the security strategy achieves consensus by taking use of hybrid algorithm based on DPoS and PoW. Simulation results have demonstrated the effectiveness of the presented approach.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their helpful comments and suggestions.

REFERENCES

[1] E. Bullich-Massagué, F. Díaz-González, M. Aragüés-Peñalba, F. Girbau-Llistuella, P. Olivella-Rosell, and A. Sumper, "Microgrid clustering architectures," *Appl. Energy*, vol. 212, pp. 340–361, Feb. 2018.

[2] S. A. Arefifar, M. Ordonez, and Y. A. I. Mohamed, "Voltage and current controllability in multi-microgrid smart distribution systems," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 817–826, Mar. 2018.

[3] D. An, Q. Yang, W. Yu, X. Yang, X. Fu, and W. Zhao, "SODA: Strategy-proof online double auction scheme for multimicrogrids bidding," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 7, pp. 1177–1190, Jul. 2018.

[4] J. Li, Y. Liu, and L. Wu, "Optimal operation for community-based multi-party microgrid in grid-connected and islanded modes," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 756–765, Mar. 2018.

[5] H. Yan, X. Zhou, H. Zhang, F. Yang, and Z. Wu, "A novel sliding mode estimation for microgrid control with communication time delays," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1509–1520, Mar. 2019.

[6] E. Mousavinejad, F. Yang, Q. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Trans. Cybernetics*, vol. 48, no. 11, pp. 3254–3264, Nov. 2018.

[7] J. B. Leite and J. R. S. Mantovani, "Development of a self-healing strategy with multiagent systems for distribution networks," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2198–2206, Sep. 2017.

[8] X. He, X. Fang, and J. Yu, "Distributed energy management strategy for reaching cost-driven optimal operation integrated with wind forecasting in multimicrogrids system," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1643–1651, Aug. 2019.

[9] A. Sharma, D. Srinivasan, and A. Trivedi, "A decentralized multiagent system approach for service restoration using DG islanding," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2784–2793, Nov. 2015.

[10] H. Liang, X. Guo, Y. Pan, and T. Huang, "Event-triggered fuzzy bipartite tracking control for network systems based on distributed reduced-order observers," *IEEE Trans. Fuzzy Syst.*, early access, Mar. 23, 2020, doi: 10.1109/TFUZZ.2020.2982618.

[11] W. Wang, H. Liang, Y. Pan, and T. Li, "Prescribed performance adaptive fuzzy containment control for nonlinear multiagent systems using disturbance observer," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 3879–3891, Sep. 2020.

[12] P. Du, Y. Pan, H. Li, and H. Lam, "Nonsingular finite-time event-triggered fuzzy control for large-scale nonlinear systems," *IEEE Trans. Fuzzy Syst.*, early access, May 6, 2020, doi: 10.1109/TFUZZ.2020.2992632.

[13] G. Jules and M. Saadat, "Agent cooperation mechanism for decentralized manufacturing scheduling," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 12, pp. 3351–3362, Dec. 2017.

[14] D. Croce *et al.*, "Overgrid: A fully distributed demand response architecture based on overlay networks," *IEEE Trans. Autom. Sci. Eng.*, vol. 14, no. 2, pp. 471–481, Apr. 2017.

[15] N. Rahbari-Asr, Y. Zhang, and M.-Y. Chow, "Consensus-based distributed scheduling for cooperative operation of distributed energy resources and storage devices in smart grids," *IET Gener. Transm. Distrib.*, vol. 10, no. 5, pp. 1268–1277, Apr. 2016.

[16] J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, "Current cyber-defense trends in industrial control systems," *Comput. Security*, vol. 87, Nov. 2019, Art. no. 101561.

[17] S. Shaik and S. G. John, "A novel distributed trust model for peer-to-peer networks," *Int. J. Comput. Eng. Res.*, vol. 3, no. 5, pp. 267–270, Oct. 2014.

[18] I. Matei, J. S. Baras, and V. Srinivasan, "Trust-based multi-agent filtering for increased smart grid security," in *Proc. 20th Mediterr. Conf. Control Autom. (MED)*, Barcelona, Spain, 2012, pp. 716–721.

[19] Y. Qin, Q. Zhang, C. Zhou, and N. Xiong, "A risk-based dynamic decision-making approach for cybersecurity protection in industrial control systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, Aug. 17, 2018, doi: 10.1109/TSMC.2018.2861715.

[20] A. Farraj, E. Hammad, A. Al Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1846–1855, Jul. 2016.

[21] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 684–694, Mar. 2018.

[22] W. Xiong, X. Luo, and W. Ma, "Games with ambiguous payoffs and played by ambiguity and regret minimising players," in *Proc. Aust. Joint Conf. Artif. Intell.*, 2012, pp. 409–420.

[23] H. Zhang, J. Wang, D. Yu, J. Han, and T. Li, "Active defense strategy selection based on static Bayesian game," in *Proc. 3rd Int. Conf. Cybersp. Technol. (CCT)*, Beijing, China, 2015, pp. 1–7.

[24] K. Huang, C. Zhou, Y. Qin, and W. Tu, "A game-theoretic approach to cross-layer security decision-making in industrial cyber-physical systems," *IEEE Trans. Ind. Electron.*, vol. 67, no. 3, pp. 2371–2379, Mar. 2020.

[25] M. Larbani, "Non cooperative fuzzy games in normal form: A survey," *Fuzzy Sets Syst.*, vol. 160, no. 22, pp. 3184–3210, Nov. 2009.

[26] F. Kacher and M. Larbani, "Existence of equilibrium solution for a non-cooperative game with fuzzy goals and parameters," *Fuzzy Sets Syst.*, vol. 159, no. 2, pp. 164–176, Jan. 2008.

[27] B. Falahati, Y. Fu, and L. Wu, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515–1524, Sep. 2012.

[28] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[29] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 9, pp. 1421–1428, Sep. 2018.

[30] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.

[31] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, p. 162, Jan. 2018.

[32] F. Xiang, W. Huaimin, and S. Peichang, "Proof of previous transactions (PoPT): An efficient approach to consensus for JCLedger," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, May 8, 2019, doi: 10.1109/TSMC.2019.2913007.

[33] M. Du, X. Ma, Z. Zhang, X. Wang, and Q. Chen, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC)*, Banff, AB, Canada, 2017, pp. 2567–2572.

[34] V. Dhillon, D. Metcalf, and M. Hooper, "Recent developments in blockchain," in *Blockchain Enabled Applications*. Berkeley, CA, USA: Apress, Jan. 2017, pp. 151–181.

[35] J. C. Harsanyi, "Games with incomplete information played by 'Bayesian' players, I–III part I. The basic model," *Manag. Sci.*, vol. 14, no. 3, pp. 159–182, Nov. 1967.

[36] J. F. Nash, "Equilibrium points in *n*-person games," *Proc. Nat. Acad. Sci.*, vol. 36, no. 1, pp. 48–49, Jan. 1950.

[37] B. Hu, C. Zhou, Y.-C. Tian, Y. Qin, and X. Junping, "A collaborative intrusion detection approach using blockchain for multimicrogrid systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1720–1730, Aug. 2019.

[38] L. Liu, Y. Liu, D. Li, S. Tong, and Z. Wang, "Barrier Lyapunov function-based adaptive fuzzy FTC for switched systems and its applications to resistance–inductance–capacitance circuit system," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3491–3502, Aug. 2020.

[39] L. Liu, Y. Liu, A. Chen, S. Tong, and C. L. P. Chen, "Integral barrier Lyapunov function-based adaptive control for switched nonlinear systems," *Sci. China F, Inf. Sci.*, vol. 63, no. 3, Feb. 2020, Art. no. 132203.

[40] L. Tang, D. Ma, and J. Zhao, "Adaptive neural control for switched non-linear systems with multiple tracking error constraints," *IET Signal Process.*, vol. 13, no. 3, pp. 330–337, May 2019.

[41] X. Li, Y.-C. Tian, G. Ledwich, Y. Mishra, X. Han, and C. Zhou, "Constrained optimization of multicast routing for wide area control of smart grid," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3801–3808, Jul. 2019.

[42] X. Li, Y.-C. Tian, Y. Mishra, G. Ledwich, and C. Zhou, "Minimizing multicast routing delay in multiple multicast trees with shared links for smart grid," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5427–5435, Sep. 2019.

[43] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, and S. Huang, "Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 10, pp. 1429–1444, Oct. 2016.

Bowen Hu received the B.S. degree in automation from Central South University, Changsha, China, in 2015. He is currently pursuing the Ph.D. degree in control science and control engineering with the School of Artificial Intelligence and Automation, Huazhong University of Science and Technology, Wuhan, China.

His main research interests include industrial control system, artificial intelligence, and cyber-physical security of smart grid.

Chunjie Zhou received the M.S. and Ph.D. degrees in control theory and control engineering from the Huazhong University of Science and Technology, Wuhan, China, in 1991 and 2001, respectively.

He is currently a Professor with the School of Artificial Intelligence and Automation, Huazhong University of Science and Technology. His research interests include safety and security control of industrial control systems, theory and application of networked control systems, and artificial intelligence.

Yu-Chu Tian (Senior Member, IEEE) received the first Ph.D. degree in computer and software engineering from the University of Sydney, Sydney, NSW, Australia, in 2009, and the second Ph.D. degree in industrial automation from Zhejiang University, Hangzhou, China, in 1993.

He is currently a Professor with the School of Computer Science, Queensland University of Technology, Brisbane, QLD, Australia. His research interests include big data computing, distributed computing, cloud computing, computer networks and communications, real-time systems, systems engineering, and cyber-physical security of industrial control systems.

Xiaoya Hu (Senior Member, IEEE) received the B.S. degree in power engineering and the M.S. and Ph.D. degrees in control theory and control engineering from the Huazhong University of Science and Technology, Wuhan, China, in 1995, 2002, and 2006, respectively.

She is currently a Professor with the Key Laboratory of Ministry of Education for Image Processing and Intelligent Control, Huazhong University of Science and Technology. Her research interests include wireless sensor networks and smart grid.

Xinjue Junping received the B.S. degree in automation from China Three Gorges University, Yichang, China, in 2018. He is currently pursuing the master's degree in new energy science and engineering with the School of China-EU Institute for Clean and Renewable Energy, Huazhong University of Science and Technology, Wuhan, China.

His main research interests include new energy generation technology and smart grid.