Distributed Hybrid-Triggering-Based Secure Dispatch Approach for Smart Grid Against DoS Attacks

Yushuai Li, *Member, IEEE,* Rufei Ren, Bonan Huang, Rui Wang, Qiuye Sun *Senior Member, IEEE,* David Wenzhong Gao, *Fellow, IEEE,* and Huaguang Zhang, *Fellow, IEEE*

***Abstract*—This economic dispatch problem has been tended to be solved by using distributed optimization algorithms which are easier to suffer from diversified cyberattacks, e.g., the denial of service (DoS) attacks. It leads to enormous secure risks for the economic operation of smart grid. To address this issue, this paper aims to propose a distributed secure dispatch method to effectively defend the DoS attacks. Firstly, considering the coexistence of attack sequence and triggering sequence, the actual affected period and actual safe period are analyzed and defined. It provides an analysis model for the subsequent algorithm design. Then, by designing switched system dynamics along with hybrid-triggering concept, a novel distributed secure dispatch strategy is presented. The proposed method can enable each distributed generator reasonably using estimation values and switched rate of system evolution to mitigate the effect of the DoS attacks. Meanwhile, contributed by the designed hybrid-triggering communication strategy, the proposed method takes advantages of reduced communication costs, flexible execution, and fast and reliable communication recuperation among distributed generators. With those efforts, the proposed method is capable of high robustness to resist the DoS attacks well. Moreover, theoretically analytic results are proposed to verify the correctness of the proposed method. Finally, simulation results are provided to show the feasibility and effectiveness of the proposed method.**

***Index Terms*—Economic dispatch, DoS attacks, smart grid, distributed algorithm.**

I. Introduction

As the extension and enhancement of conventional power system, smart grid has attracted significant attention owning to its better sustainability, reliability and feasibility, etc. Like the underlying control and stability assessment, the economic dispatch problem (EDP) is a fundamental research problem in smart grid [1], [2] or multi-energy system [3]. It aims to cooperatively manage multiple generators as well as loads to obtain maximum social welfare or minimum cost while satisfying multiple global and local operation constraints [4], [5]. In essence, the EDP is a constrained optimization problem. We are able to design centralized or distributed optimization approaches to solve this problem.

With the development of distributed technologies, the distributed optimization algorithms have emerged with increasing research enthusiasm. Compared to the centralized algorithms, the distributed algorithms possess the ability of utilizing only local communication and calculation to obtain the optimal solutions, which can effectively overcome single-point failures and support the plug-and-play feature well. Many distributed algorithms have been proposed, which can be mainly divided into three categories, i.e., the alternating direction method of multipliers (ADMM)-based methods, blockchain-based methods and consensus-based methods. Firstly, the major design concept of ADMM-based method is to employ the alternating descent fashion to make the original variable and dual variable gradually converge to optimal point. Recently, some similar ADMM methods were proposed to solve the dynamic or/and multi-period EDP, e.g., [6], [7], which possess faster convergence speed. Secondly, due to intrinsic decentralized functionality, the blockchain technology is introduced to solve the distributed EDP, which can effectively resist malicious aggregators, and achieve public storage and sharing [8], [9]. Thirdly, the consensus-based methods are successfully established by introducing consensus protocol with increasing research interests. From theoretical analysis, the Lagrangian multiplier related to the global supply-demand constraint is equivalent to the global power price. Since the power price of the whole system should be equal to the same, it is often to be set as the sharing variable or consensus variable to yield distributed implementation. Based on this concept, a set of distributed algorithms are presented, such as the lambda-iteration algorithms [10], [11], gradient descent algorithms [12]–[14], and Newton descent algorithms [15], [16], etc. Owning to the flexibility and scalability of consensus protocol, the time-delay effect [17], [18], finite-time convergence [19], [20], privacy-preserving [21], [22], time-varying network [23], [24], and ever-triggering communication [25], [26] have been further studied. In this paper, we mainly investigate the consensus-based methods.

Even though the aforementioned methods have achieved distributed dispatch with some excellent performance, the actual implementation still faces many challenges. One of them comes from the unsafe communication network environment. Note that distributed optimization algorithms work under dis-

This work was supported by European Union's Horizon 2020 research and innovation programme for the Marie Sklodowska-Curie Actions under Grant 101023244. (Corresponding author: Bonan Huang and Rufei Ren.)

Yushuai Li is with the Department of Informatics, University of Oslo, 0316 Oslo, Norway.

Rufei Ren, Bonan Huang, Wang Rui, Qiuye Sun and Huaguang Zhang are with the School of Information Science and Engineering, Northeastern University, Shenyang, Liaoning, 110004, China.

David Wenzhong Gao is with the Department of Electrical and Computer Engineering, University of Denver, Denver, CO 80208 USA.

tributed communication network which is easier to suffer from cyberattacks. Thus, network security problem has become a big concern in the distributed optimization and dispatch fields. Most of distributed algorithms employ the consensus protocol to achieve distributed computation. Several research study the resilient consensus algorithms considering cyberattacks. For instance, an observer-based consensus control strategy was presented in [27] that enables the utilization of observation to reduce the influence of DoS attacks. For leader-following multiagent system, a dual-terminal triggering approach was presented in [28], where theoretical results are provided to analyze the effect of DoS attacks. Most recently, Fang *et al.* [29] proposed a sample-data based resilient strategy to achieve consensus control in unsafe communication network. Although those work [27]–[29] have obtained some good achievements to resist DoS attacks, they mainly focus on the consensus problem. Note that the objective of consensus problem is to make each agent converge to the same value. Compared to consensus problem, there only exists one optimal solution for distributed optimization problem. For the design of distributed optimization algorithms, we consider both of the convergence and optimality. However, the consensus problem mainly focuses on the convergence. Thus, the distributed optimization problem is more complex than the consensus problem, which calls for deep research considering DoS attacks. To address this issue, some robust distributed dispatch strategies have been presented for smart grid in recent years. To be specific, literature [30], [31] studied the effects of the data integrity attacks on the distributed lambda-iteration algorithm [10]. It has been shown that the attacker can inject false data on the sharing information or/and local information to mislead the normal system operation. It results in increased economic loss and broken balance between supply and demand. To resist the data integrity attacks, the neighborhood-watch-based method [32], reputation-based neighborhood-watch mechanism [33], and the detection and correction mechanism [34] were presented. Besides the data integrity attack, the denial-of-service (DoS) attack is another common type of cyberattack. It aims to block the information transmission of the control signal or sensor data by preventing the communication channel. It is great importance to consider the effects of DoS attacks and design effective coping mechanisms. To this aim, a DoS-attack-robust dispatch strategy was presented in [35] by making use of Mix-Integer Linear Programming and priority-based restoration process to reassign the energy load. Li et al [36] proposed an attack-robust strategy based on distributed confidence level manager to detect and isolate the misbehaving generators. In fact, the detection-and-correction-based distributed dispatch method [34] is also suitable for dealing with DoS attacks. In [37], a switched Newton-Raphson algorithm was proposed, which mainly provides a mathematical mode to analyze the effects of persistent DoS attacks without consideration of resistance mechanisms.

Note that although the aforementioned distributed dispatch strategies have obtained some satisfactory results on dealing with the cyberattacks, more flexible and roubust distributed secure dispatch strategy is rare. The major reasons are illustrated as follows. On the one hand, most of dispatch strategies considering cyterattacks, i.e., [30]–[36] are built upon the lambda-iteration algorithms [10], [11]. Nevertheless, lambda-iteration algorithms require strong initial conditions. By using this method, the fault or invalidation at any iteration step caused by the cyberattacks will be accumulated to destroy the global convergence and/or optimality. It implies that lambda-iteration algorithms are more sensitive and vulnerable to the cyberattacks. Moreover, regarding to the DoS attacks, literature [34]–[36] still require that the communication network is (strongly) connected during attack period. In practice, the attacker would like to destroy the connectivity of the communication network to make the system unstable. Although the method proposed in [37] is initialization-free without the hypothesis of connected graph during attack period, it do not design any strategy against DoS attacks. Thus, it is needed to develop more effective and strong robust dispatch strategy to defend the DoS attacks. On the other hand, the existing distributed dispatch strategies considering cyberattacks are implemented in periodic or continue communication fashion, which causes unnecessary communication consumption. Currently, the event-triggering based communication strategy has been proposed and viewed as more flexible and cost saving method. In this scenario, the performance of the distributed dispatch strategy is depended on the triggering condition, which may be failure caused by the DoS attacks. The coexistence of the DoS attacks and triggering mechanism makes the algorithm design and theoretical analysis more difficult. Further deep investigation is needed.

To tackle those challenges, this paper aims to design a security dispatch strategy for smart grid against DoS attacks while providing theoretically analytic results. Our main scientific contributions are summarized as follows:

1) A novel distributed secure dispatch strategy is presented, which is obtained by co-designing switched system dynamics with hybrid-triggering mechanism. By using the proposed method, each distributed generator (DG) can not only work well during actual safe period but also slow down the system evolution to avoid divergence during actual affected period caused by the DoS attacks. Compared with [30]–[37], the proposed algorithm is capable of initialization-free, distributed implementation, asynchronous communication, and strong robustness to effectively defend the DoS attacks. Meanwhile, the hypothesis of (strongly) connected graph during attack period is not required.

2) A hybrid-triggering communication strategy composed of dynamic event-triggering mechanism and virtual periodic-triggering mechanism is proposed and embedded into the execution of the proposed method. With this effort, the dynamic event-triggering communication can be adaptively changed to virtual periodic communication during actual affected period to avoid losing its dynamic behavior and restore the communication interaction as faster as possible. Meanwhile, the advantages of dynamic event-triggering communication can be maintained, e.g., reduced communication expenditure, flexible implementation and larger inter-event time, etc.

3) By using Lyapunov analysis method, two Lemmas are presented to exhibit the conservative behavior of the proposed method during actual safe and affected periods. On the basis,

a main Theorem is provided to show the global optimality and convergence. With those efforts, we validate the correctness of the proposed approach.

The remainder is summarized as follows. Section II formulates the EDP, and introduces the distributed communication network and the model of DoS attacks. In section III, we present the main algorithm and theoretical analysis results. In section IV, simulation results are provided to verify the effectiveness of the proposed method. Finally, Section V concludes this paper.

II. Problem Formulation and Preliminaries

A. EDP Formulation

We consider a power system composed of distributed generators and loads. The objective of EDP is to minimize the total generation costs while meeting the supply-demand balance constraint and local operation constraints, i.e.,

$$\min\ Obj = \sum_{i=1}^{n} C(p_i^{dg}(t)) \tag{1}$$

$$s.t.\ \sum_{i=1}^{n} p_i^{dg}(t) = \sum_{i=1}^{n} p_i^{load}(t), \tag{2}$$

$$p_i^{dg,min} \leq p_i^{dg}(t) \leq p_i^{dg,max}, \tag{3}$$

$$-p_i^{dg,rp} \leq p_i^{dg}(t) - p_i^{dg}(t-1) \leq p_i^{dg,rp}, \tag{4}$$

where $p_i^{dg}(t)$ and $p_i^{load}(t)$ are local power generation and load, respectively; $C(p_i^{dg}(t)) = \kappa_i^1(p_i^{dg}(t))^2 + \kappa_i^2 p_i^{dg}(t) + \kappa_i^3 + \exp(\kappa_i^4 p_i^{dg}(t))$ is the cost function of ith generator; $p_i^{dg,min}$ and $p_i^{dg,max}$ are the lower and upper bounds of $p_i^{dg}(t)$, respectively; $p_i^{dg,rp}$ is the ramp rates of $p_i^{dg}(t)$ between two consecutive time steps; κ_i^1, κ_i^2, κ_i^3 and κ_i^4 are positive cost coefficients.

In essence, the EDP is an optimization problem, which can be solved by using multiple centralized or distributed optimization algorithms. For sake of convenience, we make use of $x_i(t)$ to re-denote the decision variable, $f(x_i(t))$ to re-denote the local cost function, $\jmath_i(t)$ to re-denote the local power load, and $g(x_i(t))$ to represent the function of the inequality constraint obtained from the local operation constraints. Then, the EDP can be abstracted as the following common optimization problem:

$$\min\ Obj = \sum_{i=1}^{n} f(x_i(t)) \tag{5}$$

$$s.t.\ \sum_{i=1}^{n} x_i(t) = \sum_{i=1}^{n} \jmath_i(t), \tag{6}$$

$$g(x_i(t)) \leq 0 \rightarrow x_i(t) \in \Omega_i, \tag{7}$$

where Ω_i represents the feasible operation region determined by $g(x_i)$ only.

Remark 1: In this paper, we study the EDP for smart grid. The decision variable is the power generation of each DG, i.e., $x_i(t)$. The planned load flow $\jmath_i(t)$ at each dispatch period is measured and calculated by the local load. The information of $\jmath_i(t)$ is further sent to the local DG i. Like pervious work (e.g., [6], [10]–[14], [16]–[18], [22], [23], [34], [35]), the measured load information $\jmath_i(t)$ is assumed to be known by the local DG i. On the basis, the proposed method is used to calculate each $x_i(t)$ in a distributed fashion.

Remark 2: This paper focuses on designing distributed algorithm to solve a common optimization convex problem with the form of (5-7), which can be further applied to solve the EDP. We only requires that $f(x_i)$ is strong convex (see from Definition 1 and Ω_i is closed convex set. Therein, no any specific form is required. Therefore, the proposed method is capable of solving more complex EDP considering different objective functions and constraints based on different actual models if they can be formulated as the form of (5-7). From the perspective of applications, many kinds of objections functions are strongly convex. To be specific, the well-used objective functions in EDP with quadratic-form, exponential-form and their mix meet the requirements in Definition 1. Regarding to operation constraints, the charging/discharging constraint, ramp rate constraint, capability constraint, and tradeoff constraint between optimality and possibility [37] can be abstracted into the local convex set Ω_i. Thus, those kinds of constraints can be effectively solved by using the proposed method.

Definition 1: $f(x_i(t))$ is strongly convex with the local operation region, if there exists $\Im_i > 0$ such that $\forall x_i(t), x_i'(t) \in \Omega_i$,

$$(x_i(t) - x_i'(t))^T \big(\nabla f(x_i(t)) - \nabla f(x_i'(t))\big) \geq \Im_i ||x_i(t) - x_i'(t)||^2. \tag{8}$$

B. Communication Network and Differentiated Projection

The distributed communication network among DGs is often modeled as a graph $\mathbb{G} = \{\mathbb{V}, \mathbb{E}, \mathbb{A}\}$. Therein, $\mathbb{V} = \{1, 2, \cdots, n\}$ represents the set of DGs (nodes). $\mathbb{E} = \mathbb{V} \times \mathbb{V}$ represents the set of communication edges. $\mathbb{A} = [a_{ij}]_{n\times n}$ represents the weighted adjacency matrix. If node i can receive the information from node j, then there exists an edge $(i, j) \in \mathbb{E}$. In this case, $a_{ij} = 1$; otherwise, $a_{ij} = 0$. The neighbor set of node i is denoted as $\mathcal{N}_i = \{j \in \mathbb{V} | (i, j) \in \mathbb{E}\}$. The Laplacian matrix is defined as $L = [l_{ij}]_{n\times n}$, where $l_{ij} = -a_{ij}$ for $j \neq i$ and $l_{ii} = \sum_j a_{ij}$. It is assumed that $\mathbb{G}$ is connected when the system is not subject to DoS attacks. The eigenvalues of L are ordered as $0 = \lambda_1 < \lambda_2 \leq, \cdots, \lambda_n$.

Moreover, some basis knowledge about normal cone, differentiated projection and a necessary Lemma 1 are provided. They are further used for the subsequent algorithm design and convergence analysis. To be specific, the boundary and inside of Ω_i are defined as Ω^{bo} and Ω^{in}, respectively. For each Ω_i, the corresponding normal cone at $x_i(t)$ is defined as $NC_{\Omega_i}(x_i(t)) = \{\vartheta | \vartheta^T(x_i'(t) - x_i(t)) \leq 0, \forall x'(t) \in \Omega_i\}$. We further define $\overline{NC}_{\Omega_i}(x_i(t)) = \{\vartheta | \vartheta^T(x_i'(t) - x_i(t)) \leq 0, ||\vartheta||^2 = 1, \forall x_i'(t) \in \Omega_i\}$ if $x_i(t) \in \Omega_i^{in}$, and $\overline{NC}_{\Omega_i}(x_i(t)) = \{0\}$ if $x_i(t) \in \Omega_i^{bo}$. Next, the mathematical expression for the differentiated projection of $x_i(t)$ onto Ω_i is $\Upsilon_{\Omega_i}(x_i(t), \copyright) = \lim_{\ell\to 0}\big(P_{\Omega_i}(x_i(t) + \ell\copyright) - x_i(t)\big)/\ell$, where $P_{\Omega_i}(x_i(t)) = \arg\ \min_{\hat{x}_i(t)} ||x_i(t) - \hat{x}_i(t)||$, $\forall \hat{x}_i(t) \in \Omega_i$.

Lemma 1 [12]: 1) $\Upsilon_{\Omega_i}(x_i(t), \copyright) = \copyright$ if $x_i(t) \in \Omega_i^{in}$ or $x_i(t) \in \Omega_i^{bo}$ with $\max_{\vartheta\in\overline{NC}_{\Omega_i}(x_i(t))} \copyright^T\vartheta \leq$

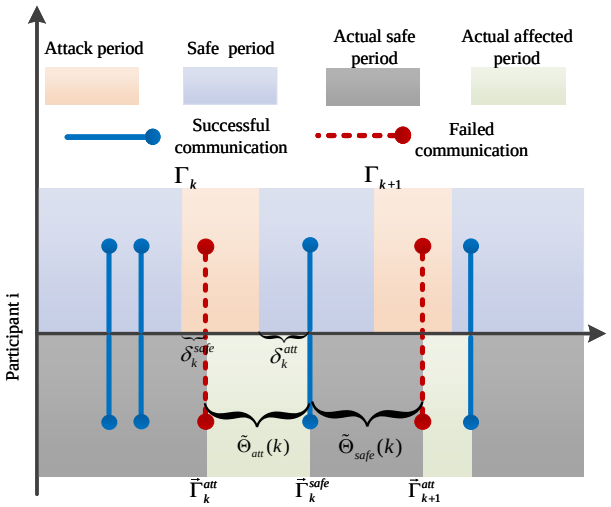

Fig. 1. Triggering sequence and attack sequence.

0); 2) $\Upsilon_{\Omega_i}(x_i(t), ©) = © - ©^T\vartheta^*\vartheta^*$ if $x_i(t) \in \Omega_i^{bo}$ with $\max_{\vartheta \in \overline{NC}_{\Omega_i}(x_i(t))} ©^T\vartheta \geq 0$, where $\vartheta^* = \arg\max_{\vartheta \in \overline{NC}_{\Omega_i}(x_i(t))} ©^T\vartheta$.

The major functionality of Lemma 1 is to make the differentiated projection show in explicit form. In this sense, it is significant to reduce the complexity of theoretical analysis.

C. DoS Attacks Model

Due to the presence of the adversaries, the communication network cannot always maintain secure. In this paper, we employ event-triggered communication strategy to achieve the information sharing among DGs. Each DG only needs to exchange information with its neighbors at discrete-time when necessary only. The adversaries are intended to affect the timeliness of information transmission, resulting in packet losses. As shown in Fig. 1, we let Γ_k represent the time sequence when kth attack is launched. The duration of each attack is denoted as Δ_k. It also means that the system suffers from DoS attack during $[\Gamma_k, \Gamma_k + \Delta_k)$. Then, the adversaries will go to sleep to accumulate energy for the next attack. The total time $[t_0, t)$ can be partitioned into attack period and safe period, denoted as $\Xi_{att}(t_0, t) = \cup\Theta_{att}(k) \cap [t_0, t)$ and $\Xi_{safe}(t_0, t) = \cup\Theta_{safe}(k) \cap [t_0, t)$, respectively. Therein, $\Theta_{att}(k) = [\Gamma_k, \Gamma_k + \Delta_k)$ and $\Theta_{safe}(k) = [\Gamma_k + \Delta_k, \Gamma_{k+1})$.

It is worth noting that the attack frequency and attack duration are the major influence factors to reflect the DoS attacks. This following well-used assumptions are imposed on the attack frequency and attack duration.

Assumption 1 (DoS frequency [38]): For any $t \geq t_0 \geq 0$, there exist positive integer N_0 and $\wp > 0$ satisfying

$$N(t_0, t) \leq N_0 + \wp(t - t_0), \tag{9}$$

where $N(t_0, t)$ is the total number of the DoS attacks.

Assumption 2 (DoS duration [38]): For any $t \geq t_0 \geq 0$, there exist $\mathcal{T}_0$ and $1 > \zeta > 0$ satisfying

$$\Xi_{att}(t_0, t) \leq \mathcal{T}_0 + \zeta(t - t_0). \tag{10}$$

Moreover, the adversaries destroy the system dynamics by tampering the triggering information. To clearly distinguish the attack sequence and triggering sequence, the coalescent triggering sequence for all participants is denoted as $\{T_{\tilde{m}}\} = \{t_i^m | \forall i \in \mathbb{V}\}$, where t_i^m represents mth triggering time of ith participant. We order $T_0 < T_1 <, \cdots, < T_{\tilde{m}}, \cdots$. Based on the aforementioned definition, it is not very difficult to verify that at least one DG is triggered at any $T_{\tilde{m}}$; meanwhile, no DG is triggered during $(T_{\tilde{m}-1}, T_{\tilde{m}})$. It can be seen from Fig. 1, DG i is needed to be triggered at the point of the red dotted line. However, it is failed since this time belongs to the attack period. A successful attack implies that at least of one triggering action is failed during the attack duration time caused by the DoS attacks. In this paper, we consider the worst case that every launched attack is a successful attack. In fact, the dwell time of kth successful attack may be not the same as the actual affected duration time, since there may exist a time interval δ_k^{att} to do the next information exchange after the attack is ended. Meanwhile, the actual safe duration time may not be the same as the defined safe period. For example, the time interval between the stating of kth attack and the latest attempt of triggering, i.e, δ_k^{safe} is safe in theory. Their relationship is shown in Fig. 1. To avoid misunderstanding, we let $\vec{\Gamma}_k^{att}$ and $\vec{\Gamma}_k^{safe}$ represent the starting time of the actual attack effect and the recovery of safe operation. On the basis, we further define $\vec{\Theta}_{att}(k) = [\vec{\Gamma}_k^{att}, \vec{\Gamma}_k^{safe})$ and $\vec{\Theta}_{safe}(k) = [\vec{\Gamma}_k^{safe}, \vec{\Gamma}_{k+1}^{att})$. Similarly, we define $\vec{\Xi}_{att}(t_0, t) = \cup\vec{\Theta}_{att}(k) \cap [t_0, t)$ and $\vec{\Xi}_{safe}(t_0, t) = \cup\vec{\Theta}_{safe}(k) \cap [t_0, t)$ as the actual safe period and actual affected period, respectively.

III. Hybrid-Triggering Based Distributed Secure Dispatch Strategy

A. Algorithm Design

In this section, a distributed secure dispatch strategy is presented to mitigate the effect of the DoS attacks under unreliable communication network environment. The designed method is designed by using switched system dynamics along with hybrid-triggering communication strategy. The mathematical expression of the switched-system dynamics is designed as

$$\dot{y}_i(t) = \begin{cases} D(y_i(t))_{safe} & t \in \vec{\Theta}_{safe}(k) \quad (11) \\ D(y_i(t))_{att} & t \in \vec{\Theta}_{att}(k) \quad (12) \end{cases}$$

with

$$D(y_i(t))_{safe} = \begin{bmatrix} \Upsilon_{\Omega_i}(x_i(t), -\nabla f_i(x_i(t)) + v_i(t_i^m)) \\ q_i^1(t_i^m) + q_i^2(t_i^m) - x_i(t) + \jmath_i(t) \\ -q_i^1(t_i^m) \\ -\hbar_i^1\tau_i(t) + \hbar_i^2\mathcal{F}_i \end{bmatrix}, \tag{13}$$

$$D(y_i(t))_{att} = \varrho \begin{bmatrix} \Upsilon_{\Omega_i}(x_i(t), -\nabla f_i(x_i(t)) + v_i(t_i^s)) \\ q_i^1(t_i^s) + q_i^2(t_i^s) - x_i(t) + \jmath_i(t) \\ -q_i^1(t_i^s) \\ 0 \end{bmatrix}, \tag{14}$$

$$\mathcal{F}_i = -\hbar_i^3||v_i(t_i^m) - v_i(t)||^2 - \hbar_i^4||w_i(t_i^m) - w_i(t)||^2 + \frac{1}{4}\sum_{i\in\mathcal{N}_i} a_{ij}||v_i(t_i^m) - v_j(t_j^m)||^2, \quad (15)$$

where $0 < \varrho < 1$; $\hbar_i^1$, $\hbar_i^2$, $\hbar_i^3$ and $\hbar_i^4$ are positive parameters needed to be designed; $y_i(t) = [x_i(t), v_i(t), w_i(t), \tau_i(t)]^T$ is the cascade of all variables. Therein, $v_i(t)$ and $w_i(t)$ are Lagrangian dual variables assisted in the calculation of the global optimal solution. Meanwhile, $\tau_i(t)$ is the extra dynamic variable used for the design of event-triggered strategy. As easier discussions, the DoS attacks will cause the failure of communication exchange. To make a clear distinction, we specify t_i^s to represent the last successful transmission attempt of ith DG with its neighbors before the system is subject to DoS attacks. $q_i^1(t_i^m)$, $q_i^2(t_i^m)$, $q_i^1(t_i^s)$ and $q_i^2(t_i^s)$ are the combined measurements of the sharing information. As shown in (13-14), each DG only needs to know it local load information $\jmath_i(t)$ that does not need to be sent to other DGs. Thus, our proposed algorithm is capable of protecting the load information well.

Apart from the design of system dynamics, how to reasonably design the communication strategy to resist the DoS attacks while occupying as little communication resources as possible is another critical issue. Based on the communication network environment, this paper focuses on designing hybrid-triggering communication strategy to address this issue, which includes the following two parts:

1) Communication strategy during actual safe period. For $t \in \vec{\Theta}_{safe}(k)$, each DG is able to share the information with its neighbors successfully at triggering time. In this scenario, the combined measurements is set as

$$q_i^1(t_i^m) = -\sum_{j\in\mathcal{N}_i} a_{ij}\big(v_i(t_i^m) - v_j(t_j^m)\big), \quad (16)$$

$$q_i^2(t_i^m) = -\sum_{j\in\mathcal{N}_i} a_{ij}\big(w_i(t_i^m) - w_j(t_j^m)\big). \quad (17)$$

Along with (13, 15-17), the dynamic event-triggering mechanism is developed to reduce the communication interaction among DGs such that the communication expenditure can be reduced accordingly. The triggering function is designed as

$$\mathcal{C}(v_i, w_i) = \hbar_i^5(\hbar_i^3||v_i(t_i^m) - v_i(t)||^2 + \hbar_i^4||w_i(t_i^m) - w_i(t)||^2 - \frac{1}{4}\sum_{j\in\mathcal{N}_i} a_{ij}||v_i(t_i^m) - v_j(t_j^m)||^2) - \tau_i(t). \quad (18)$$

where $\hbar_i^5 > 0$.

Based on (18), the next triggering time is determined by

$$t_i^{m+1} = \max\{t \geq t_i^m | \mathcal{C}(v_i, w_i) \leq 0\}, \quad (19)$$

which implies that an event is triggered once $\mathcal{C}(v_i, w_i) > 0$.

2) Communication strategy during actual affected period. For $t \in \vec{\Theta}_{att}(k)$, each DG can not exchange information with its neighbors. Each DG makes use of the last received information to estimate combined measurements. Thus, for $t \in \vec{\Theta}_{att}(k)$, we set

$$q_i^1(t_i^s) = -\sum_{j\in\mathcal{N}_i} a_{ij}\big(v_i(t_i^s) - v_j(t_j^s)\big), \quad (20)$$

$$q_i^2(t_i^s) = -\sum_{j\in\mathcal{N}_i} a_{ij}\big(w_i(t_i^s) - w_j(t_j^s)\big). \quad (21)$$

Although the estimated values mentioned above are employed in (14) to mitigate the impact of cyber attacks, it is very difficult to completely eliminate the impact of attacks. Thus, for each DG, it is needed to restore the communication interaction with its neighbors as soon as possible. In other word, we hope that δ_k^{att} is as small as possible with controllable fashion. It is worth noting that the functionality of the dynamic event-triggering strategy may be failure during $t \in \vec{\Theta}_{att}(k)$. If (18) is also employed, we cannot always ensure $\mathcal{C}(v_i, w_i) \leq 0$. Meanwhile, the maximum value of δ_k^{att} is difficult to be estimated. To this aim, the dynamic event-triggering is switched to the virtual periodic-triggering strategy, i.e.,

$$t_i^{m+1} = t_i^m + \Delta\mathcal{T}, \quad (22)$$

where $\Delta\mathcal{T}$ represents the preset time step size.

By implementing (22), each DG will try to establish communication with its neighbors every $\Delta\mathcal{T}$ time period until the DoS attacks are ended. In this way, it is not very difficult to verify that the maximum value of δ_k^{att} is equal to $\Delta\mathcal{T}$. Once the communication link is successfully established, the periodic communication strategy will be switched back to dynamic event-triggering strategy. Then, the system will go back to the actual safe period. Unlike (19), the considered periodic-triggering mechanism is only successful triggered once for each attack. It is more like a virtual operation behavior. Thus, we call it virtual periodic-triggering strategy.

Based on the aforementioned design, the flowchart of the proposed method is shown in Fig. 2. It should be noted that each agent judges the utilization of different system dynamics based on the communication conditions. As shown in Fig. 2, each agent performs dynamics (11), if communication is successful. Otherwise, it performs dynamics (12). Moreover, the major functionalities and benefits of each part of the proposed method are summarized as follows.

Firstly, the dynamics of $\dot{x}_i(t)$, $\dot{v}_i(t)$ and $\dot{w}_i(t)$ in (11, 12) are cooperated to calculate the global optimal solutions without any limitation for initialization. Therein, $v_i(t)$ and $w_i(t)$ are shared variables. By making use of consensus protocols (e.g., (16) and (17)), each DG only needs to exchange the information of $v_i(t_i^m)$ and $w_i(t_i^m)$ with its neighbors at discrete time to achieve distributed calculation, resulting in better privacy and feasibility.

Secondly, the dynamics of $\dot{\tau}_i(t)$ is employ to generate a positive $\tau_i(t)$. Since the dynamic triggering strategy is out of work during $[\vec{\Gamma}_k^{att}, \vec{\Gamma}_k^{safe})$, $\dot{\tau}_i(t)$ is switched to zero during this period. Combining with (11), (12), (18) and (19), it can be obtained that

$$\dot{\tau}_i(t) \geq -(\hbar_i^1 + \frac{\hbar_i^2}{\hbar_i^5})\tau_i(t), \quad \forall t \in \vec{\Theta}_{safe}(k) \quad (23)$$

$$\dot{\tau}_i(t) = 0. \quad \forall t \in \vec{\Theta}_{att}(k) \quad (24)$$

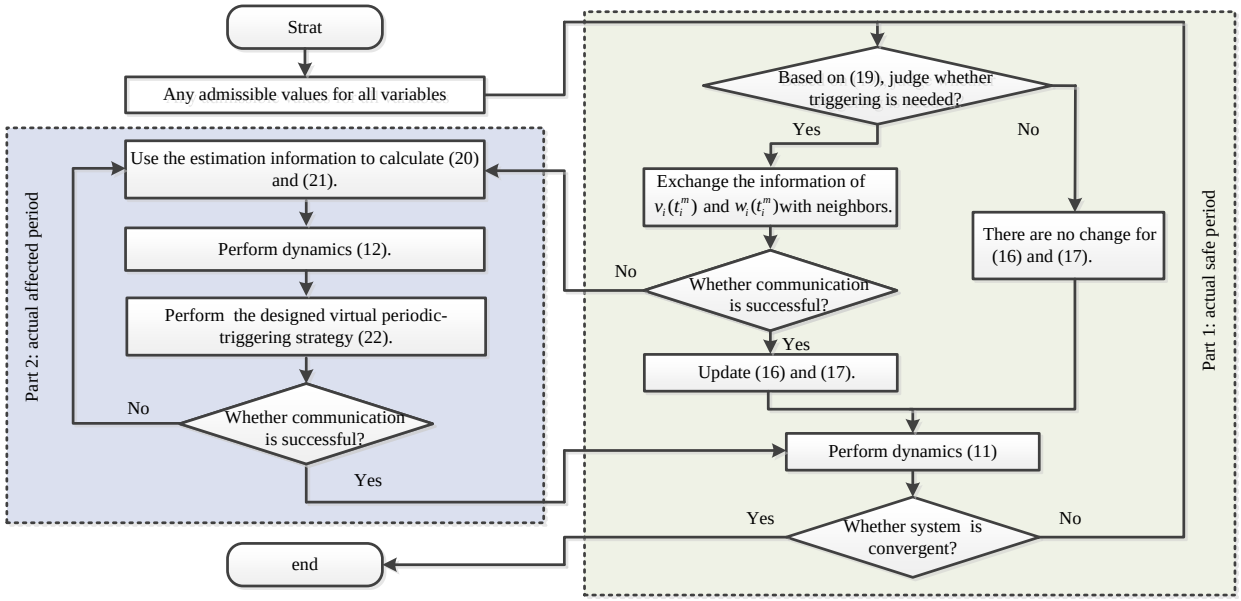

Fig. 2. Flowchart of the proposed distributed secure dispatch strategy.

By choosing any $\tau_i(0) > 0$, we can always ensure that $\tau_i(t) > 0$ and

$$\tau_i(t) \geq \tau_i(\vec{\Gamma}_k^{safe})\exp^{-(\hbar_i^1+\frac{\hbar_i^2}{\hbar_i^5})t}, \forall t \in [\vec{\Gamma}_k^{safe}, \vec{\Gamma}_{k+1}^{att}). \quad (25)$$

Of note, $\tau_i(t)$ is used to design the triggering function (18). Since $\tau_i(t) > 0$, the dynamic trigging strategy can enlarge the inter-event time interval i.e., $\{t_i^{m+1} - t_i^m | m = 1, 2, , \cdots\}$ when compared to the static one with $\tau_i(t) = 0$.

Last but not the least, different from (13), a small gain ϱ is set in (14). In fact, although we design the dynamic event-triggering mechanism to increase the inter-event time interval as larger as possible, there still may exist a margin, denoted as $\flat_i^m(t)$, to reach the limit value. It means that the system may maintain the convergence within a short period of time although the triggering is failure. Motivated by this inspiration, we design the small gain along with the estimations (i.e., (20) and (21)) to slow down the safe evolution of system dynamics during $t \in [\vec{\Gamma}_k^{att}, \vec{\Gamma}_k^{safe})$. In this way, $\flat_i^m(t)$ is indirectly enlarged such that the effect of the DoS attacks can be mitigated.

Remark 3: Distinguished from previous studies for smart grid with consideration of cyberattacks [30]–[37], the main advantages of our proposed approach are illustrated as follows. Firstly, different from [30]–[36], our proposed method is initialization-free and do not need the hypothesis that the communication is connected during attack period. In addition, our proposed method is suitable for solving common distributed optimization problem with the form as shown in (5-7). However, literature [30]–[36] are established based on lambda-iteration algorithms, which are mainly suitable for solving quadratic-form optimization problem. Thus, our proposed method processes better robustness and expansibility with relaxed conditions than [30]–[36]. Secondly, the method presented in [37] is mainly used to analyze the effect of DoS attacks, but not design resilient mechanism. In this paper, we aim at co-designing switched system and hybrid-triggering strategy to resist the DoS attacks, which possesses better practical significance. Finally, literature [30]–[37] are built upon fully periodic or continuous communication strategy. Different from them, our paper takes advantages of dynamic event-triggering mechanism, which can effectively reduce the communication costs, hold longer inter-event time, and possess better flexibility, etc.

Remark 4: Like [34], the proposed algorithm belongs to a kind of gradient-based method, which possesses the computational complexity with $O(\aleph^2)$. Therein, $\aleph$ refers to the dimensionality of x_i. The computational complexity of the Newton-based methods, e.g., [16], [37], is $O(\aleph^3)$. Thus, the computational complexity of the proposed method is lower than those Newton-based methods [16], [37] , which is beneficial for reducing computation burden.

Remark 5: It is a very significant research to estimate the convergence time upper bound of distributed algorithms, as those work proposed in [19], [20]. The integration of fixed time or finite time consensus protocols could be an effective way to expand our proposed approach with the capability of estimating the convergence time upper bound. This case is beyond the scope of our research, which will be investigated in future work.

B. Optimality and Convergence Analysis

In order to analyze the optimality and convergence of the proposed method under the designed hybrid-triggering communication strategy, we first analyze its performances during the actual safe period and the actual affected period. The corresponding theoretical results are provided in Lemma 2 and Lemma 3, respectively. Then, the main results are provided in Theorem 1.

To be specific, we first consider the case for each $t \in$

$\vec{\Theta}_{safe}(k)$. According to (11), it can be obtained that

$$\dot{X}(t) = \Upsilon_{\Omega}(X(t), -\nabla f(X(t)) + V(t^m)); \tag{26}$$
$$\dot{V}(t) = -LV(t^m) - LW(t^m) - X(t) + \jmath(t); \tag{27}$$
$$\dot{W}(t) = LV(t^m); \tag{28}$$
$$\dot{\tau}(t) = \hbar^1\tau(t) + \hbar^2\mathcal{F}, \tag{29}$$

where $\Omega = \cup\Omega_i$ refers to the Cartesian product of the set of Ω_i. $X(t)$, $V(t)$, $W(t)$, $\jmath(t)$, $V(t^m)$, $W(t^m)$, $\nabla f(X(t))$, $\tau(t)$ and $\mathcal{F}$ are the column vector forms of $x_i(t)$, $v_i(t)$, $w_i(t)$, $\jmath_i(t)$ $v_i(t_i^m))$, $w_i(t_i^m))$, $\nabla f_i(x_i(t))$, $\tau_i(t)$ and $\mathcal{F}_i$, respectively; $\hbar^1 = \text{diag}\{\hbar_i^1\}$; $\hbar^2 = \text{diag}\{\hbar_i^2\}$.

We further choose $r = \frac{1_n}{\sqrt{n}}$, $R \in \mathcal{R}^{n\times(n-1)}$, $r^T R = 0_n^T$, $R^T R = I_{n-1}$ and $RR^T = I_n - \frac{1}{n}1_n 1_n^T$. Then, we employ the following change of variables:

$$\mathcal{X}(t) = X(t) - X^*, \quad \theta(t) = [r, R]^T\mathcal{X}(t), \tag{30}$$
$$\mathcal{V}(t) = V(t) - V^*, \quad \eta(t) = [r, R]^T\mathcal{V}(t), \tag{31}$$
$$\mathcal{W}(t) = W(t) - W^*, \quad \delta(t) = [r, R]^T\mathcal{W}(t), \tag{32}$$
$$e(t) = \eta(t^m) - \eta(t), z(t) = \delta(t^m) - \delta(t), \tag{33}$$

where symbol "$*$" represents the equilibrium point. To facilitate the analysis, we further partition the changed variables as $\theta(t) = \text{col}(\theta_1(t), \theta_{2:n}(t))$, $\eta(t) = \text{col}(\eta_1(t), \eta_{2:n}(t))$, $\delta(t) = \text{col}(\delta_1(t), \delta_{2:n}(t))$, $e(t) = \text{col}(e_1(t), e_{2:n}(t))$ and $z(t) = \text{col}(z_1(t), z_{2:n}(t))$.

It can be derived from Lemma 1 that

$$\Upsilon_{\Omega_i}(x_i(t), -\nabla f_i(x_i(t)) + v_i(t_i^m)) = -\nabla f_i(x_i(t)) + v_i(t_i^m) - \beta_i(x_i(t))\varpi_i(x_i(t)), \tag{34}$$

where $\beta_i(x_i(t)) \geq 0$ and $\varpi_i(x_i(t)) \in \overline{NC}_{\Omega_i}(x_i(t))$.

Next, according to (26-34), we can obtain that

$$\dot{\theta}_1(t) = -r^T h + e_1(t) + \eta_1(t); \tag{35}$$
$$\theta_{2:n}(t) = -R^T h + e_{2:n}(t) + \eta_{2:n}(t); \tag{36}$$
$$\dot{\eta}_1(t) = -\theta_1(t); \tag{37}$$
$$\dot{\eta}_{2:n}(t) = -\theta_{2:n}(t) - R^T LR(\eta_{2:n}(t) + e_{2:n}(t)) \tag{38}$$
$$- R^T LR(\delta_{2:n}(t) + z_{2:n}(t)); \tag{39}$$
$$\dot{\delta}_1(t) = 0; \tag{40}$$
$$\dot{\delta}_{2:n}(t) = R^T LR(\eta_{2:n}(t) + e_{2:n}(t)); \tag{41}$$
$$\dot{\tau}(t) = \hbar^1\tau(t) + \hbar^2\mathcal{F}, \tag{42}$$

where $h = \nabla f(X(t)) - \nabla f(X^*) + \varpi_\Omega(X(t)) - \varpi_\Omega(X^*)$. Therein, $\varpi_\Omega(X(t))$ and $\varpi_\Omega(X^*)$ are the column vector forms of $\beta_i(x_i(t))\varpi_i(x_i(t))$ and $\beta_i(x_i^*(t))\varpi_i(x_i^*(t))$, respectively.

We consider the following candidate Lyapunov function

$$\mathbb{V}(t) = \mathbb{V}_1(t) + \mathbb{V}_2(t), \tag{43}$$

where

$$\mathbb{V}_1(t) = \frac{1}{2}a_1(||\theta(t)||^2 + ||\eta(t)||^2 + ||\delta(t)||^2) + \frac{1}{2}a_2(||\delta_{2:n}(t)||^2 + ||\eta_{2:n}(t) + \delta_{2:n}(t)||^2), \tag{44}$$
$$\mathbb{V}_2(t) = a_1\sum_i^n \tau_i(t), \tag{45}$$

where $a_1, a_2 > 0$.

The next Lemmas 2 and 3 are employed to exhibit the performances of algorithm (11-12) for any $t \in \vec{\Theta}_{safe}(k)$ and $t \in \vec{\Theta}_{att}(k)$, respectively.

Lemma 2: Suppose that $\mathbb{G}$ is connected during safe period. A set of parameters are chosen as $0 < a_1$, $\frac{\lambda_2 a_1}{3\lambda_2 - 4a_3} < a_2 < \frac{3\lambda_2}{\lambda_2 + 4a_3}$, $0 < a_3 < \min\{\frac{1}{2}\lambda_2, \frac{\sqrt{(\lambda_2\Im_i)^2 + 48\lambda_2\Im_i} - \lambda_2\Im_i}{8\Im_i}\}$, $0 < \hbar_i^1, 0 < \hbar_i^2 < 1$, $\hbar_i^3 = \frac{1}{2\Im_i} + (5 + 4\frac{a_2}{a_1})|\mathcal{N}_i|$, $\hbar_i^4 = (5\frac{a_2}{a_1} + 4)|\mathcal{N}_i|$, $\hbar_i^5 > \frac{1-\hbar_i^2}{\hbar_i^1}$ and $\tau_i(0) > 0$. Then, there exists positive constant φ_1 such that for any $t \in \vec{\Theta}_{safe}(k)$,

$$\mathbb{V}(t) \leq \mathbb{V}(\vec{\Gamma}_k^{safe})\text{exp}\big(-\varphi_1(t - \vec{\Gamma}_k^{safe})\big). \tag{46}$$

Proof: In light of (35-43), it can be obtained that

$$\begin{aligned}\dot{\mathbb{V}}(t) =& -a_1\mathcal{X}^T(t)h + a_1\theta^T(t)e(t) - a_2(\eta_{2:n}^T(t) \\ &+ \delta_{2:n}^T(t))\theta_{2:n}(t) - \frac{1}{2}a_1\eta_{2:n}^T(t)R^T LR\eta_{2:n}(t) \\ &- a_1\eta_{2:n}^T(t)R^T LR\big(\frac{1}{2}\eta_{2:n}(t) + e_{2:n}(t) + z_{2:n}(t)\big) \\ &+ a_1\delta_{2:n}^T(t)e_{2:n}(t) \\ &- \frac{1}{2}a_2\delta_{2:n}^T(t)R^T LR\delta_{2:n}(t) \\ &- a_2\delta_{2:n}^T(t)R^T LR\big(\frac{1}{2}\delta_{2:n}(t) - e_{2:n}(t) + z_{2:n}(t)\big) \\ &- a_2\eta_{2:n}(t)R^T LRz_{2:n}(t) \\ &+ a_1\sum_{i=1}^n \dot{\tau}_i(t).\end{aligned} \tag{47}$$

Combining (8) and the definition of normal cone, we have

$$\mathcal{X}^T(t)h \geq \theta^T(t)\Im\theta(t), \tag{48}$$

where $\Im = \text{diag}\{\Im_i\}$. We let $\Im^{min} = \min\{\Im_i\}$ and $\Im^{max} = \max\{\Im_i\}$.

Since $\mathbb{G}$ is connected, we have $\eta_{2:n}^T(t)R^T LR\eta_{2:n}(t) \geq \lambda_2||\eta(t)||^2$ and $\delta_{2:n}^T(t)R^T LR\delta_{2:n}(t) \geq \lambda_2||\delta(t)||^2$. It follows from (31-33) that

$$\begin{aligned}&-\eta_{2:n}^T(t)R^T LR\big(\frac{1}{2}\eta_{2:n}(t) + e_{2:n}(t)\big) \\ =&\frac{1}{2}\big(V(t^m) - V(t)\big)^T L\big(V(t^m) - V(t)\big) \\ &-\frac{1}{2}V^T(t^m)LV(t^m) \\ \leq&\sum_{i=1}^n |\mathcal{N}_i| \cdot ||v_i(t_i^m) - v_i(t)||^2 \\ &-\sum_{i=1}^n\sum_{j\in\mathcal{N}_i}\frac{1}{4}a_{ij}||v_i(t_i^m) - v_j(t_j^m)||^2,\end{aligned} \tag{49}$$

$$\begin{aligned}&-\delta_{2:n}^T(t)R^T LR\big(\frac{1}{2}\delta_{2:n}(t) + z_{2:n}(t)\big) \\ \leq&\sum_{i=1}^n |\mathcal{N}_i| \cdot ||w_i(t_i^m) - w_i(t)||^2.\end{aligned} \tag{50}$$

In addition, we have the following fact that

$$(\eta_{2:n}^T(t)+\delta_{2:n}^T(t))\theta_{2:n}(t)\le\frac{1}{2a_3}||\theta_{2:n}(t)||^2 + \frac{a_3}{2}(||\eta_{2:n}(t)||^2+||\delta_{2:n}(t)||^2), \tag{51}$$

$$\theta^T(t)e(t)\le\frac{1}{2}\theta^T(t)\Im\theta(t) + \sum_{i=1}^{n}\sum_{j\in\mathcal{N}_i}\frac{1}{2\Im_i}||v_i(t_i^m)-v_i(t)||^2, \tag{52}$$

$$\eta_{2:n}^T(t)R^TLRz_{2:n}(t)\le\frac{1}{8}\eta_{2:n}^T(t)R^TLR\eta_{2:n}(t) + \sum_{i=1}^{n}4|\mathcal{N}_i|\cdot||w_i(t_i^m)-w_i(t)||^2, \tag{53}$$

$$\delta_{2:n}^T(t)R^TLRe_{2:n}(t)\le\frac{1}{8}\delta_{2:n}^T(t)R^TLR\delta_{2:n}(t) + \sum_{i=1}^{n}4|\mathcal{N}_i|\cdot||v_i(t_i^m)-v_i(t)||^2. \tag{54}$$

Based on the aforementioned analysis and the defined triggering condition, we can further obtain that

$$\begin{aligned}\mathbb{V}(t)\le&-\frac{1}{2}\theta^T(t)(a_1\Im-\frac{a_2}{a_3})\theta(t)\\&-\big((\frac{3}{8}a_1-\frac{1}{8}a_2)\lambda_2-\frac{a_2a_3}{2}\big)||\eta(t)||^2\\&-\big((\frac{3}{8}a_2-\frac{1}{8}a_1)\lambda_2-\frac{a_2a_3}{2}\big)||\delta(t)||^2\\&-a_1\sum_{i=1}^{n}(\hbar_i^1-\frac{1-\hbar_i^2}{\hbar_i^5})\tau_i(t).\end{aligned} \tag{55}$$

We choose $a_4=\min\{\frac{1}{2}(a_1\Im^{min}-\frac{a_2}{a_3}),(\frac{3}{8}a_1-\frac{1}{8}a_2)\lambda_2-\frac{a_2a_3}{2},(\frac{3}{8}a_2-\frac{1}{8}a_1)\lambda_2-\frac{a_2a_3}{2}\}$ and $a_5=\min\{\hbar_i^1-\frac{1-\hbar_i^2}{\hbar_i^5}\}$. In light of (44), (45) and (55), we can get

$$\begin{aligned}\dot{\mathbb{V}}(t)\le&-\frac{a_4}{0.5a_1+a_2}\mathbb{V}_1(t)-a_1a_5\mathbb{V}_2(t)\\\le&-\varphi_1\mathbb{V}(t),\end{aligned} \tag{56}$$

where $\varphi_1=\min\{\frac{a_4}{0.5a_1+a_2},a_1a_5\}$. Thus, $t\in\vec{\Theta}_{safe}(k)$, we can get (46). The proof is thus completed.

Lemma 3: There exists positive constant φ_2 such that for any $t\in\vec{\Theta}_{att}(k)$,

$$\mathbb{V}(t)\le\mathbb{V}(\vec{\Gamma}_k^{att})\text{exp}\big(\varphi_2(t-\vec{\Gamma}_k^{safe})\big). \tag{57}$$

Proof: The change of variables as shown in (30-32) are employed. In addition, we let

$$\check{e}(t)=\eta(t^s)-\eta(t),\check{z}(t)=\delta(t^s)-\delta(t). \tag{58}$$

Then, we can get

$$\dot{\theta}_1(t)=\varrho\big(-r^Th+\check{e}_1(t)+\eta_1(t)\big); \tag{59}$$

$$\theta_{2:n}(t)=\varrho\big(-R^Th+\check{e}_{2:n}(t)+\eta_{2:n}(t)\big); \tag{60}$$

$$\dot{\eta}_1(t)=-\varrho\theta_1(t); \tag{61}$$

$$\dot{\eta}_{2:n}(t)=\varrho\big(-\theta_{2:n}(t)-R^TLR(\eta_{2:n}(t)+\check{e}_{2:n}(t)) \tag{62}$$

$$-R^TLR(\delta_{2:n}(t)+\check{z}_{2:n}(t))\big); \tag{63}$$

$$\dot{\delta}_1(t)=0; \tag{64}$$

$$\dot{\delta}_{2:n}(t)=\varrho\big(R^TLR(\eta_{2:n}(t)+\check{e}_{2:n}(t))\big). \tag{65}$$

The Lyapunov function (43) is utilized. Then,

$$\begin{aligned}\mathbb{V}(t)\le&-\frac{1}{2}\varrho\theta^T(t)(a_1\Im-\frac{a_2}{a_3})\theta(t)\\&-\varrho\big((\frac{3}{8}a_1-\frac{1}{8}a_2)\lambda_2-\frac{a_2a_3}{2}\big)||\eta(t)||^2\\&-\varrho\big((\frac{3}{8}a_2-\frac{1}{8}a_1)\lambda_2-\frac{a_2a_3}{2}\big)||\delta(t)||^2\\&+\varrho a_1\sum_{i=1}^{n}\hbar_i^3||v_i(t_i^s)-v_i(\vec{\Gamma}_k^{att})\\&+v_i(\vec{\Gamma}_k^{att})-v_i(t)||^2\\&+\varrho a_1\sum_{i=1}^{n}\hbar_i^4||w_i(t_i^s)-w_i(\vec{\Gamma}_k^{att})\\&+w_i(\vec{\Gamma}_k^{att})-w_i(t)||^2\\&-\varrho a_1\sum_{i=1}^{n}\sum_{i\in\mathcal{N}_i}\frac{1}{4}a_{ij}||v_i(t_i^s)-v_j(t_j^s)||^2\\\le&-\varrho\frac{1}{2}\theta^T(t)(a_1\Im-\frac{a_2}{a_3})\theta(t)\\&-\varrho\big((\frac{3}{8}a_1-\frac{1}{8}a_2)\lambda_2-\frac{a_2a_3}{2}\big)||\eta(t)||^2\\&-\varrho\big((\frac{3}{8}a_2-\frac{1}{8}a_1)\lambda_2-\frac{a_2a_3}{2}\big)||\delta(t)||^2\\&+\varrho a_1\sum_{i=1}^{n}\hbar_i^3||v_i(t_i^s)-v_i(\vec{\Gamma}_k^{att})||^2\\&+\varrho a_1\sum_{i=1}^{n}\hbar_i^4||w_i(t_i^s)-w_i(\vec{\Gamma}_k^{att})||^2\\&-\varrho a_1\sum_{i=1}^{n}\sum_{i\in\mathcal{N}_i}\frac{1}{4}a_{ij}||v_i(t_i^s)-v_j(t_j^s)||^2\\&+\varrho a_1\hbar_i^{3,max}||\eta(\vec{\Gamma}_k^{att})||^2+\varrho a_1\hbar_i^{3,max}||\eta(t)||^2\\&+\varrho a_1\hbar_i^{4,max}||\delta(\vec{\Gamma}_k^{att})||^2+\varrho a_1\hbar_i^{4,max}||\delta(t)||^2,\end{aligned} \tag{66}$$

where $\hbar_i^{3,max}=\max\{\hbar_i^3\}$ and $\hbar_i^{4,max}=\max\{\hbar_i^4\}$.

Note that the time $[t_i^s,\vec{\Gamma}_k^{att})$ belongs to $t\in\vec{\Theta}_{safe}(k)$. According to (18) and (19), we have

$$\begin{aligned}&\hbar_i^3||v_i(t_i^s)-v_i(\vec{\Gamma}_k^{att})||^2+\hbar_i^4||w_i(t_i^s)-w_i(\vec{\Gamma}_k^{att})||^2\\&-\sum_{i=1}^{n}\frac{1}{4}a_{ij}||v_i(t_i^s)-v_j(t_j^s)||^2\le\tau_i(\vec{\Gamma}_k^{att}).\end{aligned} \tag{67}$$

Moreover, according to (24), we can get $\tau_i(t)=\tau_i(\vec{\Gamma}_k^{att})$ for $t\in\vec{\Theta}_{att}(k)$. We set $a_6=a_1\hbar_i^{3,max}-(\frac{3}{8}a_1-\frac{1}{8}a_2)\lambda_2-\frac{a_2a_3}{2}\big)$, $a_7=a_1\hbar_i^{4,max}-\big((\frac{3}{8}a_2-\frac{1}{8}a_1)\lambda_2-\frac{a_2a_3}{2}\big)$, $a_8=\max\{\frac{1}{2}(a_1\Im^{max}-\frac{a_2}{a_3}),\frac{1}{2}a_1,a_6,a_7\}$, $a_9=\max\{\frac{1}{2}a_1,a_1\hbar_i^{3,max},a_1\hbar_i^{4,max}\}$ and $\varphi_2=\frac{4\varrho}{a_1}\max\{a_8,a_9\}$. Thus, it can be further derived from (66) that

$$\begin{aligned}\dot{\mathbb{V}}(t)\le&-\frac{1}{2}\varrho\theta^T(t)(a_1\Im-\frac{a_2}{a_3})\theta(t)\\&+\varrho a_6||\eta(t)||^2+\varrho a_7||\delta(t)||^2+\frac{1}{2}\varrho a_1\sum_{i=1}^{n}\tau_i(t)\\&+\varrho a_1\hbar_i^{3,max}||\eta(\vec{\Gamma}_k^{att})||^2+\varrho a_1\hbar_i^{4,max}||\delta(\vec{\Gamma}_k^{att})||^2\end{aligned}$$

$$+\frac{1}{2}\varrho a_1\sum_{i=1}^{n}\tau_i(\vec{\Gamma}_k^{att})$$
$$\leq\varphi_2\max\{\mathbb{V}(t),\mathbb{V}(\vec{\Gamma}_k^{att})\}, \tag{68}$$

which implies that, for any $t\in\vec{\Theta}_{att}(k)$, we can get (57). The proof is thus completed.

Finally, the following Theorem 1 is proposed to validate the global convergence and optimality.

Theorem 1: Let $\mathbb{G}$ be connected during safe period. Assumptions 1 and 2 are satisfied. We consider that the DoS attack frequency and duration satisfying $-\varphi_1+(\varphi_1+\varphi_2)(\zeta+\Delta\mathcal{T}\wp)<0$, where parameters φ_1 and φ_2 are obtained from Lemmas 2 and 3. The implementation of the switched system dynamics (11, 12) with the hybrid-triggering strategy (19, 22) enables each DG exponentially converging to the global optimal solutions.

Proof: We consider the variation of $\mathbb{V}(t)$ during the total time period $[t_0,t]$. According to Lemmas 2 and 3, we have that for $t\in[\vec{\Gamma}_{k-1}^{safe},\vec{\Gamma}_k^{att})$,

$$\begin{aligned}\mathbb{V}(t)\leq&\exp\big(-\varphi_1(t-\vec{\Gamma}_{k-1}^{safe})\big)\mathbb{V}(\vec{\Gamma}_{k-1}^{safe})\\ \leq&\exp\big(-\varphi_1(t-\vec{\Gamma}_{k-1}^{safe})\big)\exp\big(\varphi_2(\vec{\Gamma}_{k-1}^{safe}-\vec{\Gamma}_{k-1}^{att})\big)\mathbb{V}(\vec{\Gamma}_{k-1}^{att})\\ &\cdots\\ \leq&\exp\big(-\varphi_1(t-t_0-\vec{\Xi}_{att}(t_0,t))\\ &+\varphi_2\vec{\Xi}_{att}(t_0,t)\big)\mathbb{V}(t_0).\end{aligned} \tag{69}$$

Similar, for $t\in[\vec{\Gamma}_k^{att},\vec{\Gamma}_k^{safe})$, we have

$$\begin{aligned}\mathbb{V}(t)\leq&\exp\big(\varphi_2(t-\vec{\Gamma}_k^{safe})\big)\mathbb{V}(\vec{\Gamma}_k^{att})\\ \leq&\exp\big(\varphi_2(t-\vec{\Gamma}_k^{safe})\big)\exp\big(-\varphi_1(\vec{\Gamma}_k^{att}-\vec{\Gamma}_{k-1}^{safe})\big)\mathbb{V}(\vec{\Gamma}_{k-1}^{safe})\\ &\cdots\\ \leq&\exp\big(-\varphi_1(t-t_0-\vec{\Xi}_{att}(t_0,t))\\ &+\varphi_2\vec{\Xi}_{att}(t_0,t)\big)\mathbb{V}(t_0).\end{aligned} \tag{70}$$

According to (69) and (70), it can be concluded that $\mathbb{V}(t)\leq\exp\big(-\varphi_1(t-t_0)+(\varphi_1+\varphi_2)\vec{\Xi}_{att}(t_0,t)\big)\mathbb{V}(t_0)$, for $t>t_0$. Note that $\vec{\Theta}_{att}(k)\leq\Theta_{att}(k)+\Delta\mathcal{T}$. Thus, it can be obtained that

$$\vec{\Xi}_{att}(t_0,t)\leq\Xi_{att}(t_0,t)+\Delta\mathcal{T}N(t_0,t). \tag{71}$$

Recalling Assumptions 1 and 2, it follows from (71) that

$$\begin{aligned}\mathbb{V}(t)\leq&\exp\Big(-\varphi_1(t-t_0)+(\varphi_1+\varphi_2)\big(\mathcal{T}_0+\zeta(t-t_0)\\ &+\Delta\mathcal{T}(N_0+\wp(t-t_0))\big)\Big)\mathbb{V}(t_0)\\ \leq&\mathbb{V}(t_0)\exp\big((\varphi_1+\varphi_2)(\mathcal{T}_0+\Delta\mathcal{T}N_0)\big)\exp\Big(-(\varphi_1\\ &-(\varphi_1+\varphi_2)(\zeta+\Delta\mathcal{T}\wp)\big)(t-t_0)\Big).\end{aligned} \tag{72}$$

Since $-\varphi_1+(\varphi_1+\varphi_2)(\zeta+\Delta\mathcal{T}\wp)<0$, the system is exponentially convergent.

Next, in the equilibrium point, it can be obtained that

$$0_n=\Upsilon_\Omega(X^*,-\nabla f(X^*)+V^*); \tag{73}$$
$$0_n=-LV^*-LW^*-X^*+\jmath^*; \tag{74}$$
$$0_n=LV^*. \tag{75}$$

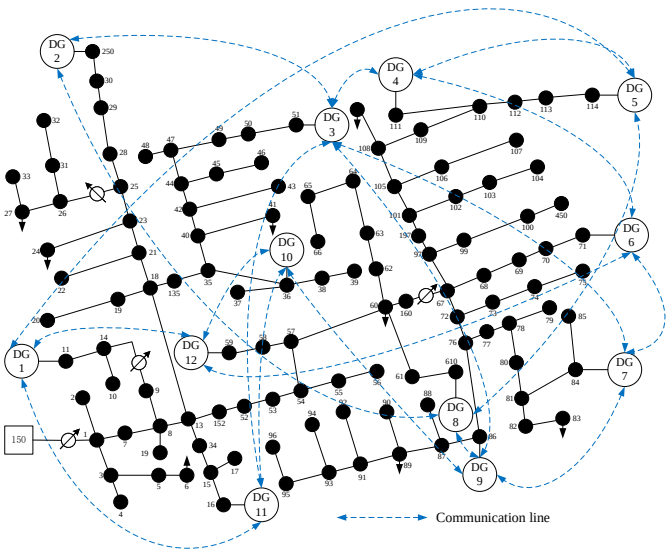

Fig. 3. Physical and original communication topologies of IEEE 123-bus test feeder

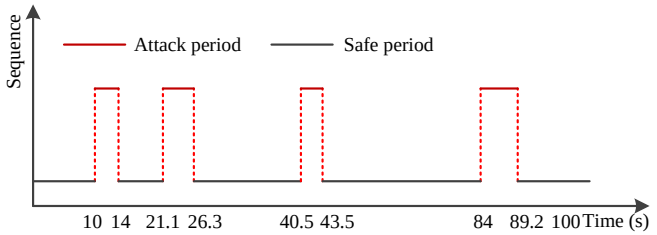

Fig. 4. DoS attack sequence

Recalling the definition of $NC_{\Omega_i}(x_i(t))$, it follows from (73-75) that

$$\sum_{i=1}^{n}x_i^*=\sum_{i=1}^{n}\jmath_i^*, \tag{76}$$
$$v_i^*=v_j^*=v^*,\forall i,j\in\mathbb{V}, \tag{77}$$
$$-\nabla f(x_i^*)+v^*\in NC_{\Omega_i}(x_i^*), \tag{78}$$

which are the Karush-Kuhn-Tucker (KKT) conditions for the studied optimization problems (5-7). It means that the optimality is satisfied.

IV. Simulation Results

In order to verify the effectiveness of the proposed distributed secure dispatch strategy and the correctness of theoretical results, we conduct three case studies on the IEEE 123-bus test feeder with twelve DGs [36]. The physical and original communication network topologies are shown in Fig. 3. Therein, each load bus will sent its load information to its nearest DG. Meanwhile, each DG will collect its local load information. The local loads for DG1 to DG12 are set as $[2.1,1.5,4.3,0.2,1.4,0.7,3.1,0.3,1.2,1.7,2.6,7.3]$MW. The parameters of the cost functions and the constraints are listed in Table I [36]. Therein, the units of κ_i^1, κ_i^2, κ_i^3, κ_i^4, $p_i^{dg,min}$, $p_i^{dg,max}$ and $p_i^{dg,rp}$ are \$/MW^{2}h, \$/MWh, \$/h, \$/MWh, MW, MW and MW, respectively. We consider a randomly

TABLE I
PARAMETERS OF LINE COSTS

No.	κ_i^1	κ_i^2	κ_i^3	κ_i^4	$p_i^{dg,min}$	$p_i^{dg,max}$	$p_i^{dg,rp}$
DG1	0.02	7.88	460	0.1	0	3.0	0.6
DG2	0.01	7.85	510	0.13	0	7.5	1.5
DG3	0.022	7.82	130	0.06	0	4.1	0.82
DG4	0.031	7.8	310	0.09	0	3.2	0.64
DG5	0.045	7.92	500	0	0	0.9	0.18
DG6	0.019	7.87	370	0.1	0	3.4	0.68
DG7	0.012	7.79	210	0.13	0	8.8	1.76
DG8	0.021	7.87	260	0.12	0	2.9	0.58
DG9	0.041	7.81	250	0.1	0	2.3	0.46
DG10	0.029	7.9	170	0.07	0	1.7	0.34
DG11	0.01	7.79	440	0.22	0	9.5	1.9
DG12	0.031	7.85	560	0.11	0	2.4	0.48

TABLE II
POWER GENERATIONS

	DG1	DG2	DG3	DG4	DG5	DG6
Proposed	2.1274	2.2820	4.1000	2.7918	0.9000	2.4094
method	DG7	DG8	DG9	DG10	DG11	DG12
	3.6943	1.7038	1.9219	1.7000	1.0579	1.7102
	DG1	DG2	DG3	DG4	DG5	DG6
ADMM	2.1265	2.2824	4.1000	2.7919	0.9000	2.4095
method	DG7	DG8	DG9	DG10	DG11	DG12
	3.6943	1.7042	1.9221	1.7000	1.0579	1.7103
	DG1	DG2	DG3	DG4	DG5	DG6
PDIP	2.1268	2.2823	4.1000	2.7915	0.9000	2.4094
method	DG7	DG8	DG9	DG10	DG11	DG12
	3.6943	1.7040	1.9219	1.7000	1.0576	1.7101

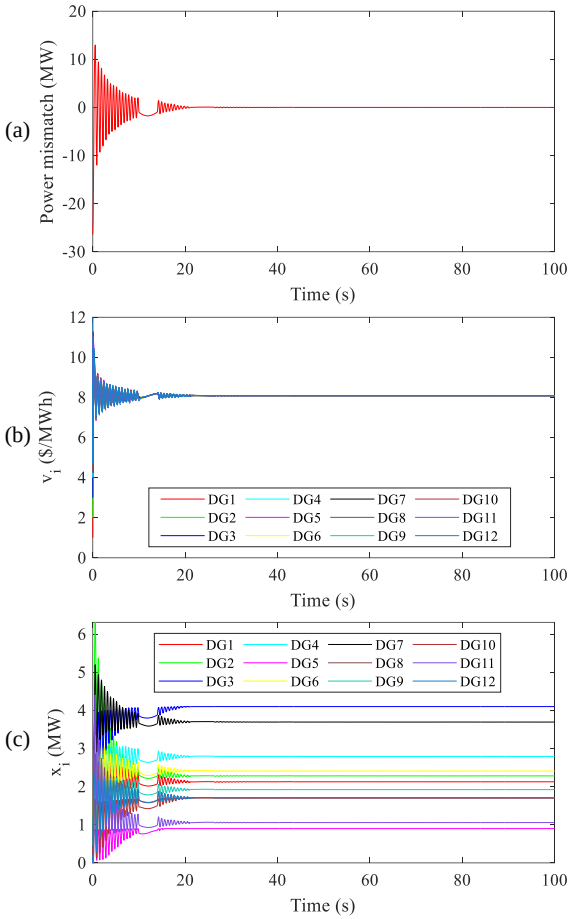

Fig. 5. Simulation results by using the proposed method under DoS attacks: (a) trajectory of power mismatch. (b) trajectory of v_i. (c) trajectory of x_i.

launched DoS attack sequence as shown in Fig. 4, which satisfies $N_0 = 2$, $\wp = 0.1532$, $\mathcal{T}_0 = 6$ and $\zeta = 0.2133$. We set $\triangle\mathcal{T} = 0.02$s. During the arrack period, we consider the worst situation that all DGs are subject to the DoS attacks.

A. Convergence and Optimality Analysis under DoS Attacks

This section mainly focuses on verifying the convergence and optimality of the proposed method under DoS attacks. By implementing the proposed method, the simulation results under the randomly selected attack sequence are shown in Figs. 5(a-c) and 6. To be specific, Fig. 5(a) shows the trajectory of the power mismatch of the global power generations and demands, i.e., $\sum_{i=1}^{n} x_i(t) - \sum_{i=1}^{n} \jmath_i(t)$. It can be seen that the power mismatch gradually converges to zero, which implies that the global supply and demand constraint is satisfied. The estimated power price for each DG, i.e., $v_i(t)$ is shown in Fig. 5(b). Therein, each $v_i(t)$ converges to the same value which is the final power market clearing price. Fig. 5(c) shows the power generations of DGs, each of which goes to stable value with the corresponding operation limits although there exist DoS attacks. Those results from Figs. 5(a-c) show that the KKT conditions are fulfilled, which demonstrates the correctness of Theorem 1. In order to clear see the calculation results, the final converge value of each DG is listed in Table II. Meanwhile, the distributed ADMM method [6] and the primal-dual interior-point (PDIP) method [39] are used to calculate the optimal solution of the same problem without considering the DoS attacks. The calculated results are also listed in Table II. It can be observed that the final calculation results of the three methods are very similar, which verifies the optimality of the proposed method again. Moreover, Fig. 6 shows the triggering instants for the twelve DGs, where the symbol "+" refers to the triggering time. In order to clearly see the triggering instants, we plot the zoomed-in time interval from $26s$ to $32s$. It is shown that each DG performs asynchronous and discrete communication fashion during actual safe periods contributed by the designed dynamic event-triggering mechanism. Meanwhile, driven by the virtual periodic-triggering mechanism, each DG can quickly recover the communication interaction with its neighbors after the DoS attacks end. To sum up, by executing the proposed switched system dynamics with designed hybrid-triggering strategy, each DG can asynchronously obtain its operation although the system is subject to DoS attacks.

B. Comparison Analysis with Distributed Dispatch Method without Resistance Strategy

The section aims to exhibit the better robustness of the proposed method by comparing with a distributed dispatch method without considering resistance strategy. We take two

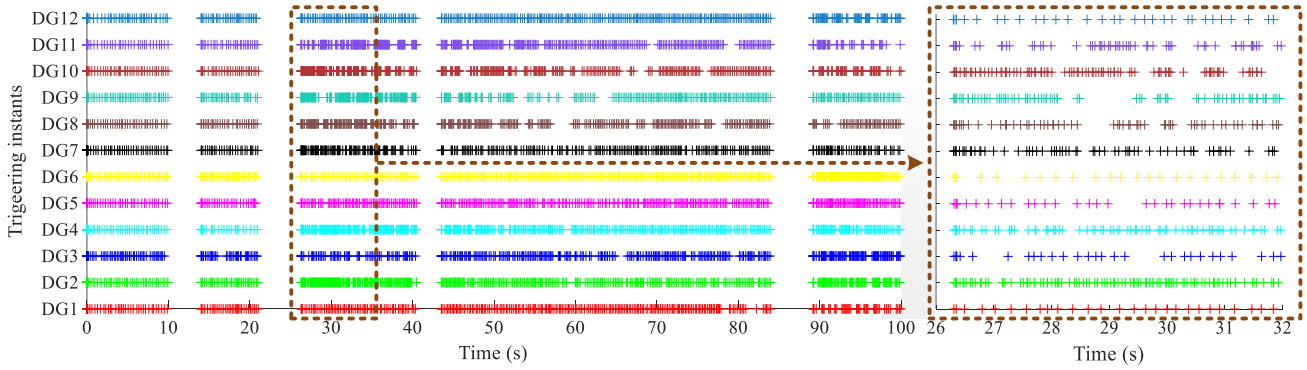

Fig. 6. Triggering sequence.

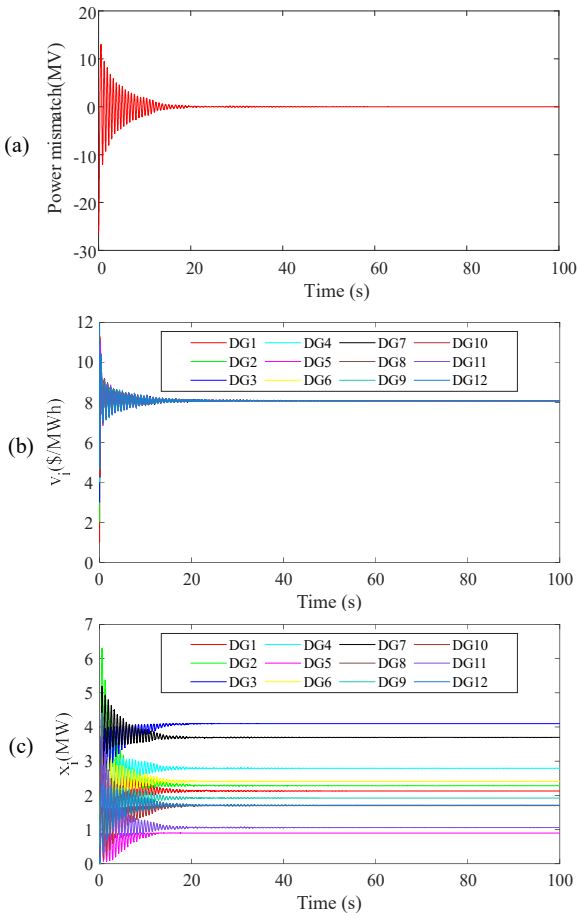

Fig. 7. Simulation results by using the proposed method without DoS attacks: (a) trajectory of power mismatch. (b) trajectory of v_i. (c) trajectory of x_i.

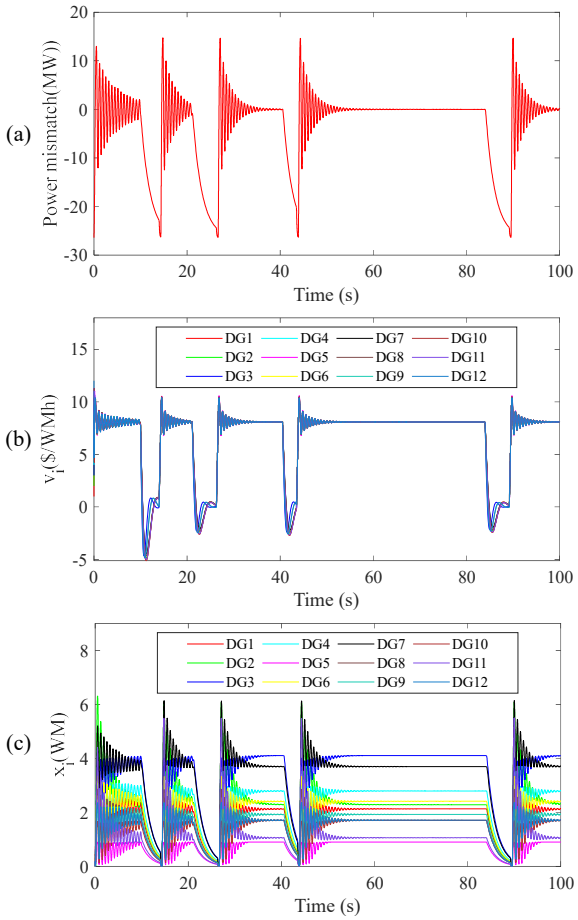

Fig. 8. Simulation results by using the method without resistance strategy under DoS attacks: (a) trajectory of power mismatch. (b) trajectory of v_i. (c) trajectory of x_i.

cases into account. In the fist case, the proposed method works under reliable communication network environment without DoS attacks. In the second case, each DG performs the dynamics $\dot{y}_i(t) = \vec{\Theta}_{safe}(k)$ with the dynamic event-triggering mechanism (19) for all time under the same DoS attack sequence. In this scenario, the proposed method degenerates to the one without any strategy against DoS attacks, which likes the one in [37] but considering the dynamic event-triggering strategy. With the same system parameters, the trajectories of the power mismatch, power generations and power prices for the two cases are depicted in Figs. 7 and 8, respectively. Compared with Figs. 5 and 7, it can be observed that the proposed method enables each DG effectively slowing down the evolution with smooth transition fashion during each actual attack period. This is because we make use of estimations along with switched gain to mitigate the effect of the DoS attacks. With this effort, the convergence process is more like the one without DoS attacks, which processes better robustness. On the contrary, if we do not design resistance

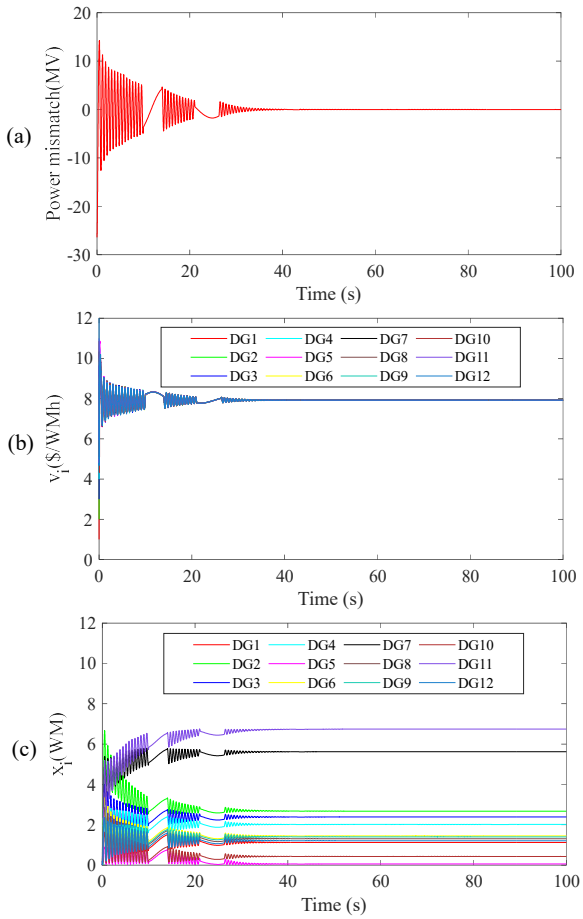

Fig. 9. Simulation results by using the proposed method under DoS attacks for quadratic-form objective function: (a) trajectory of power mismatch. (b) trajectory of v_i. (c) trajectory of x_i.

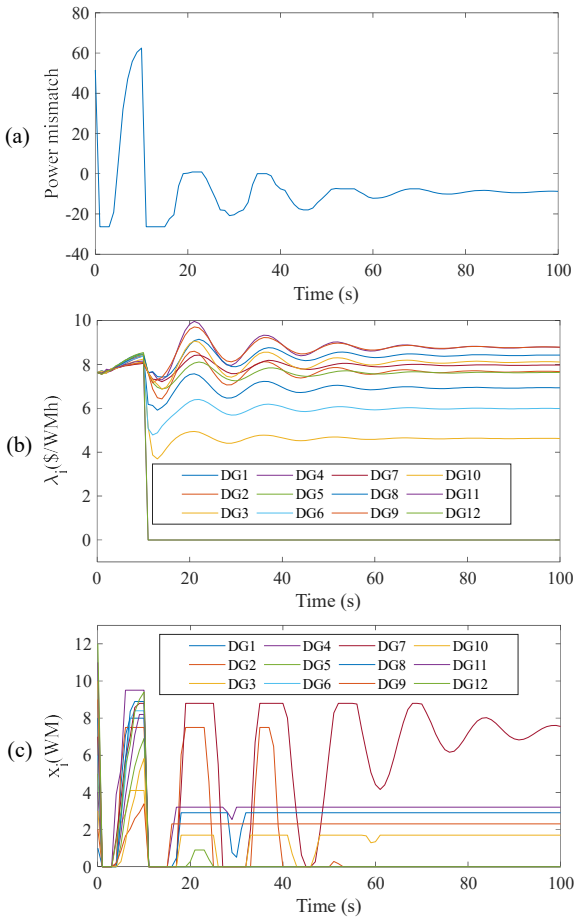

Fig. 10. Simulation results by using the DCDD method under DoS attacks for quadratic-form objective function: (a) trajectory of power mismatch. (b) trajectory of v_i. (c) trajectory of x_i.

mechanism, the trajectories of the estimated power mismatch, power generations and power prices are like those shown in Fig. 8, which is vulnerable to the DoS attacks. Once the DoS attacks occur, the convergence process will be destroyed. The aforementioned analysis results imply that the proposed method can resist the DoS attacks well, which is suitable for solving the EDP under unreliable communication network.

C. Comparison Analysis with Distributed Dispatch Method Considering Resistance Strategy

This section further demonstrates the strong robustness of the proposed method by comparing with a state-of-the-art distributed dispatch method, i,e. the detection-and-correction-based distributed dispatch (DCDD) method [34] that takes the resistance strategy into account. Note that the DCDD method is only suitable for solving EDP with the objective function in quadratic-form. For comparison analysis, we set κ_i^4 to zero; meanwhile, the remaining parameters are unchanged. Then, by performing the proposed method and the DCDD method under the randomly selected attack sequence shown in Fig. 4, the simulation results are reported in Fig. 9 and Fig. 10, respectively. Fig. 9 implies that the proposed method still enables the power mismatch converging to zero, each power generation converging to a stable value, and all estimated power prices converging to a same value. However, it can be observed from Fig. 10 that the DCDD method is sensitive to the DoS attacks, even if the detection and correction strategy is employed to defend the DoS attacks. Specifically, the power generation and demand are unbalanced, and the power generations and power prices fail to converge. This is because the DCDD method works well under the assumption that the communication network is (strongly) connected during attack period. However, in our studied case, the communication network is unconnected during attack period. On the contrary, the proposed method is designed without this assumption, which thus making it of stronger robustness than the DCDD method against DoS attacks.

V. Conclusion

In this paper, we investigate the distributed secure dispatch problem for smart grid under DoS attacks. The actual affected period and actual safe period have been analyzed within the context of discrete and asynchronous communication fashion. Then, a distributed secure dispatch strategy, composed of switched system dynamics and hybrid-triggering mechanism, has been proposed, which holds strong robustness and adaptability to defend the DoS attacks. By implementing the proposed method, each DG can still obtain its optimal operation

although the whole system is subject to malicious DoS attacks. Based on Lyapunov technology, the theoretical analysis results have been presented to verify the global convergence and optimality of the proposed method. Finally, simulation case studies have been provided to demonstrate the effectiveness of the proposed method. In future, we would like to consider both of cyberattacks and fixed/finite time convergence to expand applications of our proposed method.

REFERENCES

[1] W. Chen and T. Li, "Distributed economic dispatch for energy internet based on multiagent consensus control," *IEEE Trans. Autom. Control*, vol. 66, no. 1, pp. 137-152, 2021.

[2] T. Yang, J. George, and J. Qin, et al., "Distributed least squares solver for network linear equations," *Automatica*, vol. 113, pp. 108798, 2020.

[3] Y. Li, T. Li, and H. Zhang, et al., "Distributed resilient double-gradient-descent based energy management strategy for multi-energy system under DoS attacks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2301-2316, 2022.

[4] Z. Deng, "Distributed algorithm design for resource allocation problems of second-order multiagent systems over weight-balanced digraphs," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 6, pp. 3512-3521, 2021.

[5] L. Bai, M. Ye, and C. Sun, et al., "Distributed economic dispatch control via saddle point dynamics and consensus algorithms," *IEEE Trans. Control Syst. Technol.* vol. 27, no. 2, pp. 898-905, 2019.

[6] X. He, Y. Zhao and T. Huang, "Optimizing the dynamic economic dispatch problem by the distributed consensus-based ADMM approach," *IEEE Trans. Ind. Inf.*, vol. 16, no. 5, pp. 3210-3221, 2020.

[7] D. Xu, Q. Wu, and B. Zhou, et al., "Distributed multi-energy operation of coupled electricity, heating, and natural gas networks," *IEEE Trans. Sustain. Energy*, vol. 11, no. 4, pp. 2457-2469, 2020.

[8] S. Chen, L. Zhang, and Z. Yan, et al.,"A distributed and robust security-constrained economic dispatch algorithm based on blockchain," *IEEE Trans. Power Syst.,* vol. 37, no. 1, pp. 691-700, 2022.

[9] M. Zhang, F. Eliassen, and A. Taherkordi, et al.,"Demandresponse games for peer-to-peer energy trading with the hyperledger blockchain," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 1, pp. 19-31, 2022.

[10] S. Yang, S. Tan, and J. Xu, "Consensus based approach for economic dispatch problem in a smart grid," *IEEE Trans. Power Syst.,* vol. 28, no. 4, pp. 4416-4426, 2013.

[11] Y. Yan, Z. Chen, and V. Varadharajan, et al., "Distributed consensus-based economic dispatch in power grids using the paillier cryptosystem," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3493-3502, 2021.

[12] P. Yi, Y. Hong, and F. Liu, "Initialization-free distributed algorithms for optimal resource allocation with feasibility constraints and application to economic dispatch of power systems," *Automatica*, vol. 74, pp. 259-269, 2016.

[13] F. Guo, G. Li, and C. Wen, et al., "An Accelerated distributed gradient-based algorithm for constrained optimization with application to economic dispatch in a large-scale power system," *IEEE Trans. Syst., Man, Cybern., Syst.,* vol. 51, no. 4, pp. 2041-2053, 2021.

[14] Z. Yi, Y. Xu, and J. Hu, et al., "Distributed neurodynamic-based approach for economic dispatch in an integrated energy system," *IEEE Trans. Ind. Inf.*, vol. 16, no. 4, pp. 2245-2257, 2020.

[15] F. Mansoori and E. Wei, "A fast distributed asynchronous Newton-based optimization algorithm," *IEEE Trans. Autom. Control*, vol. 65, no. 7, pp. 2769-2784, 2020.

[16] Y. Li, D. W. Gao, and W. Gao, et al., "A Distributed Double-Newton Descent Algorithm for Cooperative Energy Management of Multiple Energy Bodies in Energy Internet," *IEEE Trans. Ind. Inf.*, vol. 17, no. 9, pp. 5993-6003, 2021.

[17] G. Chen and Z. Zhao, "Delay effects on consensus-based distributed economic dispatch algorithm in microgrid," *IEEE Trans. Power Syst.*, vol. 33, no. 1, pp. 602-612, 2018.

[18] B. Huang, L. Liu, and H. Zhang, et al., "Distributed optimal economic dispatch for microgrids considering communication delays," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1634-1642, 2019.

[19] S. Mao, Z. Dong, and P. Schultz, et al., "A finite-time distributed optimization algorithm for economic dispatch in smart grids," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 4, pp. 2068-2079, 2021.

[20] H. Liu, W. X. Zheng and W. Yu, "Continuous-time algorithms based on finite-time consensus for distributed constrained convex optimization," *IEEE Trans. Autom. Control*, doi: 10.1109/TAC.2021.3079192, 2021.

[21] A. Wang, W. Liu, and T. Dong, et al.,"DisEHPPC: enabling heterogeneous privacy-preserving consensus-based scheme for economic dispatch in smart grids," *IEEE Trans. Cybern.*, doi: 10.1109/TCYB.2020.3027572, 2021.

[22] F. Chen, X. Chen, and L. Xiang, et al.,"Distributed economic dispatch via a predictive scheme: heterogeneous delays and privacy preservation," *Automatica*, vol. 123, no. 109356, 2021.

[23] H. Li, Q. Lu, and X. Liao, et al., "Accelerated convergence algorithm for distributed constrained optimization under time-varying general directed graphs," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 7, pp. 2612-2622, 2020.

[24] L. Liu and G. Yang., "Distributed optimal economic environmental dispatch for microgrids over time-varying directed communication graph," *IEEE Trans. Netw. Sci. Eng.* , vol. 8, no. 2, pp. 1913-1924, 2021.

[25] Y. Li, H. Zhang, and X. Liang, et al., "Event-triggered based distributed cooperative energy management for multi-energy systems," *IEEE Trans. Ind. Inf.*, vol. 15, no. 14, pp. 2008-2022, 2019.

[26] H. Dai, X. Fang, and W. Chen, "Distributed event-triggered algorithms for a class of convex optimization problems over directed networks," *Automatica*, vol. 122, pp. 109256, 2020.

[27] Z. Zuo, X. Cao, and Y. Wang, et al., "Resilient consensus of multiagent systems against denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 4, pp. 2664-2675, 2022.

[28] Y. Yang, Y. Li, and D. Yue, et al., "Distributed secure consensus control with event-triggering for multiagent systems under DoS attacks," *IEEE Trans. Cybern.,* vol. 51, no. 6, pp. 2916-2928, 2021.

[29] F. Fang, J. Li, and Y. Liu, et al., "Resilient control for multiagent systems with a sampled-data model against DoS attacks," *IEEE Trans. Ind. Inf.*, doi: 10.1109/TII.2022.3165687, 2022.

[30] C. Zhao, J. He, and P. Cheng, et al., "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Trans. Ind. Electron*, vol. 64, no. 6, pp. 5107-5117, 2017.

[31] J. Duan, and M. Y. Chow, "A novel data integrity attack on consensus-based distributed energy management algorithm using local information," *IEEE Trans. Ind. Inf.*, vol. 15, no. 3, pp. 1544-1553, 2019.

[32] W. Zeng, Y. Zhang, and M. Y. Chow, "Resilient distributed energy management subject to unexpected misbehaving generation units," *IEEE Trans. Ind. Inf.*, vol. 13, no. 1, pp. 208-216, 2017.

[33] J. Duan, and M. Y. Chow, "A resilient consensus-based distributed energy management algorithm against data integrity attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4729-4740, 2019.

[34] B. Huang, Y. Li, and F. Zhan, et al., "A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks," *IEEE Trans. Ind. Inf.*, vol. 18, no. 2, pp. 880-890, Feb. 2022.

[35] Z. Zhang, D. Yue, and C. Dou, "A robust consensus-based economic dispatch strategy under DoS attack," *in Proc. 2019 IEEE ICPS, Taipei, Taiwan,* pp. 127-132, 2019.

[36] P. Li, Y. Liu, and H. Xin, "A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks," *IEEE Trans. Ind. Inf.*, vol. 14, no. 10, pp. 4343-4352, 2018.

[37] Y. Li, J. Wang, and R. Wang, et al., "A switched Newton-Raphson-based distributed energy management algorithm for multienergy system under persistent DoS attacks," *IEEE Trans. Autom. Sci. Eng.*, doi: 10.1109/TASE.2021.3104393, 2021.

[38] X. Wang, A. R. Teel, and K. Liu, et al., "Stability analysis of distributed convex optimization under persistent attacks: A hybrid systems approach," *Automatica*, vol. 111, pp. 108607, 2020.

[39] AsdS. Wright, "Primal-dual interior-point methods," Philadelphia, PA, USA: SIAM, 1997.

Yushuai Li (M'19) received the B. S. degree in electrical engineering and automation, and the Ph.D. degree in control theory and control engineering from the Northeastern University, Shenyang, China, in 2014 and 2019, respectively. He is currently a Marie Curie Researcher at the Department of Informatics, University of Oslo, Norway. His main research interests include distributed optimization and control, machine learning, digital twin, and their applications in integrated energy and transportation systems.

Rufei Ren received the B.S. degree in automation from China University of Petroleum (East China), Qingdao, China, in 2016, the M.S. degree in Control Engineering from Northeast Electric Power University, China, in 2019, he is currently working toward the doctoral degree in control engineering with Northeastern University, Shenyang, China. His main research interests include distributed control and optimization, edge computing, and multi-energy system.

Bonan Huang received the B.S. degree in electronic information engineering from Tianjin University, Tianjin, China, in 2005, and the M.A.Sc. and Ph.D. degrees in control theory and control engineering from Northeastern University, Shenyang, China, in 2008 and 2014, respectively. He is currently an Associate Professor with the School of Information Science and Engineering, Northeastern University. His research interests include the collaborative control and operation optimization of energy Internet and multienergy systems, and cyber-physical security analysis of smart energy systems.

Rui Wang received the B.S. degree in electrical engineering and automation in 2016 from Northeastern University, Shenyang, China, where he received the Ph.D. degree in power electronics and power drive in 2021. He is a lecturer in with Northeastern University. His research interest focuses on collaborative optimization of distributed generation and its stability analysis of electromagnetic timescale in energy Internet.

Qiuye Sun (M'11-SM'19) received the Ph.D. degree in 2007. He is currently a full Professor with Northeastern University and obtained Special Government Allowances from the State Council in China. He has authored or coauthored over 200 papers, authorized over 100 invention patents, and published over 10 books or textbooks. He is an Associate Editor of IEEE Trans NNLS, IET Cyber-Physical Systems, and so on. His current research interests include optimization analysis technology of power distribution network, network control of Energy Internet, Integrated Energy Systems and Microgrids.

David Wenzhong Gao (S'00-M'02-SM'03-F'20) received his M.S. and Ph.D. degrees in electrical and computer engineering, specializing in electric power engineering, from Georgia Institute of Technology, Atlanta, USA, in 1999 and 2002, respectively. He is now with the Department of Electrical and Computer Engineering, University of Denver, Colorado, USA. He is an Associate Editor for IEEE Journal of Emerging and Selected Topics in Power Electronics, and Journal of Modern Power Systems and Clean Energy. He was an editor of IEEE Transactions on Sustainable Energy. He is the General Chair for the 48th North American Power Symposium (NAPS 2016) and the IEEE Symposium on Power Electronics and Machines in Wind Applications (PEMWA 2012).

Huaguang Zhang (M'03-SM'04-F'14) received the B.S. degree and the M.S. degree in control engineering from Northeast Dianli University of China, Jilin City, China, in 1982 and 1985, respectively. He received the Ph.D. degree in thermal power engineering and automation from Southeast University, Nanjing, China, in 1991. He joined the Department of Automatic Control, Northeastern University, Shenyang, China, in 1992, as a Postdoctoral Fellow for two years. Since 1994, he has been a Professor and Head of the Institute of Electric Automation, School of Information Science and Engineering, Northeastern University, Shenyang, China. His main research interests are fuzzy control, stochastic system control, neural networks based control, nonlinear control, and their applications. He has authored and coauthored over 280 journal and conference papers, six monographs and co-invented 90 patents.