Distributed Resilient Self-Triggered Cooperative Control for Multiple Photovoltaic Generators Under Denial-of-Service Attack

Shengxuan Weng, Dong Yue, *Fellow, IEEE*, Jianbo Chen, Xiangpeng Xie, *Member, IEEE*, and Chunxia Dou, *Senior Member, IEEE*

***Abstract*—This article considers the distributed resilient cooperative control for photovoltaic generators (PVs) suffered from two types of denial-of-service (DoS) attack, where the global DoS attack jams all the communication channels and the distributed one jams each of the channels independently. The proposed control method realizes the fair utilization of all PVs, and restore the active power flow across certain transmission line and the voltage of the critical bus to their reference values. The self-triggered mechanism is introduced to ensure the control performance under the DoS attack and reduce the data flow in the communication network simultaneously. In addition, the parameter selection guidance for the resilient control method with fluctuation range, triggering frequency, and stabilization time is provided. The effectiveness of the theoretical result is verified by simulation.**

***Index Terms*—Denial-of-service (DoS) attack, distributed resilient control, distribution network, multiple photovoltaic generators (PVs), self-triggered mechanism.**

I. Introduction

DUE TO the growing concern about fossil energy depletion, carbon emission, and climate change, the current power system based on fossil fuels burning is facing a dramatic revolution. The renewable energy source (RES) with the low environmental cost, renewability, and world-wide distribution characteristics has been integrated into power system gradually [1]–[3]. Because of the potential availability, good visibility, and safe usage, the highest utilization rate among the RES is solar energy, which can be converted to electric energy by photovoltaic generators (PVs) [2]. However, the extensive integration of PVs has a negative impacts on distribution network, such as grid pollution, transient stability issues, and even voltage collapse [4], which makes it desirable to develop the appropriate control method for the power output of PVs.

The existing PVs control methods can be divided into the centralized, decentralized, and distributed modes. The centralized control requires the system-wide information acquisition and transmission, while the decentralized control is difficult to achieve the appropriate operating point of PVs [5]. These weaknesses make the centralized and decentralized controls unsuitable for numerous and geographically dispersed PV. To remedy these weaknesses, the distributed control is introduced due to its flexibility, robustness, and local communication features [6]–[11]. In the distributed control mode, each PV receives the information of neighboring PVs to update its own configured control policy to fulfill certain global control task.

The information transmission in PVs distributed control is physically realized by the digital communication technology, which means that the scheduled transmission rate can not be arbitrarily large. The periodic sampling scheme is compatible with digital communication technology. However, this scheme may generate the high data flows in communication networks since the sampling rate is calculated and selected in the worst case. This drawback will result in detrimental consequences, such as high costs, traffic congestion, and limits on critical monitoring and protection functions [12], [13]. The triggering mechanism is identified as an effective solution to this problem due to its demand-transmission character [14]–[16]. The event-triggered distributed control for PVs is studied in [17] under the perfect secure network environment, where the communication burdens are sharply reduced since the information transmission is activated only when the predefined triggering condition is satisfied.

It should be mentioned that the extensive utilization of information technology makes the adversary more permeable, and causes the communication network more vulnerable to cyber-attack. Because of the devastating effects of cyber-attack on information transmission, the network-based control performance may be degraded and even be led to failure [18]. Moreover, the distributed control mode is more susceptible to cyber-attack since a centralized supervisory node which can monitor the whole system activity is absent [19]. Typically, denial-of-service (DoS) attack, which has been listed as one of the most financially expensive security threats [18], [20], refers to destroy the information availability by preventing the delivery of control and measurement data packets. The DoS

Manuscript received 18 August 2021; accepted 16 May 2022. Date of publication 25 May 2022; date of current version 19 December 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 62073170 and Grant 62022044; in part by the Project funded by China Postdoctoral Science Foundation under Grant 2018M642294; in part by the Jiangsu Planned Projects for Postdoctoral Research Funds under Grant 2018K006A; and in part by the "1311 Talent Project" by Nanjing University of Posts and Telecommunications. This article was recommended by Associate Editor A. Trappey. *(Corresponding author: Shengxuan Weng.)*

The authors are with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: shxweng@gmail.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSMC.2022.3176460.

Digital Object Identifier 10.1109/TSMC.2022.3176460

attack should be considered as a major concern in control system because it is easy to be conducted by the adversary who has limited knowledge on the system, and it is desirable to consider the resilient control approach for power system to resist the negative effects of the DoS attack. In [21] and [22], the resilient H_∞ load frequency control for multiarea power systems is proposed considering the DoS attack. The distributed resilient control framework is investigated in [23] to address the secondary frequency regulation problem of multiple heterogeneous battery energy storage systems subject to the DoS attack. Recently, the security control method for power system under cyber-threat including the DoS attack is summarized in [24]. However, little research work has considered the topic about multiple PVs resilient control based on the triggering mechanism, which motivates the current study.

This article focuses on the development of distributed resilient control of multiple PVs in the distribution network under the DoS attack, where the triggering mechanism is considered simultaneously. It aims to restore the active power flow of certain transmission line and the voltage of a critical bus to their reference values, and realize the fair utilization of all PVs. The control task can be fulfilled overcoming the DoS attack influence and limitation of a communication resource. The main contributions of this article are summarized as follows.

1) The distributed self-triggered mechanism is introduced in the resilient control algorithm to realize the discrete on-demand transmission of information, and the triggering time instants of each PV can be adjusted adaptively according to the occurrence of the DoS attack. The proposed self-triggered mechanism ensures the control performance under cyber-attack and reduces the data flow in communication network simultaneously.
2) The fluctuation range, triggering frequency, and stabilization time are relative with the parameters in the control algorithm by explicit mathematics formulation, which provides the parameter selection guidance in practical engineering. Moreover, the effects of the DoS attack on stabilization time and triggering frequency are characterized theoretically. It is shown that the stabilization time and triggering frequency will be increased to resist the serious DoS attack with long duration and high frequency.
3) The effectiveness of proposed resilient control algorithms can be guaranteed under two types of the DoS attack, where the global DoS attack blocks all the communication channels between PVs, and the distributed one jams the certain communication channel independent of other ones.

The remainder of this article is organized as follows. Section II presents the system model, control objective, and DoS attack strategy. Section III proposes the update law of desired utilization ratio. The resilient self-triggered control strategy for PV are constructed in Sections IV and V, where the cases of global and distributed DoS attack are analyzed, respectively. The effectiveness of theory is verified by simulation in Section VI, and Section VII states the conclusion and future work.

II. Problem Formulation

A. System Model

Consider the distribution network with n three-phase inverter-based PVs. According to the utilization of decoupled d-q control method based on phase-locked loops, the output power of PV $i(i = 1, \dots, n)$ can be represented as follows [7]:

$$P_i = U_i I_{di}, \quad Q_i = -U_i I_{qi} \tag{1}$$

where P_i and Q_i are the active and reactive output power, U_i is the magnitude of terminal voltage, I_{di} and I_{qi} are the output currents in the d-axis and q-axis, respectively.

Mentioned that the active and reactive output power P_i and Q_i of all PVs satisfy the power flow equation of distribution network as in [7]

$$g(P_1, \dots, P_n, Q_1, \dots, Q_n, \chi, \mathbf{X}) = 0 \tag{2}$$

where χ is a vector of an appropriate dimension which denotes all the internal network state variables, including dynamics of the PVs, loads, and synchronized generators, and $\mathbf{X}$ is a vector including some algebraic variables in the distribution network, such as the voltages of buses and so on.

The reference values I_{di}^{ref} and I_{qi}^{ref} of the d-axis and q-axis output currents of PV i are regulated as

$$\frac{d}{dt} I_{di}^{\text{ref}} = u_{di}, \quad \frac{d}{dt} I_{qi}^{\text{ref}} = u_{qi} \tag{3}$$

where u_{di} and u_{qi} are the control inputs to be designed. Since the inner dynamics of PV are much faster than those of output power, the inner dynamics of the PVs can be ignored at the level of output power control. This implies that $I_{di} = I_{di}^{\text{ref}}$ and $I_{qi} = I_{qi}^{\text{ref}}$. As a consequence, the dynamical model of distribution network is obtained based on (1)–(3) as

$$\frac{d}{dt} P_i = \frac{U_i'}{U_i} P_i + U_i u_{di} \tag{4}$$

$$\frac{d}{dt} Q_i = \frac{U_i'}{U_i} Q_i - U_i u_{qi} \tag{5}$$

$$g(P_1, \dots, P_n, Q_1, \dots, Q_n, \chi, \mathbf{X}) = 0 \tag{6}$$

where U_i' is the derivative of U_i with respect to time t.

B. Control Objectives and Framework

When the disturbances such as load and sunlight fluctuations occur in the distribution network containing a large number of PVs, some important indicators, such as active power flow, voltage, and utilization ratio of PVs, will deviate from their specific values, and this will further damage the economic and steady operation of the power system. Under this situation, the control inputs u_{di} and u_{qi} in (4)–(6) for PV $i(i = 1, \dots, n)$ should be constructed to accomplish the following two control objectives.

Objective 1: Restore the active power flow and voltage. Denote the active power flow across certain transmission line and the voltage of a critical bus as $P_{\text{tran}}(\cdot)$ and $V_c(\cdot)$, respectively, where $P_{\text{tran}}(\cdot)$ and $V_c(\cdot)$ are the functions of output power of PVs. Design the control laws u_{di} and u_{qi} such that

$$\left| P_{\text{tran}}(\cdot) - P^{\text{ref}} \right| \le \epsilon_P, \quad \left| V_c(\cdot) - V^{\text{ref}} \right| \le \epsilon_V \tag{7}$$

where P^{ref} and V^{ref} are the reference values of active power and voltage, respectively, and the positive constants ϵ_P and ϵ_V denote the allowable fluctuation ranges.

Objective 2: Realize the fair utilization of all PVs. Denote the active and reactive power utilization ratio of PV i as $\alpha_i^P = (P_i/P_{i,\max})$ and $\alpha_i^Q = (Q_i/Q_{i,\max})$, respectively, where $P_{i,\max}$ and $Q_{i,\max}$ are the instantaneous maximum capacity of P_i and Q_i. Design the control laws u_{di} and u_{qi} such that

$$\left|\alpha_i^P - \alpha_j^P\right| \leq \epsilon_{pr}, \quad \left|\alpha_i^Q - \alpha_j^Q\right| \leq \epsilon_{qr}, \quad \forall i,j \in 1,\ldots,n \qquad (8)$$

where the positive constants ϵ_{pr} and ϵ_{qr} are the allowable fluctuation ranges.

Remark 1: Control objective 1 guarantees that the active power consumed by loads in a concerned area or feeder remains unchanged, and the reactive power is controlled to support the voltage of some critical bus. It aims to coordinate the PVs group with the overall power grid [7]. Control objective 2 makes all PVs in a designated group to operate at almost the same active and reactive power output ratios to ensure their fair utilization, where the economic and regulatory policies are considered [17].

In the proposed control framework, the detection unit measures the active power flow $P_{\text{tran}}(\cdot)$ and the voltage $V_c(\cdot)$. By comparing $P_{\text{tran}}(\cdot)$ and $V_c(\cdot)$ with their reference values P^{ref} and V^{ref}, the desired active and reactive power utilization ratios α_0^P and α_0^Q are computed and transmitted to some PVs through communication network. Each PV executes the proposed control u_{di} and u_{qi} to drive its own utilization ratios α_i^P and α_i^Q to the desired ones α_0^P and α_0^Q in order to achieve control objectives 1 and 2. The implementation of control laws u_{di} and u_{qi} only requires the local information transmitted from the neighbors of PV i to conform the distributed configuration.

The communication network represented by an undirected connected graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ is introduced for information transmission in the above control framework. The node set $\mathcal{V} = \{1,\ldots,n\}$ contains all the n PVs in distribution network. $\mathcal{E} = \{(i,j),\ if\ i \to j\} \subseteq \mathcal{V}\times\mathcal{V}$ is the edge set where the symbol $i \to j$ means that PV i can transmit its own information to PV j directly through the communication network. The neighbor set of PV i is defined as $N_i = \{j \in \mathcal{V} : (j,i) \in \mathcal{E}\}$, and it contains all the PVs which can transmit the information to PV i. The adjacency matrix of graph $\mathcal{G}$ is denoted as $A = \{a_{ij}\} \in R^{n\times n}$, where $a_{ij} = 1$ if $(i,j) \in \mathcal{E}$, otherwise $a_{ij} = 0$. Define the Laplacian matrix of graph $\mathcal{G}$ as $L = \text{diag}\{d_1,\ldots,d_n\} - A$ where $d_i = \sum_{j=1}^n a_{ij}$, and let the graph $\bar{A} = \text{diag}\{a_{10},\ldots,a_{n0}\}$ where $a_{i0} = 1$ if PV i can receive the information of desired utilization ratios from detection unit and $a_{i0} = 0$ otherwise. It is assumed that at least one of a_{i0} is equal to 1 for all i. Based on the theory in [25] and [26], the matrices L and $L + \bar{A}$ are semi-positive and positive definite, respectively.

C. DoS Attack Strategy

In a practical distribution system, the communication network is threatened by adversary in the DoS attack, which jams the communication channels to prevent the PVs from sending/receiving data hostilely [27]. The DoS attack breaks the data availability, and further leads to the failure of distribution network stable operation. The following two types of the DoS attack distinguished by the attack scope are considered in this article.

1) Global DoS Attack: The global DoS attack blocks the information transmission at all communication channels, which is representative of communication networks operating through a single access point in the "infrastructure" mode. Denote $\mathcal{A}_k = [h_k, h_k + \tau_k)$ as the kth ($k \in \mathbb{Z}_{\geq 0}$) global DoS attack time interval, where h_k and τ_k are the starting time instant and duration of the kth attack, respectively. The set of times under global DoS attack in time interval $[\tau, t]$ with $t > \tau \geq 0$ can be defined as $\mathcal{A}(\tau, t) = \bigcup_{k\in\mathbb{Z}_{\geq 0}} \mathcal{A}_k \cap [\tau, t]$, and the set of times without attack is $\mathcal{H}(\tau, t) = [\tau, t]\backslash\mathcal{A}(\tau, t)$, where the symbol $\backslash$ denotes the relative complement. For any time interval $[\tau, t]$, all of the information transmissions in communication network are prevented in $\mathcal{A}(\tau, t)$, otherwise in $\mathcal{H}(\tau, t)$.

Assumption 1: There exists constants $\eta > 0$ and $T_f > 0$ such that $n(\tau, t) \leq \eta + (t - \tau/T_f)$, where $n(\tau, t)$ denotes the number of global DoS attack off/on transitions in time interval $[\tau, t]$.

Assumption 2: There exists constants $\kappa > 0$ and $T_d > 1$ such that $|\mathcal{A}(\tau, t)| \leq \kappa + (t - \tau/T_d)$, where $|\mathcal{A}(\tau, t)|$ denotes the duration of global DoS attack in time interval $[\tau, t]$.

2) Distributed DoS Attack: The distributed DoS attack blocks the information transmission at certain communication channel independent of other ones, which is representative of communication networks operating in the "ad-hoc" mode. For edge $(i,j) \in \mathcal{E}$ in communication network $\mathcal{G}$, the set of times under distributed DoS attack in time interval $[\tau, t]$ with $t > \tau \geq 0$ is $\mathcal{A}^{ij}(\tau, t) = \bigcup_{k\in\mathbb{Z}_{\geq 0}} \mathcal{A}_k^{ij} \cap [\tau, t]$, and the set of times without attack is $\mathcal{H}^{ij}(\tau, t) = [\tau, t]\backslash\mathcal{A}^{ij}(\tau, t)$, where $\mathcal{A}_k^{ij} = [h_k^{ij}, h_k^{ij} + \tau_k^{ij})$ denotes the kth ($k \in \mathbb{Z}_{\geq 0}$) distributed DoS attack time interval on edge (i,j) with the starting time instant h_k^{ij} and duration τ_k^{ij}. For any time interval $[\tau, t]$, the information transmission between PV i and PV j is prevented in $\mathcal{A}^{ij}(\tau, t)$, otherwise in $\mathcal{H}^{ij}(\tau, t)$. It should be mentioned that the distributed DoS attack on communication channel (i,j) does not affect the other channels in $\mathcal{E}$.

Assumption 3: There exists constants $\eta^{ij} > 0$ and $T_f^{ij} > 0$, such that $n^{ij}(\tau, t) \leq \eta^{ij} + (t - \tau/T_f^{ij})$, where $n^{ij}(\tau, t)$ denotes the number of distributed DoS attack off/on transitions on edge (i,j) in time interval $[\tau, t]$.

Assumption 4: There exists constants $\kappa^{ij} > 0$ and $T_d^{ij} > 1$, such that $|\mathcal{A}^{ij}(\tau, t)| \leq \kappa^{ij} + (t - \tau/T_d^{ij})$, where $|\mathcal{A}^{ij}(\tau, t)|$ denotes the duration of the distributed DoS attack on edge (i,j) in time interval $[\tau, t]$.

Remark 2: The launch of the DoS attack needs to consume the resource and energy to inject the interfering radio signals into the communication network [28]. However, the available resource and energy for adversary are extremely restricted in a practical system. Moreover, the attack chance is decreased in general since there exists various provisions to mitigate the DoS attack in practical application, such as spreading techniques and high-pass filtering. As a result, the frequency and duration of the DoS attack are usually limited.

Assumptions 1 and 3 show the attack frequency limitation, while Assumptions 2 and 4 represent the duration limitation. These limitations are common for the DoS attack research and more details can be seen in [27] and [29]. The considered pattern of the DoS attack can capture many different scenarios, such as periodic, stochastic distribution, and protocol-aware jamming attack [30].

In the next sections, the distributed resilient cooperative control for multiple PVs will be constructed to achieve control objectives 1 and 2 under the above two types of the DoS attack. Furthermore, the self-triggered mechanism is introduced to ensure the control performance in spite of communication resource limitations.

III. Control for Desired Utilization Ratio

The following control laws (9) and (10) are constructed to update the desired active and reactive power utilization ratio α_0^P and α_0^Q for $l = 0, 1, 2, \ldots,$ respectively

$$\alpha_0^P((l+1)T) = \alpha_0^P(lT) - K_1\Big(P_{\text{tran}}(lT) - P^{\text{ref}}\Big) \tag{9}$$

$$\alpha_0^Q((l+1)T) = \alpha_0^Q(lT) - K_2\Big(V_c(lT) - V^{\text{ref}}\Big) \tag{10}$$

where T is the update period, and the parameters K_1 and K_2 are positive constants.

The control law (9) and (10) is configured at the detection unit in the proposed control framework shown in Section II-B. The detection unit computes the desired utilization ratios $\alpha_0^P((l+1)T)$ and $\alpha_0^Q((l+1)T)$ at time lT, and sets $\alpha_0^P(t) = \alpha_0^P((l+1)T)$ and $\alpha_0^Q(t) = \alpha_0^Q((l+1)T)$ for $t \in [lT, (l+1)T)$. The implementation of (9) and (10) does not rely on communication network $\mathcal{G}$, which indicates that the control performance of (9) and (10) is not affected by the DoS attack.

It can be seen from (9) that the desired active power utilization ratio α_0^P increases when the active power flow $P_{\text{tran}}(\cdot)$ is less than the reference value P^{ref}, and vice versa, and the similar phenomenon occurs for the reactive one α_0^Q. This implies the responsiveness of desired utilization ratios to the requirement of control objective 1.

Set the control laws u_{di} and u_{qi} in the following forms:

$$u_{di}(t) = \frac{P_{i,\max}}{U_i(t)}u_i^P(t) - \frac{U_i'(t)P_i(t)}{U_i(t)^2} \tag{11}$$

$$u_{qi}(t) = -\frac{Q_{i,\max}}{U_i(t)}u_i^Q(t) + \frac{U_i'(t)Q_i(t)}{U_i(t)^2} \tag{12}$$

where $u_i^P(t)$ and $u_i^Q(t)$ will be designed later.

According to (9)–(12), the dynamical model (4)–(6) can be converted into the ordinary differential system (13)–(16) around the equilibrium by using implicit function theorem for the power flow (6)

$$\frac{d}{dt}\alpha_i^P(t) = u_i^P(t) \tag{13}$$

$$\frac{d}{dt}\alpha_i^Q(t) = u_i^Q(t) \tag{14}$$

$$\alpha_0^P((l+1)T) = \alpha_0^P(lT) - K_1\Big(\varphi_1\Big(\alpha_1^P(lT), \ldots, \alpha_n^P(lT)\; \alpha_1^Q(lT), \ldots, \alpha_n^Q(lT)\Big) - P^{\text{ref}}\Big) \tag{15}$$

$$\alpha_0^Q((l+1)T) = \alpha_0^Q(lT) - K_2\Big(\varphi_2\Big(\alpha_1^P(lT), \ldots, \alpha_n^P(lT)\; \alpha_1^Q(lT), \ldots, \alpha_n^Q(lT)\Big) - V^{\text{ref}}\Big) \tag{16}$$

where the functions $\varphi_1(\alpha_1^P(lT), \ldots, \alpha_n^Q(lT)) = P_{\text{tran}}(lT)$ and $\varphi_2(\alpha_1^P(lT), \ldots, \alpha_n^Q(lT)) = V_c(lT)$. This demonstrates that the differential-algebraic system (4)–(6) under (9)–(12) is equivalent to the ordinary differential system (13)–(16) in a neighborhood of the equilibrium. In other word, the power flow (6) still holds under control law (9)–(12) around the equilibrium. In what follows, the distributed resilient control law for PVs will be designed for system (13)–(16), which is still effective for system (4)–(6) under small disturbance [17].

The following property about φ_1 and φ_2 is satisfied usually for distribution network [5].

Property 1: The function φ_1 satisfies $(\partial\varphi_1/\partial\alpha_i^P) > 0$ and $|(\partial\varphi_1/\partial\alpha_i^P)| \gg |(\partial\varphi_1/\partial\alpha_i^Q)|$, while the function φ_2 satisfies $(\partial\varphi_2/\partial\alpha_i^Q) > 0$ and $|(\partial\varphi_2/\partial\alpha_i^Q)| \gg |(\partial\varphi_2/\partial\alpha_i^P)|$.

IV. Resilient Control for PVs Under Global DoS Attack

This section constructs the distributed resilient control inputs u_i^P and u_i^Q in (11) and (12) to achieve control objectives 1 and 2 under the global DoS attack. Moreover, the self-triggered mechanism is introduced to reduce the communication burdens. Denoting the triggering time instants corresponding to control laws u_i^P and u_i^Q as the monotone increasing sequence $\{t_0^i, t_1^i, \ldots, t_k^i, \ldots\}$ and $\{\tau_0^i, \tau_2^i, \ldots, \tau_m^i, \ldots\}$, respectively, these control inputs are designed as follows:

$$u_i^P(t) = \begin{cases} \beta_P \cdot \text{sign}_{\varepsilon_P}\big(f_i^P(t_k^i)\big), & \text{if } t \in \big[t_k^i, t_{k+1}^i\big) \wedge t_k^i \in \mathcal{H}(0,t) \\ 0, & \text{if } t \in \big[t_k^i, t_{k+1}^i\big) \wedge t_k^i \in \mathcal{A}(0,t) \end{cases} \tag{17}$$

$$u_i^Q(t) = \begin{cases} \beta_Q \cdot \text{sign}_{\varepsilon_Q}\Big(f_i^Q(\tau_m^i)\Big), & \text{if } t \in \big[\tau_m^i, \tau_{m+1}^i\big) \wedge \tau_m^i \in \mathcal{H}(0,t) \\ 0, & \text{if } t \in \big[\tau_m^i, \tau_{m+1}^i\big) \wedge \tau_m^i \in \mathcal{A}(0,t) \end{cases} \tag{18}$$

where β_P, β_Q, ε_P, and ε_Q are positive constants, the functions $f_i^P(t)$ and $f_i^Q(t)$ are defined as (19) and (20) for $t \in [lT, (l+1)T)$

$$f_i^P(t) = \sum_{j\in N_i} a_{ij}\Big(\alpha_j^P(t) - \alpha_i^P(t)\Big) + a_{i0}\big(\alpha_0^P((l+1)T) - \alpha_i^P(t)\big) \tag{19}$$

$$f_i^Q(t) = \sum_{j\in N_i} a_{ij}\Big(\alpha_j^Q(t) - \alpha_i^Q(t)\Big) + a_{i0}\Big(\alpha_0^Q((l+1)T) - \alpha_i^Q(t)\Big) \tag{20}$$

and

$$\text{sign}_\varepsilon(x) = \begin{cases} \text{sign}(x), & \text{if } |x| \geq \varepsilon \\ 0, & \text{otherwise.} \end{cases}$$

The triggering time instants are determined by the following distributed self-triggered mechanism:

$$t_{k+1}^i = t_k^i + \begin{cases} \max\left\{\frac{\varepsilon_P}{2\beta_P(2|N_i|+a_{i0})}, \frac{|f_i^P(t_k^i)|}{2\beta_P(2|N_i|+a_{i0})}\right\} & \text{if } t_k^i \in \mathcal{H}(0,t) \\ \frac{\varepsilon_P}{2\beta_P(2|N_i|+a_{i0})}, & \text{if } t_k^i \in \mathcal{A}(0,t) \end{cases} \tag{21}$$

$$\tau_{m+1}^i = \tau_m^i + \begin{cases} \max\left\{\frac{\varepsilon_Q}{2\beta_Q(2|N_i|+a_{i0})}, \frac{|f_i^Q(\tau_m^i)|}{2\beta_Q(2|N_i|+a_{i0})}\right\} & \\ \qquad\qquad \text{if } \tau_m^i \in \mathcal{H}(0,t) & \\ \frac{\varepsilon_Q}{2\beta_Q(2|N_i|+a_{i0})}, \qquad \text{if } \tau_m^i \in \mathcal{A}(0,t). \end{cases} \tag{22}$$

The dynamical scenario of resilient control strategy (17)–(22) can be depicted as follows. At the triggering time instant t_k^i, PV i requests the information of active power utilization ratio $\alpha_j^P(t_k^i)$ from its neighboring PVs in N_i and the desired ratio $\alpha_0^P(t_k^i)$ from the detection unit if $a_{i0} = 1$, and then uses these information to update the control law u_i^P according to (17) to modulate its own active power output. Meanwhile, the corresponding self-triggered mechanism (21) calculates the triggering time instant t_{k+1}^i considering the issue of the global DoS attack. If t_k^i is detected to be located in the attack time interval $\mathcal{A}(0, t)$, the information acquisition launched by PV i fails and the control input u_i^P is set as 0 shown in (17) to remain the active power output of PV i unchanged. Meanwhile, the next triggering time instant is determined as $t_{k+1}^i = t_k^i + (\varepsilon_P/[2\beta_P(2|N_i| + a_{i0})])$ by the self-triggered mechanism (21), which implies that PV i will attempt to acquire the neighbors' information again after the waiting time $(\varepsilon_P/[2\beta_P(2|N_i| + a_{i0})])$. The similar character exists for the reactive power control strategy.

Remark 3: Each PV only requests its neighbors' information at its own triggering time instants in the proposed control strategy (17)–(22), which makes the control strategy appropriate for distribution network with communication resource limitation since the communication burdens can be reduced. Mentioned that the self-triggered mechanism has advantages over periodic sampling mechanism where the fixed sampling period is selected conservatively under the worst case to cause the wasting of communication resource. On the other hand, since the precomputation operation of triggering time instant is implemented in a discrete-time manner in the proposed self-triggered mechanism, the continuous state monitoring and detection, which are necessary for the event-triggered mechanism, can be avoided. Moreover, (21) and (22) demonstrate that the intertrigger time intervals satisfy $t_{k+1}^i - t_k^i \geq (\varepsilon_P/[2\beta_P(2|N_i| + a_{i0})])$ and $\tau_{m+1}^i - \tau_m^i \geq (\varepsilon_Q/[2\beta_Q(2|N_i| + a_{i0})])$ for $i \in \mathcal{V}$, which excludes the Zeno behavior.

Lemma 1: Set the parameters β_P, β_Q, ε_P, and ε_Q in (17)–(22) as $(1/T_d) + (\varepsilon_P/4\beta_P T_f) < 1$ and $(1/T_d) + (\varepsilon_Q/4\beta_Q T_f) < 1$. In each time interval $[lT, (l+1)T)$, using the distributed resilient control (17) and (18) with the self-triggered mechanism (21) and (22) yields $\lim_{t\to(lT+T^P)} \alpha_i^P(t) = \bar{\alpha}_{i,l}^P$ and $\lim_{t\to(lT+T^Q)} \alpha_i^Q(t) = \bar{\alpha}_{i,l}^Q$ if $T > \max\{T^P, T^Q\}$ where $\bar{\alpha}_{i,l}^P$ and $\bar{\alpha}_{i,l}^Q$ are some constants. Moreover, the tracking errors $|\bar{\alpha}_{i,l}^P - \alpha_0^P((l+1)T)| \leq ((n/[\lambda_{\min}(L+\bar{A})^2]))^{(1/2)}\varepsilon_P$ and $|\bar{\alpha}_{i,l}^Q - \alpha_0^Q((l+1)T)| \leq ((n/\lambda_{\min}(L+\bar{A})^2))^{(1/2)}\varepsilon_Q$, and the settling time

$$T^P = 2n(2d_{\max}+1)\lambda_{\max}(L+\bar{A})\left(\frac{1}{2\beta_P\varepsilon_P(2d_{\max}+1)} + \frac{1}{4\beta_P\varepsilon_P d_{\min}} + \frac{\kappa+(1+\eta)\frac{\varepsilon_P}{4\beta_P}}{\left(1-\frac{1}{T_d}-\frac{\varepsilon_P}{4\beta_P T_f}\right)\varepsilon_P^2}\right) \tag{23}$$

$$T^Q = 2n(2d_{\max}+1)\lambda_{\max}(L+\bar{A})\left(\frac{1}{2\beta_Q\varepsilon_Q(2d_{\max}+1)} + \frac{1}{4\beta_Q\varepsilon_Q d_{\min}} + \frac{\kappa+(1+\eta)\frac{\varepsilon_Q}{4\beta_Q}}{\left(1-\frac{1}{T_d}-\frac{\varepsilon_Q}{4\beta_Q T_f}\right)\varepsilon_Q^2}\right) \tag{24}$$

where $d_{\max} = \{\max_i\{d_i\}$, $d_{\min} = \min_i\{d_i\}$, $\lambda_{\max}(\cdot)$ and $\lambda_{\min}(\cdot)$ denote the largest and smallest eigenvalues of matrix, respectively.

Proof: Defining the variable $e_i^P(t) = \alpha_i^P(t) - \alpha_0^P((l+1)T)$ for $t \in [lT, (l+1)T)$, it yields the closed-loop system $(d/dt)e_i^P(t) = (d/dt)\alpha_i^P(t) = u_i^P(t)$ where $u_i^P(t)$ is given in (17). Without loss of generality, the following proof considers the system dynamic in time interval $[lT, (l+1)T)$ with $l = 0$. Let the vector $e^P(t) = (e_1^P(t), \ldots, e_n^P(t))^{\mathrm{T}}$, and construct the candidate Lyapunov function

$$V_1 = \frac{1}{2}\left(e^P\right)^T\left(L+\bar{A}\right)e^P.$$

The derivation of V_1 with respect to time along the solution of the closed-loop system for $t \in [t_k^i, t_{k+1}^i)$ is

$$\begin{aligned}\frac{d}{dt}V_1 &= -\sum_i u_i^P(t)f_i^P(t)\\ &= -\beta_P \sum_{i\in S_1\cap S_2} \mathrm{sign}_{\varepsilon_P}\left(f_i^P\left(t_k^i\right)\right)f_i^P(t)\end{aligned} \tag{25}$$

where $((L+\bar{A})e^P)_i = \sum_j l_{ij}e_j^P(t) + a_{i0}e_i^P(t) = \sum_j l_{ij}\alpha_j^P(t) + a_{i0}(\alpha_i^P(t) - \alpha_0^P((l+1)T)) = -f_i^P(t)$ is used and the sets are defined as $S_1 = \{i : t_k^i \in \mathcal{H}(0,t)\}$ and $S_2 = \{i : |f_i^P(t_k^i)| \geq \varepsilon_P\}$.

Since $|\alpha_i^P(t) - \alpha_i^P(t_k^i)| \leq \int_{t_k^i}^t |u_i^P(s)|ds \leq \beta_P(t - t_k^i)$ according to (13) and (17) for $i \in \mathcal{V}$, it has that

$$f_i^P(t) \geq f_i^P\left(t_k^i\right) - \beta_P(2|N_i| + a_{i0})\left(t - t_k^i\right) \tag{26}$$

$$f_i^P(t) \leq f_i^P\left(t_k^i\right) + \beta_P(2|N_i| + a_{i0})\left(t - t_k^i\right). \tag{27}$$

Combing (21), (26), and (27) yields $f_i^P(t) \geq ([f_i^P(t_k^i)]/2)$ if $f_i^P(t_k^i) \geq \varepsilon_P$, and $f_i^P(t) \leq ([f_i^P(t_k^i)]/2)$ if $f_i^P(t_k^i) \leq -\varepsilon_P$ for $t \in [t_k^i, t_{k+1}^i)$. This demonstrates that $\mathrm{sign}_{\varepsilon_P}(f_i^P(t_k^i)) = \mathrm{sign}(f_i^P(t))$ and $|f_i^P(t)| \geq ([f_i^P(t_k^i)]/2)$ when $|f_i^P(t_k^i)| \geq \varepsilon_P$. Based on (25), we have

$$\begin{aligned}\frac{d}{dt}V_1 &= -\beta_P \sum_{i\in S_1\cap S_2} \left|f_i^P(t)\right| \leq -\frac{\beta_P}{2}\sum_{i\in S_1\cap S_2}\left|f_i^P\left(t_k^i\right)\right|\\ &\leq -\frac{\beta_P}{2}\sum_{i\in S_1\cap S_2}\varepsilon_P.\end{aligned} \tag{28}$$

Formula (28) implies that there exists a fixed time instant t_P^* such that $S_1 \cap S_2 = \emptyset$ for $t > t_P^*$. Otherwise, there would be an infinite number of time intervals whose length is lower bounded by the constant $\min_i(\varepsilon_P/[2\beta_P(2|N_i| + a_{i0})])$ and on which $(d/dt)V_1 \leq -(\beta_P\varepsilon_P/2)$, and this contradicts the positive definiteness of function V_1. The above result $S_1 \cap S_2 = \emptyset$ illustrates $u_i^P(t) = 0$ and $\alpha_i^P(t) = \bar{\alpha}_{i,l}^P$ for all $i \in \mathcal{V}$ and $t > t_P^*$.

Consider the time intervals $\bar{\mathcal{A}}(\tau,t) = \cup_{k\in\mathbb{Z}_{\geq 0}}(\bar{\mathcal{A}}_k \cap [\tau,t])$ and $\bar{\mathcal{H}}(\tau,t) = [\tau,t]\backslash\bar{\mathcal{A}}(\tau,t)$ where $\bar{\mathcal{A}}_k = [h_k, h_k + \tau_k + (\varepsilon_P/4\beta_P))$. The length of interval $\bar{\mathcal{H}}(\tau,t)$

satisfies

$$\begin{aligned}&\left|\bar{\mathcal{H}}(\tau,t)\right|\\&=t-\tau-\left|\bar{\mathcal{A}}(\tau,t)\right|\\&\geq t-\tau-\left(|\mathcal{A}(\tau,t)|+(n(\tau,t)+1)\frac{\varepsilon_P}{4\beta_P}\right)\\&\geq\left(1-\left(\frac{1}{T_d}+\frac{\varepsilon_P}{4\beta_P T_f}\right)\right)(t-\tau)-\left(\kappa+(\eta+1)\frac{\varepsilon_P}{4\beta_P}\right)\end{aligned} \tag{29}$$

where Assumptions 1 and 2 are used. Since $(1/T_d)+(\varepsilon_P/4\beta_P T_f)<1$, it can be seen from (29) that there exists $t>\tau$ such that $|\bar{\mathcal{H}}(\tau,t)|>0$ for any time instant τ. Setting τ as t_P^*, it implies that there exists some time instant t_P^{**} such that each of the PVs acquires its neighbors' information successfully at least one time in the interval $[t_P^*, t_P^{**})$ since $|\bar{\mathcal{H}}(t_P^*, t_P^{**})|>0$. This together with the result $u_i^P(t)=0$ $(\forall i\in\mathcal{V},\ t>t_P^*)$ yields that $|f_i^P(t)|<\varepsilon_P$ for each $i\in\mathcal{V}$ and $t>t_P^*$. Therefore, we have $\|e^P(t)\|^2\cdot\lambda_{\min}(L+\bar{A})^2\leq\|(L+\bar{A})e^P(t)\|^2=\sum_i(f_i^P(t))^2\leq n(\varepsilon_P)^2$ for $t>t_P^*$, which further indicates the tracking error satisfies $|\bar{\alpha}_{i,l}^P-\alpha_0^P((l+1)T)|\leq(n/[\lambda_{\min}(L+\bar{A})^2])^{(1/2)}\varepsilon_P$.

The settling time T^P is estimated as follows. Supposing $u_i^P(\tilde{t})=0$ at the time instant $\tilde{t}$ for all $i\in\mathcal{V}$ and the equilibrium point is not reached, all of the PVs will attempt to request the neighboring information in the time interval $\mathcal{T}_1=[\tilde{t},\tilde{t}+(\varepsilon_P/4\beta_P d_{\min})]$. If $u_i^P(t)=0$ for $t\in\mathcal{T}_1$ and all $i\in\mathcal{V}$, we have that the information acquisition of at least one PV is unsuccessful caused by the DoS attack in $\mathcal{T}_1$. Otherwise, the equilibrium point is reached at $\tilde{t}$ which makes the contradiction. This further indicates that each of the PVs acquires its neighbors' information successfully at least one time in the time interval $\mathcal{T}_2=[\tilde{t},\tilde{t}+(\varepsilon_P/4\beta_P d_{\min})+([\kappa+(\eta+1)(\varepsilon_P/4\beta_P)]/[1-((1/T_d)+(\varepsilon_P/4\beta_P T_f))])]$ according to (29). This implies that $u_i^P\neq 0$ for at least one PV i before $|\mathcal{T}_2|$ units of time have elapsed. Moreover, based on (21) and (28), we can get that the function V_1 decreases at least $(\varepsilon_P^2/[4(2d_{\max}+1)])$ for at least $(\varepsilon_P/[2\beta_P(2d_{\max}+1)])$ units of time if $u_i^P\neq 0$ for some PV i. As a consequence, the function V_1 decreases at least $(\varepsilon_P^2/[4(2d_{\max}+1)])$ every $|\mathcal{T}_2|+(\varepsilon_P/[2\beta_P(2d_{\max}+1)])$ units of time before the equilibrium point is reached, which further implies the settling time $T^P\leq(|\mathcal{T}_2|+(\varepsilon_P/[2\beta_P(2d_{\max}+1)]))([V_1(0)]/[(\varepsilon_P^2/[4(2d_{\max}+1)])])$ since $V_1(t)\geq 0$. And then (23) can be obtained in the most conservative case since $V_1(0)\leq(n/2)\lambda_{\max}(L+\bar{A})$. The result about reactive power utilization ratio control can be proved by similar analysis mentioned above. ■

Lemma 1 shows that the proposed control law (17) and (18) drives $\alpha_i^P(t)$ (resp. $\alpha_i^Q(t)$) to the constant $\bar{\alpha}_{i,l}^P$ (resp. $\bar{\alpha}_{i,l}^Q$) in finite time T^P (resp. T^Q) with the initial value $\alpha_i^P(lT)$ (resp. $\alpha_i^Q(lT)$), and then $\alpha_i^P(t)$ (resp. $\alpha_i^Q(t)$) remains constant for $t\in[lT+T^P,(l+1)T)$ (resp. $t\in[lT+T^Q,(l+1)T)$). The settling times T^P and T^Q corresponding to each time interval $[lT,(l+1)T)$ are constant, and the tracking errors can be obtained in each time interval $[lT,(l+1)T)$ with the constant settling times and the initial values at time lT. This shows that $|\alpha_i^P(t)-\alpha_0^P((l+1)T)|\leq(n/[\lambda_{\min}(L+\bar{A})^2])^{(1/2)}\varepsilon_P$ and $|\alpha_i^Q(t)-\alpha_0^Q((l+1)T)|\leq(n/[\lambda_{\min}(L+\bar{A})^2])^{(1/2)}\varepsilon_Q$ for $t\in[lT+\max\{T^P,T^Q\},(l+1)T)$ with each l. And it further illustrates the active and reactive power utilization ratios of each PV i can be driven into an arbitrarily small neighborhood of the corresponding desired ratios with the acceptable fluctuation ranges in each time interval $[lT,(l+1)T)$ even under the global DoS attack, which is the foundation of main result given in the following theorem.

Theorem 1: Considering the case of the global DoS attack, control objectives 1 and 2 can be achieved under the desired utilization ratio control (9) and (10) and the distributed resilient self-triggered control (11) and (12) with (17)–(22) by setting the parameters as those in Lemma 1. Moreover, the fluctuation ranges in (7) and (8) satisfy

$$\epsilon_P=\left(\frac{n}{\lambda_{\min}\left(L+\bar{A}\right)^2}\right)^{\frac{1}{2}}\left(\frac{4\varepsilon_P}{K_1\left(2-K_1\sum_i M_{1,i}\right)}+\frac{2\varepsilon_Q\sqrt{\sum_i M_{2,i}}}{\sqrt{K_1K_2(\sum_i M_{1,i})(2-K_1\sum_i M_{1,i})(2-K_2\sum_i M_{2,i})}}\right)$$

$$\epsilon_V=\left(\frac{n}{\lambda_{\min}\left(L+\bar{A}\right)^2}\right)^{\frac{1}{2}}\left(\frac{4\varepsilon_Q}{K_2\left(2-K_2\sum_i M_{2,i}\right)}+\frac{2\varepsilon_P\sqrt{\sum_i M_{1,i}}}{\sqrt{K_1K_2(\sum_i M_{2,i})(2-K_1\sum_i M_{1,i})(2-K_2\sum_i M_{2,i})}}\right)$$

$$\epsilon_{pr}=2\varepsilon_P\left(\frac{n}{\lambda_{\min}(L+\bar{A})^2}\right)^{\frac{1}{2}}$$

and

$$\epsilon_{qr}=2\varepsilon_Q\left(\frac{n}{\lambda_{\min}\left(L+\bar{A}\right)^2}\right)^{\frac{1}{2}}$$

with some positive constants $M_{1,i}$ and $M_{2,i}$.

Proof: Lemma 1 illustrates that $\alpha_i^P(lT)=\alpha_0^P(lT)+\delta_i^P(lT)$ and $\alpha_i^Q(lT)=\alpha_0^Q(lT)+\delta_i^Q(lT)$ where $|\delta_i^P(lT)|\leq(n/[\lambda_{\min}(L+\bar{A})^2])^{(1/2)}\varepsilon_P$ and $|\delta_i^Q(lT)|\leq(n/[\lambda_{\min}(L+\bar{A})^2])^{(1/2)}\varepsilon_Q$ for each i and l, and thus (15) and (16) can be written as

$$\begin{aligned}&\alpha_0^P((l+1)T)\\&=\alpha_0^P(lT)-K_1\Big(\varphi_1\Big(\alpha_0^P(lT)+\delta_1^P(lT),\ldots,\alpha_0^P(lT)+\delta_n^P(lT)\\&\qquad\alpha_0^Q(lT)+\delta_1^Q(lT),\ldots,\alpha_0^Q(lT)+\delta_n^Q(lT)\Big)-P^{\mathrm{ref}}\Big)\end{aligned} \tag{30}$$

$$\begin{aligned}&\alpha_0^Q((l+1)T)\\&=\alpha_0^Q(lT)-K_2\Big(\varphi_2\Big(\alpha_0^P(lT)+\delta_1^P(lT),\ldots,\alpha_0^P(lT)+\delta_n^P(lT)\\&\qquad\alpha_0^Q(lT)+\delta_1^Q(lT),\ldots,\alpha_0^Q(lT)+\delta_n^Q(lT)\Big)-V^{\mathrm{ref}}\Big).\end{aligned} \tag{31}$$

Consider the candidate Lyapunov function for the closed-loop system (30) and (31) as

$$V_2(lT)=\left(\varphi_1(lT)-P^{\mathrm{ref}}\right)^2+\left(\varphi_2(lT)-V^{\mathrm{ref}}\right)^2.$$

The difference of V_1 with respect to time satisfies

$$\begin{aligned}\Delta V_2(lT)&=V_2((l+1)T)-V_2(lT)\\&=(\varphi_1((l+1)T)-\varphi_1(lT))(\varphi_1((l+1)T)-\varphi_1(lT)\\&\quad+2\left(\varphi_1(lT)-P^{\mathrm{ref}}\right))+(\varphi_2((l+1)T)-\varphi_2(lT))\\&\quad\cdot\left(\varphi_2((l+1)T)-\varphi_2(lT)+2\left(\varphi_2(lT)-V^{\mathrm{ref}}\right)\right).\end{aligned} \tag{32}$$

According to Property 1 and differential mean value theorem, it gets

$$\begin{aligned}
&\varphi_1((l+1)T) - \varphi_1(lT)\\
&\quad= \sum_i M_{1,i}\big(\alpha_0^P((l+1)T) - \alpha_0^P(lT)\big)\\
&\qquad+ \sum_i M_{1,i}\big(\delta_i^P((l+1)T) - \delta_i^P(lT)\big)\\
&\quad= -K_1\left(\sum_i M_{1,i}\right)\left(\varphi_1(lT) - P^{\text{ref}}\right)\\
&\qquad+ \sum_i M_{1,i}\big(\delta_i^P((l+1)T) - \delta_i^P(lT)\big)
\end{aligned}\tag{33}$$

$$\begin{aligned}
&\varphi_2((l+1)T) - \varphi_2(lT)\\
&\quad= \sum_i M_{2,i}\left(\alpha_0^Q((l+1)T) - \alpha_0^Q(lT)\right)\\
&\qquad+ \sum_i M_{2,i}\left(\delta_i^Q((l+1)T) - \delta_i^Q(lT)\right)\\
&\quad= -K_2\left(\sum_i M_{2,i}\right)\left(\varphi_2(lT) - V^{\text{ref}}\right)\\
&\qquad+ \sum_i M_{2,i}\left(\delta_i^Q((l+1)T) - \delta_i^Q(lT)\right)
\end{aligned}\tag{34}$$

where the constants $M_{1,i} = (\partial\varphi_1/\partial\alpha_i^P)|_{(\alpha_1^P,\ldots,\alpha_n^P)=\xi_1}$ and $M_{2,i} = (\partial\varphi_2/\partial\alpha_i^Q)|_{(\alpha_1^Q,\ldots,\alpha_n^Q)=\xi_2}$ with some constants $\xi_1, \xi_2 \in [0,1]^n$. Mentioned that $|\sum_i M_{1,i}(\delta_i^P((l+1)T) - \delta_i^P(lT))| \le 2\varepsilon_P(\sum_i M_{1,i})(n/[\lambda_{\min}(L+\bar{A})^2])^{(1/2)}$ and $|\sum_i M_{2,i}(\delta_i^Q((l+1)T) - \delta_i^Q(lT))| \le 2\varepsilon_Q(\sum_i M_{2,i})(n/[\lambda_{\min}(L+\bar{A})^2])^{(1/2)}$. According to LaSalle's theorem, substituting (33) and (34) into (32) yields that the trajectory of (30) and (31) converges into the set $S = \{|\varphi_1 - P^{\text{ref}}| \le \epsilon_P,\ |\varphi_2 - V^{\text{ref}}| \le \epsilon_V\}$ where ϵ_P and ϵ_V are given in this theorem. This result together with Lemma 1 concludes the proof. ■

Remark 4: The dynamical scenario of PV power regulation can be depicted as follows. The power grid is operated at the steady-state initially. When the disturbances such as load, sunlight, or reference values fluctuations occur, the system state will be deviated from the steady state. Then, the proposed PV control laws (9)–(12) and (17)–(22) adjust the power utilization ratios of PVs to stabilize the system. Mentioned that the desired power utilization ratios are calculated based on the deviations between the actual and reference values of power and voltage in (9) and (10), respectively. According to the definition of power utilization ratios, these variables are constrained in the range [0, 1]. This implies that the system can not be stabilized by PV's output power control when the extreme disturbance occurs, since the extreme disturbances (e.g., inappropriate reference value configuration) exceed the limitation of PVs regulation capability.

Remark 5: The regulation of parameters ε_P and ε_Q can influence the fluctuation range, triggering frequency, and stabilization time. Decreasing these parameters can reduce the fluctuation ranges ϵ_P, ϵ_V, ϵ_{pr}, and ϵ_{qr} according to Theorem 1, which means the higher control accuracy. However, it increases the settling time T^P and T^Q as shown in (23) and (24), which will take more time for stabilization. Moreover, it also increases the triggering frequency based on (21) and (22), which potentially increases the communication burdens. On the other hand, Increasing these parameters has the opposite effects. In practical application, these parameters should be chosen by trading between fluctuation tolerant level, communication network bandwidth limitation, and response time requirement.

Remark 6: The parameters constraints $(1/T_d) + (\varepsilon_P/4\beta_P T_f) < 1$ and $(1/T_d) + (\varepsilon_Q/4\beta_Q T_f) < 1$ in theorem means that the ratios (ε_P/β_P) and (ε_Q/β_Q) are related to the frequency and duration of the global DoS attack. The durable and dense global DoS attack implies small T_d and T_f as shown in Assumptions 1 and 2, and it further requires small ratios (ε_P/β_P) and (ε_Q/β_Q), which can be realized by decreasing the parameter ε_P and ε_Q. According to Remark 5, this indicates that the settling time and triggering frequency will be increased in order to resist the serious global DoS attack with long duration and high frequency.

V. Resilient Control for PVs Under Distributed DoS Attack

This section considers the case of the distributed DoS attack. The distributed self-triggered resilient control inputs for PV i is defined as

$$u_i^P(t) = \sum_{j=1}^n a_{ij}u_{ij}^P(t) + a_{i0}u_{i0}^P(t) \tag{35}$$

$$u_i^Q(t) = \sum_{j=1}^n a_{ij}u_{ij}^Q(t) + a_{i0}u_{i0}^Q(t). \tag{36}$$

Denoting the triggering time instant corresponding to auxiliary controls u_{ij}^P, u_{i0}^P, u_{ij}^Q, and u_{i0}^Q as t_k^{ij}, t_k^{i0}, τ_m^{ij}, and τ_m^{i0}, respectively, construct the following control laws for $t \in [lT, (l+1)T)$:

$$u_{ij}^P(t) = \begin{cases} \tilde{\beta}_P \cdot \text{sign}_{\tilde{\varepsilon}_P}\left(\alpha_j^P\left(t_k^{ij}\right) - \alpha_i^P(t_k^{ij})\right) \\ \qquad\qquad \text{if } t \in \left[t_k^{ij}, t_{k+1}^{ij}\right) \wedge t_k^{ij} \in \mathcal{H}^{ij}(0,t) \\ 0, \qquad\quad \text{if } t \in \left[t_k^{ij}, t_{k+1}^{ij}\right) \wedge t_k^{ij} \in \mathcal{A}^{ij}(0,t) \end{cases} \tag{37}$$

$$u_{ij}^Q(t) = \begin{cases} \tilde{\beta}_Q \cdot \text{sign}_{\tilde{\varepsilon}_Q}\left(\alpha_j^Q\left(\tau_m^{ij}\right) - \alpha_i^Q\left(\tau_m^{ij}\right)\right) \\ \qquad\qquad \text{if } t \in \left[\tau_m^{ij}, \tau_{m+1}^{ij}\right) \wedge \tau_m^{ij} \in \mathcal{H}^{ij}(0,t) \\ 0, \qquad\quad \text{if } t \in \left[\tau_m^{ij}, \tau_{m+1}^{ij}\right) \wedge \tau_m^{ij} \in \mathcal{A}^{ij}(0,t) \end{cases} \tag{38}$$

$$u_{i0}^P(t) = \begin{cases} \tilde{\beta}_P \cdot \text{sign}_{\tilde{\varepsilon}_P}\left(\alpha_0^P((l+1)T) - \alpha_i^P\left(t_k^{i0}\right)\right) \\ \qquad\qquad \text{if } t \in \left[t_k^{i0}, t_{k+1}^{i0}\right) \wedge t_k^{i0} \in \mathcal{H}^{i0}(0,t) \\ 0, \qquad\quad \text{if } t \in \left[t_k^{i0}, t_{k+1}^{i0}\right) \wedge t_k^{i0} \in \mathcal{A}^{i0}(0,t) \end{cases} \tag{39}$$

$$u_{i0}^Q(t) = \begin{cases} \tilde{\beta}_Q \cdot \text{sign}_{\tilde{\varepsilon}_Q}\left(\alpha_0^Q((l+1)T) - \alpha_i^Q\left(\tau_m^{i0}\right)\right) \\ \qquad\qquad \text{if } t \in \left[\tau_m^{i0}, \tau_{m+1}^{i0}\right) \wedge \tau_m^{i0} \in \mathcal{H}^{i0}(0,t) \\ 0, \qquad\quad \text{if } t \in \left[\tau_m^{i0}, \tau_{m+1}^{i0}\right) \wedge \tau_m^{i0} \in \mathcal{A}^{i0}(0,t) \end{cases} \tag{40}$$

where $\tilde{\beta}_P$, $\tilde{\beta}_Q$, $\tilde{\varepsilon}_P$, and $\tilde{\varepsilon}_Q$ are positive constants, $\mathcal{A}^{i0}(0,t)$ denotes the set of the DoS attack time on the communication channel between PV i and the detection unit, and

$\mathcal{H}^{i0}(0,t) = [0,t]\backslash\mathcal{A}^{i0}(0,t)$. The distributed self-triggered mechanism is designed as

$$t_{k+1}^{ij} = t_k^{ij} + \begin{cases} \max\left\{\frac{\tilde{\varepsilon}_P}{2\tilde{\beta}_P(|N_i|+|N_j|+a_{i0}+a_{j0})}, \frac{|\alpha_j^P(t_k^{ij})-\alpha_i^P(t_k^{ij})|}{2\tilde{\beta}_P(|N_i|+|N_j|+a_{i0}+a_{j0})}\right\} & \text{if } t_k^{ij} \in \mathcal{H}^{ij}(0,t) \\ \frac{\tilde{\varepsilon}_P}{2\tilde{\beta}_P(|N_i|+|N_j|+a_{i0}+a_{j0})}, & \text{if } t_k^{ij} \in \mathcal{A}^{ij}(0,t) \end{cases} \tag{41}$$

$$\tau_{m+1}^{ij} = \tau_m^{ij} + \begin{cases} \max\left\{\frac{\tilde{\varepsilon}_Q}{2\tilde{\beta}_Q(|N_i|+|N_j|+a_{i0}+a_{j0})}, \frac{\left|\alpha_j^Q\left(\tau_m^{ij}\right)-\alpha_i^Q\left(\tau_m^{ij}\right)\right|}{2\tilde{\beta}_Q(|N_i|+|N_j|+a_{i0}+a_{j0})}\right\} & \text{if } \tau_m^{ij} \in \mathcal{H}^{ij}(0,t) \\ \frac{\tilde{\varepsilon}_Q}{2\tilde{\beta}_Q(|N_i|+|N_j|+a_{i0}+a_{j0})}, & \text{if } \tau_m^{ij} \in \mathcal{A}^{ij}(0,t) \end{cases} \tag{42}$$

$$t_{k+1}^{i0} = t_k^{i0} + \begin{cases} \max\left\{\frac{\tilde{\varepsilon}_P}{4\tilde{\beta}_P(|N_i|+a_{i0})}, \frac{\left|\alpha_0^P((l+1)T)-\alpha_i^P\left(t_k^{i0}\right)\right|}{4\tilde{\beta}_P(|N_i|+a_{i0})}\right\} & \text{if } t_k^{i0} \in \mathcal{H}^{i0}(0,t) \\ \frac{\tilde{\varepsilon}_P}{4\tilde{\beta}_P(|N_i|+a_{i0})}, & \text{if } t_k^{i0} \in \mathcal{A}^{i0}(0,t) \end{cases} \tag{43}$$

$$\tau_{m+1}^{i0} = \tau_m^{i0} + \begin{cases} \max\left\{\frac{\tilde{\varepsilon}_Q}{4\tilde{\beta}_Q(|N_i|+a_{i0})}, \frac{\left|\alpha_0^Q((l+1)T)-\alpha_i^Q\left(\tau_m^{i0}\right)\right|}{4\tilde{\beta}_Q(|N_i|+a_{i0})}\right\} & \text{if } \tau_m^{i0} \in \mathcal{H}^{i0}(0,t) \\ \frac{\tilde{\varepsilon}_Q}{4\tilde{\beta}_Q(|N_i|+a_{i0})}, & \text{if } \tau_m^{i0} \in \mathcal{A}^{i0}(0,t). \end{cases} \tag{44}$$

Remark 7: In the control law (17)–(22) under the global DoS attack, PV i requests all of the neighbors' information simultaneously at each triggering time instant. However, in the resilient self-triggered control (35)–(44) under the distributed DoS attack, PV i requests its neighbors' information independently at the corresponding triggering time instant t_k^{ij} and τ_m^{ij} for each $j \in N_i$. This implies that the control law (35)–(44) is actually an edge-based algorithm, which is expected to be more appropriate for the case of the distributed DoS attack.

Remark 8: The self-triggered mechanism (41)–(44) implies that the intertrigger time intervals are lower bounded as $t_{k+1}^{ij} - t_k^{ij} \geq (\tilde{\varepsilon}_P/4n\tilde{\beta}_P)$ and $\tau_{m+1}^{ij} - \tau_m^{ij} \geq (\tilde{\varepsilon}_Q/4n\tilde{\beta}_Q)$ on each edge (i,j), which can exclude Zeno behavior.

Lemma 2: Set the parameters $\tilde{\beta}_P$, $\tilde{\beta}_Q$, $\tilde{\varepsilon}_P$, and $\tilde{\varepsilon}_Q$ in (35)–(44) as $(1/T_d^{ij})+(\tilde{\varepsilon}_P/[2\tilde{\beta}_P T_f^{ij}(|N_i|+|N_j|+a_{i0}+a_{j0})]) < 1$ and $(1/T_d^{ij})+(\tilde{\varepsilon}_Q/[2\tilde{\beta}_Q T_f^{ij}(|N_i|+|N_j|+a_{i0}+a_{j0})]) < 1$ for each $(i,j) \in \mathcal{E}$, and $(1/T_d^{i0})+(\tilde{\varepsilon}_P/[4\tilde{\beta}_P T_f^{i0}(|N_i|+a_{i0})]) < 1$ and $(1/T_d^{i0})+(\tilde{\varepsilon}_Q/[4\tilde{\beta}_Q T_f^{i0}(|N_i|+a_{i0})]) < 1$ for each i with $a_{i0} = 1$. In each time interval $[lT,(l+1)T)$, using the distributed resilient control (35)–(40) with the self-triggered mechanism (41)–(44) yields $\lim_{t\to(lT+\tilde{T}^P)} \alpha_i^P(t) = \tilde{\alpha}_{i,l}^P$ and $\lim_{t\to(lT+\tilde{T}^Q)} \alpha_i^Q(t) = \tilde{\alpha}_{i,l}^Q$ if $T > \max\{\tilde{T}^P, \tilde{T}^Q\}$ where $\tilde{\alpha}_{i,l}^P$ and $\tilde{\alpha}_{i,l}^Q$ are some constants. Moreover, the tracking errors $|\tilde{\alpha}_{i,l}^P - \tilde{\alpha}_{j,l}^P| \leq \tilde{\varepsilon}_P$, $|\tilde{\alpha}_{i,l}^Q - \tilde{\alpha}_{j,l}^Q| \leq \tilde{\varepsilon}_Q$, $|\tilde{\alpha}_{i,l}^P - \alpha_0^P((l+1)T)| \leq n\tilde{\varepsilon}_P$ and $|\tilde{\alpha}_{i,l}^Q - \alpha_0^Q((l+1)T)| \leq n\tilde{\varepsilon}_Q$, and the settling time

$$\tilde{T}^P = \left(\frac{\tilde{\varepsilon}_P}{4\tilde{\beta}_P(d_{\max}+1)} + \frac{\tilde{\varepsilon}_P}{4d_{\min}\tilde{\beta}_P} + \Phi_P\right)\frac{4n(d_{\max}+1)}{\tilde{\varepsilon}_P^2}$$

$$\tilde{T}^Q = \left(\frac{\tilde{\varepsilon}_Q}{4\tilde{\beta}_Q(d_{\max}+1)} + \frac{\tilde{\varepsilon}_Q}{4d_{\min}\tilde{\beta}_Q} + \Phi_Q\right)\frac{4n(d_{\max}+1)}{\tilde{\varepsilon}_Q^2}$$

where the constants

$$\Phi_P = \max\left\{\max_{(i,j)\in\mathcal{E}}\left\{\frac{\kappa^{ij} + \left(\eta^{ij}+1\right)\frac{\tilde{\varepsilon}_P}{2\tilde{\beta}_P(|N_i|+|N_j|+a_{i0}+a_{j0})}}{1-\frac{1}{T_d^{ij}}-\frac{\tilde{\varepsilon}_P}{2\tilde{\beta}_P T_f^{ij}(|N_i|+|N_j|+a_{i0}+a_{j0})}}\right\} \max_{i:a_{i0}=1}\left\{\frac{\kappa^{i0} + \left(\eta^{i0}+1\right)\frac{\tilde{\varepsilon}_P}{4\tilde{\beta}_P(|N_i|+a_{i0})}}{1-\frac{1}{T_d^{i0}}-\frac{\tilde{\varepsilon}_P}{4\tilde{\beta}_P T_f^{i0}(|N_i|+a_{i0})}}\right\}\right\}$$

$$\Phi_Q = \max\left\{\max_{(i,j)\in\mathcal{E}}\left\{\frac{\kappa^{ij} + \left(\eta^{ij}+1\right)\frac{\tilde{\varepsilon}_Q}{2\tilde{\beta}_Q(|N_i|+|N_j|+a_{i0}+a_{j0})}}{1-\frac{1}{T_d^{ij}}-\frac{\tilde{\varepsilon}_Q}{2\tilde{\beta}_Q T_f^{ij}(|N_i|+|N_j|+a_{i0}+a_{j0})}}\right\} \max_{i:a_{i0}=1}\left\{\frac{\kappa^{i0} + \left(\eta^{i0}+1\right)\frac{\tilde{\varepsilon}_Q}{4\tilde{\beta}_Q(|N_i|+a_{i0})}}{1-\frac{1}{T_d^{i0}}-\frac{\tilde{\varepsilon}_Q}{4\tilde{\beta}_Q T_f^{i0}(|N_i|+a_{i0})}}\right\}\right\}.$$

Proof: The proof is similar with that of Lemma 1 and it is explained briefly here. Without loss of generality, the following proof considers the system dynamic in time interval $[lT,(l+1)T)$ with $l=0$. Construct the candidate Lyapunov function $V_3 = (1/2)(e^P)^T e^P$. Since $|(e_j^P(t)-e_i^P(t))-(e_j^P(t_k^{ij})-e_i^P(t_k^{ij}))| \leq \int_{t_k^{ij}}^t (|(d/dt)\alpha_j^P(s)| + |(d/dt)\alpha_i^P(s)|)ds \leq \tilde{\beta}_P(|N_i|+|N_j|+a_{i0}+a_{j0})(t-t_k^{ij})$, we have $\text{sign}(e_j^P(t)-e_i^P(t)) = \text{sign}_{\tilde{\varepsilon}_P}(e_j^P(t_k^{ij})-e_i^P(t_k^{ij}))$ and $|e_j^P(t)-e_i^P(t)| \geq (1/2)|e_j^P(t_k^{ij})-e_i^P(t_k^{ij})|$ for $t \in [t_k^{ij}, t_{k+1}^{ij})$ if the edge $(i,j) \in \mathcal{E}\cap S_3\cap S_4$ according to the similar analysis shown in the proof of Lemma 1, where the sets $S_3 = \{(i,j) : |e_j^P(t_k^{ij})-e_i^P(t_k^{ij})| > \tilde{\varepsilon}_P\}$ and $S_4 = \{(i,j) : t_k^{ij} \in \mathcal{H}^{ij}(0,t)\}$. Moreover, it gets $\text{sign}(e_i^P(t)) = \text{sign}_{\tilde{\varepsilon}_P}(e_i^P(t_k^{i0}))$ and $|e_i^P(t)| \geq (3/4)|e_i^P(t_k^{i0})|$ for $t \in [t_k^{i0}, t_{k+1}^{i0})$ if $a_{i0}=1$ and $i \in S_5\cap S_6$ where the sets $S_5 = \{i : t_k^{i0} \in \mathcal{H}^{i0}(0,t)\}$ and $S_6 = \{i : |e_i^P(t_k^{i0})| > \tilde{\varepsilon}_P\}$. Let $t_k^{ij} = \max\{t_s^{ij} : t_s^{ij} \leq t\}$ for $j = 0,1,\ldots,n$, the above results indicate that the derivation of V_3 with respect to time along the solution of the closed-loop system satisfies

$$\begin{aligned}\frac{d}{dt}V_3 &= -\tilde{\beta}_P \sum_{(i,j)\in\mathcal{E}\cap S_3\cap S_4}\left(e_j^P(t)-e_i^P(t)\right)\cdot\text{sign}_{\tilde{\varepsilon}_P}\left(e_j^P\left(t_k^{ij}\right)-e_i^P\left(t_k^{ij}\right)\right) \\ &\quad - \tilde{\beta}_P \sum_{i\in S_5\cap S_6} a_{i0}\left(e_i^P(t)\right)\cdot\text{sign}_{\tilde{\varepsilon}_P}\left(e_i^P\left(t_k^{i0}\right)\right) \\ &\leq -\frac{\tilde{\beta}_P}{2}\sum_{(i,j)\in\mathcal{E}\cap S_3\cap S_4}\left|e_j^P\left(t_k^{ij}\right)-e_i^P\left(t_k^{ij}\right)\right| \\ &\quad - \frac{3\tilde{\beta}_P}{4}\sum_{i\in S_5\cap S_6} a_{i0}\left|e_i^P\left(t_k^{i0}\right)\right| \\ &\leq -\frac{\tilde{\beta}_P}{2}\sum_{(i,j)\in\mathcal{E}\cap S_3\cap S_4}\tilde{\varepsilon}_P - \frac{3\tilde{\beta}_P}{4}\sum_{i\in S_5\cap S_6} a_{i0}\tilde{\varepsilon}_P.\end{aligned} \tag{45}$$

Formula (45) implies that there exists a fixed time instant $\tilde{t}_P^*$ such that $(\mathcal{E}\cap S_3\cap S_4) = (S_5\cap S_6) = \emptyset$, $\alpha_i^P(t) = \tilde{\alpha}_{i,l}^P$, and $u_{ij}^P(t) = u_{i0}^P(t) = 0$ for any i,j and $t > \tilde{t}_P^*$.

Constructing the time intervals $\bar{\mathcal{H}}^{ij}(\tau,t)=[\tau,t]\backslash\bar{\mathcal{A}}^{ij}(\tau,t)$ and $\bar{\mathcal{H}}^{i0}(\tau,t)=[\tau,t]\backslash\bar{\mathcal{A}}^{i0}(\tau,t)$ where $\bar{\mathcal{A}}^{ij}(\tau,t)=\bigcup_{k\in\mathbb{Z}_{\geq 0}}[h_k^{ij},h_k^{ij}+\tau_k^{ij}+(\tilde{\varepsilon}_P/[2\tilde{\beta}_P(|N_i|+|N_j|+a_{i0}+a_{j0})]))\cap[\tau,t]$ and $\bar{\mathcal{A}}^{i0}(\tau,t)=\bigcup_{k\in\mathbb{Z}_{\geq 0}}[h_k^{i0},h_k^{i0}+\tau_k^{i0}+(\tilde{\varepsilon}_P/[4\tilde{\beta}_P(|N_i|+a_{i0})]))\cap[\tau,t]$, the parameters constraints $(1/T_d^{ij})+(\tilde{\varepsilon}_P/[2\tilde{\beta}_P T_f^{ij}(|N_i|+|N_j|+a_{i0}+a_{j0})])<1$ and $(1/T_d^{i0})+(\tilde{\varepsilon}_P/[4\tilde{\beta}_P T_f^{i0}(|N_i|+a_{i0})])<1$ lead that there exists some time instant $\tilde{t}_P^{**}$ such that each of the PVs acquires all of its neighbors' information successfully at least one time in the interval $[\tilde{t}_P^*,\tilde{t}_P^{**})$ since $|\bar{\mathcal{H}}^{ij}(\tilde{t}_P^*,\tilde{t}_P^{**})|>0$ and $|\bar{\mathcal{H}}^{i0}(\tilde{t}_P^*,\tilde{t}_P^{**})|>0$. This further implies that the tracking error satisfies $|\tilde{\alpha}_{i,l}^P-\tilde{\alpha}_{j,l}^P|\leq\tilde{\varepsilon}_P$ and $|\tilde{\alpha}_{i,l}^P-\alpha_0^P((l+1)T)|\leq n\tilde{\varepsilon}_P$ for all $i,j\in\mathcal{V}$. The settling time $\tilde{T}^P$ estimation method is very similar to that in the proof of Lemma 1 and we omit it here. The result about reactive power utilization ratio control can be proved by the above method. ■

Based on Lemma 2, the main result in this section can be obtained in the following theorem. The proof is very similar with that in Theorem 1 and is omitted here.

Theorem 2: Considering the case of the distributed DoS attack, control objectives 1 and 2 can be achieved under the desired utilization ratio control (9) and (10) and the distributed resilient self-triggered control (11) and (12) with (35)–(44) by setting the parameters as those in Lemma 2, the fluctuation ranges in (7) and (8) satisfy

$$\begin{aligned}\epsilon_P=&\frac{4n\tilde{\varepsilon}_P}{K_1\left(2-K_1\sum_i\tilde{M}_{1,i}\right)}\\&+\frac{2n\tilde{\varepsilon}_Q\sqrt{\sum_i\tilde{M}_{2,i}}}{\sqrt{K_1K_2\left(\sum_i\tilde{M}_{1,i}\right)\left(2-K_1\sum_i\tilde{M}_{1,i}\right)\left(2-K_2\sum_i\tilde{M}_{2,i}\right)}}\\\epsilon_V=&\frac{4n\tilde{\varepsilon}_Q}{K_2\left(2-K_2\sum_i\tilde{M}_{2,i}\right)}\\&+\frac{2n\tilde{\varepsilon}_P\sqrt{\sum_i\tilde{M}_{1,i}}}{\sqrt{K_1K_2\left(\sum_i\tilde{M}_{2,i}\right)\left(2-K_1\sum_i\tilde{M}_{1,i}\right)\left(2-K_2\sum_i\tilde{M}_{2,i}\right)}}\end{aligned}$$

$\epsilon_{pr}=\tilde{\varepsilon}_P$, and $\epsilon_{qr}=\tilde{\varepsilon}_Q$ with some positive constants $\tilde{M}_{1,i}$ and $\tilde{M}_{2,i}$.

Remark 9: Similar to the analysis in Remarks 5 and 6, decreasing the parameters $\tilde{\varepsilon}_P$ and $\tilde{\varepsilon}_Q$ in (35)–(44) reduces the fluctuation ranges ϵ_P, ϵ_V, ϵ_{pr}, and ϵ_{qr} to make a higher control accuracy. However, it increases the communication burdens and makes a longer stabilization time, and vice versa. Moreover, the worse the distributed DoS attack is, the smaller ratios $(\tilde{\varepsilon}_P/\tilde{\beta}_P)$ and $(\tilde{\varepsilon}_Q/\tilde{\beta}_Q)$ should be selected.

VI. Simulation

The effectiveness of the proposed control strategy is verified by the radial network with five PVs shown in Fig. 1. The red dashed lines denote the communication network connecting the controller of PVs and detection unit. The parameters of the test system are presented as follows.

1) The voltage at primary and secondary sides of transformer are 10 and 380 V, respectively.
2) The maximum of every PV is 10 kW + j10kVar.

TABLE I
Load Information

Load	L_1	L_2	L_3	L_4	L_5	L_6	L_7
Active power (kW)	2	1	5	3	4	6	5
Reactive power (kVar)	5	2	6	10	8	4	5

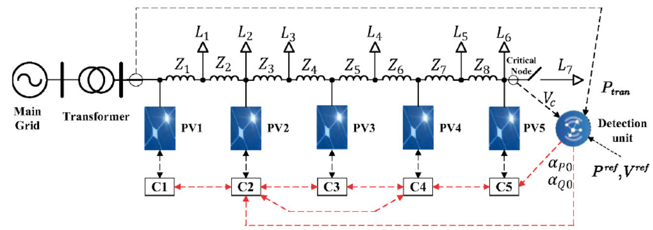


Fig. 1. Test System with multiple PVs.

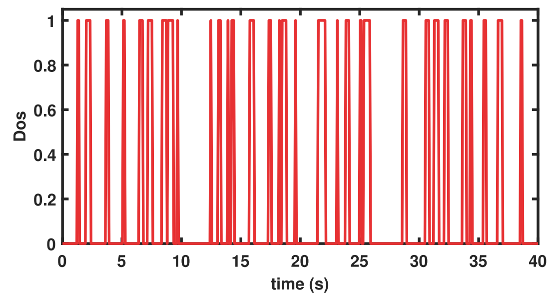


Fig. 2. Global DoS attack mode.

3) The reference values of active power flow across certain transmission line and voltage at a critical bus are set as $P^{\text{ref}}=15$ kW and $V^{\text{ref}}=311$ V.
4) The impedance of each segment of transmission line is $Z_i=0.188+j0.127\ \Omega$ for $i=1,2,\ldots,8$.
5) The spot loads are given in Table I.

Mentioned that the communication network between the PVs and detection unit is connected and suffers from the DoS attack. PV 2 and PV 5 can receive the information of desired utilization ratios α_0^P and α_0^Q from the detection unit. Each of the PVs outputs its maximal active power 10 kW and minimal reactive power 0Var at the initial stage, and then the proposed distributed resilient self-triggered control is activated at 0.8 s to regulate the power output of PVs. The expected disturbance is that load L_7 is connected to the power system at 20 s, which increases the total active and reactive power demands by 5 kW and 5 kVar, respectively.

A. System Response Under Global DoS Attack

This section considers the case of the global DoS attack where the attack signal and its dwell time are shown in Fig. 2. The value 1 at the ordinate means that all the communication channels are jammed caused by the global DoS attack and the value 0 implies that all the channels are unobstructed. The global DoS attack is turned on and off 35 times during the time interval [0, 40] s, and the starting time and duration of each attack are generated randomly with the maximal duration 0.6 s. The average duty cycle of the global DoS attack is 22.1%.

The simulation results are given in Figs. 4 and 5 by setting the parameters in the resilient control strategy (9)–(12)

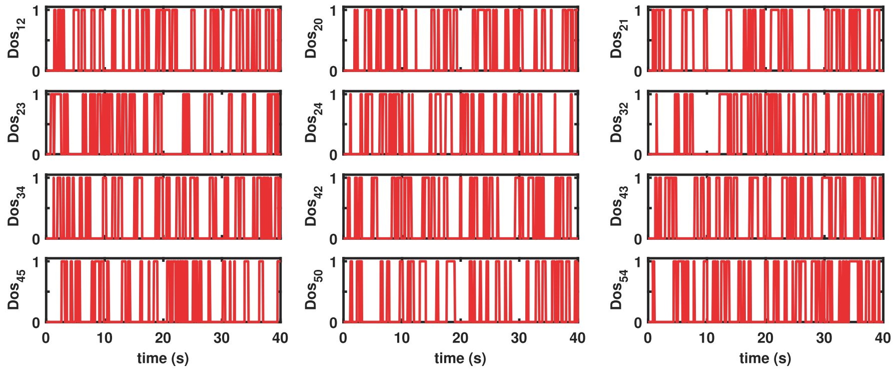
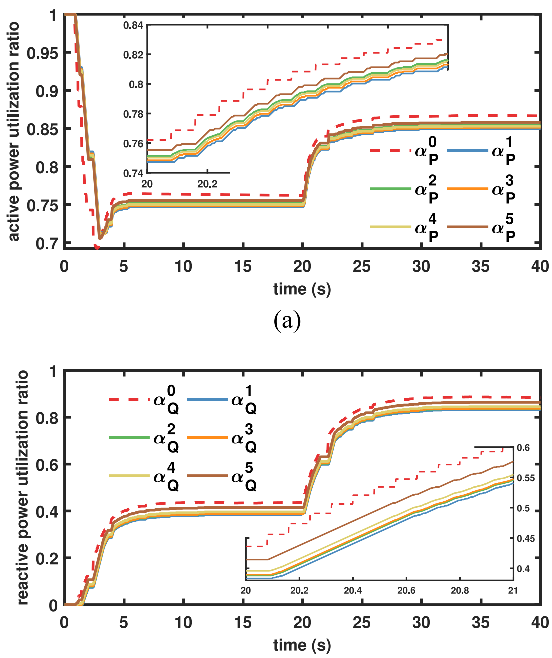


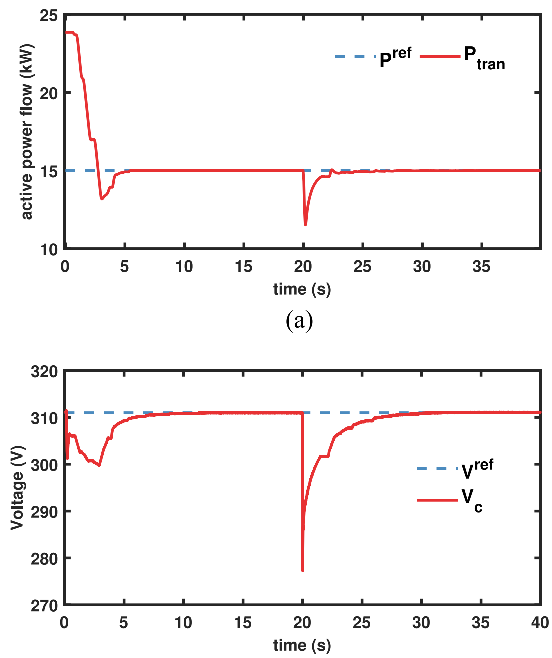
Fig. 3. Distributed DoS attack mode.



(a)

(b)

Fig. 4. Evolution of PVs' utilization ratios under the global DoS attack about: (a) active power output and (b) reactive power output.



(a)

(b)

Fig. 5. Evolution under the global DoS attack about: (a) active power across the concerned line and (b) voltage of the critical bus.

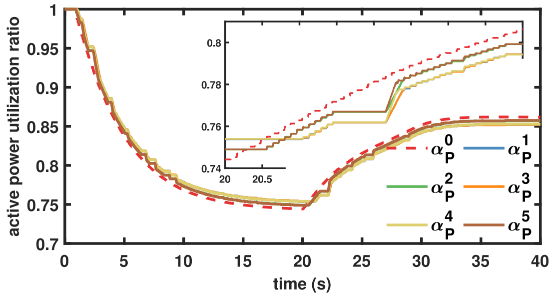
and (17)–(22) as $\varepsilon_P = \varepsilon_Q = 0.005$, $\beta_P = \beta_Q = 0.2$, $K_1 = 0.003$, $K_2 = 0.001$, and $T = 0.08$ s. Fig. 4 illustrates that the detection unit updates the desired utilization ratios every T units of time, and the active and reactive power output ratios of each PV track their desired values within an allowable deviation ranges. This demonstrates that the fair utilization of PVs can be realized under the proposed control method. Moreover, it can be seen that the power output of PVs keeps constant during the DoS attack intervals. Fig. 5 shows that the active power flow and voltage of the critical bus can be restored to their reference values at the initial stage and the load fluctuation time. The simulation results verify the effectiveness of the resilient control method of PV under the global DoS attack in achieving the control objectives given in Section II.

B. System Response Under Distributed DoS Attack

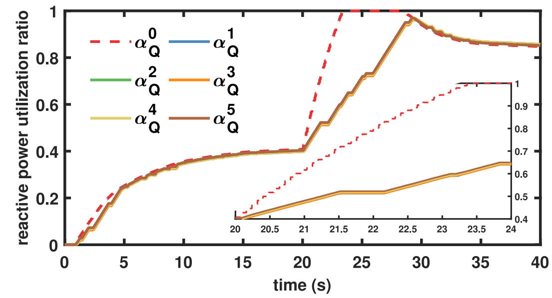
The case of the distributed DoS attack is considered in this section, and the attack signals and dwell time are shown in Fig. 3, where DoS attack affects each of the communication channels independently and the average duty cycle is given as Table II. For each channel, the total number of the DoS attack is 30 and the starting time and duration are random. Setting the parameters in control law (9)–(12) and (35)–(44) as $\tilde{\varepsilon}_P = \tilde{\varepsilon}_Q = 0.005$, $\tilde{\beta}_P = \tilde{\beta}_Q = 0.4$, $K_1 = 0.003$, $K_2 = 0.002$ and $T = 0.08$ s, Figs. 6 and 7 illustrate the ability of proposed resilient control method in reaching control objectives 1 and 2 under

TABLE II
DoS AVERAGE DUTY CYCLE OVER COMMUNICATION CHANNELS

Channel	Duty cycle	Channel	Duty cycle
{1,2}	32.13%	{2.0}	29.63%
{2,1}	31.84%	{2,3}	30.2%
{2,4}	25.45%	{3,2}	32.27%
{3,4}	30.97%	{4,2}	31.1%
{4,3}	36.35%	{4,5}	28.42%
{5,4}	27.43%	{5,0}	32.91%

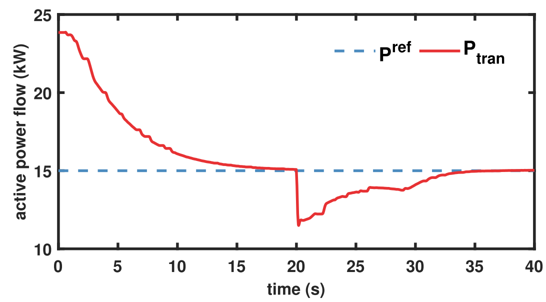


(a)

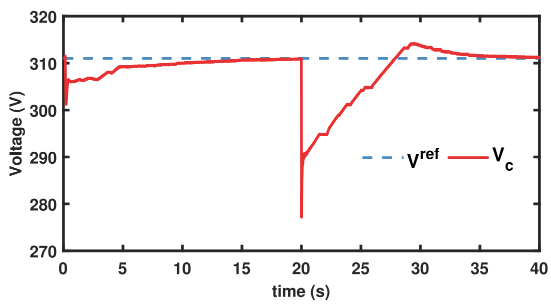


(b)

Fig. 6. Evolution of PVs' utilization ratios under the distributed DoS attack about: (a) active power output and (b) reactive power output.



(a)



(b)

Fig. 7. Evolution under the distributed DoS attack about: (a) active power across the concerned line and (b) voltage of the critical bus.

the distributed DoS attack. Compared with the results shown in Figs. 4 and 5 under the global DoS attack, the stabilization time is lengthened and the overshoot occurs in the case of the distributed DoS attack given in Figs. 6 and 7. Compared with the case of the global DoS attack, it seems from the simulation results that more control performance should be sacrificed to resist the distributed DoS attack.

VII. Conclusion

This article has investigated the distributed resilient cooperative control for multiple PVs in distribution network under two types of the DoS attack, where the global DoS attack jams all the communication channels and the distributed one jams each of the channels independently. It aims to realize the fair utilization of all PVs, and restore the active power flow across certain transmission line and the voltage of the critical bus to their reference values, respectively. Moreover, the self-triggered mechanism is introduced to reduce the communication burdens. The theoretical analysis explains that the control task can be fulfilled overcoming the DoS attack influence and limitation of communication resource. Furthermore, the impacts of DoS attack duration and frequency on the stabilization time and triggering frequency are characterized. The simulation result is provided to verify the effectiveness of the theoretical method. Our future research topics focus on the other types of cyber-attack in the distributed control of PVs, such as replay attack, false data injection attack, and the attack with stealthy characteristic.

References

[1] F. Katiraei and M. R. Iravani, "Power management strategies for a microgrid with multiple distributed generation units," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1821–1831, Nov. 2006.

[2] M. Malinowski, J. I. Leon, and H. Abu-Rub, "Solar photovoltaic and thermal energy systems: Current technology and future trends," *Proc. IEEE*, vol. 105, no. 11, pp. 2132–2146, Nov. 2017.

[3] H. Zhang, D. Yue, X. Xie, S. Hu, and S. Weng, "Multi-elite guide hybrid differential evolution with simulated annealing technique for dynamic economic emission dispatch," *Appl. Soft Comput.*, vol. 34, pp. 312–323, Sep. 2015.

[4] F. Yang, Q. Sun, Q.-L. Han, and Z. Wu, "Cooperative model predictive control for distributed photovoltaic power generation systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 4, no. 2, pp. 414–420, Jun. 2016.

[5] H. Xin, Z. Lu, Z. Qu, D. Gan, and D. Qi, "Cooperative control strategy for multiple photovoltaic generators in distribution networks," *IET Control Theory Appl.*, vol. 5, no. 14, pp. 1617–1629, 2011.

[6] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, Jan. 2007.

[7] H. Xin, Z. Qu, J. Seuss, and A. Maknouninejad, "A self-organizing strategy for power flow control of photovoltaic generators in a distribution network," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1462–1473, Aug. 2011.

[8] X. Chen *et al.*, "Consensus-based distributed control for photovoltaic-battery units in a DC microgrid," *IEEE Trans. Ind. Electron.*, vol. 66, no. 10, pp. 7778–7787, Oct. 2019.

[9] R. Zhang and B. Hredzak, "Nonlinear sliding mode and distributed control of battery energy storage and photovoltaic systems in AC microgrids with communication delays," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 5149–5160, Sep. 2019.

[10] Y. Pan, A. Sangwongwanich, Y. Yang, and F. Blaabjerg, "Distributed control of islanded series PV-battery-hybrid systems with low communication burden," *IEEE Trans. Power Electron.*, vol. 36, no. 9, pp. 10199–10213, Sep. 2021.

[11] N. Poursafar, S. Taghizadeh, M. J. Hossain, and J. M. Guerrero, "An optimized distributed cooperative control to improve the charging performance of battery energy storage in a multiphotovoltaic islanded DC microgrid," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1170–1181, Mar. 2022.

[12] X.-M. Zhang and Q.-L. Han, "Network-based H_∞ filtering using a logic jumping-like trigger," *Automatica*, vol. 49, no. 5, pp. 1428–1435, 2013.

[13] S. S. Kia, J. Cortés, and S. Martínez, "Distributed event-triggered communication for dynamic average consensus in networked systems," *Automatica*, vol. 59, pp. 112–119, Sep. 2015.

[14] S. Hu, D. Yue, X. Xie, Y. Ma, and X. Yin, “Stabilization of neural-network-based control systems via event-triggered control with nonperiodic sampled data,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 3, pp. 573–585, Mar. 2018.

[15] X. Chen, H. Yu, and F. Hao, “Prescribed-time event-triggered bipartite consensus of multiagent systems,” *IEEE Trans. Cybern.*, vol. 52, no. 4, pp. 2589–2598, Apr. 2022.

[16] A. I. Rikos and C. N. Hadjicostis, “Event-triggered quantized average consensus via ratios of accumulated values,” *IEEE Trans. Autom. Control*, vol. 66, no. 3, pp. 1293–1300, Mar. 2021.

[17] S. Weng, D. Yue, and J. Shi, “Distributed cooperative control for multiple photovoltaic generators in distribution power system under event-triggered mechanism,” *J. Franklin Inst.*, vol. 353, no. 14, pp. 3407–3427, 2016.

[18] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, “Bibliographical review on cyber attacks from a control oriented perspective,” *Annu. Rev. Control*, vol. 48, pp. 103–128, Jan. 2019.

[19] P. Li, Y. Liu, H. Xin, and X. Jiang, “A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks,” *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4343–4352, Oct. 2018.

[20] A. Cetinkaya, H. Ishii, and T. Hayakawa, “An overview on denial-of-service attacks in control systems: Attack models and security analyses,” *Entropy*, vol. 21, no. 2, p. 210, 2019.

[21] J. Liu, Y. Gu, L. Zha, Y. Liu, and J. Cao, “Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1665–1678, Aug. 2019.

[22] C. Peng, J. Li, and M. Fei, “Resilient event-triggering H_∞ load frequency control for multi-area power systems with energy-limited DoS attacks,” *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 4110–4118, Sep. 2017.

[23] L. Ding, Q.-L. Han, B. Ning, and D. Yue, “Distributed resilient finite-time secondary control for heterogeneous battery energy storage systems under denial-of-service attacks,” *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4909–4919, Jul. 2020.

[24] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, “A survey on security communication and control for smart grids under malicious cyber attacks,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1554–1569, Aug. 2019.

[25] R. Olfati-Saber and R. M. Murray, “Consensus problems in networks of agents with switching topology and time-delays,” *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1520–1533, Sep. 2004.

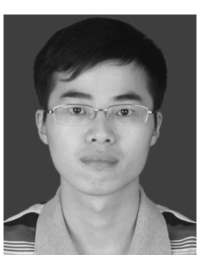
[26] Y. Hong, J. Hu, and L. Gao, “Tracking control for multi-agent consensus with an active leader and variable topology,” *Automatica*, vol. 42, no. 7, pp. 1177–1182, 2006.

[27] Z. Feng and G. Hu, “Secure cooperative event-triggered control of linear multiagent systems under DoS attacks,” *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 3, pp. 741–752, May 2020.

[28] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2005, pp. 46–57.

[29] S. Feng and P. Tesi, “Resilient control under denial-of-service: Robust design,” *Automatica*, vol. 79, pp. 42–51, May 2017.

[30] D. Senejohnny, P. Tesi, and C. De Persis, “A jamming-resilient algorithm for self-triggered network coordination,” *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 981–990, Sep. 2018.



Shengxuan Weng received the B.S. degree in applied mathematics from the School of Mathematics and Statistics, Huazhong University of Science and Technology, Wuhan, China, in 2009, and the Ph.D. degree in automation from the School of Automation, Huazhong University of Science and Technology, in 2014.

He is currently an Associate Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include distributed control, multiagent systems, and control approach in microgrid and smart grid.

Dong Yue (Fellow, IEEE) received the Ph.D. degree in automation from the South China University of Technology, Guangzhou, China, in 1995.

He is currently a Professor and the Dean of the Institute of Advanced Technology and the College of Automation and AI, Nanjing University of Posts and Telecommunications, Nanjing, China. He has published more than 250 articles in international journals and two books. He holds more than 50 patents. His research interests include analysis and synthesis of networked control systems, multiagent systems, optimal control of power systems, and the Internet of Things.

Prof. Yue has served as an Associate Editor for *IEEE Industrial Electronics Magazine*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, *Journal of the Franklin Institute*, and *International Journal of Systems Sciences*, and the Guest Editor for Special Issue on New Trends in Energy Internet: Artificial Intelligence-based Control, Network Security and Management and IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS.

Jianbo Chen received the B.S. degree in automation from the School of Electrical Engineering and Automation, Nanjing University of Posts and Telecommunications, Nanjing, China, in 2015, where he is currently pursuing the Ph.D. degree in automation.

His current research interests include distributed control, event-triggered control, parallel control of multiple inverters, and power quality improvement of the microgrid.

Xiangpeng Xie (Member, IEEE) received the B.S. and Ph.D. degrees in engineering from Northeastern University, Shenyang, China, in 2004 and 2010, respectively.

From 2012 to 2014, he was a Postdoctoral Fellow with the Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan, China. He is currently a Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include fuzzy modeling and control synthesis, state estimations, optimization in process industries, and intelligent optimization algorithms.

Chunxia Dou (Senior Member, IEEE) received the B.S. and M.S. degrees in automation from Northeast Heavy Machinery Institute, Qiqihaer, China, in 1989 and 1994, respectively, and the Ph.D. degree in measurement technology and instrumentation from the Institute of Electrical Engineering, Yanshan University, Qinhuangdao, China, in 2005.

In 2010, she joined the Department of Engineering, Peking University, Beijing, China, where she was a Postdoctoral Fellow for two years. Since 2005, she has been a Professor with the Institute of Electrical Engineering, Yanshan University, and a Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. Her current research interests include multiagent-based control, event-triggered hybrid control, distributed coordinated control, and multimode switching control and their applications in power systems, microgrids, and smart grids.