Distributed Cooperative Event-Triggered Control of Cyber-Physical AC Microgrids Subject to Denial-of-Service Attacks

Jamali, Mahmood ; Reza Baghaee, Hamid; Sadabadi, Mahdieh S.; B. Gharehpetian, Gevork; Anvari-Moghaddam, Amjad

Published in:
I E E E Transactions on Smart Grid

DOI (link to publication from Publisher):
10.1109/TSG.2023.3259545

Publication date:
2023

Document Version
Accepted author manuscript, peer reviewed version

Distributed Cooperative Event-Triggered Control of Cyber-Physical AC Microgrids Subject to Denial-of-Service Attacks

Mahmood Jamali, Hamid Reza Baghaee, *Member, IEEE*, Mahdieh S. Sadabadi, *Senior Member, IEEE*, Gevorg B. Gharehpetian, *Senior Member, IEEE*, and Amjad Anvari-Moghaddam, *Senior Member, IEEE*

***Abstract*—This paper addresses the event-triggered distributed cooperative secure secondary control for islanded cyber-physical inverter-based ac microgrids (MGs) under the energy-limited denial of service (DoS) attacks. The DoS attack refers to the prevention of information exchange among Distributed Energy Resources (DERs) in the secondary control level. In this paper, an event-triggered mechanism (ETM) is employed to improve communication efficiency and reduce control command updates. Based on the last successful local and neighboring transmission attempt, an estimator is proposed which is only activated over attack periods. In addition, this study investigates the contribution of both DERs and Distributed Energy Storage Systems (DESS) in ac MGs. Finally, the performance of the proposed control scheme is evaluated by an offline digital time-domain simulation on a test MG system through different scenarios in MATLAB/Simulink environment. Also, the effectiveness and accuracy of the controller are verified by comparison with several previous studies.**

***Index Terms*—Distributed secondary control, DoS attacks, event-triggered mechanism, SoC balancing, voltage regulation and frequency synchronization.**

NOMENCLATURE

A. Main DERs Variables

v_i^n, w_i^n	Voltage and frequency reference values.
v_{odi}, v_{oqi}	Direct and quadrature components of the output voltage.
P_i, Q_i, SoC_i	Active power, reactive power and state of charge.
m_i^P, n_i^Q, m_i^S	Active power, reactive power and state of charge droop gains.
υ_i, u_i^ω, u_i^P, u_i^S	Auxiliary voltage, frequency, active power ans state of charge inputs.

B. Controllers Parameters

c_v, c_ω, c_P, c_S	Positive control gains.
K_v, K_ω, K_P,K_S	Designed control matrices.
ξ_i^v, ξ_i^ω, ξ_i^P, ξ_i^S	Measurements errors of voltage, frequency, active power and state of charge.
d_i^v, d_i^ω	Consensus errors of the measurement values and the reference values of voltage and frequency.
q_i^v, q_i^ω, q_i^P, q_i^S	Consensus errors of voltage, frequency, active power and state of charge.
$\hat{q}_i^v$, $\hat{q}_i^\omega$, $\hat{q}_i^P$, $\hat{q}_i^S$	Estimated consensus errors of voltage, frequency, active power and state of charge.
γ, α^v, α^ω,α^P, α^S	Positive constants.
β_i^v, β_i^ω, β_i^P, β_i^S	Constants $\in (0,1)$.
E_i^v, E_i^ω, E_i^P, E_i^S	Triggering functions of voltage, frequency, active power, and state of charge.
$t_{i,v}^k$, $t_{i,\omega}^k$, $t_{i,P}^k$, $t_{i,S}^k$	k-the triggering sequence of voltage, frequency, active power, and state of charge.

M. Jamali is with the Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield S1 3JD, United Kingdom, (e-mail: mahmood.jamali@sheffield.ac.uk).

H.R. Baghaee is with the Faculty of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, Iran, e-mail: hrbaghaee@modares.ac.ir.

G. B. Gharehpetian is with the Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran, (e-mail: grptian@aut.ac.ir).

M.S. Sadabadi is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London, United Kingdom (e-mail: m.sadabadi@qmul.ac.uk).

A. Anvari-Moghaddam is with the Department of Energy, Aalborg University, Aalborg 9220, Denmark, (e-mail: aam@energy.aau.dk).

I. INTRODUCTION

MICROGRIDS (MGs) have been introduced as interconnected small-scale Distributed Energy Resources (DERs) consisting of Distributed Generations (DGs), Distributed Energy Storage Systems (DESS), and loads. MGs can generally operate in the grid-connected mode or the islanded mode. In this paper, the focus is on the islanded mode, where the MG becomes disconnected from the main grid. The main control goals of islanded cyber-physical MGs are to keep voltage and frequency to their reference values, and also State of Charge (SoC) balancing of DESS [1]. To meet control objectives, a hierarchical control structure has been introduced, including three levels: primary (droop control, primary stabilization, Plug and Play (PnP) functionality among DGs), secondary (restoration of voltage and frequency), and tertiary (optimal energy management) [2]. Due to unavoidable deviations of voltage and frequency from their rated values in the steady-state caused by droop control at the primary level, the secondary control layer is employed to achieve voltage regulation and frequency synchronization [3]. The secondary controller can be implemented in a centralized, decentralized, or distributed manner [4]. Because of major drawbacks of the central control strategy, e.g., single-point failures, poor PnP capability, and low fault tolerance performance [5], the distributed control strategy has been proposed for the secondary control level to improve the performance and reliability of MGs.

In the distributed control manner, the cyber-physical MG can be viewed as a cooperative system where each DER represents an agent. The communication among local controllers allows the cooperation of DER units and smooth switching operations [6]–[10]. Although communication infrastructures make the distributed control implementation possible, might conduct disparate limitations and issues in MGs, e.g. time-delay [11], [12], [13], fault [1], [14] and infinite-time problem for the consensus [15].

In addition, cyber-physical MGs are more prone to various kinds of cyber attacks in a distributed manner that can destabilize the MG and affect its performance. Cyber attacks in control systems can be mainly categorized into False Data Injection (FDI) [16] and denial of service (DoS) attacks [17]. FDI attacks change or destroy the real data in sensors, actuators, and communication networks by injecting or modifying the signals [18], [13]. Researchers in [19] present an attack-resilient control framework for ac MGs regardless of the FDI in communication and control channels by introducing a hidden layer. Also, an observer-based finite-time control scheme is proposed in [20] to improve the resilience of ac MGs under FDI attacks. Even though there exist several research studies on attack-resilient control of ac MGs under FDI attacks, papers focusing on DoS attacks only investigate stability analysis of MGs [21], [22]. In [23], a game strategy defense mechanism is also introduced to deal with the DoS attack issues in MGs, but it is assumed that all players cannot achieve the global equilibrium point simultaneously.

Note that some literature has only addressed distributed event-triggered control of "*dc MGs*" in presence of DoS attacks [24]–[26].Moreover, most of the reported works have presented continuous-time control schemes, where data communication among DERs and control updates from the secondary layer are accomplished continuously for each instance. Applying such controllers might lead to computation burden and inefficient use of communication resources. In other words, continuous data transmissions are not essential for the desired control performance in the secondary layer. For example, authors in [27] have developed a secondary controller for energy storage systems against DoS attacks, where an acknowledgment-based attack identification approach and a communication network recovery method is used to alleviate the effect of attacks. However, this control strategy still relies on continuous control updates. As a result, event-triggered control mechanisms are employed in the secondary control layer of MGs to avoid generating unnecessary information exchange [28]–[31].

While the discussed papers are very encouraging, further research is yet required to address the resilient event-triggered control of ac MGs under DoS. In this paper, a distributed cooperative event-triggered secondary control scheme is proposed for islanded ac MGs exposed to DoS attacks. To do so, an estimator—operating during the attack period—is designed to predict the neighbors' states for each DER whereas the MG system is subject to attacks. Then, Event-Triggered Mechanisms (ETM) are applied to determine control updates for each DG/DESS. The main feature of the proposed control scheme is that each DER/DESS can decide when to update the control input in its triggering instants, which results in reducing the number of control updates. The distributed cooperative control scheme is combined with ETM into the secondary control layer to return voltage/frequency, active power-sharing, and SoC balancing on track under random DoS attacks. The non-occurrence of the Zeno phenomenon is also proved in the closed-loop control system of the MG. The paper's contributions are summarized as follows.

- A resilient event-triggered distributed cooperative control scheme is proposed for islanded ac MGs in the secondary layer, which can restore the voltage/frequency and ensure active power management and SoC matching against DoS attacks (see Fig. 1).
- The event-based scheme and the triggering functions are based on two different measurements. The advantage is that each DER/DESS can decide when need to update its control input independent of other DER units.
- Different from the current approaches that fix the control command to either zero or a constant value, such as [24]–[26], the proposed control scheme exploits an estimator for setting secondary control signals. Furthermore, the proposed event-triggered function also works during DoS attack intervals, improving communication efficiency and reducing control updates.

II. Preliminaries

A. Notation

$\mathbb{R}^{n\times n}$ indicates the set of all real matrices with n rows and n columns. $\mathbb{N}$ is the set of natural numbers. $M > 0$ denotes M is a real symmetric and positive definite matrix. I_N expresses the $N \times N$ identity matrix.

B. Graph Theory

The communication topology among DERs/DESS is described by an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ where $\mathcal{V} = \{\nu_i : i \in \mathbb{N}\}$ is a set of nodes, representing each DER in the MG, and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is a set of edges. If the node ν_i can exchange data with the other node ν_j, there exists an edge $(\nu_i, \nu_j) \in \mathcal{E}$ between them. $\mathcal{A} \in \mathbb{R}^{N\times N}$ is defined as the adjacency matrix, where $a_{ij} = a_{ji}$, $a_{ii} = 0$ and $a_{ij} > 0$ if the *i*-th DER can obtain (send) the data from (to) the *j*-th DER and, otherwise, $a_{ij} = 0$. The set of neighbors of DER *i* is defined as $N_i = \{\nu_j \in \mathcal{V} : (\nu_j, \nu_i) \in \mathcal{E}\}$. The Laplacian matrix of the graph $\mathcal{G}$ associated with $\mathcal{A}$ is defined as $\mathcal{L} = [l_{ij}] \in \mathbb{R}^{\mathbb{N}\times\mathbb{N}}$, where $l_{ii} = \sum_{j\neq i} a_{ij}$, when $i = j$. In the communication network of MGs, the supposed values for voltage and frequency are sent by a leader, that is accessible for only some DERs. $\bar{\mathcal{G}} = diag[a_{i0}]$ is defined as a diagonal matrix where $a_{i0} > 0$ if the *i*-th DER (ν_i) receive information from the leader and, or else $a_{i0} = 0$. Moreover, the symmetric information exchange matrix is defined as $H = L + \bar{\mathcal{G}}$.

C. Inverter-based MG dynamics

The MG system is considered as a cyber-physical system including a device layer that consists of the physical components, control levels, and communication layer. According to the physical structure of MGs; consisting of DC energy sources,

LCL filters, and voltage source converters (VSC); the dynamics for the design of controllers can be obtained. According to [1], the following droop equations for the *i*-th DG/DES is given as follows.

$$\begin{cases} \omega_i = \omega_i^n - m_i^P P_i & \text{if DER} \in \text{DGs} \\ \omega_i = \omega_i^n - m_i^P P_i - m_i^S(1 - SoC_i) & \text{if DER} \in \text{DESS} \end{cases}, \tag{1}$$

$$\begin{cases} v_{odi} = v_i^n - n_i^Q Q_i \\ v_{oqi} = 0 \end{cases} \tag{2}$$

where v_{odi} and v_{oqi} are *d-q* components of the voltage, w_i^n and v_i^n are the reference values provided by the secondary control layer, P_i, and Q_i are the active and reactive powers of *i*-th DG/DES, m_i^p, n_i^q, and m_i^S are the droop coefficients, respectively. In the islanded mode, the initial charge of DESS might be different. Therefore, their contribution to power management might speed up the discharge process of units with a lower amount of energy. Hence, it is necessary to ensure that each DES's contribution to power management is proportional to its SoC for an efficient operation. For the SoC estimation, the coulomb counting rule is employed. Irrespective of the power losses in the VSC, and considering the efficiency factor equal to 1, the simplified coulomb rule is declared as follows.

$$SoC_i = SoC_{i,0} - \frac{1}{C_i v_{dc}} \int P_i \, dt \tag{3}$$

where $SoC_{i,0}$, v_{dc}, and C_i express the initial charge, DC voltage of the battery side, and capacity of each storage system, respectively. The dynamic models of the control loops and filters of each DER unit can be presented as follows.

$$\begin{cases} \dot{\delta}_i = \omega_i^{nom} - m_i^P P_i - \omega_{com} \\ \dot{P}_i = \omega_{ci} \left(v_{odi} i_{odi} + v_{oqi} i_{oqi} - P_i \right) \\ \dot{Q}_i = \omega_{ci} \left(v_{odi} i_{oqi} - v_{oqi} i_{odi} - Q_i \right) \\ \dot{i}_{ldi} = \frac{-R_{fi}}{L_{fi}} i_{ldi} + \omega_{com} i_{lqi} + \frac{v_i^{nom} - n_i^Q Q_i - v_{odi}}{L_{fi}} \\ \dot{i}_{lqi} = \frac{-R_{fi}}{L_{fi}} i_{lqi} - \omega_{com} i_{ldi} - \frac{v_{oqi}}{L_{fi}} \\ \dot{v}_{odi} = \omega_{com} v_{oqi} + \frac{i_{ldi} - i_{odi}}{C_{fi}} \\ \dot{v}_{oqi} = -\omega_{com} v_{odi} + \frac{i_{lqi} - i_{oqi}}{C_{fi}} \\ \dot{i}_{odi} = \frac{-R_{fi}}{L_{ci}} i_{odi} + \omega_{com} i_{oqi} + \frac{v_{odi} - v_{bdi}}{L_{ci}} \\ \dot{i}_{oqi} = \frac{-R_{fi}}{L_{ci}} i_{oqi} - \omega_{com} i_{odi} + \frac{v_{oqi} - v_{bqi}}{L_{ci}} \end{cases} \tag{4}$$

where δ_i is the phase angle of the *i*-the DG unit, ω_{ci} is the cut-off frequency of the output filter, i_{odi}, i_{oqi}, i_{ldi} and i_{lqi} are the direct and quadrature elements of the *i*-th DG current and the output current of the filter, respectively; v_{bdi} and v_{bqi} stand for the terminal voltage of the output connector filter, ω_{com} represents the common rotating frequency, R_{fi}, L_{fi}, C_{fi} and L_{ci} are the elements of the LCL filter.

Then, the nonlinear dynamics of each DG/DES in MGs presented in (4) can be described as follows.

$$\begin{cases} \dot{x}_i = f_i(x_i) + W_i(x_i)\Psi_i + r_{i1}(x_i)u_{i1} + r_{i2}(x_i)u_{i2} \\ y_{i1} = g_{i1}(x_i) \\ y_{i2} = g_{i2}(x_i) + u_{i2} \end{cases} \tag{5}$$

where Ψ_i is considered as a disturbance vector $\Psi_i = [\omega_{com} \, v_{bdi} \, v_{bqi}]^T$, the state vector is $x_i = [\delta_i \; P_i \; Q_i \; i_{Ldi} \; i_{Lqi} \; v_{odi} \; v_{oqi} \; i_{odi} \; i_{oqi}]^T$, $u_i = [u_{i1} \, u_{i2}]^T$ and $y_i = [y_{i1} \, y_{i2}]^T$ are the input and output vector, respectively. Given (4), $f_i(.)$, $W_i(.)$, $r_i(.)$, and $g_i(.)$ can be simply elaborated.

As the dynamics of DER units are nonlinear, thus, feedback linearization is essential to convert the nonlinear dynamics of DERs to a linear form. By utilizing the input-output feedback linearization technique, the secondary control problem becomes a tracking control problem. For the secondary voltage control of MGs, let us define $D_i(x_i) = f_i(x_i) + W_i(x_i)\Psi_i$, then, the voltage dynamics of each DG is presented as follows.

$$\begin{cases} \ddot{y}_{i1} = \dot{v}_{odi} \\ \ddot{y}_{i2} = \ddot{v}_{odi} = L^2_{D_i \, g_{i1}} + L_{r_{i1}} L_{D_{i1} \, g_{i1} \, u_{i1}} \end{cases} \tag{6}$$

where $L_{D_i} g_i = [\partial g_i / \partial x_i] D_i(x_i)$ and $L^2_{D_i \, g_{i1}} = [\partial L_{D_i \, g_{i1}} / \partial x_i] D_i(x_i)$ denotes Lie Derivative [32] of g_{i1} with D_i. Thus, one can write (6) as $\dot{y}_i = A y_i + B \upsilon_i$, where $\upsilon_i = L^2_{D_i} g_{i1} + L_{r_{i1}} L_{D_i g_{i1}} u_{i1}$ is the virtual input, $y_i = [v_{odi} \; \dot{v}_{odi}]^T = [y_{i1} \; y_{i1,1}]^T$, $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $B = [0 \quad 1]^T$. Thus, the control command can be declared as $u_{i1} = \frac{(-L^2_{D_i} g_{i1} + \upsilon_i)}{(L_{r_{i1}} L_{D_i g_{i1}})}$. The secondary control level tries to force proper voltage control commands υ_i as y_{i1} reaches the reference voltage regardless of the presence of DoS attacks in the communication layer. This objective can be mathematically expressed as follows.

$$\lim_{t \to \infty} v_{odi} - v_0 = 0 \tag{7}$$

where v_o is the desired voltage value.

In this paper, the cooperative controller, as opposed to the competitive control, points out that all DER units play a role in one group to reach a common synchronization purpose. Such distributed cooperative controllers are categorized into the tracking synchronization problems, where "*the voltages of all DER units*" get synchronized by a leader node acting as a commander. It is important to mention that in general tracking problems of multi-agent systems, all state trajectories of the system can reach the desired values. However, in MGs, due to the existence of low resistance between transmission lines, all voltages are not converged to the same value and there is slight divergence at the steady-state. This causes to have voltage differences and, as a consequence, current flow in the transmission lines between units.

D. DoS Attack Model

The DoS attacks with an unlimited energy level are discontinuous and make the system unstable, preventing DERs controllers from sending/receiving data. During DoS attacks, information among DERs is not accessible and is violated. The network topology is changed over the DoS attack period, which means that some data transmissions among DERs are terminated. Due to the resource limitation, the attacker needs to inactive sleep intervals to supply their energy for the next adversary. Thus, the entire time is spilt into two periods: the normal section for communication without attacks, and cyber-attack intervals.

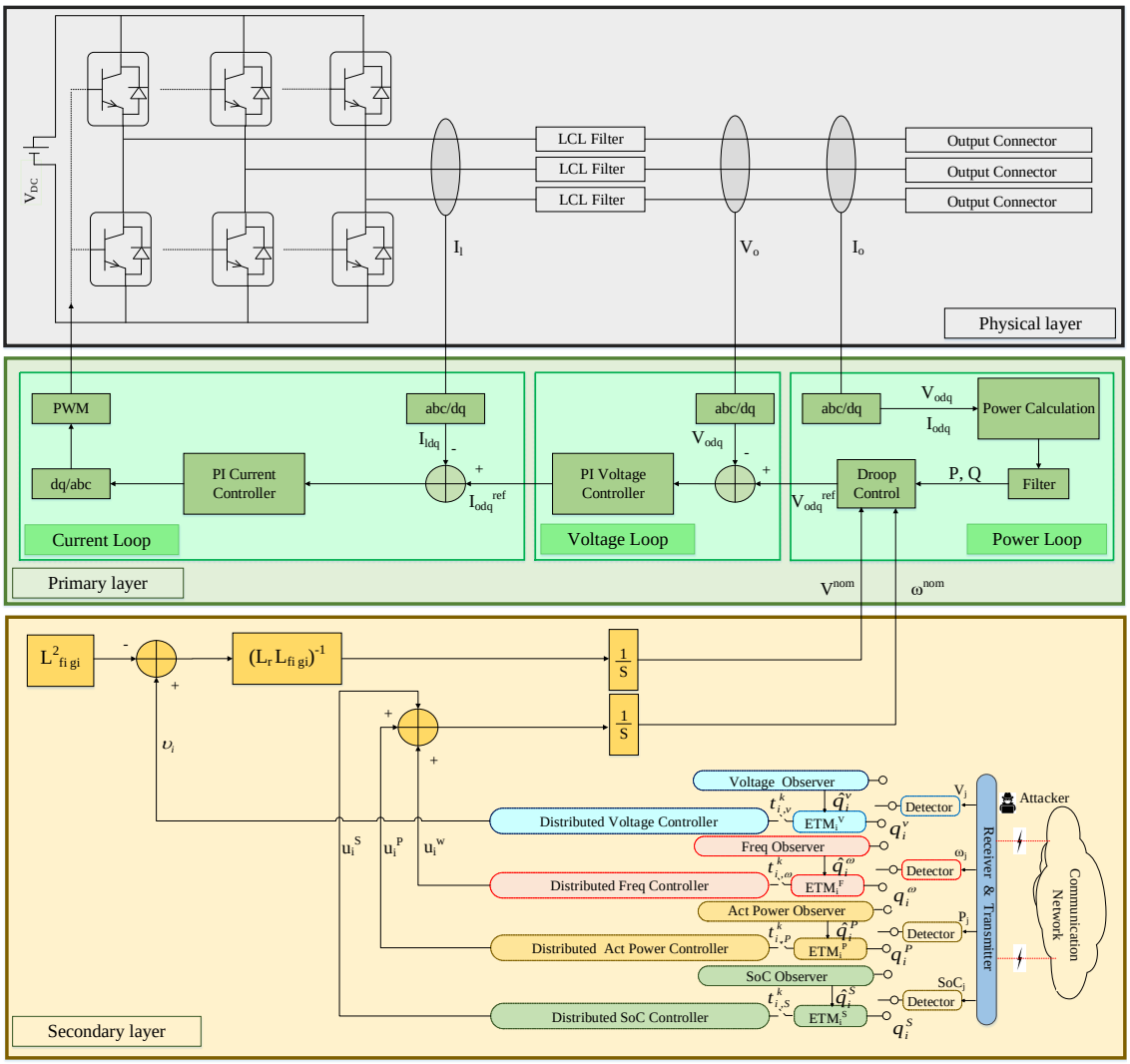

Fig. 1: Cyber-physical microgrid layers schematic including physical and cyber layers (consisting of primary and secondary control layers, communication links, and measurement and protection devices). The proposed event-triggered distributed cooperative control scheme for each DER unit is presented in the secondary layer. The attacker aims to block the communication channels and prevent the data exchange.

The paralyzed interval is represented as $\Pi_m = [t_m, t_m + \Delta_m]$ where $m \in \mathbb{N}$, t_m is the instant that a DoS attack is launched, and Δ_m states the length of intervals over which the communication network is under attack. The set of the intervals where communication is denied, can be defined as $\Xi_a(t,\tau) = \cup\, \Pi_m \cup [\tau, t]$. Similarly, the set of time instants with a normal interaction is $\Xi_s(\tau, t) = [\tau, t] \backslash \Xi_a(t,\tau)$. $|\Xi_a(t,\tau)|$ and $|\Xi_s(t,\tau)|$ denote the total lengths of the attacker being active and sleeping over $[\tau, t]$, respectively [24]. Due to the energy limitation of the attacker, the following common assumptions are made in this paper.

Assumption 1. (Attack Frequency): For any $t > 0$, there exist $F_f > 0$ such that $\Gamma_a(t_0,\ t) < F_f(t - t_0)$, where Γ_a is the total number of DoS attacks over $[t_0, t]$.

Assumption 2. (Attack Duration): For any $t > 0$, there exists $\pi_a > 0$ such that $T_a(t_0, t) \leq T_0 + \frac{t-t_0}{\pi_a}$, where T_a is the total time interval of DoS attack during $[t_0, t)$ and $T_0 > 0$.

Remark 1. It is worth notifying that if the MG is repeatedly under DoS attacks, the DER units cannot have neighbour-to-neighbour information exchange. Such attacks need to be connected to a continuous energy supply which is not practical. From this view, both Assumptions 1 and 2, which are fairly common in the literature [33]–[35], are necessary to be taken.

Note that this paper does not focus on the attack detection approaches although the DoS attack detection methods have been widely investigated in the literature, for example, see [36]. The attack detector can be implemented by means of network-based mechanisms such as anomaly-based detection, learning-based algorithms, and attack recognition mechanisms based on computer vision. Hence, the detector in Fig. 1 is presented to show that the proposed observer is activated whenever the communication link is blocked.

III. Distributed cooperative resilience event-triggered voltage controller design

In this section, the distributed event-triggered secure problem of voltage regulation in the presence of DoS attacks is presented. Then, the stability of the closed-loop control system subject to DoS attacks and the non-occurrence of the Zeno behavior for all DERs are analyzed. To do so, it is required to consider two cases for the stability analysis: 1) without DoS attacks and 2) with DoS attacks:

1) For the first case, the distributed cooperative event-based scheme for each DG/DES is designed as follows.

$$\upsilon_i(t) = c_v K_v(q_i^v(t_{i,v}^k) + d_i^v(t_{i,v}^k)) \qquad t_{i,v}^k \le t < t_{i,v}^{k+1} \quad (8)$$

where c_v is a positive control gain $q_i^v = \sum_{j\in\mathcal{N}_i} a_{ij}(y_j - y_i)$, $d_i^v = a_{i0}(y_i - y_{ref})$, $t_{i,v}^k$ stands for the triggering sequence of communication instants, and K_v is a control gain that will be defined in Subsection III-A. At triggering instants, the *i*-th DG/DES requires to sample the information of its neighbors and the leader to update the control input $\upsilon_i(t)$. The measurement errors are defined as follows.

$$\begin{cases} \xi_i^v = q_i^v(t_{i,v}^k) - q_i^v(t) \\ \bar{\xi}_i^v = d_i^v(t_{i,v}^k) - d_i^v(t) \end{cases} \quad i = 1, 2, ..., N. \quad (9)$$

2) In this case, the following estimator is introduced to anticipate the states of the system in (6) over the attacking intervals.

$$\begin{cases} \dot{\hat{y}}_i = A\hat{y}_i + B\upsilon_i & t \in \Pi_m \\ \dot{\hat{y}}_i = y_i(t_i^l) & t = t_m \end{cases} \quad (10)$$

where t_i^l is the last successful exchange attempt between neighbouring DERs. The control scheme during the attack interval is presented as $\upsilon_i(t) = c_v K_v(\hat{q}_i^v(t_{i,v}^k) + \hat{d}_{i,v}^k(t_{i,v}^k))$, where $\hat{q}_i^v = \sum_{j\in\mathcal{N}_i} a_{ij}(\hat{y}_j - \hat{y}_i)$ and $\hat{d}_i^v = a_{i0}(\hat{y}_i - y_{ref})$. The estimator is just activated during the attack period. DERs will be aware of the attack occurrence if the data of other DERs is no longer available. The last estimation value is kept until the communication status of the MG restores to the normal condition.

A. Stability analysis

Forming the controllability matrix $Co = [B \quad AB]$, it is obvious that the pair (A, B) is controllable, then there exists a matrix $Q > 0 \in \mathbb{R}^{n\times n}$ that is the solution of the following Riccati inequality.

$$A^TQ + QA - 2QBB^TQ + \alpha^v Q < 0 \quad (11)$$

where $\alpha^v > 0$ and the matrix K_v in (8) is designed as $K_v = -B^TQ$. Note that the consensus error is defined as $\varepsilon_i^v = y_i(t) - y_{ref}$. Therefore, by considering (8) and (9), the dynamics of the error can be obtained as follows.

$$\dot{\varepsilon}_i^v = A\varepsilon_i^v + c_v BK_v(q_i^v + d_i^v + \xi_i^v + \bar{\xi}_i^v). \quad (12)$$

The compact form of (12) can be written as $\dot{\boldsymbol{\varepsilon}}^v = (I_N\otimes A - H\otimes BK_v)\boldsymbol{\varepsilon}_i^v + (I_N\otimes c_vBK_v)\boldsymbol{\xi}^v + (I_N\otimes c_vBK_v)\bar{\boldsymbol{\xi}}^v$, where $\boldsymbol{\xi}^v = ({\xi_1^v}^T, ..., {\xi_N^v}^T)^T$, and $\bar{\boldsymbol{\xi}}^v = ({\bar{\xi}_1^v}^T, ..., {\bar{\xi}_N^v}^T)^T$.

Theorem 1. *Let $\beta_i^v \in (0,1)$, γ be a positive constant and, $|N_i|$ denotes the number of DGs. Consider a connected and undirected graph among DERs, the consensus of voltages of each DG/DES in the MG can be obtained in the communication area with/without (Ξ_a and Ξ_s) attacks under the control scheme in* (8) *and the following voltage triggering function.*

$$\begin{aligned} &ETM_i^v : t_{i,v}^{k+1} = \inf\{t > t_{i,v}^k | \, E_i^v > 0\}, \\ &E_i^v = \|\xi_i^v(t)\|^2 + \left\|\bar{\xi}_i^v(t)\right\|^2 - {h_i^v}^2{\varphi_i^v}^2(t) \end{aligned} \quad (13)$$

where $\varphi_i^v = \|q_i^v(t)\| + \|d_i^v(t)\|$ and

$$h_i^v = \sqrt{\frac{\beta_i^v(B - 2\|QBB^TQ\| c_v\gamma^{-1})}{(4|N_i|^2 + 2{a_{i0}}^2)\|QBB^TQ\|}}. \quad (14)$$

Proof. First, we choose the following Lyapunov candidate for the case that there are no DoS attacks in the communication layer.

$$V_1(t) = {\boldsymbol{\varepsilon}^v}^T(I_N\otimes Q)\boldsymbol{\varepsilon}^v \quad (15)$$

where Q is chosen such that $V_1(t) > 0$. Note that due to the assumption on the graph topology, there is an orthogonal matrix θ such that $\bar{\varepsilon}^v = (\theta\otimes I_n)\varepsilon^v$, $\xi_x^v = (\theta\otimes I_n)\xi^v$ and $\bar{\xi}_x^v = (\theta\otimes I_n)\bar{\xi}^v$ with $\theta\theta^T = I_N$. Also, it is easy to show that $\theta^TH\theta = diag\{\lambda_{\min}(H), ..., \lambda_{max}(H)\}$ and $\sum_{i=1}^N {\bar{\varepsilon}_i^v}^T\bar{\varepsilon}_i^v = \sum_{i=1}^N {\varepsilon_i^v}^T\varepsilon_i^v$. By differentiating V_1, one can obtain

$$\begin{aligned} \dot{V}_1(t) &= {\varepsilon^v}^T[I_N\otimes(A^TQ + QA) - 2c_vH\otimes QBB^TQ]\boldsymbol{\varepsilon}^v + \\ &\quad 2c_v{\boldsymbol{\varepsilon}^v}^T(I_N\otimes QBB^TQ)\bar{\boldsymbol{\xi}}^v + 2c_v{\boldsymbol{\varepsilon}^v}^T(I_N\otimes QBB^TQ)\boldsymbol{\xi}^v \\ &= {\bar{\boldsymbol{\varepsilon}}^v}^T[I_N\otimes(A^TQ + QA) - 2c_vH\otimes QBB^TQ]\bar{\boldsymbol{\varepsilon}}^v + \\ &\quad 2c_v{\boldsymbol{\varepsilon}^v}^T(I_N\otimes QBB^TQ)\hat{\boldsymbol{\xi}}_x^v + 2c_v{\boldsymbol{\varepsilon}^v}^T(I_N\otimes QBB^TQ)\boldsymbol{\xi}_x^v \end{aligned} \quad (16)$$

and,

$$\begin{aligned} \dot{V}_1(t) &\le \sum_{i=1}^N {\bar{\varepsilon}_i^v}^T[A^TQ + QA - 2c_v\lambda_{\min}(H)\otimes QBB^TQ]\bar{\varepsilon}_i^v + \\ &\quad 2c_v\sum_{i=1}^N {\bar{\varepsilon}_i^v}^TQBB^TQ\bar{\xi}_{x,i}^v - 2c_v\sum_{i=1}^N {\bar{\varepsilon}_i^v}^TQBB^TQ{\xi_{x,i}}^v \\ &\le \alpha^v\sum_{i=1}^N(\|{\varepsilon_i}^v\|)^2 + 2c_v\sum_{i=1}^N\|{\varepsilon_i}^v\|\left\|QBB^TQ\right\|\|\xi_i^v\| + \\ &\quad 2c_v\sum_{i=1}^N\|{\varepsilon_i}^v\|\left\|QBB^TQ\right\|\left\|\bar{\xi}_i^v\right\|. \end{aligned} \quad (17)$$

Based on the fact that $\mu\|m\|^2 + \frac{1}{\mu}\|n\|^2 \ge 2\|m\|\|n\|$ for any

m and n, where $\mu > 0$, one can obtain that

$$2\sum_{i=1}^{N}\|\varepsilon_i{}^v\|\left\|QBB^TQ\right\|\|\xi_i^v\|+2\sum_{i=1}^{N}\|\varepsilon_i{}^v\|\left\|QBB^TQ\right\|\left\|\bar{\xi}_i^v\right\|$$
$$\leq\left\|QBB^TQ\right\|\sum_{i=1}^{N}\left(\frac{2}{\mu}\|\varepsilon_i{}^v\|^2+\mu(\|\xi_i{}^v\|^2+\left\|\bar{\xi}_i^v\right\|^2)\right)$$
$$=\frac{2}{\mu}\left\|QBB^TQ\right\|\sum_{i=1}^{N}\|\varepsilon_i{}^v\|^2+\mu\left\|QBB^TQ\right\|\times$$
$$\sum_{i=1}^{N}(\|\xi_i{}^v\|^2+\left\|\bar{\xi}_i^v\right\|^2). \tag{18}$$

According to the triggering condition in (13), one can get

$$\|\xi_i{}^v\|^2+\left\|\bar{\xi}_i^v\right\|^2\leq h_i^{v2}\left(\|q_i^v(t)\|^2+2\|d_i^v(t)\|\ \|q_i^v(t)\|+\right.$$
$$\left.\|q_i^v(t)\|^2\right)-2h_i^{v2}(\left\|\sum_{j\in\mathcal{N}}a_{ij}(y_j-y_i)\right\|^2+a_{i0}\|y_{ref}-y_i\|^2)$$
$$\leq 4h_i^{v2}|N_i|\sum_{j\in\mathcal{N}_i}\|\varepsilon_i^v\|^2+2h_i^{v2}a_{i0}\|\xi_i{}^v\|^2. \tag{19}$$

Substituting (18) and (19) into (17), it yields

$$\dot{V}_1(t)\leq\alpha^v\sum_{i=1}^{N}\|\varepsilon_i{}^v\|^2+2\left\|QBB^TQ\right\|\sum_{i=1}^{N}\|\varepsilon_i{}^v\|^2+$$
$$4h_i^{v2}\ |N_i|\ \left\|QBB^TQ\right\|\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i}\|\varepsilon_i{}^v\|^2+ \tag{20}$$
$$2h_i^{v2}\left\|QBB^TQ\right\|\sum_{i=1}^{N}a_{i0}^2\|\varepsilon_i{}^v\|^2$$

and,

$$\dot{V}_1\leq(\alpha^v-2\left\|QBB^TQ\right\|\frac{\mu}{\gamma}\sum_{i=1}^{N}(4|N_i|^2+2a_{i0}^2)\|\varepsilon_i{}^v\|^2$$
$$+h_i^{v2}c_v\gamma\left\|QBB^TQ\right\|\sum_{i=1}^{N}(4|N_i|^2+2a_{i0}^2)\|\varepsilon_i{}^v\|^2$$
$$=(\alpha^v-2c_v\left\|QBB^TQ\right\|)(1-\beta_i^v)\sum_{i=1}^{N}\|\varepsilon_i{}^v\|^2$$
$$\leq-\eta_1^vV_1(t) \tag{21}$$

where $\eta_1^v=\left[(-\alpha^v+2\,c_v\gamma^{-1}\left\|QBB^TQ\right\|)\frac{(1-\beta_i^v)}{\lambda_{\min}(Q)}\right]$. Let $\hat{\varepsilon}_i^v=\hat{y}_i(t)-y_{ref}$, then similar to the case without attacks, the following Lyapanov function is chosen.

$$V_2(t)=\hat{\boldsymbol{\varepsilon}}^{vT}(I_N\otimes Q)\hat{\boldsymbol{\varepsilon}}^v. \tag{22}$$

The time-derivative of the above Lyapanov candidate is

$$\dot{V}_2(t)=\hat{\boldsymbol{\varepsilon}}^{vT}[I_N\otimes(A^TQ+QA)-2c_vH\otimes QBB^TQ]\hat{\boldsymbol{\varepsilon}}^v+$$
$$2c_v\hat{\boldsymbol{\varepsilon}}^{vT}(I_N\otimes QBB^TQ)\hat{\boldsymbol{\xi}}+2c_v\hat{\boldsymbol{\varepsilon}}^{vT}(I_N\otimes QBB^TQ)\hat{\boldsymbol{\xi}}^v \tag{23}$$

where $\hat{\xi}_i^v=\hat{q}_i^v(t_{i,v}^k)-\hat{q}_i^v(t)$ and $\hat{\bar{\xi}}_i^v=\hat{d}_i^v(t_{i,v}^k)-\hat{d}_i^v(t)$. In accordance with the definition of DoS attack in Section II-D, one can obtain

$$\begin{cases}V_1(t)<e^{-\eta_1^v|\,\Xi_s(t_0,t)\,|}V_1(t_0)\\ V_2(t)<e^{-\eta_2^v|\,\Xi_a(t_0,t)\,|}V_2(t_0)\end{cases}. \tag{24}$$

By taking some steps similar to [33], and define $V(t)=V_1+V_2$, it is obtained that

$$V(t)\leq e^{(\eta_1^v+\eta_2^v)(T_0+\Delta)}\,e^{-\delta^v(t-t_0)}\,V(t_0) \tag{25}$$

where $\delta^v=\eta_1^v-[(\eta_1^v+\eta_2^v)/\tau_a-\eta^*]$. It should be noted that for all $t>t_0$, $|\Xi_s(t-t_0)|=t-t_0-|\Xi_a(t-t_0)|$ and $-\eta_1^v\,|t-t_0-\Xi_s(t_0,t)|+\eta_2^v\,|t-t_0-\Xi_a(t_0,t)|\leq-\eta_1^v(t-t_0)+(\eta_1^v+\eta_2^v)\left(T_0+\frac{t-t_0}{\tau_a}+N_f(t_0,t)\Delta\right)$. The inequality (25) implies that $V(t)$ is bounded and converges exponentially to zero at the stationary, which means that the consensus of DERs' voltage is achieved. This completes the proof. □

Remark 2. The proposed estimator in (10) plays a crucial role during the attack intervals. In several previous works related to cooperative systems subject to DoS attacks such as [25] and [37], the control inputs are set to be zero. The proposed estimator is developed over an unreliable network based on the MG dynamics and measurements. Once a DG/DES does not receive data from its neighbors, the estimators are activated to anticipate the states in (6) for the controllers. In the other words, after launching attacks, the estimated values are utilized in the triggering functions. To demonstrate the privilege of the proposed control scheme with the observer, comparison results will be rendered later in Section V.

Remark 3. The control scheme in (8) depicts that the voltage control signal is only updated at specific instants based on the triggering functions in (14). The next triggering instant ($t_{i,v}^k$) depends on the values of the measurement errors in (9). Therefore, when the triggering function does not satisfy the defined condition in (13), there is no update for the control scheme in (8). Specifically, the values of q_i^v and d_i^v remain fixed until the next triggering instant takes place.

Next, we show that the Zeno behavior is excluded from the control system of MGs. Note that Zeno behavior exists in the control loop when an infinite number of discrete transitions happen in a finite time interval.

Theorem 2. *Consider a MG with undirected and connected communication topology, under the distributed cooperative event-triggered control low in* (8) *with the triggering function* (13)*. The Zeno behavior will be excluded if the positive lower bound $t_i^*=t_{i,v}^{k+1}-t_{i,v}^k$ of any two event intervals satisfies the following condition*

$$t_i^*>\frac{\psi_i^{v2}(t_{i,v}^k)\sqrt{1-\frac{1}{1+h_i^{v2}}}}{2\,\|A\|\,\psi_i^{v2}(t_{i,v}^k)\sqrt{1-\frac{1}{1+h_i^{v2}}}+2\psi_i^{v2}(t_{i,v}^k)\,\sigma_i^v(t_{i,v}^k)} \tag{26}$$

where $\sigma_i^v(t_{i,v}^k)=\max\{||Ad_i^v(t_{i,v}^k)-B\upsilon_i(t)||,\,||Aq_i^v(t_{i,v}^k)+\sum_{j\in\mathcal{N}_i}a_{ij}B\,(\upsilon_j-\upsilon_i)||\}$.

Proof. We consider the case without attacks to prove the

theorem. However, it can be extended to the attack case. Adopting the traditional method to exclude Zeno behavior of (13), one can obtain that

$$\begin{aligned}&\frac{d}{dt}(\|\xi_i^v\|^2)+\frac{d}{dt}(\|\bar{\xi}_i^v\|^2)\leq 2\|\xi_i^v\|\frac{d}{dt}(\|\xi_i^v\|)+\\&2\|\bar{\xi}_i^v\|\frac{d}{dt}(\|\bar{\xi}_i^v\|)\leq 2\|\xi_i^v\|\ \|\dot{q}_i^v\|+2\|\bar{\xi}_i^v\|\left\|\dot{d}_i^v\right\|\leq 2a_{i0}\|\bar{\xi}_i^v\|\\&\times\|Ay_{ref}-Ay_i-B\,\upsilon_i\|+2\|\xi_i^v\|\ \|Aq_i^v+\\&\sum_{j\in\mathcal{N}_i}a_{ij}B(\upsilon_j-\upsilon_i)\|\leq 2\|\bar{\xi}_i^v\|\left(Ad_i^v(t_{i,v}^k)-A\xi_i^v-B\upsilon_i\right)\\&+2\|\xi_i^v\|\left(-A\xi_i^v+q_i^v(t_{i,v}^k)\right)+\sum_{j\in\mathcal{N}_i}a_{ij}B(\upsilon_j-\upsilon_i)\end{aligned}\tag{27}$$

and, also

$$\begin{aligned}&\frac{d}{dt}(\|\xi_i^v\|^2)+\frac{d}{dt}(\|\bar{\xi}_i^v\|^2)\leq 2\|A\|\ \|\bar{\xi}_i^v\|^2+2\|\bar{\xi}_i^v\|\\&\times\left\|\,d_i^v(t_{i,v}^k)-B\upsilon_i\right\|+2\|A\|\ \|\xi_i^v\|^2+2\|\xi_i^v\|\ \|Ad_i^v(t_{i,v}^k)\\&-B\upsilon_i+\sum_{j\in\mathcal{N}_i}a_{ij}B(\upsilon_j-\upsilon_i)\|\\&\leq\ 2\ \|A\|\left(\|\xi_i^v\|^2\ +\|\bar{\xi}_i^v\|^2\right)+2\max\{\left\|Ad_i^v(t_{i,v}^k)-B\upsilon_i\right\|\\&\quad\|Aq_i^v(t_{i,v}^k)+\sum_{j\in\mathcal{N}_i}a_{ij}B(\upsilon_j-\upsilon_i)\}\ \left(\|\xi_i^v\|\ +\left\|\bar{\xi}_i^v\right\|\right)\|.\end{aligned}\tag{28}$$

Let us define $\varsigma_i^{v2}=\|\xi_i^v\|^2+\|\bar{\xi}_i^v\|^2$, then, the above inequality can be written as follows

$$\frac{d}{dt}(\varsigma_i^{v2})\leq 2\|A\|\ \varsigma_i^{v2}+2\sigma_i^v(t_{i,v}^k)\varsigma_i^v.\tag{29}$$

The sufficient condition for the triggering function at the triggering instants can be considered as follows.

$$\varsigma_i^{v2}=\|\xi_i^v\|^2\ +\|\bar{\xi}_i^v\|^2\leq(1-\frac{1}{1+h_i^{v2}})\,\varphi_i^{v2}(t_{i,v}^k).\tag{30}$$

Considering $q_i^v(t_{i,v}^k)$ and $d_i^v(t_{i,v}^k)$, there exists a link $\psi_i^v(t_{i,v}^k)>\varphi_i^v(t_{i,v}^k)$, so that $\varsigma_i^{v2}\leq(1-\frac{1}{1+h_i^{v2}})\varphi_i^{v2}(t_{i,v}^k)$. Combining (29) and (30), the positive lower bound t_i^* is computed as (26). Therefore, the inequality $t_{i,v}^{k+1}-t_{i,v}^k>0$ exists and the interval between events is strictly positive. This completes the proof. □

IV. Distributed resilient event-triggered frequency and active power controller design

In this section, distributed resilient frequency, active power management, and SoC balancing control schemes are suggested to reach secondary control objectives despite DoS attacks in communication networks. To this end, according to (1), the following independent controllers are considered such that $m_1^pP_1=m_2^pP_2=...=m_N^pP_N$ and $m_1^S(1-SoC_1)=m_2^S(1-SoC_2)=...=m_N^S(1-SoC_N)$

$$\begin{cases}\dot{\omega}_i=u_i^\omega\\ m_i^P\dot{P}_i=u_i^P\\ m_i^S(1-SoC_i)=u_i^S\end{cases}.\tag{31}$$

Similar to the previous section, the secure consensus schemes in normal communication without attacks can be defined as follows.

$$\begin{cases}u_i^\omega(t)=c_\omega K_\omega(q_i^\omega(t_{i,\omega}^k)+d_i^\omega(t_{i,\omega}^k)) & t_{i,\omega}^k\leq t<t_{i,\omega}^{k+1}\\ u_i^P(t)=c_PK_Pq_i^P(t_{i,P}^k) & t_{i,P}^k\leq t<t_{i,P}^{k+1}\\ u_i^S(t)\ =c_SK_sq_i^S(t_{i,S}^k) & t_{i,S}^k\leq t<t_{i,S}^{k+1}\end{cases}\tag{32}$$

where c_ω, c_P and c_S are positive control gains, $q_i^\omega=\sum_{j\in\mathcal{N}_i}a_{ij}(\omega_j-\omega_i)$, $q_i^P=\sum_{j\in\mathcal{N}_i}a_{ij}(m_i^PP_j-m_j^PP_i)$, $q_i^S=\sum_{j\in\mathcal{N}_i}a_{ij}(m_i^SSoC_j-m_j^SSoC_i)$,$d_i^\omega=a_{i0}(\omega_i-\omega_{ref})$, $t_{i,\omega}^k$, $t_{i,P}^k$, and $t_{i,S}^k$ stand for the triggering sequence of communication instants. For the attack case, q_i^ω, q_i^P, and q_i^S are replaced with their estimated values similar to the voltage controller presented in Section III. Finally, the following triggering functions are given as follows.

$$\begin{cases}E_i^\omega=\|\xi_i^\omega(t)\|^2+\|\bar{\xi}_i^\omega(t)\|^2-h_i^{\omega2}\varphi_i^{\omega2}(t)\\ E_i^P=\|\xi_i^P(t)\|^2+\|\bar{\xi}_i^P(t)\|^2-h_i^{P2}\varphi_i^{P2}(t)\\ E_i^S=\|\xi_i^S(t)\|^2+\|\bar{\xi}_i^S(t)\|^2-h_i^{S2}\varphi_i^{S2}(t)\end{cases}\tag{33}$$

where $\xi_i^\omega=q_i^\omega(t_{i,\omega}^k)-q_i^\omega(t)$, $\bar{\xi}_i^\omega=d_i^\omega(t_{i,\omega}^k)-d_i^\omega(t)$, $\xi_i^P=q_i^P(t_{i,P}^k)-q_i^P(t)$, $\xi_i^S=q_i^S(t_{i,S}^k)-q_i^S(t)$, $\varphi_i^\omega=\|q_i^\omega(t)\|+\|d_i^\omega(t)\|$, $\varphi_i^P=\|q_i^P(t)\|$, $\varphi_i^S=\|q_i^S(t)\|$ and h_i^ω, h_i^P, and h_i^S are defined as follows.

$$\begin{aligned}h_i^\omega&=\sqrt{\frac{\beta_i^\omega(B-2\|Q^2\|\,c_\omega\gamma^{-1})}{(4|N_i|^2+2a_{i0}{}^2)\,\|Q^2\|}}\\ h_i^P&=\sqrt{\frac{\beta_i^P(B-2\|Q^2\|\,c_P\gamma^{-1})}{(4|N_i|^2+2a_{i0}{}^2)\,\|Q^2\|}}\\ h_i^S&=\sqrt{\frac{\beta_i^S(B-2\|Q^2\|\,c_S\gamma^{-1})}{(4|N_i|^2+2a_{i0}{}^2)\,\|Q^2\|}}\end{aligned}\tag{34}$$

where $\beta_i^n,\in\ (0,1)$ for $n\in\{\omega,P,S\}$. The attack-resilient protocol for the frequency restoration in the second layer can be written as follows.

$$\begin{cases}\omega_i^n=\int(u_i^\omega+u_i^P)d\tau & \text{if DER}\ \in\ \text{DGs}\\ \omega_i^n=\int(u_i^\omega+u_i^P+u_i^S)d\tau & \text{if DER}\ \in\ \text{DESS}\end{cases}.\tag{35}$$

Remark 4. It is worth noting that by applying control schemes (32) and using the triggering functions (33), the secondary control objectives are achieved, and the Zeno behavior will be excluded. They can be proved with some modifications and taking similar steps in Theorem 1 and Theorem 2.

V. Case study

For the evaluation of the proposed method through the event-trigger mechanism, several simulation results of the islanded ac MG (shown in Fig. 2) are presented in this section, conducted in MATLAB/Simulink environment. The MG parameters are similar to the ones presented in [1] and [9]. The lines among buses are displayed by a series of resistance and inductance branches. The DGs/DESS exchange information

via an undirected graph topology depicted in Fig. 3 and only DG #1 and DES #2 can receive the frequency and voltage supposed values.

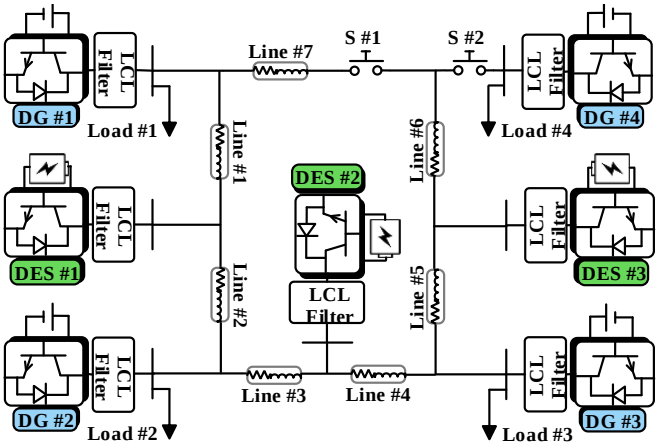

Fig. 2: Single-line diagram of the test MG.

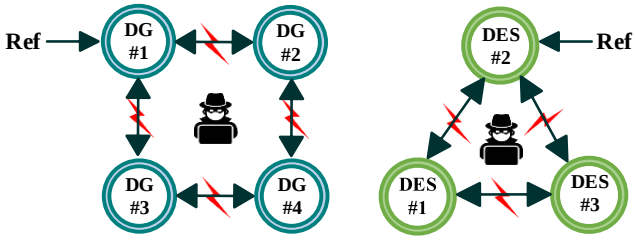

Fig. 3: Communication topology for DGs and DESS.

The simulations are carried out under several scenarios, which evaluate the accuracy and effectiveness of the proposed scheme while facing small-signal disturbances such as load change and PnP functionality of DERs. Moreover, the results are compared with some different previously relevant studies. Should be noted that due to the impedance impact of transmission lines, reactive power management and voltage regulation could not be attained at the same time, unless under specific configurations [38]. It should be noted that by exploiting the proposed control scheme, the accurate voltage regulation might result in significant errors in reactive power management and vice versa. This paper specifically focuses on the secondary voltage control design. However, one can find out that the proposed control scheme does not considerably deteriorate the reactive power management. This means that due to the impedance effect of transmission/distribution lines, both accurate reactive power-sharing and voltage regulation can not be achieved simultaneously (As pointed out in [38]). Therefore, accurate voltage regulation results in large errors in reactive power-sharing. Conversely, the precise reactive power-sharing leads to poor voltage regulation. Thus, a trade-off should be made between voltage regulation and reactive power-sharing accuracy. In this section, we only focus on the secondary voltage control; however, we have found that the proposed secondary controller does not worsen the reactive power-sharing

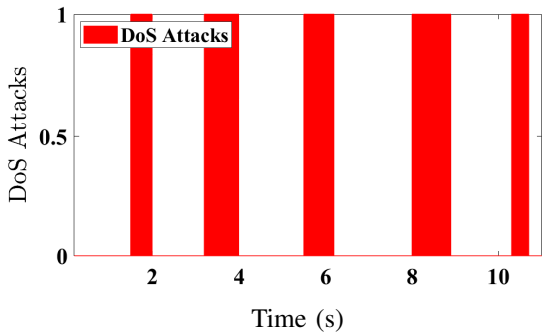

Fig. 4: Signal of DoS attacks.

among DERs (DGs and DESs) before applying the secondary control.

A. Performance Evaluation

Here, the performance of the event-triggered algorithm in the restoration of voltage, frequency, active power management, and SoC balancing in the presence of DoS attacks is verified for the islanded ac MG. The control parameters are selected as $c_v = 70$, $c_\omega = c_P = c_s = 50$, and $\gamma = 5$, $\beta^v = 0.7$, $\beta^\omega = \beta^P = \beta^s = 0.001$ and $\alpha^v = 75$, $\alpha^\omega = \alpha^P = \alpha^s = 70$. Solving LMI (11) by using MOSEK [39], the gain matrix for voltage, frequency, active power and SoC can be calculated as $K^v = \begin{bmatrix} 0 \\ 38 \end{bmatrix}$, and $K^\omega = K^P = K^s = 35$. Considering the results in [34], DoS attack signals are simulated based on Fig. 4, where $\Xi_a = 3.3$ and $\Gamma_a = 5$ satisfying Assumption 1 and 2. The simulations for scenarios are performed as

- At t = 0.75s, the proposed secondary protocol is activated;
- At t = 1.5s, S #1 is closed;
- At t = 2.5s, load #3 is increased (200%) and then reduced to the primary value at t = 4.5s, respectively;
- At t = 6s, the S #1 is opened;
- At t = 7.5s, for the PnP scenario, S #2 is opened and DG #4 is plugged out and then plugged in at t = 9.5s by closing S #2, respectively.

Operating the primary layer causes the MG to face some deviations in the voltage and frequency from the nominal values in the steady-state responses. Hence, the proposed resilience event-triggered controllers in (8) and (32) are applied at t = 0.75s. The secondary controller time scale to properly response is in the second range [40]. As it can be seen from Fig. 5 and Fig. 6, by enforcing the secondary control layer, the state trajectories reach the steady-state values after some seconds and the MG is in the steady-state. Thus, all the following scenarios take place after the MG has been settled.

At t=1.5s, S #1 is closed to change the configuration of the MG to a radial distribution network. At t = 6s, S #1 is opened to change the MG topology to the beginning formation. As a result of such changes, the output powers are increased at first and then decreased while the voltage and frequency controllers respond well to the disturbances. The load change scenario is also investigated at t=2.5s and t=4.5s. In the end, to show the robust performance of the proposed protocol under

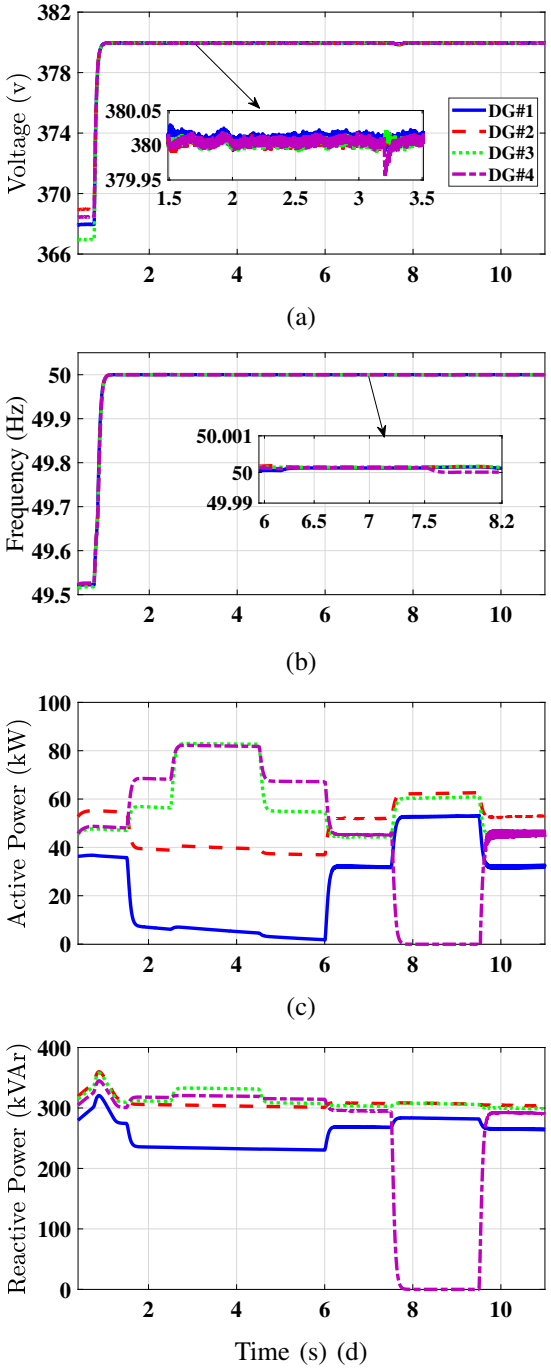

Fig. 5: Performance of the proposed scheme for DGs: (a) voltage, (b) frequency, (c) active power, and (d) reactive powers.

PnP functionality, DG #4 is plugged off from the MG and then re-joined at t = 7.5s and t = 9.5s, respectively. The other DGs generate more power to compensate for the deficiency originating from the DG outage. In this stage, some chattering in the outage power of DG #4 can be observed. Although the initial SoCs of DESS are different, the convergence of the SoC level of each unit to a common value is also achieved (Fig. 6)). Fig. 7 shows the control updates of voltage and frequency secondary controller for each DG in a highlighted interval, respectively. The total number of control updates for voltage

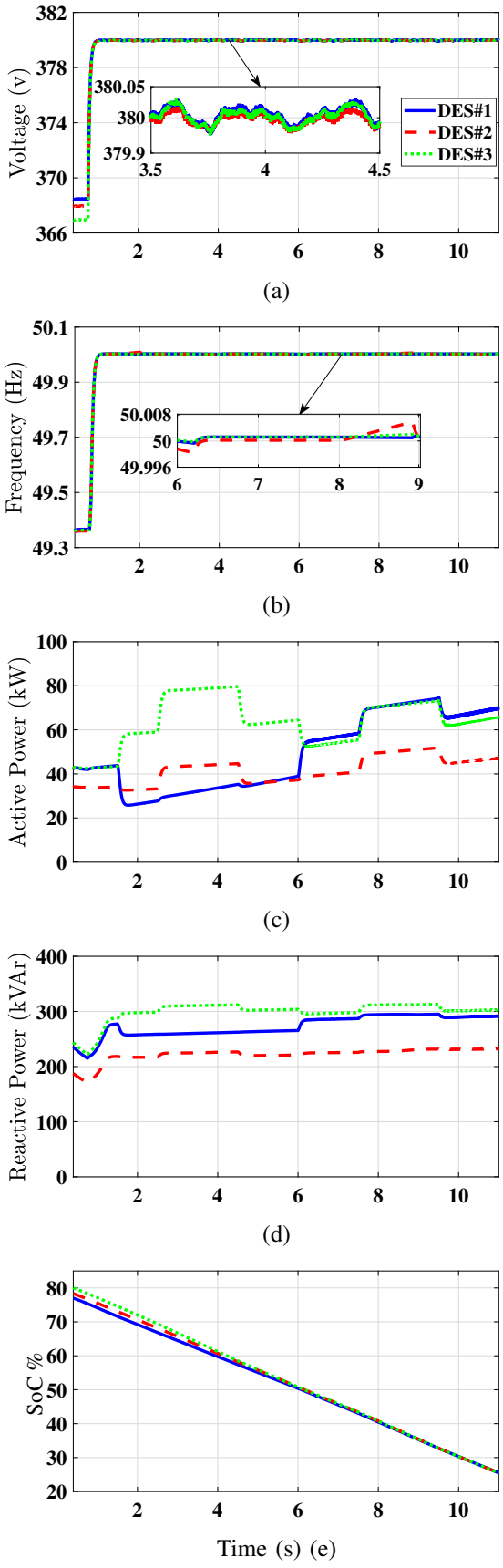

Fig. 6: Performance of the proposed scheme for DGs: (a) voltage, (b) frequency, (c) active power, (d) reactive powers and (e) SoC.

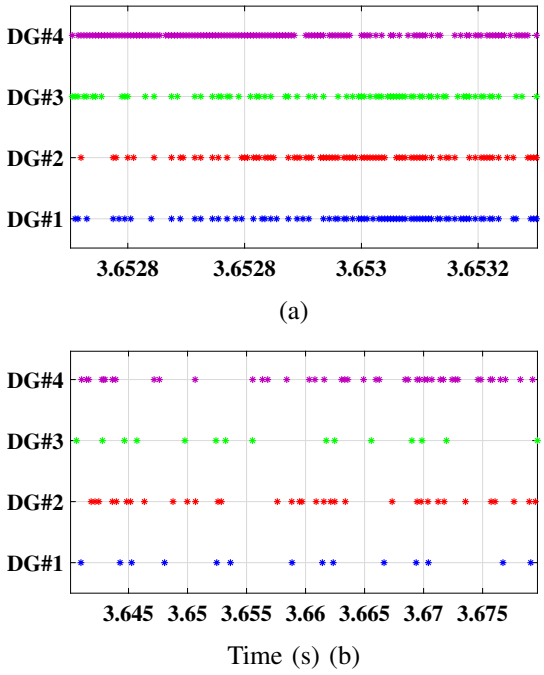

Fig. 7: Control update instants of the proposed method for DGs: (a) voltage controller and (b) frequency controller.

and frequency of each DG for the entire simulation time is indicated in Table. I. It is obvious that the event-triggering communication mechanism leads to fewer control updates than ideal, continuous, and periodic ones. It should be noted that the event-triggered control scheme does not impact the performance of the MG, and the presented scheme shows enough resiliency against DoS attacks.

It is worth mentioning that DoS attacks conduce to the loss of communication channels in the graph network so that the neighbours cannot get contacted through the attacked channels. The focus of the paper is to design a resilient secondary controller and the stability of microgrids while the cyber layer is subjected to DoS attacks. On the other hand, when it comes to PnP functionality, the DER unit is "*physically*" disconnected from the MG topology. Therefore, this unit is not engaged anymore for the load supply and, it is not able to transmit power across the MG. While in the case of DoS attacks in any commutation lines, it is still required to keep the voltage and frequency of a particular DER unit to the prescribed values. In this section, it is shown that the proposed secondary controller can still keep its robustness against the PnP scenario of one DG. The robust control design for the physical layer (the primary layer) of MGs against PnP has been discussed in the literature, see [41]–[43].

B. Comparison with Previous Methods

To verify the effectiveness of the proposed control scheme for the regulation problem of the DGs against DoS attacks, the comparison results with several distributed secondary control methods in the literature. Simulation results presented in Fig. 8 show the voltage, frequency, and active power of DG #3 for each algorithm. The sequences of the DoS attack are considered

TABLE I: The total number of control updates of the proposed event-triggered control scheme for DER units during the simulation time. The sampling time for the simulation is $T_s = 5 \times 10^{-5}$s.

Unit\Controller	Voltage controller	Frequency controller
DG#1	139107	32152
DG#2	136317	18455
DG#3	135934	21550
DG#4	138080	23472
DES#1	81373	8271
DES#2	78235	5163
DES#3	82233	13699

similar to Fig. 4. The following methods are chosen for the comparison.

- Firstly, the conventional controller in [7] is investigated, which utilizes the typical cooperative controller for voltage and frequency regulation based on measurement errors and an ideal communication topology.
- The next case is the distributed sliding mode control scheme in [15], which guarantees a finite-time voltage regulation and frequency synchronization subjected to uncertainties. The input dynamic extension technique is adopted in order to decrease the control signal chattering.
- Then, the resilient distributed secondary voltage and frequency control method in [44] is considered that guarantees the boundedness of synchronization errors for all units under deception attacks. This paper employs a distributed state observer to estimate the standard behavior of the states inspect to cyber-attacks.
- The last comparison case is the approach presented in [20], where a distributed observer-based finite-time control scheme with confidence factors and trust factors are suggested to improve the resilience of MGs under attack. The proposed controllers limit the effect of attacks on ac MGs.

As can be seen in Fig. 8, the conventional algorithm in [7] does not respond well under attack conditions. The performance of sliding mode control algorithm in [15] is not proper; however, it is observed that the voltage and frequency can return to their original values faster than the conventional method. As expected, the resilient method presented in [44] and [20] demonstrate relatively desirable performances against DoS attacks since they use observers in their design procedures. But, there are deviations from the nominal values when the attacks occur; because the controllers have been designed for resilience against another type of attack. Worth to be notified that the presented controller in [20] shows a little more robustness in comparison with the method in [44], which is an obvious outcome due to employing the trust and confidence factors. Nevertheless, in both algorithms, the control update instants are continuous, which causes increasing communication in comparison with the proposed control scheme. It can be concluded that the proposed control scheme comparatively provides desirable voltage and frequency synchronization with less controller updates when the MG faces DoS attacks.

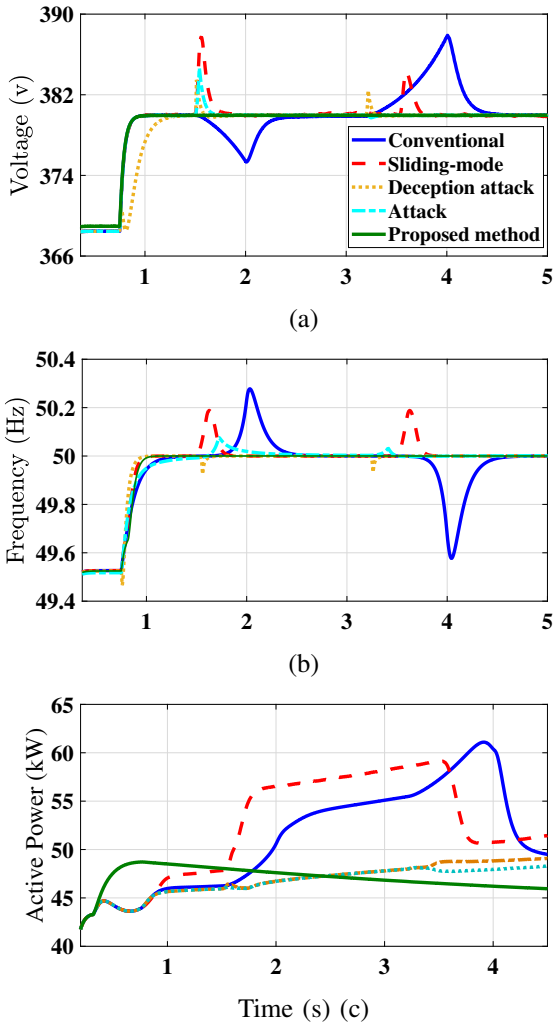

Fig. 8: Comparison of the proposed resilient control scheme with previously reported studies in [7], [15], [44], [20]: (a) voltage, (b) frequency, and (c) active power of DG #3.

VI. Conclusion

In this paper, an event-triggered resilient distributed voltage and frequency consensus-based control scheme subject to DoS attacks was proposed in the secondary layer of islanded cyber-physical ac MGs. By employing the proposed control schemes, voltage regulation and frequency synchronization along with accurate active power management and SoC matching were achieved. A state estimator was considered when launching the attack to anticipate the MG's states and attenuate the effects of attacks. Also, the ETM was designed to significantly reduce the number of control updates without Zeno behavior. The performance of the event-triggered secure voltage and frequency algorithms was validated for a couple of scenarios through digital time-domain simulations in the MATLAB/Simulink environment. The future scope of this research is to generalize this study to the attack-resilience problem of cyber-physical ac MGs in the presence of actuator cyber-attacks and faults.

References

[1] A. Afshari, M. Karrari, H. R. Baghaee, G. Gharehpetian, and S. Karrari, "Cooperative fault-tolerant control of microgrids under switching communication topology," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 1866–1879, 2019.

[2] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1963–1976, 2012.

[3] A. Afshari, M. Karrari, H. R. Baghaee, and G. B. Gharehpetian, "Distributed fault-tolerant voltage/frequency synchronization in autonomous ac microgrids," *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 3774–3789, 2020.

[4] Y. Khayat, Q. Shafiee, R. Heydari, M. Naderi, T. Dragičević, J. W. Simpson-Porco, F. Dörfler, M. Fathi, F. Blaabjerg, J. M. Guerrero *et al.*, "On the secondary control architectures of ac microgrids: An overview," *IEEE Transactions on Power Electronics*, vol. 35, no. 6, pp. 6482–6500, 2019.

[5] P. Ge, Y. Zhu, T. Green, and F. Teng, "Resilient secondary voltage control of islanded microgrids: An ESKBF-based distributed fast terminal sliding mode control approach," *IEEE Transactions on Power Systems*, vol. 36, pp. 1059–1070, 2020.

[6] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2586–2633, 2020.

[7] A. Bidram, A. Davoudi, F. L. Lewis, and Z. Qu, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Generation, Transmission & Distribution*, vol. 7, no. 8, pp. 822–831, 2013.

[8] Q. Shafiee, V. Nasirian, J. C. Vasquez, J. M. Guerrero, and A. Davoudi, "A multi-functional fully distributed control framework for AC microgrids," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3247–3258, 2016.

[9] N. M. Dehkordi, N. Sadati, and M. Hamzeh, "Fully distributed cooperative secondary frequency and voltage control of islanded microgrids," *IEEE Transactions on Energy Conversion*, vol. 32, no. 2, pp. 675–685, 2016.

[10] A. Afshari, M. Karrari, H. R. Baghaee, G. B. Gharehpetian, and J. M. Guerrero, "Robust cooperative control of isolated AC microgrids subject to unreliable communications: A low-gain feedback approach," *IEEE Systems Journal*, vol. 16, no. 1, pp. 55–66, 2021.

[11] J. Lai, H. Zhou, X. Lu, X. Yu, and W. Hu, "Droop-based distributed cooperative control for microgrids with time-varying delays," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1775–1789, 2016.

[12] M. Raeispour, H. Atrianfar, H. R. Baghaee, and G. B. Gharehpetian, "Distributed lmi-based control of heterogeneous microgrids considering fixed time-delays and switching topologies," *IET Renewable Power Generation*, vol. 14, no. 12, pp. 2068–2078, 2020.

[13] A. Afshari, M. Karrari, H. R. Baghaee, and G. Gharehpetian, "Resilient synchronization of voltage/frequency in AC microgrids under deception attacks," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2125–2136, 2020.

[14] M. A. Shahab, B. Mozafari, S. Soleymani, N. M. Dehkordi, H. M. Shourkaei, and J. M. Guerrero, "Distributed consensus-based fault tolerant control of islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 37–47, 2019.

[15] A. Pilloni, A. Pisano, and E. Usai, "Robust finite-time frequency and voltage restoration of inverter-based microgrids via sliding-mode cooperative control," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 1, pp. 907–917, 2017.

[16] M. R. Khalghani, J. Solanki, S. K. Solanki, M. H. Khooban, and A. Sargolzaei, "Resilient frequency control design for microgrids under false data injection," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 3, pp. 2151–2162, 2020.

[17] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under DoS attacks: A unified game approach," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1786–1794, 2016.

[18] D. Ding, Z. Wang, D. W. Ho, and G. Wei, "Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks," *Automatica*, vol. 78, pp. 231–240, 2017.

[19] M. S. Sadabadi, S. Sahoo, and F. Blaabjerg, "A fully resilient cyber-secure synchronization strategy for AC microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 12, pp. 13 372–13 378, 2021.

[20] R. Lu, J. Wang, and Z. Wang, "Distributed observer-based finite-time control of AC microgrid under attack," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 157–168, 2020.

[21] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4066–4075, 2018.

[22] J. Liu, Y. Du, S.-i. Yim, X. Lu, B. Chen, and F. Qiu, "Steady-state analysis of microgrid distributed control under denial of service attacks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2020.

[23] B. Zhang, C. Dou, D. Yue, J. H. Park, and Z. Zhang, "Attack-defense evolutionary game strategy for uploading channel in consensus-based secondary control of islanded microgrid considering dos attack," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 2, pp. 821–834, 2021.

[24] M. Mola, N. Meskin, K. Khorasani, and A. Massoud, "Distributed event-triggered consensus-based control of DC microgrids in presence of DoS cyber attacks," *IEEE Access*, vol. 9, pp. 54 009–54 021, 2021.

[25] S. Hu, P. Yuan, D. Yue, C. Dou, Z. Cheng, and Y. Zhang, "Attack-resilient event-triggered controller design of DC microgrids under DoS attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 2, pp. 699–710, 2019.

[26] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Multilayer resilience paradigm against cyber attacks in DC microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 3, pp. 2522–2532, 2020.

[27] 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 Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4909–4919, 2019.

[28] J. Shi, D. Yue, and S. Weng, "Distributed event-triggered mechanism for secondary voltage control with microgrids," *Transactions of the Institute of Measurement and Control*, vol. 41, no. 6, pp. 1553–1561, 2019.

[29] P. Ge, B. Chen, and F. Teng, "Event-triggered distributed model predictive control for resilient voltage control of an islanded microgrid," *International Journal of Robust and Nonlinear Control*, vol. 31, no. 6, pp. 1979–2000, 2021.

[30] J. Lai, X. Lu, X. Yu, and A. Monti, "Stochastic distributed secondary control for AC microgrids via event-triggered communication," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 2746–2759, 2020.

[31] S. Sahoo and J. C.-H. Peng, "A localized event-driven resilient mechanism for cooperative microgrid against data integrity attacks," *IEEE Transactions on Cybernetics*, vol. 51, pp. 3687–3698, 2020.

[32] H. K. Khalil and J. W. Grizzle, *Nonlinear systems*. Prentice hall Upper Saddle River, NJ, 2002, vol. 3.

[33] Y. Yang, Y. Li, D. Yue, Y.-C. Tian, and X. Ding, "Distributed secure consensus control with event-triggering for multiagent systems under DoS attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 6, pp. 2916–2928, 2020.

[34] Z. Feng and G. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Transactions on Control Systems Technology*, vol. 28, no. 3, pp. 741–752, 2019.

[35] X.-G. Guo, P.-M. Liu, J.-L. Wang, and C. K. Ahn, "Event-triggered adaptive fault-tolerant pinning control for cluster consensus of heterogeneous nonlinear multi-agent systems under aperiodic dos attacks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1941–1956, 2021.

[36] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu, "Detection of denial-of-service attacks based on computer vision techniques," *IEEE Transactions on Computers*, vol. 64, no. 9, pp. 2519–2533, 2014.

[37] J. Liu, X. Lu, and J. Wang, "Resilience analysis of DC microgrids under denial of service threats," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 3199–3208, 2019.

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

[39] M. ApS, *The MOSEK optimization toolbox for MATLAB manual. Version 9.0.*, 2019. [Online]. Available: http://docs.mosek.com/9.0/toolbox/index.html

[40] D. E. Olivares, A. Mehrizi-Sani, A. H. Etemadi, C. A. Cañizares, R. Iravani, M. Kazerani, A. H. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke *et al.*, "Trends in microgrid control," *IEEE Transactions on smart grid*, vol. 5, no. 4, pp. 1905–1919, 2014.

[41] M. S. Sadabadi, Q. Shafiee, and A. Karimi, "Plug-and-play voltage stabilization in inverter-interfaced microgrids via a robust control strategy," *IEEE Transactions on Control Systems Technology*, vol. 25, no. 3, pp. 781–791, 2016.

[42] P.-H. Huang, P. Vorobev, M. Al Hosani, J. L. Kirtley, and K. Turitsyn, "Plug-and-play compliant control for inverter-based microgrids," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 2901–2913, 2019.

[43] S. Riverso, F. Sarzo, and G. Ferrari-Trecate, "Plug-and-play voltage and frequency control of islanded microgrids with meshed topology," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1176–1184, 2014.

[44] A. Afshari, M. Karrari, H. R. Baghaee, and G. Gharehpetian, "Resilient synchronization of voltage/frequency in AC microgrids under deception attacks," *IEEE Systems Journal*, vol. 15, pp. 2125–2136, 2020.