IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 19, 2021, accepted March 31, 2021, date of publication April 5, 2021, date of current version April 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3070918

Distributed Event-Triggered Consensus-Based Control of DC Microgrids in Presence of DoS Cyber Attacks

MINA MOLA[1], NADER MESKIN[1], (Senior Member, IEEE), KHASHAYAR KHORASANI[2], (Member, IEEE), AND AHMED MASSOUD[1], (Senior Member, IEEE)

[1]Electrical Engineering Department, Qatar University, Doha, Qatar
[2]Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada

Corresponding author: Nader Meskin (nader.meskin@qu.edu.qa)

This work was supported by the Qatar National Research Fund (a member of the Qatar Foundation) through National Priorities Research Program (NPRP) Grant under Grant 10-0105-170107. Open Access funding provided by the Qatar National Library.

ABSTRACT In this paper, the problem of distributed event-based control of large scale power systems in presence of denial-of-service (DoS) cyber attacks is addressed. Towards this end, a direct current (DC) microgrid composed of multiple interconnected distributed generation units (DGUs) is considered. Voltage stability is guaranteed by utilizing decentralized local controllers for each DGU. A distributed discrete-time event-triggered (ET) consensus-based control strategy is then designed for current sharing in the DGUs. Through this mechanism, transmissions occur while a specified event is triggered to prevent unessential utilization of communication resources. The asymptotic stability of the ET-based controller is shown formally by using Lyapunov stability via linear matrix inequality (LMI) conditions. The behavior of the DGUs subject to DoS cyber attacks are also investigated and sufficient conditions for secure current sharing are obtained. Towards this end, a switching framework is considered between the communication and attack intervals in order to derive sufficient conditions on frequency and duration of DoS cyber attacks to reach the secure current sharing. The validity and capabilities of the presented approach is confirmed through a simulation case study.

INDEX TERMS Distributed event-based control, denial-of-service (DoS) cyber attack, DC microgrid, current sharing, asymptotic stability, consensus-based control, linear matrix inequality (LMI).

I. INTRODUCTION

A microgrid is a group of the low-voltage electrical system consisting of multiple distributed generation units (DGUs), loads, and storage devices interconnected through power lines [1]. The AC microgrid is the standard model of a microgrid used in residential, commercial, and industrial consumers and has attracted a lot of attention in the field of AC microgrids control [2], [3]. However, DC microgrid has several advantages over AC microgrid, such as improved overall efficiency, appropriate interfacing of batteries and DC power sources, and the increasing number of DC loads, which have made DC microgrid an attractive research topic [4]–[6]. Having the opportunity to utilize renewable energy sources by DC microgrid and the widespread usage in modern-designed vehicles such as train, aircraft, watercraft are representative examples of DC microgrid application and usage. Extensive use in industries makes DC microgrids an emerging subject that has recently achieved much research attention [7].

Current sharing and voltage regulation of DC microgrids are the main two control challenges of these systems. The optimal voltage regulation strategy results in the desired output voltage of each microgrid, while the current-sharing control strategy divides, shares, and dedicates balanced current to each DC microgrid [7]–[11]. Hierarchical control schemes have been developed in the literature to achieve both objectives [12]. Although centralized controllers satisfy the

The associate editor coordinating the review of this manuscript and approving it for publication was Bin Zhou.

voltage stabilization and precise current sharing goals [12], the computational and communication burden of these architectures increase by the larger size of microgrids. Moreover, a single-point-of-failure in the central control unit may lead to malfunction of the entire system [13]. This is the main reason why decentralized and distributed regulators, such as droop controllers [12], are preferred. Being a communication-less approach, droop controllers may lead to voltage deviations from reference values. Consequently, secondary control layer with consensus algorithms have been deployed and combined with the droop controller to deal with the deviation problem [13]–[15].

Scalability criteria have become one of the most important characteristics of control-scheme designs in distributed systems. Physical wide range of distributed microgrid systems has attracted researches' interest toward scalable control strategies, particularly aiming at current (power) sharing [7], [8], [14], [16]–[18]. In a distributed control scheme, each subsystem can receive information from its neighbors, resulting in their overall performance improvement. Therefore, this approach has been developed as a viable scheme for large-scale systems as in [19], [20]. Moreover, information exchanges among subsystems are transmitted over networks, which may generate a heavy communication burden. Event-triggered control (ETC) techniques receive much attention in recent years to avoid the unnecessary utilization of communication resources (refer to for instance [21]–[27]).

In the distributed ETC of large-scale systems, each subsystem transmits its information through the network based on certain event-triggering conditions. Data transmission only takes place when event-triggering conditions are violated, and hence the communication cost is considerably reduced [28]. In [29], the DC microgrid was controlled with an ET communication-based voltage droop control strategy to ensure power sharing. The proposed DC microgrid was composed of distributed energy resources (DERs) in which the DER layer was composed of a distributed source connected to a DC/DC converter with a specific duty cycle. A distributed nonlinear ETC approach was developed in [30] for current sharing and voltage regulation in an electrical network model of a DC microgrid. This DC microgrid includes converters and local and public loads. In [31], a distributed discrete-time algorithm is developed to achieve proportional load current sharing and average bus voltage regulation in discrete-time DC microgrids. A periodic event-triggered discrete-time algorithm is proposed to reduce the communication requirement and avoid the Zeno phenomenon.

The ET-based control approaches [29], [30] do not guarantee the Zeno behavior (infinite events over a finite time interval) exclusion which is an important issue in evaluation of the controller performance. Indeed, the Zeno phenomenon describes the behavior of the ET-based controller when the system is subjected to an unbounded number of events in a finite and bounded duration of a given time interval. This can occur when the controller unsuccessfully attempts to satisfy the event-triggered condition more rapidly that would lead to sending infinite number of data in a finite interval. In other words, feasibility and practicality of the ET-based controller should be considered by showing the Zeno behavior exclusion. However, this important fact is not guaranteed in the above approaches [29], [30].

Recently, cyber security of power systems against malicious cyber attacks has attracted significant attention. Adversaries may disrupt power systems by launching malicious attacks on the physical system layer and/or the communication network layer. Several security results on cyber attacks against the power grids have been addressed in [32]–[36]. One of the most common malicious attacks is the denial of service (DoS), which can congest the communication channels by sending large quantities of unauthentic packets. This cyber-attack is regularly the main reason for a heavy transmission burden and consumes unusual amounts of network bandwidth resulting in interruptions in the network [37]. Hence, it blocks the transmission medium and interrupts regular communication for a period of time.

Analysis of the DoS cyber attacks on load frequency control (LFC) of power systems under different communication schemes have been recently addressed in [32], [37]–[39]. The analysis of DoS cyber attacks under event-triggered load frequency control of single area power system was carried out in [37]. The average dwell time design approach is utilized to establish exponential stability criteria based on the choice of appropriate rate of allowable DoS attack duration for the entire running time of system and time delay margins. A similar kind of approach was used for multi-area LFC system in [38], where the study investigated the maximum degree of tolerance of LFC system against DoS attack and the total length of DoS attacks time for assuring stability of the LFC system was obtained [37]. An event-triggered based approach for interconnected power systems that tolerates the lack of data because of the DoS attack was presented in [32]. It concentrated on developing resilient control without a *priori* knowledge of additional DoS attacks probability distributions. The influence of DoS attack in the form of uncertainty of event triggering condition in networked control systems was discussed in [39]. Moreover, event-triggered H_∞ control for networked control systems under denial-of-service attacks is addressed in [40] which reduces excessive utilization of communication resources. In this paper, sufficient conditions for the stability of the system are achieved by using LMI conditions.

DC microgrid systems rely on real-time operation and in presence of DoS cyber attacks may become unstable and damaged [41]. In [42], a distributed monitoring scheme for attack detection in large-scale linear systems applied to DC microgrids is presented. The recommended architecture utilizes a Luenberger observer as well as a bank of unknown-Input Observers at each subsystem to provide attack detection capabilities. In [43], the attack-resilient event-triggered control synthesis approach for a networked nonlinear DC microgrid system under DoS attacks was addressed. An event-triggered switched system model of the nonlinear DC microgrid was established and an average dwell-time method and piecewise Lyapunov functional method were employed to show the asymptotic stability of the system. However, in this work only stability of the microgrid was evaluated and the current sharing which is one of the main challenges in these systems, was not considered. Therefore, the secure current sharing problem of DGUs in a DC microgrid subject to cyber attacks is an important problem that needs to be formally investigated. In [44], the reactive power sharing problem of an AC microgrid under DoS attacks is addressed. A periodic ET update method is proposed which can avoid the Zeno phenomenon. The tolerance range of DoS frequency and duration for the DG related to the smallest event-interval time of the ET update method is found. However, the microgrid type and modeling, the ET mechanism, and the stability analysis approach in our paper are totally different from [44].

In this paper, a DC microgrid system including different types of DGUs is considered, where voltage stabilization is guaranteed by using a decentralized local controller for each DGU. A distributed discrete-time ET consensus-based controller is then designed for current sharing in DGUs. A state-dependent threshold is then designed for proper ET condition using the secondary controller. Indeed, stability of the overall microgrid is then guaranteed by using the Lyapunov stability results, and design parameters are found via solving a linear matrix inequity (LMI). The advantages of our proposed approach are in reducing the cost of the network communication and improving its security since the data transmission will be based on the ETC system conditions. Finally, the overall microgrid subject to the DoS cyber attack is considered and sufficient conditions for the secure current sharing are determined by applying a switching framework between the communication and the cyber attack intervals.

The main contributions of this paper are summarized as follows:

- A discrete-time ET consensus-based control methodology for the DGU is investigated and developed in order to achieve proportional current sharing in a DC microgrid. This event-based secondary controller is designed based on a linear discrete-time consensus protocol in which each DGU transmits its information through the network channels when the event-triggering conditions are violated, and hence the communication cost is considerably reduced. The DC microgrid modeling in our paper is different from those in [29] and [30]. The microgrid system type in [44] is AC microgrid which is totally different from our proposed system. Specifically there is no need to consider the Zeno phenomena in our proposed event-triggered secondary controller since it is implemented in a discrete-time framework whereas the works in [29] and [30] proposed continuous-time event-triggered controllers without investigating the exclusion of the Zeno phenomena. The ET mechanism and the technique of avoiding Zeno phenomena in our proposed event-triggered secondary controller is different from [44].
- The vulnerabilities of our proposed discrete-time event-triggering mechanism to DoS cyber attacks in DC microgrid systems are investigated. Towards this end, a switching framework is developed and sufficient conditions on frequency and duration of DoS cyber attacks are derived in order to simultaneously guarantee secure current sharing and voltage regulation. In other words, a switching framework is considered between the communication and attack intervals in order to derive sufficient conditions on frequency and duration of DoS cyber attacks to reach the secure current sharing and the stability of the overall microgrid. In [31], a periodic event-triggered discrete-time algorithm is proposed to achieve proportional load current sharing and average bus voltage regulation in discrete-time DC microgrids. In comparison to [31], a continuous-time DC microgrid is considered in our paper and the ET condition is different. Furthermore, the overall microgrid is exposed to DoS cyber attacks. In [43], an attack-resilient event-triggering mechanism was proposed for a nonlinear DC microgrid system subject to intermittent DoS attacks where the DoS frequency and DoS duration were characterized in the stability criterion. As compared to [43], the system modeling in our proposed approach is different and moreover importantly both current sharing and voltage regulation in the DC microgrid are considered. The stability analysis approach in our paper is different from [44]. Moreover, in our proposed approach the DoS attack impacts on the voltage stability is addressed which was not noticed in [44]. In other words, in our proposed approach by using Lyapunov stability approach, the linear matrix inequality conditions that ensure the voltage stability and current sharing are obtained.

The remainder of the paper is organized as follows. In Section II, the description of microgrid system is presented and the problem formulation is provided in Section III. The stability analysis of the overall microgrid and the main results without and with the presence of DoS cyber attacks are analyzed in Section IV. In Section V, simulation results are provided to confirm the efficacy of the proposed method and to illustrate the efficiency of the proposed ET consensus-based method in achieving voltage regulation and current sharing of the DC microgrid in the presence of DoS cyber attack. Finally, conclusions are presented in Section VI.

II. MICROGRID SYSTEM DESCRIPTION

In this section, we describe the model of the microgrid and the control systems. A DC microgrid consists of N DGUs that are connected to each other through power lines. An undirected graph (digraph) $\mathcal{G}_e = (\nu, \varepsilon_e, w_e)$ is used to illustrate the microgrid where the nodes, $\nu \in \{1, \ldots, N\}$, show the DGUs, and the edges, $\varepsilon_e \in \nu \times \nu$, represent the power lines. Moreover, the diagonal matrix w_e with $w_{e,ii} = w_{e,i}$ is used to show the weight matrix, where $w_{e,i}$ is the associated edge weight for the edge $e_i \in \varepsilon_e$. Note that the direction of edges specifies a reference direction for positive currents, and the edges weights are related to the corresponding line conductances, $\frac{1}{R_{ij}}$. The Laplacian matrix of the physical system is given by $L_e = q_e w_e q_e^\top$, where q_e denotes the incidence matrix of $\mathcal{G}_e$. The set of neighbors of the ith node is denoted by $N_i = \{j \in \nu : (i, j) \in \varepsilon_e\}$. The microgrid takes advantage of a communication network such that each local controller can obtain information from its neighbors. Moreover, this paper assumes that the information network topology is the same as the physical topology.

Here, we consider a hierarchical control architecture with two objectives: keeping local stability of subsystems and achieving consensus of the second state variable among the large-scale system's subsystems. The equipped DGU with the proposed ET hierarchical control is shown in Fig. 1. A DC voltage source is used to model the renewable resource in each DGU and provides a local load through a DC-DC converter. The local DC load and the PCC are connected through an RL filter.

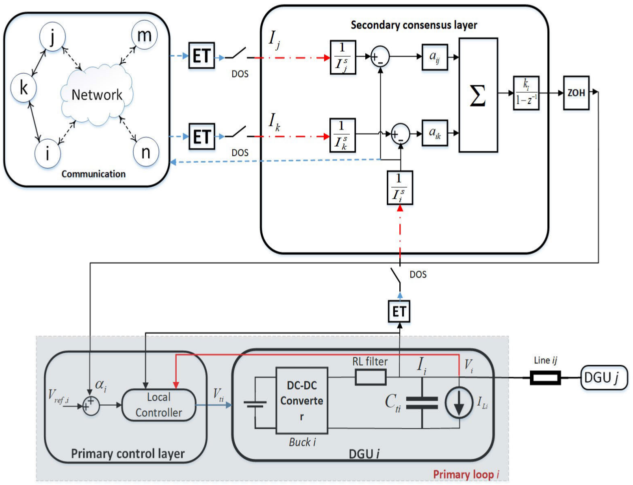

FIGURE 1. The *i*-th DGU having a complete hierarchical control in communication with its neighbors in presence of the DoS cyber attack.

The dynamics model of the i-th DGU is given as follows [45]:

$$\frac{\mathrm{d}V_i(t)}{\mathrm{d}t} = \frac{1}{C_{ti}}(I_i(t) - I_{Li}(t)) + \sum_{j \in N_i} \frac{1}{C_{ti}R_{ij}}(V_j(t) - V_i(t)),$$
$$\frac{\mathrm{d}I_i(t)}{\mathrm{d}t} = \frac{1}{L_{ti}}V_{ti}(t) - \frac{R_{ti}}{L_{ti}}I_i(t) - \frac{1}{L_{ti}}V_i(t), \; i = 1, \ldots, N, \quad (1)$$

where $V_i(t)$, $I_i(t)$ and $I_{Li}(t)$ denote the load voltage, generated current, and local current demand, respectively, L_{ti}, C_{ti}, R_{ti}, and R_{ij} denote filter inductance, shunt capacitor, filter resistance, and line resistance, respectively. $V_i(t), I_i(t)$ denote the states, $V_{ti}(t), I_{Li}(t)$ denote inputs, $V_j(t)$ is the point of common coupling (PCC) voltage of the DGUi's neighbors, and $\frac{1}{R_{ij}}$ denotes the conductance of the power line connecting DGUs i and j.

The primary decentralized controller is given to regulate each PCC's voltage and guarantee the overall microgrid's stability. Measurements of $V_i(t)$ and $I_i(t)$ are exploited as well as the local regulator of each DGU to create the command $V_{ti}(t)$ of the i-th DC-DC converter and guarantees a reference signal $V_{\mathrm{ref},i}(t)$ is tracked. The control loop of the converter is the local controller which is assumed in the model.

In general, not all the DGUs can provide the demanded local current loads and require power from other DGUs. Hence, the currents between DGUs should be shared proportional to their generation capacity and this is achieved by designing the secondary current sharing controller. Moreover, in order to minimize the voltages deviation at PCCs, the secondary controller's objective is to also guarantee the same average voltage value among all the PCCs.

In particular, for generation efficiency improvement, it is usually required to share the total current demand among different DGUs in proportion to their corresponding energy sources (proportional current sharing). Conventionally, each DGU broadcasts its current at every time instant which may lead to inefficient utilization of communication resources. Instead of this conventional approach, an ET-based mechanism is introduced in this paper, in which the transmission occurs only when a certain event is triggered. The architecture of the proposed distributed ET consensus-based secondary control for the microgrid is shown in Fig. 2.

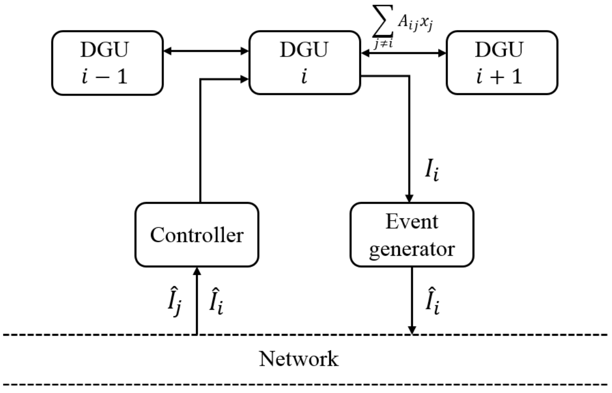

FIGURE 2. ET consensus-based secondary control system for current sharing in the microgrid.

III. PROBLEM FORMULATION

A. DC MICROGRID MODEL

The state space representation of the i-th DGU can be written as follows:

$$\dot{x}_i(t) = A_{ii}x_i(t) + \sum_{j \in N_i} A_{ij}x_j + B_i u_i(t) + M_i d_i(t), \qquad (2)$$

where $x_i(t) = [V_i(t), I_i(t)]^\top$, $i = 1, 2, \ldots, N$ denotes the local state, $u_i(t) = V_{ti}(t)$ denotes the primary control input, and $d_i(t) = I_{Li}(t)$ denotes the exogenous input. It is assumed that the current demands of the DGUs, $I_{Li}(t)$, are piece-wise constant current loads. The matrix A_{ii} is the local state transition matrix, A_{ij} describes the interconnection between DGUs i and j, and B_i is the control input matrix. These matrices are defined as follows [11]:

$$A_{ii} = \begin{bmatrix} \sum\limits_{j\in N_i} -\frac{1}{R_{ij}C_{ti}} & \frac{1}{C_{ti}} \\ -\frac{1}{L_{ti}} & -\frac{R_{ti}}{L_{ti}} \end{bmatrix}, \quad A_{ij} = \begin{bmatrix} \frac{1}{R_{ij}C_{ti}} & 0 \\ 0 & 0 \end{bmatrix},$$
$$B_i = \begin{bmatrix} 0 \\ \frac{1}{L_{ti}} \end{bmatrix}, \quad M_i = \begin{bmatrix} -\frac{1}{C_{ti}} \\ 0 \end{bmatrix}.$$

B. HIERARCHICAL CONTROL MODEL

This section considers the hierarchical control strategy, which ensures subsystems local stability and guarantees current sharing among DGUs. This two-layered control strategy is explained in the following.

1) DECENTRALIZED PRIMARY CONTROLLER

In the first step, an augmented state variable $\zeta_i(t)$ is introduced to presents the required integrator action in the primary local controller. The dynamics of $\zeta_i(t)$ is given by $\dot{\zeta}_i(t) = V_{\text{ref},i}(t) - V_i(t) + \alpha_i(t)$, where $V_{\text{ref},i}(t)$ denotes the reference for the voltage $V_i(t)$, and $\alpha_i(t) \in \mathbb{R}$ denotes the secondary control input. Hence, the resulting augmented system model with an integrator is now given as follows:

$$\dot{\hat{x}}_i(t) = \hat{A}_{ii}\hat{x}_i(t) + \sum_{j\in N_i} \hat{A}_{ij}\hat{x}_j + \hat{B}_i u_i(t) + \hat{G}_i\alpha_i(t)$$
$$+ \hat{M}_i\hat{d}_i(t), \quad i = 1, 2, \ldots, N, \tag{3}$$

where $\hat{x}_i(t) = [x_i^\top(t), \zeta_i(t)]^\top$ is the local state and $\hat{d}_i(t) = [d_i^\top(t), V_{\text{ref},i}]^\top$ is the exogenous input. The matrices in (3) are now given as follows:

$$\hat{A}_{ii} = \begin{bmatrix} A_{ii} & 0 \\ -H_i & 0 \end{bmatrix}, \quad \hat{A}_{ij} = \begin{bmatrix} A_{ij} & 0 \\ 0 & 0 \end{bmatrix},$$
$$\hat{B}_i = \begin{bmatrix} B_i \\ 0 \end{bmatrix}, \quad \hat{M}_i = \begin{bmatrix} M_i & 0 \\ 0 & 1 \end{bmatrix}, \quad \hat{G}_i = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Note that the pair $(\hat{A}_{ii}, \hat{B}_i)$ is controllable, and hence the system (3) is stabilizable.

In the second step, in order to guarantee the stability of the overall microgrid and to regulate the voltage at each PCC, a decentralized state feedback controller is designed as follows [11]:

$$u_i(t) = K_i\hat{x}_i(t), \tag{4}$$

such that $(A_{ii} + B_iK_i)$ is Hurwitz where the gain matrix K_i can be obtained based on the dynamics of the i-th DGU and the power line parameters of the neighboring DGUs via LMI conditions [46].

2) DISTRIBUTED ET CONSENSUS-BASED SECONDARY CONTROLLER

An event-based secondary controller is now designed based on a linear discrete-time consensus protocol to achieve current sharing in a DC microgrid. Denoting $\tau_k^i h \subset \mathbb{Z}^+$ as the k-th time instant that events are triggered in the subsystem i, with h denoting as the sampling period, the latest transmitted i-th DGU current signal, $\hat{I}_i(\tau h)$, $\tau \in \mathbb{Z}^+$, is defined as follows:

$$\hat{I}_i(\tau h) = \begin{cases} I_i(\tau_k^i h), & \text{when an event occurs} \\ I_i(\tau_{k-1}^i h), & \text{otherwise} \end{cases} \tag{5}$$

where $I_i(\tau_{k-1}^i h)$ is the i-th DGU current at the last event-triggered instant. For notation of simplicity, we omit the sampling time h when referring to discrete-time instants, i.e. $\hat{I}_i(\tau) = \hat{I}_i(\tau h)$.

The following control objective is defined for the event-based proportional current sharing of the microgrid.

Control Objective for Proportional Current Sharing:

Current sharing is obtained at steady state, if the overall load current is proportionally shared among DGUs, i.e.,

$$\frac{\hat{I}_i(\tau)}{I_i^s} = \frac{\hat{I}_j(\tau)}{I_j^s}, \tag{6}$$

where $I_i^s > 0$ denotes the i-th DGU current generation capacity.

The proposed secondary ET consensus-based controller for the i-th DGU is given as follows:

$$\alpha_i(\tau+1) = \alpha_i(\tau) + h[-k_{I,i}\sum_{j\in N_i} a_{ij}(w_i\hat{I}_i(\tau) - w_j\hat{I}_j(\tau))], \tag{7}$$

where $w_i = \frac{1}{I_i^s}$ and $k_{I,i}$ is the local gain of the i-th DGU.

Note that at the triggering instants τ_k^j, the j-th DGU will communicate with its neighbors and share the value of $I_j(\tau)$. The secondary control input is then generated by using the zero-order hold as follows:

$$\alpha_i(t) = \alpha_i(\tau), \ t \in [\tau h, (\tau+1)h). \tag{8}$$

Although the i-th DGU has access to its own current $I_i(t)$, the ET consensus-based controller (7) uses the last broadcast current $\hat{I}_i(\tau)$. This is to ensure that the average of DGUs' initial currents is preserved throughout the evolution of the system. The subsequent event instants are determined by the event-triggering mechanism, which is given as follows:

$$\tau_{k+1}^i = \inf\{\tau > \tau_k^i : |I_i(\tau_k^i) - I_i(\tau)| > \sigma_i|\alpha_i(\tau)|\}, \tag{9}$$

where $\sigma_i > 0$ is a scalar to be designed as a trade off between the network utilization and the control performance. In fact, in order to guarantee the ET-based current sharing in DGUs, the currents information should be transmitted only when condition (9) is met.

It should be noted that in the ET condition (9), the continuous states are not needed and as it was discussed earlier, the conditions are only checked in the sampling periods due to the consideration of $\hat{I}_i(\tau) = \hat{I}_i(\tau h)$. In other words, the event-triggered-based secondary layer controller in (7) is designed in a discrete framework but the results are inserted into the main continuous system (3) in a continuous format by using the ZOH in (8).

The error between the latest broadcasted current signal and the i-th DGU current is defined as $e_i(\tau) = \hat{I}_i(\tau) - I_i(\tau)$.

Note that at time τ^i_{k+1}, a new event is triggered so that the error signal $e_i(\tau)$ is reset to $e_i(\tau^i_{k+1}) = 0$. Consequently, the following inequality can be written which holds for all τ:

$$|e_i(\tau)| \leq \sigma_i |\alpha_i(\tau)|. \tag{10}$$

and it follows that:

$$e^\top(\tau)e(\tau) - \alpha^\top(\tau)\Sigma\alpha(\tau) \leq 0, \tag{11}$$

where $e(\tau) = [e^\top_1(\tau), e^\top_2(\tau), \ldots, e^\top_N(\tau)]^\top$, $\alpha(\tau) = [\alpha^\top_1(\tau), \alpha^\top_2(\tau), \ldots, \alpha^\top_N(\tau)]^\top$, and $\Sigma = \operatorname{diag}(\sigma^2_1, \sigma^2_2, \ldots, \sigma^2_N)$.

Remark 1: It is assumed that the transmitted data in the event-based communication network can be available for the neighbors without delay. In other words, when the data is updated based on the event-triggered condition, the updated data will be available for the neighboring DGU at the moment. Delay in the network channel is another important problem in large-scale networks which will be taken into consideration in our future works.

C. DENIAL-OF-SERVICE (DoS) ATTACK

A DoS attack is defined as a period of time at which the currents cannot be transmitted successfully through the network communication channels. Cyber attacks with unlimited energy make the overall system unstable. However, in reality the attackers need inactive sleep intervals for energy recovery. Therefore, it is assumed that the length and frequency of cyber attacks are limited. According to the above fact, the entire time is divided into communication intervals and cyber attack intervals, where in the communication intervals the event-based data transmission is performed successfully but in the cyber attack intervals the data transmission is terminated.

Defining $\{h_z\}_{z\in Z^+}, h_0 \geq 0$, as the sequence of the DoS attack, the time interval of the zth DoS attack could be expressed as $H_z = [h_z, h_z + \Delta_z)$, where $\Delta_z \geq 0$ is the length of the zth DoS attack time interval in which data transmissions are disrupted. The sets of cyber attack and successful communication time instants in a given interval $[\lambda, \tau)$ are defined as follows, respectively:

$$\Pi_a(\lambda, \tau) = \bigcup_{z\in Z^+} H_z \bigcap [\lambda, \tau), \tag{12}$$

$$\Pi_c(\lambda, \tau) = [\lambda, \tau) \setminus \Pi_a(\lambda, \tau), \tag{13}$$

where $\tau, \lambda \in Z^+$ and $\tau \geq \lambda$.

The general format of the DoS attack is shown in Fig. 3. The sequence of time instants that the current is transferred successfully is denoted by τ^i_m. In practical cases, the system update rules are performed on a digital platform. Hence, it is assumed that there exists a time delay Δ' between the end of the DoS cyber attack ($\tau = h_z + \Delta_z$) and the successful transmission of the data ($\tau = \tau^i_{m+1}, m = 1, \ldots$) as shown in Fig. 3. Therefore, the z-th time interval that the triggering condition (9) does not hold is as follows:

$$\mathcal{N}_z = [h_z, h_z + \Delta_z + \Delta'). \tag{14}$$

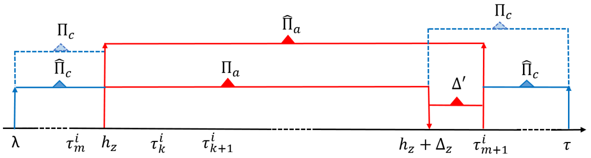

FIGURE 3. Time intervals in presence of the DoS attack.

and consequently, any time interval $[\lambda, \tau)$ can be represented as follows:

$$[\lambda, \tau) = \hat{\Pi}_c(\lambda, \tau) \bigcup \hat{\Pi}_a(\lambda, \tau). \tag{15}$$

where $\hat{\Pi}_a(\lambda, \tau) = \bigcup \mathcal{N}_z \bigcap [\lambda, \tau)$ and $\hat{\Pi}_c(\lambda, \tau) = [\lambda, \tau) \setminus \hat{\Pi}_a(\lambda, \tau)$.

Let $\underline{\Delta} = \min\{\tau^i_{k+1} - \tau^i_k\}$ and $\Lambda_z = h_{z+1} - h_z$ denote the minimum possible sampling rate (lower bound on the inter-sampling rate) and the time elapsing between any two successive DoS triggering, respectively. In case of the discrete framework, the lower bound on the inter-sampling rate will be 1. It is worth noting that if $\Lambda_z < 1$ then overall microgrid stability can be lost in spite of the ET secondary control update strategy. Hence, in order to assure the stability, the frequency at which the DoS can occur must be sufficiently small as compared to the minimum sampling rate. The following assumptions are considered on the cyber attack frequency and duration [47], [48].

DoS Frequency : For all $T_2 > T_1 > T_0$, there exist $\eta_D > 0$ and $\tau_D > 1$ such that

$$N_a(T_1, T_2) \leq \eta_D + \frac{T_2 - T_1}{\tau_D}, \tag{16}$$

where $N_a(T_1, T_2)$ is the total number of the DoS *off/on* transitions over $[T_1, T_2)$ and τ_D is the parameter whose inverse provides an upper bound on the average frequency of the DoS *off/on* transitions, i.e., average number of the DoS *off/on* transitions per unit time.

DoS Duration : For all $T_2 > T_1 > T_0$, $T_0 > 0$ and $\lambda_a > 0$, the cyber attack duration over $[T_1, T_2)$ is defined as follows:

$$\Pi_a(T_1, T_2) \leq T_0 + \frac{T_2 - T_1}{\lambda_a}, \tag{17}$$

where λ_a is the parameter whose inverse provides an upper bound on the average duration of the DoS per unit time.

IV. STABILITY ANALYSIS AND CURRENT SHARING

In this section, it is shown that stability of the overall microgrid controlled by utilizing (7) is achieved and the event-based current sharing objective is satisfied with and without the presence of DoS cyber attacks. Using the primary controller, the following relationship holds [45]:

$$V_i(t) = V_{\mathrm{ref},i} + \alpha_i(t), \quad i = 1, \ldots, N, \tag{18}$$

Therefore, the following expression for the microgrid can be obtained:

$$V(t) = \bar{V}_{\mathrm{ref}} + \alpha(t), \quad i = 1, \ldots, N, \tag{19}$$

where $\bar{V}_{\text{ref}} = [V_{\text{ref},1}, V_{\text{ref},2}, \ldots, V_{\text{ref},N}]^\top$. The collective dynamics of the secondary ET consensus-based controller for the microgrid can be written as follows:

$$\begin{aligned}\alpha(\tau+1) &= \alpha(\tau) + h[-K_I L_e W(I(\tau)+e(\tau))],\\ &= \alpha(\tau) + h[-LW(I(\tau)+e(\tau))], \quad (20)\end{aligned}$$

where $L = K_I L_e$ denotes the Laplacian matrix of $\mathcal{G}_e$ with w_e replaced by $K_I w_e$, $K_I = \text{diag}(k_{I,1}, k_{I,2}, \ldots, k_{I,N})$, $W = \text{diag}(\frac{1}{I_1^s}, \ldots, \frac{1}{I_N^s})$, and $I(\tau) = [I_1(\tau), I_2(\tau), \ldots, I_N(\tau)]^\top$.

Given (19) and (20) and knowing that the current of DGUs is $I(\tau) = I_L(\tau) - q_e I_l(\tau)$ and the line current is $I_l(\tau) = -w_e q_e^\top V(\tau)$, one can obtain the following relationship:

$$\begin{aligned}\alpha(\tau+1) = \alpha(\tau) + h[-Q\alpha(\tau) - LWe(\tau)\\ - LWI_L(\tau) - Q\bar{V}_{\text{ref}}], \quad (21)\end{aligned}$$

where $I_L(\tau) = [I_{L1}(\tau), I_{L2}(\tau), \ldots, I_{LN}(\tau)]^\top$ denotes the vector of local load currents, $I_l(\tau) = [I_{l1}(\tau), I_{l2}(\tau), \ldots, I_{lN}(\tau)]^\top$ denotes the vector of line currents, $Q = LWM$, and $M = q_e w_e q_e^\top$. Consequently, due to the fact that the load currents $I_{Li}(\tau)$ and the reference voltages $V_{\text{ref},i}$ are bounded, the following system is considered for stability analysis of the linear system (21), namely:

$$\alpha(\tau+1) = A'\alpha(\tau) - B'e(\tau), \quad (22)$$

where $A' = (I - hQ)$ and $B' = hLW$.

A. WITHOUT DoS ATTACK

In the proposed distributed discrete-time ET consensus-based control methodology for the microgrid, each DGU transmits its information through the network channels based on the ET protocol (7) which guarantees the current sharing. Data transmission only takes place when the event-triggering conditions are violated, and hence the communication cost is considerably reduced.

Theorem 1: Consider the system (3) subject to the ET protocol (7). It follows that under Assumption 1 all DGUs can achieve current sharing under the triggering condition (9) and the overall microgrid (22) is stable if there exist a symmetric positive-definite matrix $P \in \mathbb{R}^{N\times N}$, and a positive definite diagonal matrix $\Sigma \in \mathbb{R}^{N\times N}$, such that the following LMI condition holds:

$$\begin{bmatrix} A'^\top PA' - P + \Sigma & -A'^\top PB' \\ -B'^\top PA' & -I + B'^\top PB' \end{bmatrix} < 0. \quad (23)$$

Proof 1: First the stability analysis of the overall microgrid is shown. System (22) is stable if there exists a discrete-time quadratic Lyapunov function $S_a(\tau) = \alpha^\top(\tau)P\alpha(\tau)$ with $P > 0$ such that the following inequality holds:

$$\begin{aligned}S_a(\tau+1) - S_a(\tau) = \alpha^\top(\tau+1)P\alpha(\tau+1)\\ -\alpha^\top(\tau)P\alpha(\tau) < 0. \quad (24)\end{aligned}$$

Considering the event-triggering condition (11), the sufficient condition for satisfying (24) is obtained by the following LMI:

$$\begin{aligned}\alpha^\top(\tau+1)P\alpha(\tau+1) - \alpha^\top(\tau)P\alpha(\tau) - e^\top(\tau)e(\tau)\\ +\alpha^\top(\tau)\Sigma\alpha(\tau) < 0. \quad (25)\end{aligned}$$

Substituting (22) into (25), and after some algebraic manipulations, the LMI (23) is achieved.

Next, the current sharing objective is shown. The distributed controller (7) leads to current sharing at the steady state which can be expressed as follows:

$$0 = -k_{I,i}\sum_{j\in N_i} a_{ij}(w_i\hat{I}_i(\tau) - w_j\hat{I}_j(\tau)), \quad (26)$$

which is equivalent to:

$$0 = -k_{I,i}\sum_{j\in N_i} a_{ij}[w_i(I_i(\tau)+e_i(\tau)) - w_j(I_j(\tau)+e_j(\tau))],$$

which can compactly be expressed for all DGUs as follows:

$$0 = -K_I L_c W\bar{I} - K_I L_c We(\tau), \quad (27)$$

where $\bar{I} = [\bar{I}_1, \bar{I}_2, \ldots, \bar{I}_N]^\top$ is the steady state solution of $I(\tau)$. Equation (27) can be expressed as follows:

$$0 = -LW(\bar{I} + e(\tau)). \quad (28)$$

According to properties of the Laplacian matrix, it is concluded from (28) that $W(\bar{I} + e(\tau)) \in \mathcal{R}(\mathbb{1})$, where $\mathcal{R}(\mathbb{1})$ denotes the range of $\mathbb{1}$, i.e., all elements of $W(\bar{I} + e(\tau))$ are identical. Therefore, it is shown that (6) is satisfied and the event-based proportional current sharing is achieved. This completes the proof of the theorem.

Remark 2: It should be emphasized that the proposed event-triggered secondary controller is implemented in a discrete-time framework, and hence there is no need to consider the Zeno phenomena while the previous works in [29], [30] proposed continuous-time event-triggered controllers without investigating the existence of the Zeno phenomena. The main challenge for the continuous-time framework is that in current sharing controller the even-triggered mechanism depends only on the current of the DGU, i.e. I_i while generally it should depend on both states of the DGU, i.e. I_i and V_i.

B. WITH DoS CYBER ATTACK

In presence of the DoS cyber attack, the event-based data transmission is disrupted which can affect the stability of the overall microgrid. Towards this end, the behavior of DGUs subject to the DoS cyber attack needs to be investigated and sufficient conditions for secure current sharing should be determined. Towards this goal, a switching framework similar to [47], [48] and [49] is considered between the communication and the cyber attack intervals in order to derive sufficient conditions for secure current sharing.

To evaluate the system behavior in presence of the DoS cyber attacks the dynamics of the overall microgrid should be obtained. In the DoS intervals H_z, the error definition is as follows:

$$e(\tau) = \hat{I}(h_z) - I(\tau), \quad (29)$$

where $\hat{I}(h_z)$ represents the last successful broadcast current up to h_z. Considering the DGU currents by $I(\tau) = I_L(\tau) - q_e I_l(\tau)$, the line currents as $I_l(\tau) = -w_e q_e^\top V(\tau)$, and the DGUs PCC voltages as $V(\tau) = \bar{V}_{\text{ref}} + \alpha(\tau)$, the following equality holds:

$$I(\tau) = I_L(\tau) + M\bar{V}_{\text{ref}} + M\alpha(\tau). \tag{30}$$

Substituting (30) into (29) the following equation can be written:

$$e(\tau) = \hat{I}(h_z) - I_L - M\bar{V}_{\text{ref}} - M\alpha(\tau). \tag{31}$$

Substituting (31) into (22), yields:

$$\alpha(\tau+1) = (A' + B'M)\alpha(\tau) - B'(\hat{I}(h_z) - I_L - M\bar{V}_{\text{ref}}).$$

Consequently, the following system is considered for stability analysis of the overall microgrid during the DoS intervals:

$$\alpha(\tau+1) = (A' + B'M)\alpha(\tau). \tag{32}$$

Note that $\hat{I}(h_z)$ remains constant in the DoS intervals.

The following theorem is now provided to show that the secure current sharing is achieved over two different time intervals, provided that the cyber attack frequency and attack duration satisfy a certain condition.

Theorem 2: Consider the system (3) in presence of the DoS cyber attack subject to the ET protocol (7). It follows that under Assumption 1 all the DGUs can achieve current sharing for all time intervals (communication and attack intervals) under the triggering condition (9) and the overall microgrid (22) is stable if there exist symmetric positive-definite matrices $R \in \mathbb{R}^{N\times N}$ and $P \in \mathbb{R}^{N\times N}$, a positive definite diagonal matrix $\Sigma \in \mathbb{R}^{N\times N}$, and constants $0 < \eta_1 < 1$ and $0 < \eta_2 < 1$ such that the following LMIs holds:

$$\begin{bmatrix} A'^\top PA' + (\eta_1 - 1)P + \Sigma & -A'^\top PB' \\ -B'^\top PA' & -I + B'^\top PB' \end{bmatrix} < 0, \tag{33}$$

$$(A' + B'M)^\top R(A' + B'M) - R - \eta_2 R < 0 \tag{34}$$

and the cyber attack duration and frequency of the DoS would satisfy:

$$\frac{1}{\lambda_a} + \frac{\Delta' + \log_\Xi \gamma}{\tau_D} \leq \log_\Xi \frac{1}{1-\eta_1}, \tag{35}$$

where $\Xi = \frac{1+\eta_2}{1-\eta_1}$ and $\gamma = \max(\frac{\lambda_{\max}(P)}{\lambda_{\min}(R)}, \frac{\lambda_{\max}(R)}{\lambda_{\min}(P)}, 1)$.

Proof 2: Based on the switching mode approach, two types of Lyapunov functions are considered, namely $S(\tau) = S_\kappa(\tau)$ where $\kappa \in \{a, b\}$. In order to address the switching framework between the communication and cyber attack intervals, it is assumed that in communication intervals there exists a discrete quadratic Lyapunov function $S_a(\tau) = \alpha^\top(\tau)P\alpha(\tau)$ with $P > 0$ and $0 < \eta_1 < 1$ such that the following inequality is satisfied:

$$S_a(\tau+1) - S_a(\tau) \leq -\eta_1 S_a(\tau). \tag{36}$$

Considering the event-triggering condition (11), equation (36) is satisfied if there exists $0 < \eta_1 < 1$ such that the following inequality is satisfied:

$$S_a(\tau+1) + (\eta_1 - 1)S_a(\tau) - e^\top(\tau)e(\tau) + \alpha^\top(\tau)\Sigma\alpha(\tau) < 0. \tag{37}$$

Substituting (22) into (37) and after some algebraic manipulations, the LMI condition (33) is obtained.

In presence of the DoS cyber attack, a quadratic Lyapunov function is considered as $S_b(\tau) = \alpha^\top(\tau)R\alpha(\tau)$ with $R > 0$ such that the following inequality holds:

$$\begin{aligned} S_b(\tau+1) - S_b(\tau) = \alpha^\top(\tau+1)&R\alpha(\tau+1) \\ &- \alpha^\top(\tau)R\alpha(\tau) < \eta_2 S_b(\tau). \end{aligned} \tag{38}$$

where $0 < \eta_2 < 1$. In this interval, the communication is interrupted by hackers and by substituting (32) into (38), the following inequality is obtained:

$$\alpha^\top(\tau)((A' + B'M)^\top R(A' + B'M) - R - \eta_2 R)\alpha(\tau) < 0, \tag{39}$$

which is equal to the LMI condition (34).

In this switching framework, let $S(\tau) = S_{\kappa(\tau)}(\tau)$, $\kappa(t) \in \{a, b\}$ with $S_a(\tau)$ and $S_b(\tau)$ as defined above. Then, it follows from (36) and (38) that:

$$S(\tau) \leq \begin{cases} (1-\eta_1)^{(\tau - h_{z-1} - \Delta_{z-1})} S_a(h_{z-1} + \Delta_{z-1}), \\ \qquad \tau \in [h_{z-1} + \Delta_{z-1} + \Delta', h_z) \\ (1+\eta_2)^{(\tau - h_z)} S_b(h_z), \\ \qquad \tau \in [h_z, h_z + \Delta_z + \Delta'). \end{cases} \tag{40}$$

For $\tau \in [h_{z-1} + \Delta_{z-1} + \Delta', h_z)$, we have:

$$\begin{aligned} S(\tau) &= (1-\eta_1)^{(\tau - h_{z-1} - \Delta_{z-1})} S_a(h_{z-1} + \Delta_{z-1}) \\ &\leq \gamma(1-\eta_1)^{(\tau - h_{z-1} - \Delta_{z-1})} S_b(h_{z-1} + \Delta_{z-1}) \\ &\leq \ldots \\ &\leq \gamma^z (1-\eta_1)^{|\hat{\Pi}_c(\tau_0,\tau)|} (1+\eta_2)^{|\hat{\Pi}_a(\tau_0,\tau)|} S_a(\tau_0). \end{aligned} \tag{41}$$

Note that by considering $S_a(\tau) \leq \frac{\lambda_{\max}(P)}{\lambda_{\min}(R)} S_b(\tau)$ and $S_b(\tau) \leq \frac{\lambda_{\max(R)}}{\lambda_{\min}(P)} S_a(\tau)$, we can conclude that $S_a(\tau) \leq \gamma S_b(\tau)$, and $S_b(\tau) \leq \gamma S_a(\tau)$ where $\gamma = \max(\frac{\lambda_{\max}(P)}{\lambda_{\min}(R)}, \frac{\lambda_{\max}(R)}{\lambda_{\min}(P)}, 1)$.

For $\tau \in [h_z, h_z + \Delta_z + \Delta')$, it follows that:

$$\begin{aligned} S(\tau) &= (1+\eta_2)^{(\tau - h_z)} S_b(h_z) \\ &\leq \gamma(1+\eta_2)^{(\tau - h_z)} S_a(h_z) \\ &\leq \ldots \\ &\leq \gamma^{z+1} (1-\eta_1)^{|\hat{\Pi}_c(\tau_0,\tau)|} (1+\eta_2)^{|\hat{\Pi}_a(\tau_0,\tau)|} S_a(\tau_0). \end{aligned} \tag{42}$$

According to the cyber attack frequency definition (16), during the time interval $\tau \in (h_{z-1} + \Delta_{z-1}, h_z)$ and $\tau \in [h_z, h_z + \Delta_z + \Delta')$, the total number of DoS cyber attacks is equal to $N_a(\tau_0, \tau) = z$ and $N_a(\tau_0, \tau) = z + 1$, respectively. Hence, equations (41) and (42) could be written as follows:

$$S(\tau) \leq \gamma^{N_a(\tau_0,\tau)} (1-\eta_1)^{|\hat{\Pi}_c(\tau_0,\tau)|} \times (1+\eta_2)^{|\hat{\Pi}_a(\tau_0,\tau)|} S_a(\tau_0). \tag{43}$$

Note that we have $|\hat{\Pi}_c(\tau_0,\tau)| = \tau - \tau_0 - |\hat{\Pi}_a(\tau_0,\tau)|$, $|\hat{\Pi}_a(\tau_0,\tau)| = |\Pi_a(\tau_0,\tau)| + (1+N_a(\tau_0,\tau))\Delta'$ and by substituting these terms into (43), it follows that:

$$\begin{aligned}
S(\tau) &\leq \gamma^{N_a(\tau_0,\tau)}(1-\eta_1)^{(\tau-\tau_0-|\hat{\Pi}_a(\tau_0,\tau)|)} \\
&\quad \times(1+\eta_2)^{|\hat{\Pi}_a(\tau_0,\tau)|}S(\tau_0) \\
&\leq \gamma^{N_a(\tau_0,\tau)}(1-\eta_1)^{(\tau-\tau_0-|\Pi_a(\tau_0,\tau)|-(1+N_a(\tau_0,\tau))\Delta')} \\
&\quad \times(1+\eta_2)^{(|\Pi_a(\tau_0,\tau)|+(1+N_a(\tau_0,\tau))\Delta')}S(\tau_0) \\
&\leq \gamma^{N_a(\tau_0,\tau)}(1-\eta_1)^{(\tau-\tau_0)} \\
&\quad \times(\frac{1+\eta_2}{1-\eta_1})^{(T_0+\frac{\tau-\tau_0}{\lambda_a}+(1+N_a(\tau_0,\tau))\Delta')}S(\tau_0) \\
&\leq (1-\eta_1)^{(\tau-\tau_0)} \\
&\quad \times(\frac{1+\eta_2}{1-\eta_1})^{(T_0+\frac{\tau-\tau_0}{\lambda_a}+(1+N_a(\tau_0,\tau))\Delta'+N_a(\tau_0,\tau)\log_\Xi\gamma)}S(\tau_0) \\
&\leq (\frac{1+\eta_2}{1-\eta_1})^{(T_0+\Delta')} \\
&\quad \times(1-\eta_1)^{(\tau-\tau_0-\frac{\tau-\tau_0}{\lambda_a}-\Delta' N_a(\tau_0,\tau)-N_a(\tau_0,\tau)\log_\Xi\gamma)} \\
&\quad \times(1+\eta_2)^{(\frac{\tau-\tau_0}{\lambda_a}+\Delta' N_a(\tau_0,\tau)+N_a(\tau_0,\tau)\log_\Xi\gamma)}S(\tau_0) \\
&\leq (\frac{1+\eta_2}{1-\eta_1})^{(T_0+\Delta')} \\
&\quad \times(1-\eta_1)^{(\frac{\lambda_a-1}{\lambda_a}(\tau-\tau_0)-(\Delta'+\log_\Xi\gamma)N_a(\tau_0,\tau))} \\
&\quad \times(1+\eta_2)^{(\frac{1}{\lambda_a}(\tau-\tau_0)+(\Delta'+\log_\Xi\gamma)N_a(\tau_0,\tau))}S(\tau_0) \qquad (44)
\end{aligned}$$

Considering (16), inequality (44) can be written as follows:

$$\begin{aligned}
S(\tau) &\leq (\frac{1+\eta_2}{1-\eta_1})^{(T_0+\Delta')} \\
&\quad \times(1-\eta_1)^{(\frac{\lambda_a-1}{\lambda_a}(\tau-\tau_0)-(\Delta'+\log_\Xi\gamma)(\eta_D+\frac{\tau-\tau_0}{\tau_D}))} \\
&\quad \times(1+\eta_2)^{(\frac{1}{\lambda_a}(\tau-\tau_0)+(\Delta'+\log_\Xi\gamma)(\eta_D+\frac{\tau-\tau_0}{\tau_D}))}S(\tau_0) \\
&\leq (\frac{1+\eta_2}{1-\eta_1})^{(T_0+\Delta'+\eta_D(\Delta'+\log_\Xi\gamma))} \\
&\quad \times\Bigg((1-\eta_1)^{(\frac{\lambda_a-1}{\lambda_a}-\frac{\Delta'+\log_\Xi\gamma}{\tau_D})} \\
&\quad \times(1+\eta_2)^{(\frac{1}{\lambda_a}+\frac{\Delta'+\log_\Xi\gamma}{\tau_D})}\Bigg)^{(\tau-\tau_0)}S(\tau_0). \qquad (45)
\end{aligned}$$

It can be concluded from (45) that the overall microgrid (22) is stable and the secure current sharing is achieved if:

$$\begin{aligned}
\lim_{\tau\to\infty} S(\tau) \leq \lim_{\tau\to\infty}\Bigg[&(\frac{1+\eta_2}{1-\eta_1})^{(T_0+\Delta'+\eta_D(\Delta'+\log_\Xi\gamma))} \\
&\times\Bigg((1-\eta_1)^{(\frac{\lambda_a-1}{\lambda_a}-\frac{\Delta'+\log_\Xi\gamma}{\tau_D})} \\
&\times(1+\eta_2)^{(\frac{1}{\lambda_a}+\frac{\Delta'+\log_\Xi\gamma}{\tau_D})}\Bigg)^{(\tau-\tau_0)}S(\tau_0)\Bigg] \to 0. \qquad (46)
\end{aligned}$$

Consequently, (46) is satisfied if we can ensure the following condition:

$$\begin{aligned}
(1-\eta_1)^{(\frac{\lambda_a-1}{\lambda_a}-\frac{\Delta'+\log_\Xi\gamma}{\tau_D})}&(1+\eta_2)^{(\frac{1}{\lambda_a}+\frac{\Delta'+\log_\Xi\gamma}{\tau_D})} < 1 \\
\Longrightarrow (\frac{1+\eta_2}{1-\eta_1})^{(\frac{1}{\lambda_a}+\frac{\Delta'+\log_\Xi\gamma}{\tau_D})} &< \frac{1}{1-\eta_1} \\
\Longrightarrow \frac{1}{\lambda_a}+\frac{\Delta'+\log_\Xi\gamma}{\tau_D} &\leq \log_\Xi\frac{1}{1-\eta_1}. \qquad (47)
\end{aligned}$$

This completes the proof of the theorem.

V. SIMULATION RESULTS

In this section, simulation results are provided to show the efficiency and capabilities of our proposed distributed discrete-time ET consensus-based control for current sharing and voltage stabilization of DC microgrids. A microgrid that is composed of 5 DGUs is considered in Fig. 4. It can be noted in Fig. 4 that the physical and communication graphs are considered as undirected. DGUs scaling factors are set to $I_1^s = 1, I_2^s = 4, I_3^s = 2, I_4^s = 4, I_5^s = 1$, and the voltage reference of the DGUs is set to $V_{\text{ref}} = [40, 50, 48, 42, 46]^\top$. The piece-wise constant load currents of the DGUs 1-5 are depicted in Fig. 5. This figure shows that the current demands of the DGUs, $I_{Li}(t)$, are considered as time-varying piece-wise constant current loads. The electrical parameters of the DGUs and the tie lines parameters are given in Tables 1 and 2 and the primary controller gains are obtained from [10]:

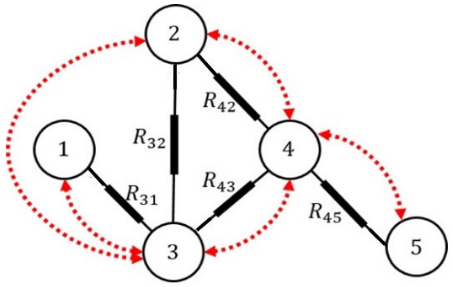

FIGURE 4. Physical topology of the DC microgrid that is composed of 5 DGUs.

TABLE 1. DGUs electrical parameters.

DGU	Resistance $R_t(\Omega)$	Capacitance $C_t(mF)$	Inductance $L_t(mH)$
DGU 1	0.2	2.2	1.8
DGU 2	0.3	1.9	2.0
DGU 3	0.1	1.7	2.2
DGU 4	0.5	2.5	3.0
DGU 5	0.4	2.0	1.3

TABLE 2. Tie lines parameters.

Connected DGUs	Resistance $R_{ij}(\Omega)$	Inductance $L_{ij}(\mu H)$
(1,3)	0.07	2.1
(2,3)	0.04	2.3
(2,4)	0.08	1.8
(3,4)	0.07	1
(4,5)	0.05	2

The sampling period and the secondary discrete-time ET-based controller gains are considered as $h = 0.01$ and

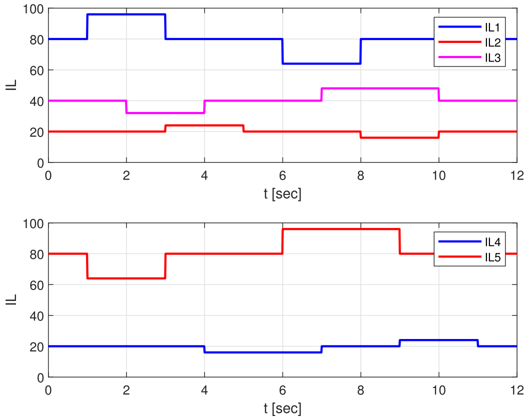

FIGURE 5. The local load currents of the DGUs 1-5.

$K_I = \mathrm{diag}(0.1, 0.1, 0.05, 0.05, 0.1)$, respectively. The matrix σ is obtained by solving the LMI (23) which leads to $\sigma = \mathrm{diag}(0.243, 0.244, 0.243, 0.245, 0.242)$.

Figure 6 shows the performance of the proposed event-triggered control sharing control for voltage regulation, and current sharing, and as shown in this figure, the overall microgrid is stable via primary controllers and the current sharing is achieved by the discrete-time ET consensus-based controller. It is also seen from Figure 6 that the voltage balancing is also achieved and the average PCCs voltages are the identical at the steady state.

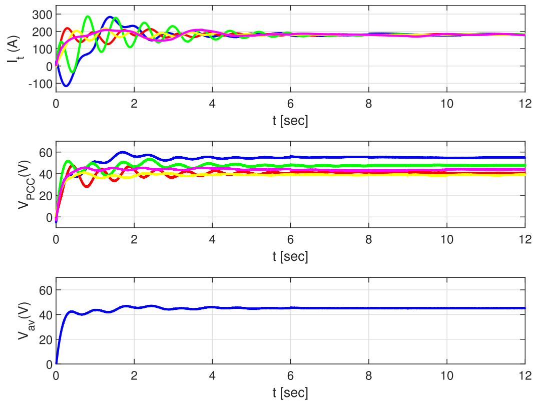

FIGURE 6. The voltage, current, and average PCCs voltage of the DGUs.

The DGUs broadcast currents are shown in Fig. 7. The ability of the event-triggering scheme in adjusting the broadcast periods is demonstrated in this figure. It follows from this figure that the transmission currents do not update continuously and the data exchanges are reduced. The inter-event intervals of the DGU 1, where each stem shows the length of the time period between the event and the previous one are shown in Fig. 8. For example, if the value of a stem in Fig. 8 is 150, it implies that during the past 150 time steps no DGU 1 current data is sent to the network. Moreover, it can be concluded from the simulation results that the currents data transmission rates are reduced by 16.73%, 41.38%, 90.25%, 55.20%, and 38.47% for the DGUs 1 to 5, respectively.

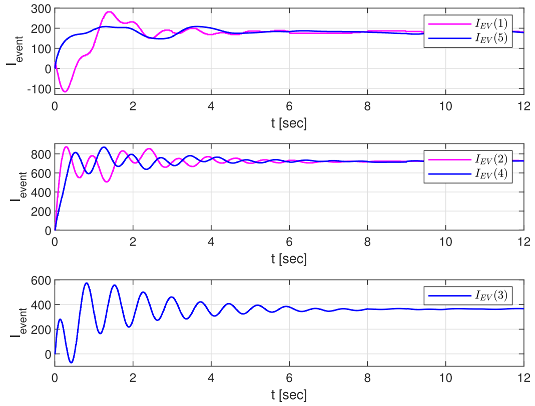

FIGURE 7. The broadcast currents of the DGUs.

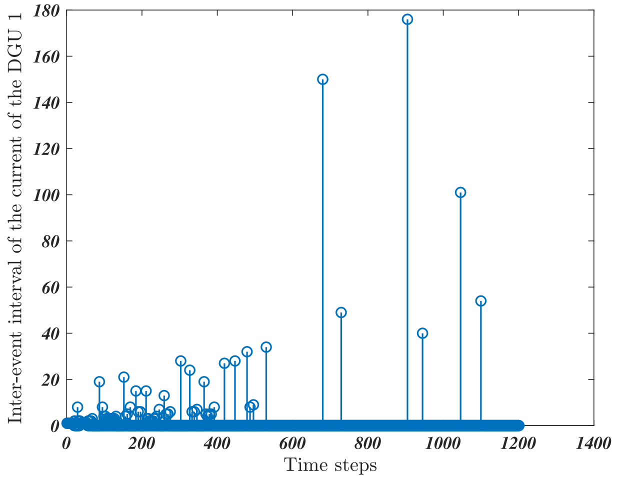

FIGURE 8. The inter-event interval for current of the DGU 1.

In presence of the DoS cyber attack, it is expected that $\eta_D = 0.1$ and $\Delta' = 0.01$. In the time interval including 400 samples (4 seconds), it is assumed that $\tau_D = 20$ where the sampling rate is $h = 0.01$. Consequently, based on the attack frequency definition (16), the total number of DoS *off/on* transitions over $[0, 400)$ satisfies $N_a(0, 400) \leq 0.1 + \frac{400-0}{20} = 20.1$. In order to gain the maximum stability margin we assume that $\eta_1 = 0.99$ and $\eta_2 = 0.01$ by which the LMIs (33) and (34) are satisfied. In this case, in accordance with Theorem 2, the upper bound on the average duration of the DoS cyber attacks is achieved $\frac{1}{\lambda_a} = 0.6$. Consequently, based on (17), the attack duration is obtained as $\Pi_a(0, 400) \leq (400 \times 0.6) = 240$ which implies that in each 400 samples, the maximum tolerable duration of cyber attacks can be 240 samples. In this simulation process, in each 400 samples, the cyber attacks frequency and duration are presumed to be 6 and 170 samples, respectively, which are smaller than the theoretical bounds. The procedure for selecting cyber attacks in the remaining intervals are the same.

According to the DoS characteristics, the grey areas in Fig. 9 depict the sequence of DoS cyber attacks which are

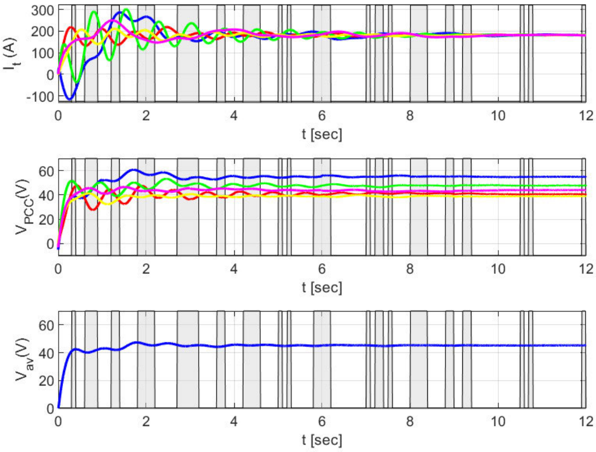

FIGURE 9. The voltage, current, and average PCCs voltage of the DGUs in presence of the DoS cyber attacks corresponding to the tolerable level of DoS attack.

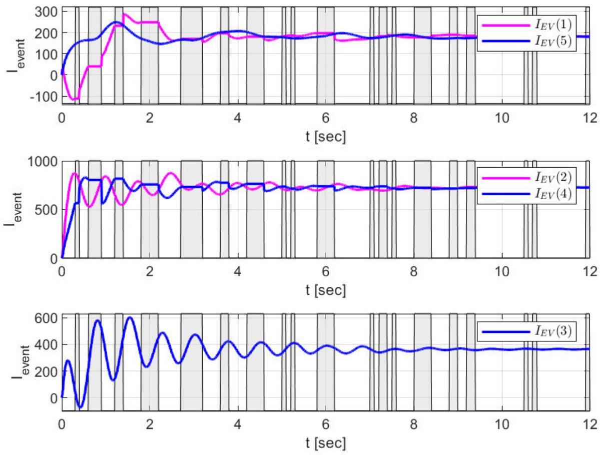

FIGURE 10. Data transmissions of the DGUs in presence of the DoS cyber attacks corresponding to the tolerable level of DoS attack.

injected in the DGUs 1 and 4, as an example. It should be noted that it is not required to have synchronized DoS attacks in different channels and they can be independent. Voltage regulation, current sharing, and average PCCs voltage of the DGUs in presence of the DoS cyber attacks are depicted in Fig. 9. In this figure, it is shown that the overall microgrid is stable and the current sharing is achieved by the proposed discrete-time ET consensus-based controller. The average PCCs voltages are identical at the steady state and the voltage balancing is also achieved. The DGUs broadcast currents in presence of the DoS cyber attacks are shown in Fig. 10. It is concluded from this figure that the event-triggering scheme works well in adjusting the broadcast periods and currents data transmission rates are reduced by 72.19%, 89.34%, 97.58%, 94.5%, and 90% for the DGUs 1 to 5, respectively.

The maximum tolerable DoS cyber attacks in the microgrid is also tested in our case study simulation results. The maximum tolerable duration of cyber attacks was achieved 240 samples in each 400 samples. This duration is increased to be higher than the allowable bound for the DGU 4 as an example. To show the effects of duration of the cyber attacks on the current sharing, 3 attacks with total duration of 270 samples are applied in the DGU 4 in every 400 samples. It can be seen that the overall microgrid is disrupted when duration of cyber attacks does not meet the requirements that are obtained in equation (17). Voltage regulation, current sharing, and average PCCs voltage of DGUs in presence of permissible DoS cyber attacks in the DGU 1 and impermissible DoS cyber attacks in the DGU 4 are depicted in Fig. 11. In this figure, it is shown that the overall microgrid is disturbed and stability of the system can be impaired. Moreover, the average PCCs voltages are not the same at steady state and the voltage balancing requirement is not achieved. The DGUs broadcast currents in presence of the DoS cyber attacks, are shown in Fig. 12. Note that the permissible DoS cyber attacks in the DGU 1 are shown in Fig. 9, and impermissible intervals of the DoS cyber attacks in the DGU 4 are shown in the grey areas in Figures 11 and 12.

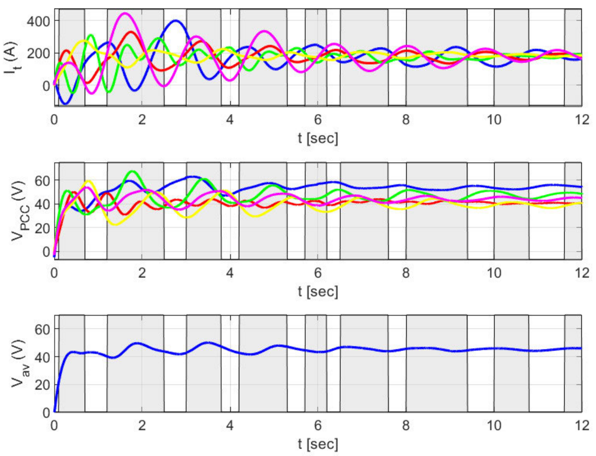

FIGURE 11. The voltage, current, and average PCCs voltage of the DGUs in presence of the impermissible DoS cyber attacks in the DGU 4.

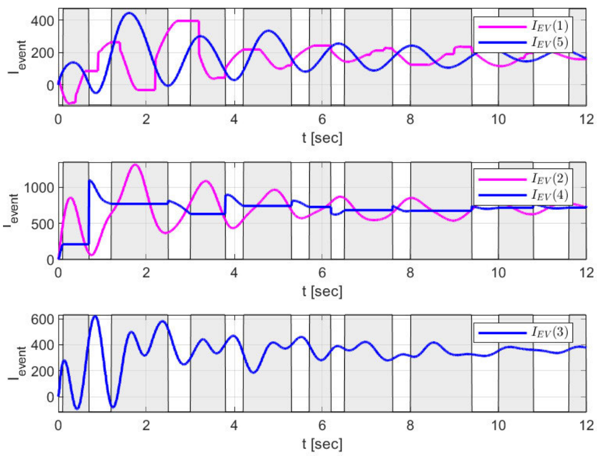

FIGURE 12. Data transmissions of the DGUs in presence of the impermissible DoS cyber attacks in the DGU 4.

Note that the voltage deviation in practical DC power distribution networks should be within 5% of the nominal value. In our proposed ET consensus-based controller for the DC microgrid without the presence of DoS cyber attacks the voltage at the PCC of each DGU remains within this admissible range. For example, the DGU 3 PCC voltage shown in green line in Fig. 6 remains within the range of 48.07±1.44V at steady state, implying that voltage deviations are less than 2.99% of the nominal value $V = 48.07$V. In presence of permissible DoS cyber attacks, the DGU 3 PCC voltage shown in Fig. 9 remains within the range of 48.07 ± 1.94V. This implies that voltage deviations are less than 4% of the nominal value $V = 48.07$V at steady state. However, in presence of impermissible DoS cyber attacks, the DGU 3 PCC voltage shown in Fig. 11 changes in the range of 48.07 ± 7.07V. This implies that voltage deviations are more than 14.7% of the nominal value $V = 48.07$V at steady state and stability of the microgrid has been compromised.

It should be noted that in [43] a nonlinear DC microgrid in presence of intermittent DoS attacks was considered and the DoS frequency and DoS duration were determined to guarantee stability of the system. In our proposed discrete-time event-triggering strategy, the cyber attack duration and frequency of the DoS were specified to ensure not only the stability, but also current sharing of the DC microgrid as depicted in Fig. 9.

VI. CONCLUSION

In this paper, a distributed discrete-time ET consensus-based controller for a DC microgrid that is composed of multiple DGUs is developed. The proposed ET based controller achieves current sharing and reduces the communication rate of the network objectives that would enhance the resiliency of the overall microgrid security and reduce the communication cost. The proposed event-triggered secondary controller is implemented in a discrete-time framework and hence there is no need to consider the Zeno phenomena. Stability of the overall microgrid using this hierarchical control framework is shown quantitatively through Lyapunov stability theory. In presence of the DoS cyber attacks, the overall microgrid is analyzed and sufficient conditions on frequency and duration of DoS cyber attacks are determined in order to reach the secure current sharing. In future work, the problem of secure current sharing in presence of other types of cyber attacks will be investigated.

REFERENCES

[1] R. H. Lasseter and P. Paigi, "Microgrid: A conceptual solution," in *Proc. IEEE 35th Annu. Power Electron. Specialists Conf.*, Jun. 2004, pp. 4285–4291.

[2] J. Schiffer, T. Seel, J. Raisch, and T. Sezi, "Voltage stability and reactive power sharing in inverter-based microgrids with consensus-based distributed voltage control," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 1, pp. 96–109, Jan. 2016.

[3] J. W. Simpson-Porco, F. Dörfler, and F. Bullo, "Voltage stabilization in microgrids via quadratic droop control," *IEEE Trans. Autom. Control*, vol. 62, no. 3, pp. 1239–1253, Mar. 2017.

[4] T. Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC microgrids—Part I: A review of control strategies and stabilization techniques," *IEEE Trans. Power Electron.*, vol. 31, no. 7, pp. 4876–4891, Jul. 2016.

[5] A. T. Elsayed, A. A. Mohamed, and O. A. Mohammed, "DC microgrids and distribution systems: An overview," *Electr. Power Syst. Res.*, vol. 119, pp. 407–417, Feb. 2015.

[6] M. Mola, A. Afshar, N. Meskin, and M. Karrari, "Distributed fast fault detection in DC microgrids," *IEEE Syst. J.*, early access, Nov. 20, 2020, doi: 10.1109/JSYST.2020.3035323.

[7] M. Cucuzzella, S. Trip, C. De Persis, X. Cheng, A. Ferrara, and A. van der Schaft, "A robust consensus algorithm for current sharing and voltage regulation in DC microgrids," *IEEE Trans. Control Syst. Technol.*, vol. 27, no. 4, pp. 1583–1595, Jul. 2019.

[8] S. Trip, M. Cucuzzella, X. Cheng, and J. Scherpen, "Distributed averaging control for voltage regulation and current sharing in DC microgrids," *IEEE Control Syst. Lett.*, vol. 3, no. 1, pp. 174–179, Jan. 2019.

[9] M. Cucuzzella, S. Trip, and J. Scherpen, "A consensus-based controller for DC power networks," *IFAC-PapersOnLine*, vol. 51, no. 33, pp. 205–210, 2018.

[10] M. Tucci, L. Meng, J. Guerrero, and G. Ferrari-Trecate, "Consensus algorithms and plug-and-play control for current sharing in DC microgrids," *ArXiv*, vol. abs/1603.03624, 2016

[11] M. Tucci, S. Riverso, J. C. Vasquez, J. M. Guerrero, and G. Ferrari-Trecate, "A decentralized scalable approach to voltage control of DC islanded microgrids," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 6, pp. 1965–1979, Nov. 2016.

[12] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. De Vicuna, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158–172, Jan. 2011.

[13] L. Meng, T. Dragicevic, J. Roldan-Perez, J. C. Vasquez, and J. M. Guerrero, "Modeling and sensitivity study of consensus algorithm-based distributed hierarchical control for DC microgrids," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1504–1515, May 2016.

[14] J. Zhao and F. Dörfler, "Distributed control and optimization in DC microgrids," *Automatica*, vol. 61, pp. 18–26, Nov. 2015.

[15] M. Andreasson, D. V. Dimarogonas, H. Sandberg, and K. H. Johansson, "Control of MTDC transmission systems under local information," in *Proc. 53rd IEEE Conf. Decis. Control*, Dec. 2014, pp. 1335–1340.

[16] C. De Persis, E. R. A. Weitenberg, and F. Dörfler, "A power consensus algorithm for DC microgrids," *Automatica*, vol. 89, pp. 364–375, Mar. 2018.

[17] P. Prabhakaran, Y. Goyal, and V. Agarwal, "A novel communication-based average voltage regulation scheme for a droop controlled DC microgrid," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1250–1258, Mar. 2019.

[18] J. A. Belk, W. Inam, D. J. Perreault, and K. Turitsyn, "Stability and control of ad hoc DC microgrids," in *Proc. IEEE 55th Conf. Decis. Control (CDC)*, Dec. 2016, pp. 3271–3278.

[19] J. Chen, R. Ling, and D. Zhang, "Distributed non-fragile stabilization of large-scale systems with random controller failure," *Neurocomputing*, vol. 173, pp. 2033–2038, Jan. 2016.

[20] C. Conte, C. N. Jones, M. Morari, and M. N. Zeilinger, "Distributed synthesis and stability of cooperative distributed model predictive control for linear systems," *Automatica*, vol. 69, pp. 117–125, Jul. 2016.

[21] C. Peng, J. Zhang, and H. Yan, "Adaptive event-triggering H_∞ load frequency control for network-based power systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 2, pp. 1685–1694, Jul. 2017.

[22] Y. Batmani, M. Davoodi, and N. Meskin, "Event-triggered suboptimal tracking controller design for a class of nonlinear discrete-time systems," *IEEE Trans. Ind. Electron.*, vol. 64, no. 10, pp. 8079–8087, Oct. 2017.

[23] X. Zheng, H. Zhang, and H. Yan, "Distributed H_∞ filtering for active semi-vehicle suspension systems through network with limited capacity," in *Proc. 35th Chin. Control Conf. (CCC)*, Jul. 2016, pp. 7352–7357.

[24] Z.-G. Wu, Y. Xu, R. Lu, Y. Wu, and T. Huang, "Event-triggered control for consensus of multiagent systems with fixed/switching topologies," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 10, pp. 1736–1746, Oct. 2018.

[25] Z. Gu, P. Shi, and D. Yue, "An adaptive event-triggering scheme for networked interconnected control system with stochastic uncertainty," *Int. J. Robust Nonlinear Control*, vol. 27, no. 2, pp. 236–251, Jan. 2017.

[26] M. Davoodi, N. Meskin, and K. Khorasani, "Event-triggered multiobjective control and fault diagnosis: A unified framework," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 298–311, Feb. 2017.

[27] S. Yan, S. K. Nguang, and Z. Gu, "H_∞ weighted integral event-triggered synchronization of neural networks with mixed delays," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2365–2375, Jun. 2020.

[28] T. Shi, T. Tang, and J. Bai, "Distributed event-triggered control co-design for large-scale systems via static output feedback," *J. Franklin Inst.*, vol. 356, no. 17, pp. 10393–10404, Nov. 2019.

[29] D. Pullaguram, S. Mishra, and N. Senroy, "Event-triggered communication based distributed control scheme for DC microgrid," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 5583–5593, Sep. 2018.

[30] R. Han, L. Meng, J. M. Guerrero, and J. C. Vasquez, "Distributed nonlinear control with event-triggered communication to achieve current-sharing and voltage regulation in DC microgrids," *IEEE Trans. Power Electron.*, vol. 33, no. 7, pp. 6416–6433, Jul. 2018.

[31] B. Fan, J. Peng, Q. Yang, and W. Liu, "Distributed periodic event-triggered algorithm for current sharing and voltage regulation in DC microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 577–589, Jan. 2020.

[32] 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, 2016.

[33] M. Chlela, D. Mascarella, G. Joós, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018.

[34] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. Syst. Secur.*, vol. 14, no. 1, p. 13, 2011.

[35] 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.

[36] 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.

[37] Y. Shen, M. Fei, and D. Du, "Cyber security study for power systems under denial of service attacks," *Trans. Inst. Meas. Control*, vol. 41, no. 6, pp. 1600–1614, Apr. 2019.

[38] Y. Shen, M. Fei, D. Du, W. Zhang, S. Stanković, and A. Rakić, "Cyber security against denial of service of attacks on load frequency control of multi-area power systems," in *Advanced Computational Methods in Energy, Power, Electric Vehicles, and Their Integration*. Singapore: Springer, 2017, pp. 439–449.

[39] H. Sun, C. Peng, W. Zhang, T. Yang, and Z. Wang, "Security-based resilient event-triggered control of networked control systems under denial of service attacks," *J. Franklin Inst.*, vol. 356, no. 17, pp. 10277–10295, Nov. 2019.

[40] L. Zhang, S. K. Nguang, and S. Yan, "Event-triggered H_∞ control for networked control systems under denial-of-service attacks," *Trans. Inst. Meas. Control*, vol. 43, no. 5, pp. 1077–1087, 2021.

[41] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "SINR-based DoS attack on remote state estimation: A game-theoretic approach," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 3, pp. 632–642, Sep. 2017.

[42] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3800–3815, Sep. 2020.

[43] 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 Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 2, pp. 699–710, Feb. 2020.

[44] B. Wang, Q. Sun, and D. Ma, "A periodic event-triggering reactive power sharing control in an islanded microgrid considering DoS attacks," in *Proc. 15th IEEE Conf. Ind. Electron. Appl. (ICIEA)*, Nov. 2020, pp. 170–175.

[45] M. Tucci, L. Meng, J. M. Guerrero, and G. Ferrari-Trecate, "Stable current sharing and voltage balancing in DC microgrids: A consensus-based secondary control layer," *Automatica*, vol. 95, pp. 1–13, Sep. 2018.

[46] M. Tucci, S. Riverso, J. C. Vasquez, J. M. Guerrero, and G. Ferrari-Trecate, "Voltage control of DC islanded microgrids: A decentralized scalable approach," in *Proc. 54th IEEE Conf. Decis. Control (CDC)*, Dec. 2015, pp. 3149–3154.

[47] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

[48] Z. Feng, G. Wen, and G. Hu, "Distributed secure coordinated control for multiagent systems under strategic attacks," *IEEE Trans. Cybern.*, vol. 47, no. 5, pp. 1273–1284, May 2017.

[49] Y. Xu, M. Fang, Z.-G. Wu, Y.-J. Pan, M. Chadli, and T. Huang, "Input-based event-triggering consensus of multiagent systems under denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 4, pp. 1455–1464, Apr. 2020.

MINA MOLA received the B.Sc. degree from the Shiraz University of Technology, Shiraz, Iran, in 2009, and the M.Sc. degree from the Iran University of Science and Technology, in 2013. From April 2018 to June 2020, she was a Research Assistant with Qatar University. Her research interests include fault diagnosis, large scale systems, power systems, and optimization control.

NADER MESKIN (Senior Member, IEEE) received the B.Sc. degree from the Sharif University of Technology, Tehran, Iran, in 1998, the M.Sc. degree from the University of Tehran, Tehran, in 2001, and the Ph.D. degree in electrical and computer engineering from Concordia University, Montreal, QC, Canada, in 2008. He was a Postdoctoral Fellow with Texas A&M University at Qatar, Doha, Qatar, from January 2010 to December 2010. He is currently an Associate Professor with Qatar University, Doha, and an Adjunct Associate Professor with Concordia University. He has published more than 220 refereed journal and conference papers. His research interests include FDI, multiagent systems, active control for clinical pharmacology, cyber-security of industrial control systems, and linear parameter varying systems.

KHASHAYAR KHORASANI (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical and computer engineering from the University of Illinois at Urbana–Champaign, in 1981, 1982, and 1985, respectively. From 1985 to 1988, he was an Assistant Professor with the University of Michigan at Dearborn. Since 1988, he has been with Concordia University, Montreal, Canada, where he is currently a Professor and the Concordia University Tier I Research Chair with the Department of Electrical and Computer Engineering and Concordia Institute for Aerospace Design and Innovation (CIADI). His main research interests include nonlinear and adaptive control, cyber-physical systems and cyber-security, intelligent and autonomous control of networked unmanned systems, fault diagnosis, isolation and recovery (FDIR), diagnosis, prognosis, and health management (DPHM), satellites, unmanned vehicles, and neural networks/machine learning. He has authored or coauthored over 450 publications in these areas. He has served as an Associate Editor for the IEEE Transactions on Aerospace and Electronic Systems.

AHMED MASSOUD (Senior Member, IEEE) received the B.Sc. (Hons.) and M.Sc. degrees from the Faculty of Engineering, Alexandria University, Alexandria, Egypt, in 1997 and 2000, respectively, and the Ph.D. degree in electrical engineering from Heriot-Watt University, Edinburgh, U.K., in 2004. He is currently a Professor with the Department of Electrical Engineering, College of Engineering, Qatar University. He has published more than 100 journal articles in the fields of power electronics, energy conversion, and power quality. He holds five U.S. patents. His research interests include power electronics, energy conversion, renewable energy, and power quality.