Cyber-Resilient Self-Triggered Distributed Control of Networked Microgrids Against Multi-Layer DoS Attacks

Pudong Ge, *Student Member, IEEE,* Boli Chen, *Member, IEEE* and Fei Teng, *Senior Member, IEEE*

***Abstract*—Networked microgrids with high penetration of distributed generators have ubiquitous remote information exchange, which may be exposed to various cyber security threats. This paper, for the first time, addresses a consensus problem in terms of frequency synchronisation in networked microgrids subject to multi-layer denial of service (DoS) attacks, which could simultaneously affect communication, measurement and control actuation channels. A unified notion of Persistency-of-Data-Flow (PoDF) is proposed to characterise the data unavailability in different information network links, and further quantifies the multi-layer DoS effects on the hierarchical system. With PoDF, we provide a sufficient condition of the DoS attacks under which the consensus can be preserved with the proposed edge-based self-triggered distributed control framework. In addition, to mitigate the conservativeness of offline design against the worst-case attack across all agents, an online self-adaptive scheme of the control parameters is developed to fully utilise the latest available information of all data transmission channels. Finally, the effectiveness of the proposed cyber-resilient self-triggered distributed control is verified by representative case studies.**

***Index Terms*—Resilience, networked microgrids, distributed control, self-triggered networks, denial of service (DoS)**

I. Introduction

THE energy source has been transforming from traditional fossil fuel based power generations to inverter-based renewable energy resources driven by the development of low/zero-carbon societies [1]. Rapidly developing inverter-based distributed energy resources (DERs) gradually dominate power systems [2], [3]. Reconstructing high-DER-penetrated power systems into multi-microgrids, i.e. networked microgrids (MGs) is one of the significant pathways of improving the resilience [4], [5]. However, the integration of increasing DERs (using the concept of networked MGs) has lead to more complicated information flows and tighter cyber-physical fusion [6] between DER devices and information systems in order to support efficient control logic. The large scale integration of distributed DERs restricts the applicability of traditional centralised control methods due to the communication constraints and vulnerability against single-point failure, which drives the rapid development of distributed control methods [7], [8].

Such cyber-physical system has inevitably left multi-MG systems exposed to uncertainties from the physical environment and malicious cyber attacks from cyberspace. One of the most significant cyber-layer issues is known as denial-of-service (DoS) or jamming attacks, which intend to disrupt communication and data exchange among networked MG information systems to deteriorate control and operation performance. Therefore, resilient distributed control has been receiving significant attention in recent years. Various control methods have been proposed to enhance the resilience of cyber-physical MGs against DoS attacks, including time-varying sampling strategies [9]–[11], Lyapunov-based analysis [12]–[14], H_∞ control [15], [16], switched system design [17]–[19] and reinforcement learning [20]. To efficiently manage the information flow, the concept of event-/self-triggered control strategies [21] is developed to enable aperiodic communication, sensing and actuation [22]. With the event-/self-triggered framework, a class of effective DoS countermeasures are designed by constructing suitable triggering mechanisms inferred from Lyapunov arguments [10], [11], [23]–[26]. For instance, the works presented in [10], [11] propose an adaptive sampling mechanism whereby the impact of DoS attacks can be mitigated by increasing the sampling rate under attacks.

Existing literature on DoS attacks can be generalised into two categories: 1) attacks only over neighbouring communication links, 2) attacks over the sensing-communication-actuation chain. The neighbouring communication links admittedly are the most vulnerable to attackers as discussed in [9]–[11], [14], [18], [24], [25]. Ref. [23], though mentioning multi-layer DoS attacks, still focuses on the effects on communication channels. However, the sensing and actuation channels are also worthy of consideration. Some recent works start to investigate the attacks over sensing-communication-actuation chains, by either focusing on the single-layer sensing and actuation channels while ignoring communication channels [12], or simply regarding DoS attack effects on the chains as overdue input updates [13], [16], [17]. In this context, there is still a lack of understanding of the diverse impact of DoS attacks against different layers of the sensing-communication-actuation chain in a hierarchical control framework of power systems.

In fact, a hierarchical control framework adopted by networked MGs relies on more complex information network. On this occasion, each DG involves remote (e.g., telemetered)

This work was supported by EPSRC under Grant EP/W028662/1 and by The Royal Society under Grant RGS/R1/211256. (Corresponding author: Dr Fei Teng (f.teng@imperial.ac.uk)).

Pudong Ge and Fei Teng are with the Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2AZ, U.K. (pudong.ge19@imperial.ac.uk; f.teng@imperial.ac.uk)

Boli Chen is with the Department of Electronic and Electrical Engineering, University College London, London WC1E 6BT, U.K. (boli.chen@ucl.ac.uk)

sensing and control actuation with its MG centre controller (MGCC). Hence, cyber attacks could simultaneously occur on communication links for inter-MG data sharing, measurement and actuation channels for intra-MG aggregation and distribution respectively. In particular, the adversary can erase the data sent to actuators or to block the sensor measurement. This motivates the resilience enhancement against multi-layer DoS for networked MGs within a hierarchical control framework. In this context, this paper proposes a novel scheme that, for the first time, addresses multi-layer DoS attacks targeting the neighbouring communication, sensor measurement and control actuation channels of networked MGs with hierarchically controlled DERs. The main contributions are summarized as follows:

1) To characterise multi-layer DoS attacks within different data flow channels among networked MGs, we propose a unified notion of Persistency-of-Data-Flow (PoDF). The notion PoDF is of significance in evaluating the effects of multi-layer DoS attacks.
2) With an edge-based control logic, the proposed self-triggered ternary controller enables asynchronous data collection and processing for each MG from all its neighbours as opposed to existing methods in that relays on synchronous communication. This remarkable feature of asynchronous data collection and processing turns out to be of major significance to ensure consensus properties in the presence of multi-layer DoS attacks.
3) An adaptive scheme of the control and communication policies is devised by utilising timestamps of successful information exchange attempts in different information network links. As such, the conservativeness of the edge-based self-triggered control designed from a global perspective can be significantly reduced.

The remainder of this paper is organized as follows. In Section II, the cyber-physical model of networked MGs and the self-triggered consensus concept are provided. Section III introduces the adaptive distributed self-triggered consensus controller with reduced conservativeness that is proved to be resilient against multi-layer DoS attacks. Simulation results are presented in Section IV and Section V concludes this paper.

II. Preliminaries and Problem Formulation

A. Problem Statement

The networked MGs discussed in this paper are controlled under a hierarchical framework, as shown in Fig. 1, where each MG employs one central coordinator called MGCC to aggregate the measured information and to distribute the calculated commands. In each MG shown in Fig. 1(a), one MGCC manages all dispatchable DERs and aggregates their operational states. Each MGCC exchanges its own aggregated state information with other neighbouring MGCCs through a distributed communication network, to enable distributed coordination, as depicted in Fig. 1(b).

The basic idea of such a hierarchical framework is to aggregate DGs, with small capacities but in large quantities inside one MG to support system operation. Such a hierarchical framework [27] avoids a curse of dimensionality within a fully centralised control, while modularized distributed control avoids the large-scale complex communication network of a fully distributed framework.

To effectively regulate each MG, an aggregated dynamic model can be built through some equivalent methods [4], [28], [29], even if there exist nodes without DGs (refer to [30]). To summarise, consider a droop-controlled equivalent modelling, for each MG i, we have the equivalent parameters

$$m_{Pi} = \frac{1}{\sum_{j\in\mathcal{C}_i}\frac{1}{m_i^{Pj}}},\ \omega_i = \frac{\sum_{j\in\mathcal{C}_i}\frac{\omega_i^j}{\omega_c m_i^{Pj}}}{\sum_{j\in\mathcal{C}_i}\frac{1}{\omega_c m_i^{Pj}}} \tag{1}$$

where $\mathcal{C}_i$ contains all DGs of MG i. In MG i, m_i^{Pj}, ω_i^j denote the frequency droop coefficient and angular frequency of DG j, and m_{Pi}, ω_i are respectively the equivalent frequency droop coefficient and the equivalent angular frequency of MG i (similar to the concept of the Center of Inertia). ω_c denotes the cut-off frequency of low-pass filter in the inverter control loop.

The objective is to enable each MG to participate frequency synchronisation using

$$\omega_{ni} = \omega_i + m_{Pi}P_i \tag{2}$$

where ω_{ni} is the nominal set point for frequency regulation; P_i is the summation of active power output of the ith MG.

The primary control through (2) can not eliminate the frequency deviations from the reference, and the secondary control is employed to achieve frequency synchronisation and accurate active power sharing, i.e.,

$$\lim_{t\to\infty}|\omega_i-\omega_j|=0,\ \lim_{t\to\infty}\omega_i=\omega_{\text{ref}} \tag{3}$$

$$\lim_{t\to\infty}\left|\frac{P_i}{P_{\max,i}}-\frac{P_j}{P_{\max,j}}\right|=0 \tag{4}$$

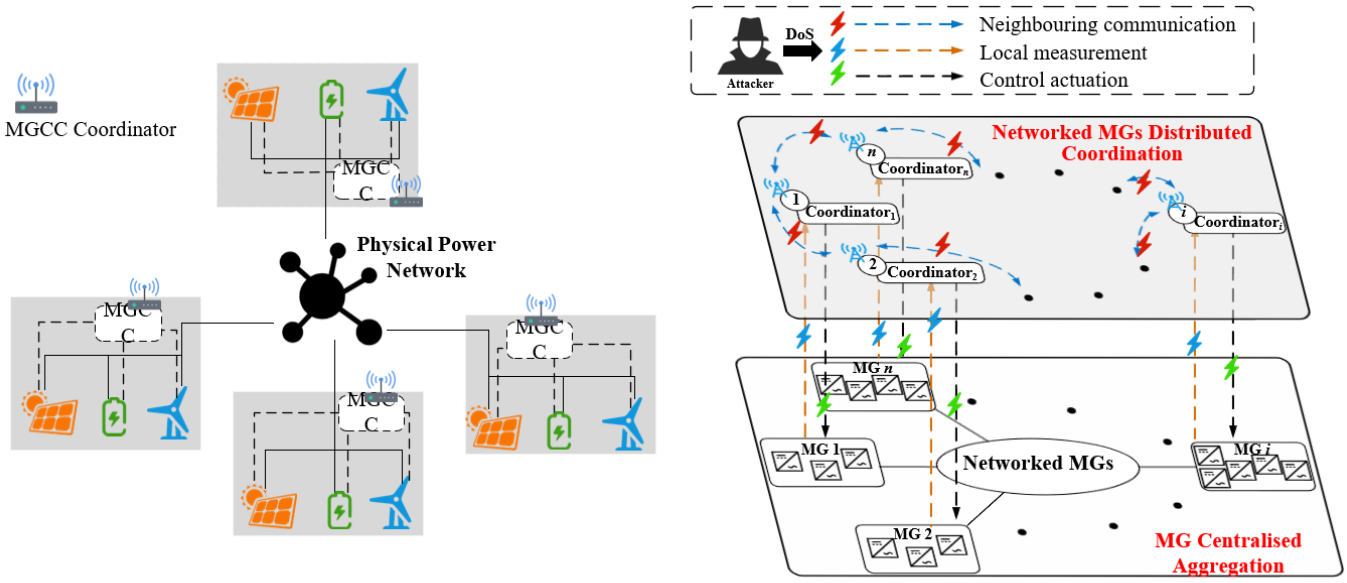
where $P_{\max,i}$ denotes the active power ratings of the ith generator, and (4) is equivalent to $\lim_{t\to\infty}|m_{Pi}P_i - m_{Pj}P_j| = 0$ by approximately setting frequency droop coefficients.

To formulate the control problem, we differentiate (2) and choose the changing rates of frequency and active power output as control variables $\dot{\omega}_{ni} = \dot{\omega}_i + m_{Pi}\dot{P}_i = u_{\omega i} + u_{Pi}$ with $u_{\omega i}, u_{Pi}$ being the auxiliary control inputs that have been widely utilised in [31], [32]. Such that, we can obtain

$$\dot{\boldsymbol{x}}_\omega = \boldsymbol{u}_\omega, \dot{\boldsymbol{x}}_P = \boldsymbol{u}_P \tag{5}$$

where $\boldsymbol{x}_\omega = [\omega_1,\ldots,\omega_n]^\top$, $\boldsymbol{x}_P = [m_{P1}P_1,\ldots,m_{Pn}P_n]^\top$, $\boldsymbol{u}_\omega = [u_{\omega 1},\ldots,u_{\omega n}]^\top$ and $\boldsymbol{u}_P = [u_{P1},\ldots,u_{Pn}]^\top$. Owing to the similar formulation of modelling (5) for frequency and active power, we hereafter omit the subscript ω, P, i.e., $x_i := \omega_i$ or $x_i := m_{Pi}P_i$, to design the control algorithm that can be applied to both frequency regulation and active power sharing.

The communication topology of networked MGs can be modelled by an undirected graph $\mathcal{G} = \{\mathcal{I}, \mathcal{E}\}$, where $\mathcal{I} = \{1, 2, \ldots, m\}$ is a set of MGs, $\mathcal{E} \subseteq \mathcal{I}\times\mathcal{I}$ is a set of edges, and m is the number of MGs. An edge (j, i) means that the ith MG can receive information from the jth MG and j is a neighbour of i. The set of neighbours of MG i is described by $\mathcal{N}_i = \{j : (j, i) \in \mathcal{E}\}$ with $d_i = |\mathcal{N}_i|$ denoting the cardinality of $\mathcal{N}_i$. The corresponding adjacency matrix



(a) Physical Layout of Networked MGs

(b) Hierarchical Framework of Cyber-Physical Networked MGs

Fig. 1. Hierarchically controlled networked MGs.

$\mathcal{A} = [a_{ij}] \in \mathbb{R}^{m\times m}$ is formed by $a_{ii} = 0$; $a_{ij} > 0$ if $(j,i) \in \mathcal{E}$, otherwise $a_{ij} = 0$. The communication topology is denoted by the matrix $\mathcal{A}$, which is assumed to be connected to guarantee the consensus performance [33].

As shown in Fig. 1, different channels, i.e., measurement, communication and actuation are vulnerable to cyberattacks due to the hierarchical structure. In this paper, we consider data unavailability issues affecting all channels. Under multi-layer DoS attacks, the frequency synchronisation problem based on dynamics (5) becomes: *how to design efficient control laws to update input vectors* $\boldsymbol{u}_\omega, \boldsymbol{u}_P$ *to reach both* (3) *and* (4) *under DoS attacks?*

B. Preliminary of Distributed Ternary Control

System (5) can be recast in the form of (6), which has been addressed in the literature by a distributed ternary control mechanism. Some basic concepts concerning the ternary control are presented below with more detailed discussion in [25] and [26]. The system is formed by a triplet of n-dimensional variables $(x,u,\theta) \in \mathbb{R}^n \times \mathbb{R}^d \times \mathbb{R}^d$, where x,u,θ are the vectors of node states, controls and clock variables respectively. u,θ are both edge-based variables with $d := \sum_{i=1}^n d_i$ defined in Section II-A. The system dynamics of distributed ternary control are governed by:

$$\dot{x}_i = u_i = \sum_{j\in\mathcal{N}_i} u_{ij} \tag{6}$$

$$\begin{cases} x_i(t) = x_i(t^-) \quad \forall i \in \mathcal{I} \\ u_{ij}(t) = \begin{cases} \operatorname{sign}_\varepsilon\left(D_{ij}(t)\right), & \text{if } (i,j) \in \mathcal{J}(\theta,t) \\ u_{ij}(t^-), & \text{otherwise} \end{cases} \\ \theta_{ij}(t) = \begin{cases} f_{ij}\left(x(t)\right), & \text{if } (i,j) \in \mathcal{J}(\theta,t) \\ \theta_{ij}(t^-), & \text{otherwise} \end{cases} \end{cases} \tag{7}$$

where $i \in \mathcal{I}$, $j \in \mathcal{N}_i$. The control input u_i aggregates contributions of all edges $(j,i) \in \mathcal{E}$, and u_{ij} represents the control action on node i of the communication link from node j to node i. Through (7), u_{ij}, θ_{ij} are updated only when the clock variable θ_{ij} reaches zero, i.e., $(i,j) \in \mathcal{J}(\theta,t) = \{(i,j) : j \in \mathcal{N}_i \wedge \theta_{ij}(t^-) = 0\}$ where $\theta_{ij}(t^-) = \lim_{\tau\to t}\theta_{ij}(\tau)$. Specifically,

$$\begin{aligned} f_{ij}\left(x(t)\right) &= \max\left\{\frac{|D_{ij}(t)|}{2(d_i+d_j)}, \frac{\varepsilon}{2(d_i+d_j)}\right\} \\ D_{ij}(t) &= x_j(t) - x_i(t) \\ \operatorname{sign}_\varepsilon(z) &:= \begin{cases} \operatorname{sign}(z), & \text{if } |z| \geq \varepsilon \\ 0, & \text{otherwise} \end{cases} \end{aligned} \tag{8}$$

with $\varepsilon > 0$, a user designed sensitivity parameter (consensus error bound); $u_{ij} \in \{-1, 0, 1\}$ from a quantiser $\operatorname{sign}_\varepsilon(z)$.

III. Resilient Frequency Regulation of MGs Against Multi-Layer DoS Attacks

In this section, we design a DoS-resilient control strategy for global consensus to mitigate the joint impacts of multi-layer DoS attacks in the networked MGs frequency control. We firstly model the multi-layer DoS attacks and analyse the effects on the data flow serving for the frequency regulation. Inspired by the concept of self-triggered control, the adaptive distributed self-triggered control is proposed, and its consensus stability and convergence time are theoretically analysed. Before proposing the DoS-resilient control, we give a comprehensive modelling of multi-layer DoS attacks.

A. Denial-of-Service Attacks Modelling

To model DoS attacks, $\Xi(t_1,t_2)$ and $\Theta(t_1,t_2)$ are respectively defined as the under-attack and healthy subsets of the time interval $[t_1,t_2)$. By $n(t_1,t_2)$ denoting the incidence of

DoS inactive/active transitions within the time interval $[t_1, t_2)$, the following assumption are introduced [23], [25], where a more comprehensive information on DoS frequency and duration is provided.

Assumption 1 (DoS Frequency and Duration): There exist $\eta \in \mathbb{R}_{\geq 0}, \kappa \in \mathbb{R}_{\geq 0}$ and $\tau^f \in \mathbb{R}_{\geq 0}, \tau^d \in \mathbb{R}_{\geq 0}$ such that

$$\text{Frequency}: \quad n(t_1, t_2) \leq \eta + \frac{t_2 - t_1}{\tau^f}, \tag{9}$$

$$\text{Duration}: \quad |\Xi(t_1, t_2)| \leq \kappa + \frac{t_2 - t_1}{\tau^d}. \tag{10}$$

To model multi-layer DoS attacks in a unified form, the Persistency-of-Communication (PoC) in [25] is generalized and extended to a notion of PoDF owing to the independence of DoS on diverse channels of data transmission.

Proposition 1 (Persistency-of-Data-Flow (PoDF)): For any transmission channel $\mu \in \{\mathcal{I} \cup \mathcal{E}\}$[1] serving for the distributed control, if multi-layer DoS sequences satisfy Assumption 1 respectively with coefficients τ_μ^f, τ_μ^d, such that $\phi_\mu(\tau_\mu^f, \tau_\mu^d, \Delta_\mu^*) := \frac{1}{\tau_\mu^d} + \frac{\Delta_\mu^*}{\tau_\mu^f} < 1$, where $\Delta_\mu^* := \min \Delta_\mu$. Then, for any unsuccessful data transmission attempt t_μ^k, at least one successful transmission occurs within the time interval $[t_\mu^k, t_\mu^k + \Phi_\mu]$ with $\Phi_\mu := \frac{\kappa_\mu + (\eta_\mu + 1)\Delta_\mu^*}{1 - \phi_\mu(\tau_\mu^f, \tau_\mu^d, \Delta_\mu^*)}$.

Proof: The proof is similar to that in the Appendix A of [25], thus omitted here. ∎

Proposition 1 describes the impact of multi-layer DoS attacks on each data flow channel. Δ_μ^* denotes the minimum time interval between two sequential attempts of data flow, which is different for the three different types of data transmissions. In practice, Δ_μ^* can be known a priori, though conservatively, based on the specification of the system. More specifically, $\Delta_i^*, \Delta_{i0}^*$ depend on the performance of each MGCC, while Δ_{ij}^* is determined by (13), which is introduced later.

Assumption 2: Assuming that both local-level DoS attacks (measurement and control actuation DoS) occur with similar chance, which is less frequent than that on the neighbouring communication channels, such that $\tau_i^f \approx \tau_{i0}^f, \tau_i^d \approx \tau_{i0}^d \Longrightarrow \Phi_i \approx \Phi_{i0}$ and $\Phi_i \leq \Phi_{ij}, \Phi_{i0} \leq \Phi_{ij}$ according to the definition in Proposition 1 and its footnotes.

B. DoS Resilient Consensus Control Algorithm

The distributed control protocol (6)–(8) is based on the hypothesis that the MGCC has access to both local state $x_i(t)$ and neighbouring state $x_j(t)$ at the triggering time, and therefore not valid for multi-layer DoS attacks. To ensure the cyber-resilient consensus in such a scenario, we design an adaptive self-triggered control protocol to achieve resilience under multi-layer DoS attacks (the corresponding stability criteria will be discussed later in Section III-C and Section III-D). The nominal discrete transition (7) is modified as follows:

$$\begin{cases} x_i(t) = x_i(t^-) \quad \forall i \in \mathcal{I} \\ u_{ij}(t) = \begin{cases} \text{sign}_\varepsilon\left(D_{ij}(\bar{t})\right), & (i,j) \in \mathcal{J}(\theta,t) \wedge t \in \Theta_{ij}(0,t) \\ 0, & (i,j) \in \mathcal{J}(\theta,t) \wedge t \in \Xi_{ij}(0,t) \\ u_{ij}(t^-), & \text{otherwise} \end{cases} \\ \theta_{ij}(t) = \begin{cases} f_{ij}\left(x(\bar{t})\right), & (i,j) \in \mathcal{J}(\theta,t) \wedge t \in \Theta_{ij}(0,t) \\ \dfrac{\varepsilon_{ij}}{2(d_i + d_j)}, & (i,j) \in \mathcal{J}(\theta,t) \wedge t \in \Xi_{ij}(0,t) \\ \theta_{ij}(t^-), & \text{otherwise} \end{cases} \end{cases} \tag{11}$$

with asynchronous clock rate across all network links $\dot{\theta}_{ij}(t) = -R_{ij}$ and individual sensitivity parameters ε_{ij} satisfying:

$$0 < \varepsilon \leq \varepsilon_{ij}. \tag{12}$$

where ε represents the minimally acceptable consensus error that avoids Zeno-behaviour of all edges. The utilization of R_{ij} and ε_{ij}, for each edge as opposed to the uniform parameters used in the nominal scheme (6)-(8) is a remarkable feature, and it turns out to be useful in the context of consensus performance as will be discussed in Section III-D. The map $f_{ij} : \mathbb{R}^2 \to \mathbb{R}_{>0}$ is defined as $f_{ij}\left(x(\bar{t})\right) = \max\left\{\frac{|D_{ij}(\bar{t})|}{2(d_i+d_j)}, \frac{\varepsilon_{ij}}{2(d_i+d_j)}\right\}$.

Let $\{t_{ij}^k\}_{k \in \mathbb{Z}_{\geq 0}}$ be the sequence of communication-triggering attempt. It is immediate to show that a dwell-time property is ensured between consecutive sequences:

$$\Delta_{ij} := t_{ij}^{k+1} - t_{ij}^k \geq \frac{\varepsilon_{ij}}{2R_{ij}(d_i + d_j)} \geq \frac{\varepsilon}{4R_{ij} d_{\max}} \tag{13}$$

where $d_{\max} = \max_{i \in \mathcal{I}} d_i$. This ensures the adaptive self-triggered control (11) to be Zeno-free. The item $D_{ij}(\bar{t})$ of (11) is designed to mitigate the cooperative impacts of multi-layer DoS, i.e., $D_{ij}(\bar{t}) = x_j(\bar{t}_j) - x_i(\bar{t}_i)$, where "$\bar{t}$" denotes latest time instant when the state is available.

For the sake of further analysis, we define

Definition 1 (Secure Consensus): Given the system (6), a graph $\mathcal{G}$ and a distributed self-triggered resilient consensus controller with edge-based control u_{ij}, the networked systems are said to be consensus under multi-layer DoS attacks if for any initial condition, $x(t)$ converges in finite time to a point belonging to the set by defining $\delta = \varepsilon(n-1)$

$$\{x \in \mathbb{R}^n : |x_i(t) - x_j(t)| < \delta \quad \forall (i,j) \in \mathcal{I} \times \mathcal{I}\}. \tag{14}$$

Remark 1: The consensus error bound of the distributed system δ derives from edges and can be designed appropriately as small as possible to ensure the system consensus performance, i.e., frequency regulation and active power sharing accuracy, just for being Zeno-free.

In the following, the distributed control system stability will be analysed in terms of parameter design, followed by the convergence analysis in line with (14). The network behaviour of the networked system (6), (11)-(13) is analysed in the presence of multi-layer DoS attacks. The analysis is carried out

[1] $\mu := ij$, communication channel $(i,j) \in \mathcal{E} : j \in \mathcal{N}_i$; $\mu := i$, measurement channel of subsystem $i \in \mathcal{I}$; $\mu := i0$, control actuation channel of subsystem $i \in \mathcal{I}$.

in two steps: 1) we assume uniform clock rate and consensus error bound, such that $R_{ij} = R$, $\varepsilon_{ij} = \varepsilon$, $\forall i \in \mathcal{I}$, $j \in \mathcal{N}_i$ and provide the stability condition in a global sense, and 2) with the additional degrees of freedom endowed by ε_{ij} and R_{ij}, we provide less conservative design criteria by which the consensus remains guaranteed.

C. Control Parameter Design and Stability Analysis

After the MGCC i updates the associated input u_{ij} related to its neighbour j by (11), its transmission through the actuation channels could also be blocked due to DoS attacks. To better demonstrate the effects of DoS attacks on the actuation channels, two sequences of time instants for any $(i,j) \in \mathcal{E}$ are defined: $\{t_{ij}^k : k \in \mathbb{N}\}$ and $\{s_{ij}^k : k \in \mathbb{N}\}$. The sequence t_{ij}^k denotes the time instants at which both local and neighbouring states are updated after $(i,j) \in \mathcal{J}(\theta,t)$ satisfies, while the sequence s_{ij}^k denotes the corresponding time instants at which transmission attempts of control actuation from (11) are successful. Then, two sequences have the property of $0 \leq s_{ij}^k - t_{ij}^k \leq \Phi_{i0}$.

Theorem 1: Consider the distributed control system (6), (11) subject to multi-layer DoS attacks. If Assumption 1 and Assumption 2 hold and

$$\varepsilon > 2d_{\max}\Phi_{\mathcal{I}+2\mathcal{I}0}^{\max},\ R > \frac{\varepsilon}{2\left[\varepsilon - 2d_{\max}\Phi_{\mathcal{I}+2\mathcal{I}0}^{\max}\right]} \tag{15}$$

with $\Phi_{\mathcal{I}+2\mathcal{I}0}^{\max} = \Phi_{\mathcal{I}}^{\max} + 2\Phi_{\mathcal{I}0}^{\max}$, $\Phi_{\mathcal{I}}^{\max} = \max_{i\in\mathcal{I}}\Phi_i, \Phi_{\mathcal{I}0}^{\max} = \max_{i\in\mathcal{I}}\Phi_{i0}$, then $x(t)$ reaches consensus in finite time as described in (14).

Proof: Consider any time t, there exists two successive time instants of successful control actuation that satisfy $s_{ij}^k \leq t < s_{ij}^{k+1}$. During the time period $[s_{ij}^k, s_{ij}^{k+1})$, the control input that is updated through (11) at the time instant t_{ij}^k will be applied. For each $(i,j) \in \mathcal{E} : j \in \mathcal{N}_i$, we have the following inequality:

$$t - t_{ij}^k \leq \frac{f_{ij}(x(\bar{t}_{ij}^k))}{R} + 2\Phi_{i0} \tag{16}$$

Then if $D_{ij}(\bar{t}_{ij}^k) \geq \varepsilon$,

$$\begin{aligned} D_{ij}(t) &= x_j(t) - x_i(t) \\ &\overset{(a1)}{\geq} D_{ij}(t_{ij}^k) - (d_i + d_j)(t - t_{ij}^k) \\ &\overset{(a2)}{\geq} D_{ij}(\bar{t}_{ij}^k) - d_i\Phi_i - d_j\Phi_j - (d_i + d_j)(t - t_{ij}^k) \\ &\overset{(a3)}{\geq} D_{ij}(\bar{t}_{ij}^k)(1-\frac{1}{2R}) - d_i(\Phi_i + 2\Phi_{i0}) - d_j(\Phi_j + 2\Phi_{i0}) \end{aligned} \tag{17}$$

where (a1) derives from identifiable neighbours and control inputs, and (a2), (a3) are from Proposition 1 and (16) respectively, then (17) can be expressed as

$$D_{ij}(t) \geq D_{ij}(\bar{t}_{ij}^k)(1 - \frac{1}{2R}) - 2d_{\max}\Phi_{\mathcal{I}+2\mathcal{I}0}^{\max} > 0 \tag{18}$$

If $D_{ij}(\bar{t}_{ij}^k) \leq -\varepsilon$, an analogous inequality holds

$$D_{ij}(t) \leq D_{ij}(\bar{t}_{ij}^k)(1 - \frac{1}{2R}) + 2d_{\max}\Phi_{\mathcal{I}+2\mathcal{I}0}^{\max} < 0 \tag{19}$$

Define error terms as $e_i = x_i - \frac{1}{n}\sum_{i=1}^n x_i$ and $\boldsymbol{e} = [e_i]_{N\times 1}$. Consider a candidate Lyapunov function $V(t) = \frac{1}{2}\boldsymbol{e}^T\boldsymbol{e}$ and define $\mathcal{S} := |D_{ij}(\bar{t}_{ij}^k)| \geq \varepsilon \wedge t_{ij}^k \in \Theta_{ij}(0,t)$, then the derivative of $V(t)$ under the controller (11):

$$\begin{aligned} \dot{V}(t) &= \sum_{i=1}^n e_i\dot{e}_i = \sum_{i=1}^n e_i \sum_{j\in\mathcal{N}_i:\mathcal{S}} \mathrm{sign}_\varepsilon\left(D_{ij}(\bar{t})\right) \\ &= -\frac{1}{2}\sum_{(i,j)\in\mathcal{E}:\mathcal{S}} D_{ij}(t)\mathrm{sign}_\varepsilon\left(D_{ij}(\bar{t})\right) \\ &\leq -\frac{1}{2}\sum_{(i,j)\in\mathcal{E}:\mathcal{S}} \Bigg[\varepsilon\left(1 - \frac{1}{2R}\right) \\ &\qquad - 2d_{\max}(\Phi_{\mathcal{I}}^{\max} + 2\Phi_{\mathcal{I}0}^{\max})\Bigg] \overset{(b)}{<} 0 \end{aligned} \tag{20}$$

where (b) derives by applying (15) in Theorem 1. As a result, (20) shows the convergence of Theorem 1. Thus, *secure consensus* defined in Definition 1 can be reached. ■

Based on the results stated in Theorem 1, the convergence time can be characterised.

Corollary 1 (Convergence Time): Consider $T_\star$ as the convergence time of the distributed control system (6), (11). It holds that

$$T_\star \leq \frac{2\varepsilon(d_{\max} + d_{\min}) + 8Rd_{\max}d_{\min}\Phi_{\mathcal{I}\mathcal{J}+2\mathcal{I}0}^{\max}}{\varepsilon d_{\min}\left[\varepsilon(1 - \frac{1}{2R}) - 2d_{\max}\Phi_{\mathcal{I}+2\mathcal{I}0}^{\max}\right]}V(0) \tag{21}$$

where $\Phi_{\mathcal{I}\mathcal{J}+2\mathcal{I}0}^{\max} = \Phi_{\mathcal{I}\mathcal{J}}^{\max} + 2\Phi_{\mathcal{I}0}^{\max}$, $\Phi_{\mathcal{I}\mathcal{J}}^{\max} = \max_{i\in\mathcal{I},j\in\mathcal{N}_i}\Phi_{ij}$, $d_{\min} = \min_{i\in\mathcal{I}} d_i$.

Proof: Consider the Lyapunov function based stability analysis (20), for any successful communication attempt t_{ij}^k with $|D_{ij}(\bar{t}_{ij}^k)| \geq \varepsilon$, the function V decreases at least with the rate of $\rho := \frac{1}{2}\left[\varepsilon(1 - \frac{1}{2R}) - 2d_{\max}\Phi_{\mathcal{I}+2\mathcal{I}0}^{\max}\right]$ by at least $(\varepsilon/4Rd_{\max})$ units of time (as inferred from (13)) under the enhanced adaptive controller (11).

We consider any $t > 0$ the consensus has not yet been reached and $u_{ij}^\star(t) = 0$, thus the next communication attempt through edge $(i,j) \in \mathcal{E}$ will occur at the following time period $[t, t + \varepsilon/4Rd_{\min}]$. The most conservative scenario is that over this time period $u_{ij}^\star = 0$. Due to the effect of DoS on communication channels, one successful communication attempt will certainly occurs before $(t + \varepsilon/4Rd_{\min} + \Phi_{ij})$ even at the most conservative scenario.

Then, we consider the effect of DoS on control actuation channels. After u_{ij} is updated at t_{ij}^k, the successful control actuation attempt $u_{ij}^\star(s_{ij}^k) = u_{ij}(\bar{t}_{ij}^k)$ occurs at $s_{ij}^k \in \left[t_{ij}^k, t_{ij}^k + \Phi_{i0}\right]$. The time-duration of $u_{ij}^\star(s_{ij}^k)$ contributing to the consensus is determined by the next successful control actuation attempt, which can be defined as $s_{ij}^{k+1} \in \left[t_{ij}^{k+1}, t_{ij}^{k+1} + \Phi_{i0}\right]$. We assume $u_{ij}^\star(s_{ij}^k)$ will be lasting for at least $(\varepsilon/4Rd_{\max} + \Delta t)$ with $0 \leq \Delta t \leq \Phi_{i0}$, thus, we conclude that V decreases by at least $[\rho(\varepsilon/4Rd_{\max} + \Delta t)]$ every $(\Phi_{ij} + \varepsilon/4Rd_{\min} + \varepsilon/4Rd_{\max} + \Delta t)$ units of time. There-

fore, the convergence time

$$\begin{aligned} T_\star &\leq \frac{\varepsilon/4Rd_{\min}+\Phi_{ij}+\Phi_{i0}+\varepsilon/4Rd_{\max}+\Delta t}{\rho(\varepsilon/4Rd_{\max}+\Delta t)}V(0) \\ &\leq \frac{\varepsilon/4Rd_{\min}+\Phi_{ij}+2\Phi_{i0}+\varepsilon/4Rd_{\max}}{\rho\varepsilon/4Rd_{\max}}V(0) \\ &\leq \frac{2\left(\varepsilon/4Rd_{\min}+\varepsilon/4Rd_{\max}+\Phi^{\max}_{\mathcal{IJ}}+2\Phi^{\max}_{\mathcal{I}0}\right)}{\left[\varepsilon(1-\frac{1}{2R})-2d_{\max}(\Phi^{\max}_{\mathcal{I}}+2\Phi^{\max}_{\mathcal{I}0})\right]\varepsilon/4Rd_{\max}}V(0) \\ &= \frac{2\varepsilon(d_{\max}+d_{\min})+8Rd_{\max}d_{\min}(\Phi^{\max}_{\mathcal{IJ}}+2\Phi^{\max}_{\mathcal{I}0})}{\varepsilon d_{\min}\left[\varepsilon(1-\frac{1}{2R})-2d_{\max}(\Phi^{\max}_{\mathcal{I}}+2\Phi^{\max}_{\mathcal{I}0})\right]}V(0) \end{aligned} \tag{22}$$

■

D. Conservativeness Mitigation under DoS Attacks

The global consensus criteria (15) given in Theorem 1, though can be designed offline, are inferred from the global worst case analysis in terms of PoDF (uniform bounds across all the MGCC nodes), thereby being conservative and could lead to degraded consensus accuracy. In this section, under the procedure of DoS resilient control protocol summarised in Algorithm 1, less conservative criteria are derived from a local perspective (Theorem 2) to further improve the control performance.

Theorem 2: Consider the distributed system (6) subject to multi-layer DoS attacks and the edge-based control (11). If each subsystem can individually choose its parameters ε_{ij} and R_{ij}, such that $\forall\, i \in \mathcal{I}, \forall\, j \in \mathcal{N}_i$,

$$\begin{aligned} \varepsilon_{ij} &> d_i(\Phi_i+2\Phi_{i0})+d_j(\Phi_j+2\Phi_{i0}) \\ R_{ij} &> \frac{\varepsilon_{ij}}{2\left[\varepsilon_{ij}-d_i(\Phi_i+2\Phi_{i0})-d_j(\Phi_j+2\Phi_{i0})\right]} \end{aligned} \tag{23}$$

then the global consensus (14) can be guaranteed.

Proof: See Appendix A-A. ■

For the reason that the cyber vulnerability of different links may vary, there exists $\Phi_i \leq \Phi^{\max}_{\mathcal{I}}, \Phi_{i0} \leq \Phi^{\max}_{\mathcal{I}0}, \forall i \in \mathcal{I}$, thus the condition (23) is less conservative than (15). Furthermore, although Proposition 1 gives bounded time interval Φ_μ that can be utilized to design parameters, not every attack attempt leads to the worst data flow block, i.e., the time to achieve a successful data flow would not be Φ_μ all the time. Using the bounds to stabilise the system as Theorem 1 may lead to excessive conservativeness. Therefore, a self-adaptive scheme is utilised to mitigate the conservativeness.

For the controller of each subsystem i, assume the kth communication attempt is successful at t^k_{ij}, we define the following time instants:

$$t^k_{i,i} := t^k_{ij} - \bar{t}^k_i, \quad t^k_{i,j} := t^k_{ij} - \bar{t}^k_j, \quad t^k_{i0} := s^k_{ij} - t^k_{ij} \tag{24}$$

where $t^k_{i,i}, t^k_{i,j}$ are available at t^k_{ij} whereas t^k_{i0} is not know until $t = s^k_{ij}$. To estimate t^k_{i0}, let us consider an unsuccessful control actuation attempt at $\breve{s}_{ij} \in [t^k_{ij}, s^k_{ij})$ and $\hat{t}^k_{i0}$ the estimate of t^k_{i0}. As we know that the next attempt will be made at $\breve{s}_{ij}+\Delta^*_{i0}$, we keep updating $\hat{t}^k_{i0}$ via $\hat{t}^k_{i0} = \breve{s}_{ij}+\Delta^*_{i0}-t^k_{ij}$ until the next successful attempt. As such, there always exists a time instant $\bar{t} < s^k_{ij}$, such that for all $t \in [\bar{t}, s^k_{ij})$, $\hat{t}^k_{i0} = t^k_{i0}$. It implies that t^k_{i0} is known prior to s^k_{ij}.

Algorithm 1: DoS Resilient Distributed Consensus Control

Initialisation: for all $i \in \mathcal{I}$ and $j \in \mathcal{N}_i$, set $\theta_{ij}(0^-) = 0$, $u_{ij}(0^-) = 0$, $u^\star_{ij}(0^-) = 0$;
/* Local State Update from Sensors to Controllers */
foreach $i \in \mathcal{I}$ **do**
  if $t \in \Theta_i(0,t)$ **then**
    i updates $x_i(\bar{t}) = x_i(t)$;
  end
end
/* Edge-Based Control Update in Controllers */
foreach $i \in \mathcal{I}$ **do**
  foreach $j \in \mathcal{N}_i$ **do**
    while $\theta_{ij}(t) > 0$ **do**
      i applies the control $u_i(t) = \sum_{j\in\mathcal{N}_i} u_{ij}(t)$;
    end
    if $\theta_{ij}(t) \leq 0 \wedge t \in \Theta_{ij}(0,t)$ **then**
      i updates $u_{ij}(t) = \mathrm{sign}_\varepsilon(D_{ij}(\bar{t}))$;
      i updates $\theta_{ij}(t) = f_{ij}(x(\bar{t}))$;
    else if $\theta_{ij}(t) \leq 0 \wedge t \in \Xi_{ij}(0,t)$ **then**
      i updates $u_{ij}(t) = 0$;
      i updates $\theta_{ij}(t) = \frac{\varepsilon_{ij}}{2(d_i+d_j)}$;
    end
  end
end
/* Control Actuation */
foreach $i \in \mathcal{I}$ **do**
  if $u_i(t)$ *is updated* $\wedge\ t \in \Theta_{i0}(0,t)$ **then**
    $u^\star_i(t) = u_i(t)$;
  end
end
// **note:** $u_i(t)$ denotes the desired control output, while $u^\star_i(t)$ denotes the actual control input of the subsystem. $u_i(t) = u^\star_i(t)$ if the actuation channel is not attacked.

Proposition 2: For any control actuation during $[s^k_{ij}, s^{k+1}_{ij})$, the following control inputs are equivalent to the system:

$$\begin{aligned} u'_{ij}(t) &= \mathrm{sign}_\varepsilon\left(D_{ij}(\bar{t}^k_{ij})\right)\frac{\vartheta^k_{ij}}{\vartheta^k_{ij}+\Phi_{i0}}, s^k_{ij} \leq t < s^{k+1}_{ij} \\ \Longleftrightarrow u_{ij}(t) &= \begin{cases} \mathrm{sign}_\varepsilon\left(D_{ij}(\bar{t}^k_{ij})\right), & s^k_{ij} \leq t < t^{k*}_{ij} \\ 0, & t^{k*}_{ij} \leq t < s^{k+1}_{ij} \end{cases} \end{aligned} \tag{25}$$

where $\vartheta^k_{ij} = \frac{\theta^k_{ij}}{R^k_{ij}} = \frac{f_{ij}(x(\bar{t}^k_{ij}))}{R^k_{ij}}$ and $s^k_{ij} + \frac{(\vartheta^k_{ij})^2}{\vartheta^k_{ij}+\Phi_{i0}} \leq t^{k*}_{ij} \leq t^{k+1}_{ij}$.

Proof: See Appendix A-B. ■

Although the consensus error bound ε_{ij} guaranteed in Theorem 2 is less conservative than (15), it still relies on the PoDF conditions, which is inevitably conservative. Next, we show that a tighter consensus error bound can be achieved if an online self-adaptation mechanism of ε_{ij} and R_{ij} is permitted after each successful communication attempt.

Corollary 2 (Self-Adaptive Scheme): Consider the distributed system (6) subject to multi-layer DoS attacks and the edge-based control (11) with control input u'_{ij} in Proposition 2, if ε_{ij} and R_{ij} can be adapted after each successful communication attempt, such that

$$\varepsilon_{ij}^k > \Gamma_{ij}^k,\ R_{ij}^k > \frac{\varepsilon_{ij}^k}{2\left[\varepsilon_{ij}^k - \Gamma_{ij}^k\right]} \tag{26}$$

where $\Gamma_{ij}^k = d_i(t_{i,i}^k + t_{i0}^k) + d_j(t_{i,j}^k + t_{i0}^k)$ with $t_{i,i}^k$, t_{i0}^k, $t_{i,j}^k$ defined in (24), then the secure consensus condition (14) can be preserved.

Proof: See Appendix A-C. ■

After the kth successful communication attempt of edge $(i,j) \in \mathcal{E} : j \in \mathcal{N}_i$, Γ_{ij}^k is already known before the control actuation attempt. Then we can choose appropriate $\varepsilon_{ij}^k, R_{ij}^k$ to satisfy (26), and the corresponding clock variable θ_{ij}^k and control variable $u_{ij}^k = u'_{ij}$ can be obtained from (11) and (25) respectively. To make the proposed self-adaptive scheme clear, we summarise it in Algorithm 2.

Remark 2: The conditions shown in (26) are equivalent to $\varepsilon_{ij}^k > \left[1 + \frac{1}{2R_{ij}^k - 1}\right]\Gamma_{ij}^k, R_{ij}^k > 0.5$, which explicitly shows the relationship between two designed parameters. The selection of $\varepsilon_{ij}^k, R_{ij}^k$ is subject to a trade-off between consensus accuracy and computation burden. More specifically, smaller ε_{ij}^k leads to more accurate consensus performance in terms of (12) but requires larger R_{ij}^k, which means more frequent communication between MGCCs. Hence, the parameter selection in practice should consider both the communication capability and accuracy requirement of networked MGs case-by-case.

Algorithm 2: Self-Adaptive Scheme for DoS Resilient Distributed Consensus Control

```
foreach (i, j) ∈ E do
    foreach communication attempt k do
        if attempt is unsuccessful then
            apply (11) and Algorithm 1 to the
              unsuccessful solution;
        else if attempt is successful then
            design ε_ij^k, R_ij^k using (26);
            calculate θ_ij^k as (11) and u_ij^k = u'_ij as (25);
        end
    end
end
```

Remark 3: Under Corollary 2, the adverse effects of multi-layer DoS attacks can be classified as "identifiable" and "non-identifiable" depending on the extent to which the convervativeness of global consensus criteria (15) can be mitigated, as shown in Fig. 2. More specifically, the "identifiable" means those DoS attacks can be noticed before control command calculation by the definition of (24) (e.g., communication and measurement DoS), while the "non-identifiable" means the actuated commands are not updated as desired due to DoS attacks that block the next actuation attempt (e.g., actuation DoS). The "non-identifiable" effects come always with actuation DoS attacks and are mitigated by using Proposition 2, which brings extra conservativeness. Besides the desired effects, such separation of identifiable and non-identifiable effects can effectively avoid the over conservative design using the fully worst scenario owing to intensive DoS attacks are a low-frequency event.

Remark 4: Compared to [23]–[25], the main contributions of the proposed method are: 1) consideration of the multi-layer DoS attacks in all channels of local measurement, neighbouring communication and control actuation, 2) consideration of asynchronous data collection and processing, as major significance, to ensure consensus properties in the presence of multi-layer DoS attacks, 3) the proposed adaptive scheme can significantly reduce the conservativeness involved in the algorithm [25]. These contributions lead to a dedicated resilient control design with rigorous analysis for resilience guarantees. To show the superior of the proposed method, comprehensive comparisons with [23]–[26] will be provided in Section IV-A.

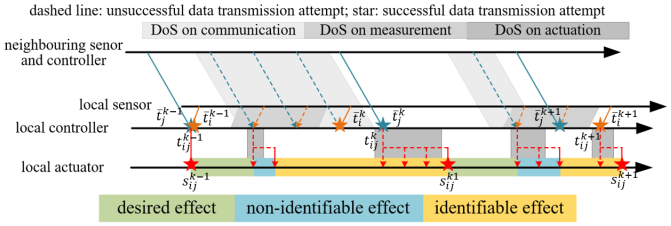


Fig. 2. Sequential control scenarios under multi-layer DoS attacks.

IV. Results

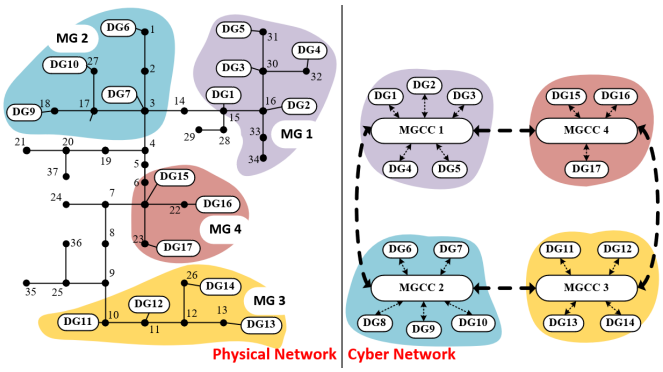
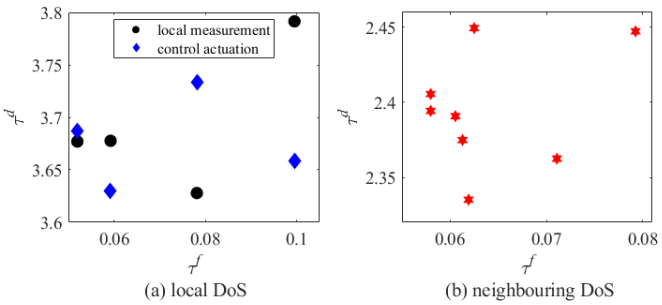


Fig. 3. A networked MGs topology modified by IEEE 37 bus test system.

TABLE I
Power Ratings of DGs

MG 1		MG 2		MG 3		MG 4	
DG 1	20 kW	DG 6	20 kW	DG 11	15 kW	DG 15	10 kW
DG 2	15 kW	DG 7	20 kW	DG 12	20 kW	DG 16	10 kW
DG 3	15 kW	DG 8	15 kW	DG 13	20 kW	DG 17	15 kW
DG 4	15 kW	DG 9	15 kW	DG 14	15 kW		
DG 5	15 kW	DG 10	10 kW				



(a) local DoS (b) neighbouring DoS

Fig. 4. τ^f and τ^d values among networked MGs: (a) measurement and control actuation; (b) neighbouring communication.

To verify the effectiveness of the proposed DoS resilient control of networked MGs, a modified IEEE 37 nodes system [34] with four MGs is established in MATLAB/Simulink as shown in Fig. 3. The network topology follows $\mathcal{A} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$, which satisfies the consensus requirement discussed in Section II-A . Each MG incorporates several inverter-based DGs, the power ratings of which are detailed in Table I. In the simulation, the proposed secondary controller is activated at $t = 5\,\mathrm{s}$, and before only the primary controller is used, which tends to lead to larger frequency synchronous deviations. Furthermore, the load changes (prevalent in the power networks) are introduced at $t = 30\,\mathrm{s}$ and $t = 45\,\mathrm{s}$, respectively. Finally, multi-layer DoS attacks acting on local and neighbouring links of the power network are illustrated in Fig. 4.

A. Validation of the Proposed Method

To show the impact of multi-layer DoS attacks and the performance of the proposed resilient secondary control strategy which is based on Corollary 2, we compare the performance with existing methods [23]–[26]. The results are shown in Fig. 5, where each row corresponds to a typical controller and the three columns (from left to right) indicate the three simulation cases of different DoS attacks. As it can be seen, control performance deteriorates under either neighbouring DoS attacks or local DoS attacks (see (a) to (b)), and the degradation becomes more significant when local DoS attacks are introduced (see (b) to (c)). Considering only the neighbouring-communication-attack can not nullify the effects of local DoS attacks (see (e) to (f)). The resulting undesired oscillations may trigger the power grid protection mechanism, and consequently, lead to large-scale load shedding or power outage. Hence, the resilience against multi-layer DoS attacks is of great significance for enhancing the reliability of the networked MGs. The results presented in the third row (i.e., (g), (h) and (i)) show that system resilience is preserved by the proposed DoS-resilient control method although the multi-layer DoS attacks slow down the frequency convergence speed. Moreover, frequency synchronisation and active power sharing are shown by equivalence inside each MG in Fig. 6, where the accuracy is also guaranteed in a hierarchical framework. Take MG 2 as an example, the active power sharing is kept at all stages by a fixed ratio $4:4:3:3:2$, as specified by their power ratings.

B. Benefits of the Self-Adaptive Scheme

Under the DoS attacks of Fig. 4, we evaluate the performance of the controller designed in line with the global consensus criteria (see Theorem 1), which considers the worst scenario of DoS attacks by PoDF. The results are shown in Fig. 7(a). In contrast to Fig. 5(i) that is obtained using the self-adaptive scheme, the steady state consensus error in Fig. 7(a) is much greater due to the fact that the sensitivity parameter, ε, has to be set to a conservative value $\varepsilon = 1.2624\,(\Phi^{\max}_{\mathcal{I}=\mathcal{I}0} = 0.0526)$ to satisfy the global design criterion Eq. (15). If DoS attacks become less severe and intensive, after re-designing the the sensitivity parameter, the consensus accuracy is improved for both control designs, as can be seen in Fig. 7(b) and Fig. 7(c). However, enhanced consensus accuracy is guaranteed in both cases by the less conservative design criteria given in Corollary 2.

C. Impacts of Attacks in Different Channels

The proposed DoS-resilient control framework gives different mitigation methods for identifiable and non-identifiable DoS attacks as described in Remark 3. In order to evaluate the impacts of both types of attacks and to what extent each attack can be mitigated, we successively decrease the frequency and duration for measurement, communication or actuation DoS attacks based on the original setting given in Fig. 4. The resulting multi-layer DoS attacks are characterised in the first row of Fig. 8. The corresponding performances of each scenario are shown in 2nd and 3rd rows of the same column. As discussed in Remark 3, the mitigation of the non-identifiable attacks is more conservative compare to that of identifiable ones. This is explicitly reflected in Fig. 8, as the extenuation (by frequency and duration reduction) of the actuation attacks (which certainly bring non-identifiable effects) yields the most noticeable improvements in terms of frequency tracking among the three cases (see Scenario 3). In other words, under the proposed resilient self-triggered method based on Corollary 2, a sequence of DoS attack that acts on actuation channels has the most significant impact on the control performance, therefore, it is more beneficial to harden cyber security of actuation channels compared to the other two.

V. Conclusion

In this paper, we propose a DoS resilient distributed self-triggered control method of networked MGs systems. Multi-layer DoS attacks on different channels of data flow are considered: DoS attacks on neighbouring communication, measurement and control actuation channels. The quantitative description of such attacks, named by PoDF is employed to analyse the global stability criteria and convergence time of the consensus evolution. Then, the conservativeness induced by control design in the worst case is overcome by a self-adaptive scheme which classifies effects of DoS attacks into identifiable

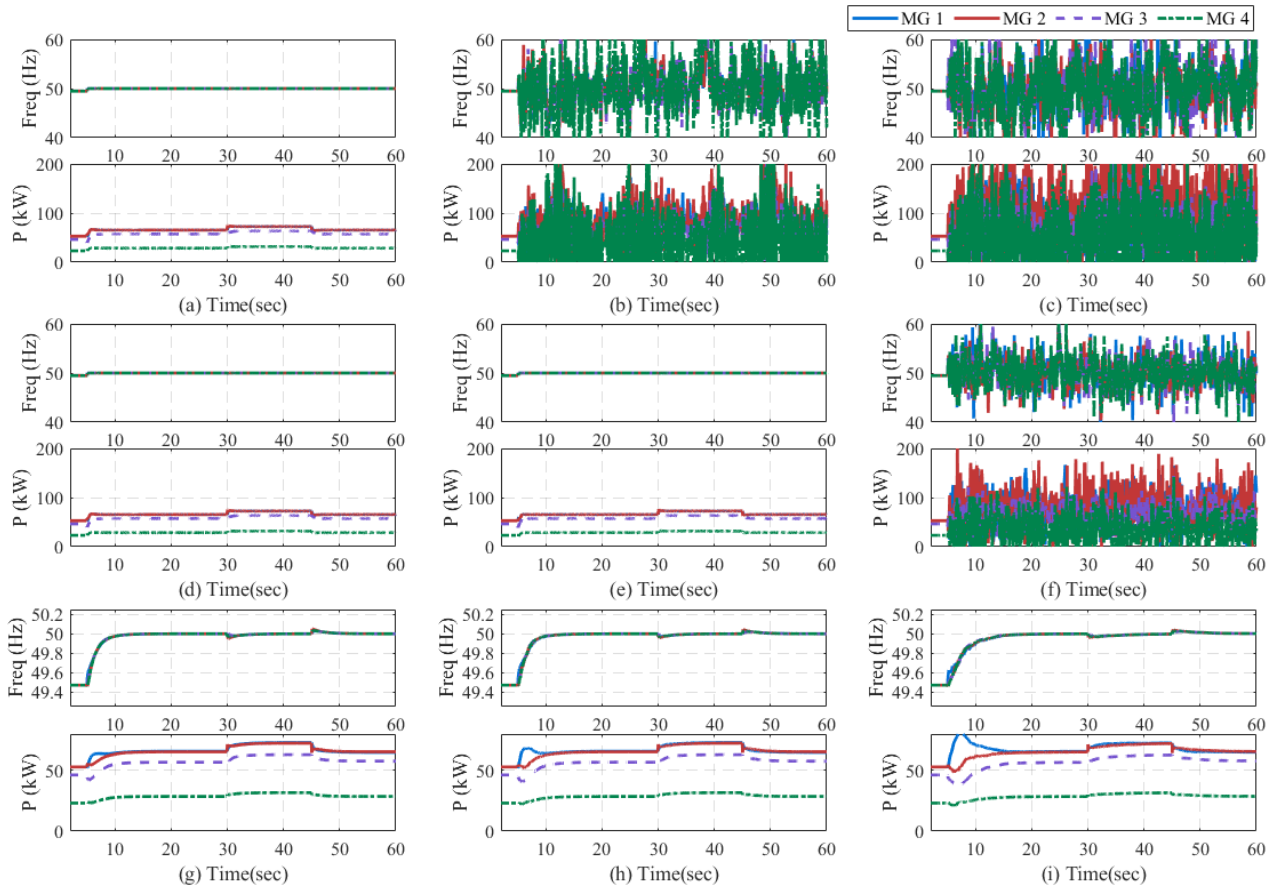


Fig. 5. Performance evaluation of frequency synchronisation and active power sharing. 1st row, i.e., (a), (b), (c) are using (7) designed without considering any DoS attacks [26]; 2nd row, i.e., (d), (e), (f) are using ternary control (7) designed only considering neighbouring DoS attacks [23]–[25]; 3rd row, i.e., (g), (h), (i) are using the proposed resilient control designed considering multi-layer DoS attacks; 1st column, i.e., (a), (d), (g): none DoS attacks exist; 2nd column, i.e., (b), (e), (h): only communication DoS attacks exist; 3rd column, i.e., (c), (f), (i): multi-layer DoS attacks exist.

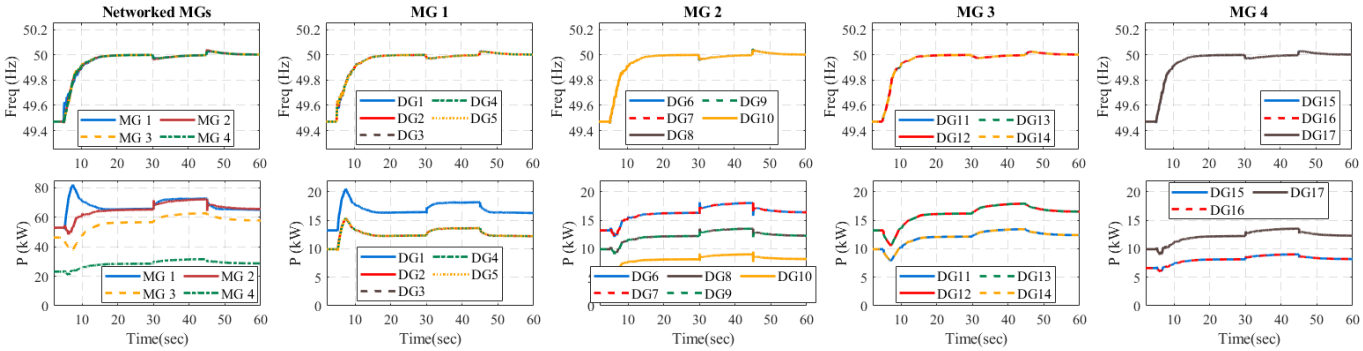


Fig. 6. Frequency synchronisation and active power sharing inside MGs.

and non-identifiable parts. Through simulations conducted by MATLAB/Simulink, the effectiveness of such a multi-layer-DoS resilient strategy is illustrated with separate analysis of DoS attacks on local or neighbouring data transmissions.

In this paper, we assume all channels in information systems vulnerable to DoS attacks. However, in some cases, if the attacker has limited resources, there is an optimisation problem to allocate attack resources to maximise/minimise the consequences, which in turn suggests an optimization problem for the defender to allocate the defence resources, which is, however, out of the scope of this paper and will be discussed in other future works. In addition, this paper only investigates the system dynamics that are modelled by the first-order, and it is interesting to conduct research on more accurately modelled networked MGs. Moreover, cybersecurity issues do not only include DoS, thus deception attacks such as false data injection (FDI) will be considered in the future.

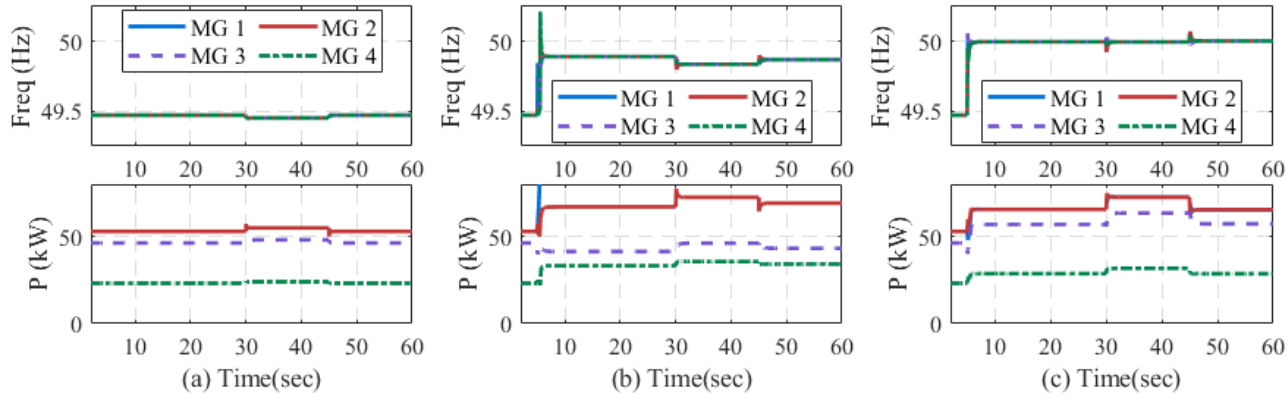


Fig. 7. Conservativeness validation of Theorem 1. (a): intensive DoS attacks using controller satisfying Theorem 1; (b) and (c): less intensive DoS attack using controllers satisfying Theorem 1 and Corollary 2, respectively.

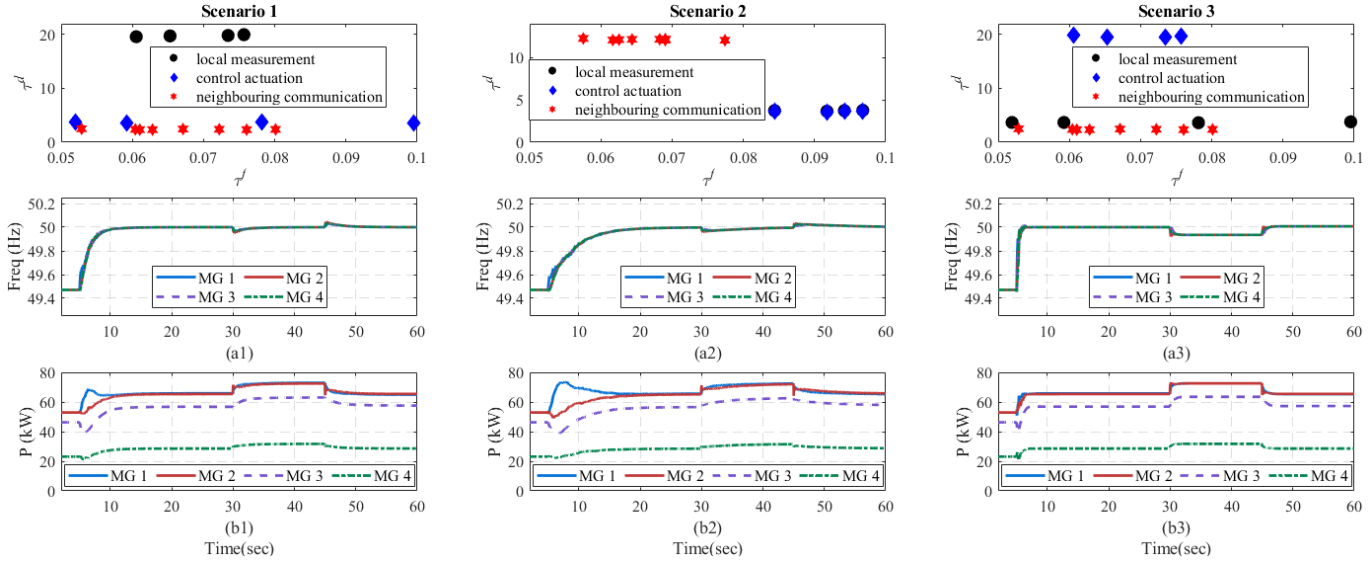


Fig. 8. Performance comparisons with decreased DoS attacks on three type of channels separately: measurement (Scenario 1, 1st column), communication (Scenario 2, 2nd column) and actuation (Scenario 3, 3rd column).

APPENDIX A
PROOF

A. Proof of Theorem 2

Proof: From the proof of Theorem 1, the inequality (18) and (19) can be replaced by

$$\begin{cases} D_{ij}(t) \geq D_{ij}(\bar{t}_{ij}^k)(1-\dfrac{1}{2R_{ij}}) - d_i(\Phi_i+2\Phi_{i0}) \\ \qquad\qquad - d_j(\Phi_j+2\Phi_{i0}),\ \text{if } D_{ij}(\bar{t}_{ij}^k) \geq \varepsilon_{ij} \\ D_{ij}(t) \leq D_{ij}(\bar{t}_{ij}^k)(1-\dfrac{1}{2R_{ij}}) + d_i(\Phi_i+2\Phi_{i0}) \\ \qquad\qquad + d_j(\Phi_j+2\Phi_{i0}),\ \text{if } D_{ij}(\bar{t}_{ij}^k) \leq -\varepsilon_{ij} \end{cases} \tag{27}$$

Then, (20) can be replaced by

$$\dot{V}(t) \leq -\frac{1}{2}\sum_{(i,j)\in\mathcal{E}:\mathcal{S}} \Big[\varepsilon_{ij}(1-\frac{1}{2R_{ij}}) - d_i(\Phi_i+2\Phi_{i0}) - d_j(\Phi_j+2\Phi_{i0})\Big] < 0 \tag{28}$$

which shows the convergence using (23) in Theorem 2. Thus, the secure consensus (14) is achieved. ■

B. Proof of Proposition 2

Proof: By the inequality $s_{ij}^{k+1} - t_{ij}^{k+1} = t_{i0}^{k+1} \leq \Phi_{i0}$ and $t_{ij}^{k+1} - s_{ij}^k = \vartheta_{ij}^k$, if $\text{sign}_\varepsilon\left(D_{ij}(\bar{t}_{ij}^k)\right) = 1 \Rightarrow u'_{ij}(t) > 0, t \in [s_{ij}^k, s_{ij}^{k+1})$,

$$\int_{s_{ij}^k}^{s_{ij}^{k+1}} u'_{ij}(t)dt \leq \int_{s_{ij}^k}^{t_{ij}^{k+1}+\Phi_{i0}} u'_{ij}(t)dt \tag{29}$$

if $\text{sign}_\varepsilon\left(D_{ij}(\bar{t}_{ij}^k)\right) = -1 \Rightarrow u'_{ij}(t) < 0, t \in [s_{ij}^k, s_{ij}^{k+1})$,

$$\int_{s_{ij}^k}^{s_{ij}^{k+1}} u'_{ij}(t)dt \geq \int_{s_{ij}^k}^{t_{ij}^{k+1}+\Phi_{i0}} u'_{ij}(t)dt \tag{30}$$

Combining (29) and (30), the contribution of control actuation during $[s_{ij}^k, s_{ij}^{k+1})$ is limited:

$$\begin{aligned} \int_{s_{ij}^k}^{s_{ij}^{k+1}} \left|u'_{ij}(t)\right| dt &\leq \left|\text{sign}_\varepsilon\left(D_{ij}(\bar{t}_{ij}^k)\right)\right| \vartheta_{ij}^k \\ &= \int_{s_{ij}^k}^{t_{ij}^{k+1}} \left|\text{sign}_\varepsilon\left(D_{ij}(\bar{t}_{ij}^k)\right)\right| dt + \int_{t_{ij}^{k+1}}^{s_{ij}^{k+1}} 0\ dt \end{aligned} \tag{31}$$

Thus, from (31), we can know if u'_{ij} is actuated, it has the equivalent contribution of

$$u_{ij}(t) = \begin{cases} \text{sign}_\varepsilon\left(D_{ij}(\bar{t}_{ij}^k)\right), & s_{ij}^k < t < t_{ij}^{k*} \\ 0, & t_{ij}^{k*} < t < s_{ij}^{k+1} \end{cases}$$

where $s_{ij}^k + \frac{(\vartheta_{ij}^k)^2}{\vartheta_{ij}^k + \Phi_{i0}} \leq t_{ij}^{k*} \leq t_{ij}^{k+1}$. In particular, $t_{ij}^{k*} = s_{ij}^k + \frac{(\vartheta_{ij}^k)^2}{\vartheta_{ij}^k + \Phi_{i0}}$ implies $t_{ij}^{k+1} = s_{ij}^{k+1}$. ■

C. Proof of Corollary 2

Proof: If $D_{ij}(\bar{t}_{ij}^k) \geq \varepsilon_{ij}^k$, (17) in Theorem 1 can be modified as the following

$$\begin{aligned} D_{ij}(t) &\geq D_{ij}(t_{ij}^k) - (d_i + d_j)(t - t_{ij}^k) \\ &\overset{(c)}{\geq} D_{ij}(\bar{t}_{ij}^k) - d_i t_{i,i}^k - d_j t_{i,j}^k - (d_i + d_j)(t_{i0}^k + \vartheta_{ij}^k) - 0 \times \Phi_{i0} \\ &= D_{ij}(\bar{t}_{ij}^k)(1 - \frac{1}{2R_{ij}^k}) - d_i(t_{i,i}^k + t_{i0}^k) - d_j(t_{i,j}^k + t_{i0}^k) \end{aligned}$$

where (c) comes from Proposition 2. Followed by the similar process as (18)-(20), we obtain $\dot{V}(t) < 0$ remains guaranteed with (26). Similarly, secure consensus (14) is achieved. ■

REFERENCES

[1] F. Creutzig, J. C. Goldschmidt, P. Lehmann, E. Schmid, F. von Blücher, C. Breyer, B. Fernandez, M. Jakob, B. Knopf, S. Lohrey *et al.*, "Catching two european birds with one renewable stone: Mitigating climate change and eurozone crisis by an energy transition," *Renewable and Sustainable Energy Reviews*, vol. 38, pp. 1015–1028, 2014.

[2] J. Wang, R. El Kontar, X. Jin, and J. King, "Electrifying high-efficiency future communities: Impact on energy, emissions, and grid," *Advances in Applied Energy*, vol. 6, p. 100095, 2022.

[3] J. Wang and X. Lu, "Sustainable and resilient distribution systems with networked microgrids," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 238–241, 2020.

[4] A. Gholami and A. Sun, "Stability of multi-microgrids: New certificates, distributed control, and braess's paradox," *IEEE Transactions on Control of Network Systems*, 2021.

[5] P. Ge, F. Teng, C. Konstantinou, and S. Hu, "A resilience-oriented centralised-to-decentralised framework for networked microgrids management," *Applied Energy*, vol. 308, p. 118234, 2022.

[6] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 110–127, Feb. 2015.

[7] 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.

[8] P. Ge, Y. Zhu, T. C. 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, no. 2, pp. 1059–1070, Mar. 2021.

[9] C. Deng, F. Guo, C. Wen, D. Yue, and Y. Wang, "Distributed resilient secondary control for dc microgrids against heterogeneous communication delays and dos attacks," *IEEE Transactions on Industrial Electronics*, 2021.

[10] Z. Lian, F. Guo, C. Wen, C. Deng, and P. Lin, "Distributed resilient optimal current sharing control for an islanded dc microgrid under dos attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4494–4505, 2021.

[11] P. Danzi, M. Angjelichinoski, Č. Stefanović, T. Dragičević, and P. Popovski, "Software-defined microgrid control for resilience against denial-of-service attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5258–5268, 2019.

[12] 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, 2019.

[13] S. Hu, F. Yang, S. Gorbachev, D. Yue, V. Kuzin, and C. Deng, "Resilient control design for networked dc microgrids under time-constrained dos attacks," *ISA transactions*, 2022.

[14] Y. Wan, C. Long, R. Deng, G. Wen, X. Yu, and T. Huang, "Distributed event-based control for thermostatically controlled loads under hybrid cyber attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 11, pp. 5314–5327, 2021.

[15] 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, 2022.

[16] Z. Hu, S. Liu, W. Luo, and L. Wu, "Resilient distributed fuzzy load frequency regulation for power systems under cross-layer random denial-of-service attacks," *IEEE Transactions on Cybernetics*, 2020.

[17] 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, 2020.

[18] X.-K. Liu, C. Wen, Q. Xu, and Y.-W. Wang, "Resilient control and analysis for dc microgrid system under dos and impulsive fdi attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 3742–3754, 2021.

[19] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE transactions on smart grid*, vol. 9, no. 5, pp. 4702–4711, 2018.

[20] P. Chen, S. Liu, B. Chen, and L. Yu, "Multi-agent reinforcement learning for decentralized resilient secondary control of energy storage systems against dos attacks," *IEEE Transactions on Smart Grid*, 2022.

[21] W. Heemels, K. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*. Maui, HI, USA: IEEE, Dec. 2012, pp. 3270–3285.

[22] D. V. Dimarogonas, E. Frazzoli, and K. H. Johansson, "Distributed event-triggered control for multi-agent systems," *IEEE Transactions on Automatic Control*, vol. 57, no. 5, pp. 1291–1297, 2011.

[23] 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, 2020.

[24] W. Xu, G. Hu, D. W. Ho, and Z. Feng, "Distributed secure cooperative control under denial-of-service attacks from multiple adversaries," *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3458–3467, 2019.

[25] D. Senejohnny, P. Tesi, and C. D. Persis, "A Jamming-Resilient Algorithm for Self-Triggered Network Coordination," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, p. 10, 2018.

[26] C. De Persis and P. Frasca, "Robust Self-Triggered Coordination With Ternary Controllers," *IEEE Transactions on Automatic Control*, vol. 58, no. 12, pp. 3024–3038, Dec. 2013.

[27] S. N. Backhaus, L. Dobriansky, S. Glover, C.-C. Liu, P. Looney, S. Mashayekh, A. Pratt, K. Schneider, M. Stadler, M. Starke *et al.*, "Networked microgrids scoping study," Los Alamos National Lab.(LANL), Los Alamos, NM (United States), Tech. Rep., 2016.

[28] J. Chen, M. Liu, and F. Milano, "Aggregated model of virtual power plants for transient frequency and voltage stability analysis," *IEEE Transactions on Power Systems*, vol. 36, no. 5, pp. 4366–4375, 2021.

[29] M. H. Roos, P. H. Nguyen, J. Morren, and J. Slootweg, "Aggregation of component-based grid-feeding der and load models for simulation of microgrid islanding transients," *Electric Power Systems Research*, vol. 189, p. 106759, 2020.

[30] F. Dorfler and F. Bullo, "Kron reduction of graphs with applications to electrical networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 60, no. 1, pp. 150–163, 2013.

[31] A. Bidram, A. Davoudi, and F. L. Lewis, "A multiobjective distributed control framework for islanded ac microgrids," *IEEE Transactions on industrial informatics*, vol. 10, no. 3, pp. 1785–1798, 2014.

[32] N. M. Dehkordi, N. Sadati, and M. Hamzeh, "Distributed robust finite-time secondary voltage and frequency control of islanded microgrids," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3648–3659, 2017.

[33] W. Ren, R. W. Beard, and E. M. Atkins, "A survey of consensus problems in multi-agent coordination," in *Proceedings of the 2005, American Control Conference, 2005.* IEEE, 2005, pp. 1859–1864.

[34] P. Ge, X. Dou, X. Quan, Q. Hu, W. Sheng, Z. Wu, and W. Gu, "Extended-State-Observer-Based Distributed Robust Secondary Voltage and Frequency Control for an Autonomous Microgrid," *IEEE Transactions on Sustainable Energy*, vol. 11, no. 1, pp. 195–205, Jan. 2020.