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

Pudong Ge\textsuperscript{b}, Student Member, IEEE, Boli Chen\textsuperscript{a}, Member, IEEE, and Fei Teng\textsuperscript{c}, 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], [10], [11], Lyapunov-based analysis [12], [13], [14], $H\infty$ control [15], [16], switched system design [17], [18], [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], [24], [25], [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], [10], [11], [14], [18], [24], [25]. Reference [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 channels, 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) sensing and control actuation with its MG central 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 sensing-communication-actuation chain in a hierarchical framework, as shown in Fig. 1, where each MG involves 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

$$m_{Pi} = \frac{1}{\sum_{j \in C_i} \frac{1}{m_{Pj}}}$$

where $C_i$ contains all DGs of MG $i$. In MG $i$, $m_{Pj}$, $\omega_i$ denote the frequency droop coefficient and angular frequency of DG $j$, and $m_{Pi}$, $\omega_i$ are respectively the equivalent frequency droop coefficient and the equivalent angular frequency of MG $i$ (similar to the concept of the Center of Inertia). $\omega_{cl}$ 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

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

where $\omega_{ni}$ is the nominal set point for frequency regulation; $P_i$ is the summation of active power output of the $i$th 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.,

$$\lim_{t \to \infty} |\omega_i - \omega_{ref}| = 0, \lim_{t \to \infty} x_i = x_{ref}$$

$$\lim_{t \to \infty} \frac{|P_i|}{P_{max,i} - P_{max,j}} = 0$$

where $P_{max,i}$ denotes the active power ratings of the $i$th generator, and (4) is equivalent to $\lim_{t \to \infty} |m_{Pj}P_i - m_{Pi}P_j| = 0$ 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 $\dot{\omega}_{ni} = \dot{\omega}_i + m_{Pi}\dot{P}_i = u_{oi} + u_{P}$, with $u_{oi}$, $u_{P}$ being the auxiliary control inputs that have been widely utilised in [31], [32]. Such that, we can obtain

$$\dot{x}_o = u_o, \dot{u}_P = u_P$$

where $x_o = [\omega_1, \ldots, \omega_n]^{\top}$, $x_P = [m_{P1}P_1, \ldots, m_{PN}P_N]^{\top}$, $u_o = [u_{o1}, \ldots, u_{on}]^{\top}$ and $u_P = [u_{P1}, \ldots, u_{PN}]^{\top}$. Owing to the similar formulation of modelling (5) for frequency and active power, we hereafter omit the subscript $o$, $P$, 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.

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...
The communication topology of networked MGs can be modelled by an undirected graph \( G = (\mathcal{I}, \mathcal{E}) \), 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 \(i\)th MG can receive information from the \(j\)th 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 \( \tilde{A} = [a_{ij}] \in \mathbb{R}^{m \times m} \) 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 \( A \), 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 \( u_o, u_P \) 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 \(x, u, \theta\) are the vectors of node states, controls and clock variables respectively. \(u, \theta\) 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:

\[
\dot{x}_i = u_i = \sum_{j \in \mathcal{N}_i} u_{ij}
\]

where \(i \in \mathcal{I}\). 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), \(u_{ij}, \theta_{ij}\) are updated only when the clock variable \(\theta_{ij}\) reaches zero, i.e., \((i, j) \in \mathcal{F}(\theta, t) = \{(i, j): j \in \mathcal{N}_i \land \theta_{ij}(\tau^-) = 0\}\) where \(\theta_{ij}(\tau^-) = \lim_{\tau \rightarrow \tau^-} \theta_{ij}(\tau)\). Specifically,

\[
\begin{align*}
    x_i(t) &= x_i(t^-) \quad \forall i \in \mathcal{I} \\
    u_{ij}(t) &= \begin{cases} 
    \operatorname{sign}(D_{ij}(t)), & \text{if } (i, j) \in \mathcal{F}(\theta, t) \\
    u_i(\tau^-), & \text{otherwise}
    \end{cases} \\
    \theta_{ij}(t) &= \begin{cases} 
    f_{ij}(x(t)), & \text{if } (i, j) \in \mathcal{F}(\theta, t) \\
    \theta_{ij}(\tau^-), & \text{otherwise}
    \end{cases}
\end{align*}
\]

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

\[
\text{Frequency: } n(t_1, t_2) \leq \eta + \frac{t_2 - t_1}{\tau^f},
\]

\[
\text{Duration: } |\Xi(t_1, t_2)| \leq \kappa + \frac{t_2 - t_1}{\tau^d}.
\]

To model multi-layer DoS attacks in a unified form, the Persistence-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 (Persistence-of-Data-Flow (PoDf)): For any transmission channel $\mu \in \{\mathcal{I} \cup \mathcal{E}\}$ serving for the distributed control, if multi-layer DoS sequences satisfy Assumption 1 respectively with coefficients $\tau^f_\mu, \tau^d_\mu$, such that $\phi_\mu(\tau^f_\mu, \tau^d_\mu, \Delta^*_\mu) := \frac{1}{\tau^f_\mu} + \frac{\Delta^*_\mu}{\tau^d_\mu} < 1$, where $\Delta^*_\mu := \min \Delta_\mu$. Then, for any unsuccessful data transmission attempt $\tau^f_\mu$, at least one successful transmission occurs within the time interval $[\tau^f_\mu, \tau^f_\mu + \Phi^*_\mu]$ with $\Phi^*_\mu := \frac{\kappa_\mu + (\theta_\mu + 1)\Delta^*_\mu}{1 - \phi_\mu(\tau^f_\mu, \tau^d_\mu, \Delta^*_\mu)}$.

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

Proposition 1 describes the impact of multi-layer DoS attacks on each data flow channel. $\Delta^*_\mu$ 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, $\Delta^*_\mu$ can be known a priori, though conservatively, based on the specification of the system. More specifically, $\Delta^*_f, \Delta^*_d$ depend on the performance of each MGCC, while $\Delta^*_0$ 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 $\tau^f_\mu \approx \tau^f_0, \tau^d_\mu \approx \tau^d_0 \Rightarrow \Phi^*_\mu \approx \Phi^*_0 \text{ and } \Phi_0 \leq \Phi_\mu, \Phi_0 \leq \Phi^*_\mu$ 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:

\[
\begin{align*}
\chi_i(t) &= x_i(t) & \forall i \in \mathcal{I} \\
\nu_{ij}(t) &= \text{sign}_i(D_{ij}(\bar{t})) & \text{if } (i, j) \in \mathcal{G}(\theta, t) \land t \in \Theta_{ij}(0, t) \\
\nu_{ij}(t) &= 0, & \text{if } (i, j) \in \mathcal{G}(\theta, t) \land t \in \Xi_{ij}(0, t) \\
\omega_{ij}(t) &= -R_{ij} \nu_{ij}(t) & \text{if } (i, j) \in \mathcal{G}(\theta, t) \land t \in \Xi_{ij}(0, t) \\
\theta_{ij}(t) &= \frac{1}{2(d_{ij} + d^2)} & \text{otherwise,}
\end{align*}
\]

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

\[
0 < \epsilon < \epsilon_{ij}.
\]

where $\epsilon$ represents the minimally acceptable consensus error that avoids Zeno-behaviour of all edges. The utilization of $R_{ij}$ and $\epsilon_{ij}$ 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 well as discussed in Section III-D. The map $f_{ij} : \mathbb{R}^2 \rightarrow \mathbb{R}_{>0}$ is defined as $f_{ij}(x(t)) = \max\{\frac{|D_{ij}(t)|}{2(d_{ij} + d^2)}, \epsilon_{ij} \}$.

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

\[
\Delta_{ij} := t^k_{ij} - t^k_{ij-1} \geq \frac{\epsilon_{ij}}{2R_{ij}(d_i + d_j)} \geq \frac{\epsilon}{4R_{ij}d_{\max}}
\]

where $d_{\max} = \max_{i \in \mathcal{I}} d_i$. This ensures the adaptive self-triggered control (11) to be Zeno-free. The item $D_{ij}(t)$ of (11) is designed to mitigate the cooperative impacts of multi-layer DoS, i.e., $D_{ij}(t) = x_j(t) - x_i(t)$, where $\bar{t}^D$ 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 $\delta = \varepsilon(n - 1)$.

\[
\left\{ x(t) \in \mathbb{R}^n : |x_i(t) - x_j(t)| < \delta \quad \forall (i, j) \in \mathcal{I} \times \mathcal{I} \right\}.
\]
additional degrees of freedom endowed by $e_{ij}$ and $R_d$, 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 $0 \leq s_{ij}^k - t_{ij}^k \leq \Phi_{ij}$.

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

$$\varepsilon > 2d_{\max} \Phi_{ij}^{\max} \frac{\sqrt{2}}{I_{ij} + 2\Delta T_{ij}} \quad R > \frac{\varepsilon}{2} - 2d_{\max} \Phi_{ij}^{\max} \frac{\sqrt{2}}{I_{ij} + 2\Delta T_{ij}}$$

with $\Phi_{ij}^{\max} = \Phi_{ij}^{\max} + 2\Phi_{ij}^{\max}$, $\Phi_{ij}^{\max}$ is defined as $\max_{i \in \mathcal{I}, j \in \mathcal{N}_i} \Phi_{ij}$, $\Phi_{ij}^{\max}$ is the initial value of $\Phi_{ij}$. 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:

$$t - t_{ij}^k \leq \frac{f_{ij}(s_{ij}^k)}{R} + 2\Phi_{ij}$$

(16)

Then if $D_{ij}(t_{ij}^k) \geq \varepsilon$, $D_{ij}(t) \geq x_j(t) - x_i(t)$

(a1) \quad \geq D_{ij}(t_{ij}^k) - (d_i + d_j)(t - t_{ij}^k)

(a2) \quad \geq D_{ij}(t_{ij}^k) - d_i\Phi_i - d_j\Phi_j - (d_i + d_j)(t - t_{ij}^k)

(a3) \quad \geq D_{ij}(t_{ij}^k) \left(1 - \frac{1}{2R}\right) - d_i(\Phi_i + 2\Phi_{ij}) - d_j(\Phi_j + 2\Phi_{ij})$

(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

$$D_{ij}(t) \geq D_{ij}(t_{ij}^k) \left(1 - \frac{1}{2R}\right) - 2d_{\max} \Phi_{ij}^{\max} \frac{\sqrt{2}}{I_{ij} + 2\Delta T_{ij}} > 0$$

(18)

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

$$D_{ij}(t) \leq D_{ij}(t_{ij}^k) \left(1 - \frac{1}{2R}\right) + 2d_{\max} \Phi_{ij}^{\max} \frac{\sqrt{2}}{I_{ij} + 2\Delta T_{ij}} < 0$$

(19)

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

$$\dot{V}(t) = \sum_{i=1}^{n} e_i \dot{e}_i = \sum_{i=1}^{n} e_i \sum_{j \in \mathcal{N}_i} \text{sign}(D_{ij}(t))$$

$$= -\frac{1}{2} \sum_{(i,j) \in \mathcal{E} \cap S} D_{ij}(t) \text{sign}(D_{ij}(t))$$

$$\leq -\frac{1}{2} \sum_{(i,j) \in \mathcal{E} \cap S} \left[ e^T \left(1 - \frac{1}{2R}\right) - 2d_{\max} \Phi_{ij}^{\max} \frac{\sqrt{2}}{I_{ij} + 2\Delta T_{ij}} \right] \lesssim 0$$

(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 $T_*$ as the convergence time of the distributed control system (6), (11). It holds that

$$T_* = \frac{2\varepsilon(d_{\min} + d_{\max}) + 8Rd_{\max}d_{\min} \Phi_{ij}^{\max} \frac{\sqrt{2}}{I_{ij} + 2\Delta T_{ij}}}{\varepsilon(1 - \frac{1}{2R}) - 2d_{\max} \Phi_{ij}^{\max} \frac{\sqrt{2}}{I_{ij} + 2\Delta T_{ij}}}$$

(21)

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

**Proof:** Consider the Lyapunov function based stability analysis (20), for any successful communication attempt $t_{ij}^k$ with $|D_{ij}(t_{ij}^k)| \geq \varepsilon$, the function $V$ decreases at least with the rate of

$$\rho := \frac{1}{2} \left[ e^T(1 - \frac{1}{2R}) - 2d_{\max} \Phi_{ij}^{\max} \frac{\sqrt{2}}{I_{ij} + 2\Delta T_{ij}} \right] \geq \frac{\varepsilon}{4Rd_{\max}}$$

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 $u_{ij}^*(t) = 0$, 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 $u_{ij}^* = 0$. 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 $u_{ij}^*(t_{ij}^k) = u_{ij}(t_{ij}^k)$ occurs at $t_{ij}^k \in [t_{ij}^k, t_{ij}^k + \Phi_{ij}]$. The time-duration of $u_{ij}^*(t_{ij}^k)$ contributing to the consensus is determined by the next successful control actuation attempt, which can be defined as $s_{ij}^{k+1} \in [t_{ij}^k, t_{ij}^k + \Phi_{ij}]$. We assume $u_{ij}^*(t_{ij}^k)$ will be lasting for at least $(\varepsilon/4Rd_{\max} + \Delta t)$ with $0 \leq \Delta t \leq \Phi_{ij}$, thus, we conclude that $V$ decreases by at least

$$\rho(\varepsilon/4Rd_{\max} + \Delta t)$$

every $(\Phi_{ij} + \varepsilon/4Rd_{\max} + \varepsilon/4Rd_{\max} + \Delta t)$ units of time. Therefore, the convergence time

$$T_* = \frac{\varepsilon/4Rd_{\min} + \Phi_{ij} + \Phi_{ij} + \varepsilon/4Rd_{\max} + \Delta t}{\rho(\varepsilon/4Rd_{\max} + \Delta t)} V(0)$$

$$\leq \frac{\varepsilon/4Rd_{\min} + \Phi_{ij} + 2\Phi_{ij} + \varepsilon/4Rd_{\max}}{\rho \varepsilon/4Rd_{\max}} V(0)$$

(22)
\[
\begin{align*}
V(0) & \leq 2\left(\frac{\varepsilon}{4Rd_{\text{min}}} + \frac{\varepsilon}{4Rd_{\text{max}}} + \Phi_{\text{max}}^{I, I} + 2\Phi_{\text{max}}^{I, 0} \right) V(0) \\
& = \frac{2\varepsilon(d_{\text{max}} + d_{\text{min}}) + 8Rd_{\text{max}}d_{\text{min}}}{\varepsilon d_{\text{min}}\left(1 - \frac{1}{2R}\right) - 2d_{\text{max}}\Phi_{\text{max}}^{I, I} + 2\Phi_{\text{max}}^{I, 0}} V(0)
\end{align*}
\]

(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 \(\varepsilon_{ij}\) and \(R_{ij}\), such that \(\forall i \in I, \forall j \in N_i,\)

\[
\varepsilon_{ij} > d_i(\Phi_i + 2\Phi_0) + d_j(\Phi_j + 2\Phi_0)
\]

\[
R_{ij} > \frac{2|\varepsilon_{ij} - d_i(\Phi_i + 2\Phi_0) - d_j(\Phi_j + 2\Phi_0)|}{\varepsilon_{ij}}
\]

(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 \(\Phi_i \leq \Phi_{\text{max}}^{I, I}, \Phi_0 \leq \Phi_{\text{max}}^{I, 0}, \forall i \in I, \) thus the condition (23) is less conservative than (15). Furthermore, although Proposition 1 gives bounded time interval \(\Phi_\theta\) 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 \(\Phi_\theta\) 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 \(k\)th communication attempt is successful at \(t_{ij}^k\), we define the following time instants:

\[
t_{ij}^k := t_{ij}^k - \bar{t}_i, \quad t_{ij} := t_{ij} - \bar{t}_i, \quad t_{ij}^0 := s_{ij} - t_{ij}^k
\]

(24)

where \(t_{ij}^k, \bar{t}_i\) are available at \(t_{ij}^k\) whereas \(t_{ij}^0\) is not known until \(t = s_{ij}\). To estimate \(t_{ij}^0\), let us consider an unsuccessful control attempt at \(s_{ij} \in [t_{ij}^k, s_{ij}^k]\) and \(t_{ij}^0\) the estimate of \(t_{ij}^0\). As we know that the next attempt will be made at \(s_{ij} + \Delta s_{ij}\), we keep updating \(t_{ij}^0\) via \(t_{ij}^0 = \bar{s}_{ij} + \Delta s_{ij} - t_{ij}^0\) until the next successful attempt. As such, there always exists a time instant \(\bar{t} < s_{ij}^k\), such that for all \(t \in [\bar{t}, s_{ij}^k], t_{ij}^0 = \bar{t}_{ij}^0\). It implies that \(t_{ij}^0\) is known prior to \(s_{ij}^k\).

\[
\text{Algorithm 1: DoS Resilient Distributed Consensus Control}
\]

1. **Initialisation:** for all \(i \in I\) and \(j \in N_i\), set \(\theta_j(0^-) = 0, \ u_j(0^-) = 0, u_j^k(0^-) = 0;\)

2. /* Local State Update from Sensors to Controllers */

3. foreach \(i \in I\)

4. if \(t \in \Theta_j(0, t)\) then

5. \(i\) updates \(x(t) = x(t)\);

6. end

7. /* Edge-Based Control Update in Controllers */

8. foreach \(j \in N_i\)

9. while \(\theta_j(t) > 0\) do

10. \(i\) applies the control \(u_j(t) = \sum_{\delta \in N_j} u_j(\delta);\)

11. end

12. if \(\theta_j(t) \leq 0 \lor t \in \Theta_j(0, t)\) then

13. \(i\) updates \(u_j(t) = \text{sign}(D_j(x(t)));\)

14. \(i\) updates \(\theta_j(t) = f_j(x(t));\)

15. else if \(\theta_j(t) \leq 0 \lor t \in \Theta_j(0, t)\) then

16. \(i\) updates \(u_j(t) = 0;\)

17. \(i\) updates \(\theta_j(t) = \frac{\varepsilon_j}{2(d_i + d_j)};\)

18. end

19. end

20. while \(\text{Control Actuation} \) do

21. foreach \(i \in I\)

22. if \(u_j(t)\) is updated \(\lor t \in \Theta_j(0, t)\) then

23. \(u_j^e(t) = u_j(t);\)

24. end

25. end

// note: \(u_j(t)\) denotes the desired control output, while \(u_j^e(t)\) denotes the actual control input of the subsystem. \(u_j(t) = u_j^e(t)\) if the actuation channel is not attacked.

**Proposition 2:** For any control actuation during \([s_{ij}^k, s_{ij}^{k+1}];\)

the following control inputs are equivalent to the system:

\[
u_j(t) = \text{sign}_x\left(D_j\left(t_{ij}^k\right)\right)\frac{\varepsilon_j^k}{\varepsilon_j^{k} + \Phi_{\text{max}}^{I, I}}, s_{ij}^k \leq t < s_{ij}^{k+1}
\]

\[
\equiv u_j(t) = \begin{cases} 
\text{sign}_x\left(D_j\left(t_{ij}^k\right)\right), s_{ij}^k \leq t < s_{ij}^{k+1} \\
0, \quad t_{ij}^k \leq t < s_{ij}^{k+1}
\end{cases}
\]

(25)

where \(\varepsilon_j^k = \varepsilon_j^{k} + \frac{f_j(s_{ij}^k)}{\varepsilon_j^{k}}\) and \(s_{ij}^k = f_j(s_{ij}^k) < s_{ij}^{k+1}\).

**Proof:** See Appendix A-B.

Although the consensus error bound \(\varepsilon_{ij}\) 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 \(\varepsilon_{ij}\) 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 $\varepsilon_{ij}$ and $R_{ij}$ can be adapted after each successful communication attempt, such that

$$\varepsilon_{ij}^k > \Gamma_{ij}^k, \quad R_{ij}^k > \frac{\varepsilon_{ij}^k}{2[\Gamma_{ij}^k - \varepsilon_{ij}^k]}$$

(26)

where $\Gamma_{ij}^k = d_i(r_{ij}^k + r_{i0}^k) + d_j(r_{ij}^k + r_{j0}^k)$ with $r_{ij}^k$, $r_{i0}^k$, $r_{j0}^k$ defined in (24), then the secure consensus condition (14) can be preserved.

**Proof:** See Appendix A-C.

After the $k$th successful communication attempt of edge $(i, j) \in \mathcal{E}$ : $j \in N_i$, $\Gamma_{ij}^k$ 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 $\theta_{ij}^k$ 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 $\varepsilon_{ij}^k > [1 + \frac{1}{2R_{ij}^k - 1}]\Gamma_{ij}^k R_{ij}^k > 0.5$, 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 $\varepsilon_{ij}^k$ 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.

**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 conservativeness 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], [24], [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], [24], [25], [26] will be provided in Section IV-A.

**IV. RESULTS**

To verify the effectiveness of the proposed DoS resilient control of networked MGs, a modified IEEE...
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], [24], [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.

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 | | | | |

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 $t = 5$ 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 $t = 30$ s and $t = 45$ 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], [24], [25], [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, \( \varepsilon \), has to be set to a conservative value \( \varepsilon = 1.2624 (\Phi_{\text{max}}/I_{\inf}) = 0.0526 \) to satisfy the global design criterion Eq. (15). If DoS attacks become less severe and intensive, after re-designing 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 than 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, when the proposed resilient self-triggered method is 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 cybersecurity 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 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.

APPENDIX A

Proof

A. Proof of Theorem 2

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

\[
\begin{aligned}
D_{ij}(t) &\geq d_i(\Phi_i + 2\Phi_0) - d_j(\Phi_j + 2\Phi_0) \\
&\ 
\end{aligned}
\]

\[
\begin{aligned}
D_{ij}(t) &\leq d_i(\Phi_i + 2\Phi_0) + d_j(\Phi_j + 2\Phi_0) \\
&\ 
\end{aligned}
\]

Then, (20) can be replaced by

\[
\dot{V}(t) \leq -\frac{1}{2} \sum_{(i,j) \in \mathcal{E} : S} \left[ \epsilon_{ij} \left( 1 - \frac{1}{2R_{ij}} \right) - d_i(\Phi_i + 2\Phi_0) - d_j(\Phi_j + 2\Phi_0) \right] < 0
\]

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 \( \dot{s}_{ij}^{k+1} - t_{ij}^{k+1} = t_{ij}^{k+1} - \Phi_0 \) and \( \dot{s}_{ij}^{k+1} - \dot{s}_{ij} = \Phi_0 \) if \( \text{sign}(D_{ij}(\tau_{ij})) = 1 \Rightarrow u_{ij}^*(t) > 0, t \in [s_{ij}^k, s_{ij}^{k+1}] \),

\[
\int_{s_{ij}^k}^{s_{ij}^{k+1}} u_{ij}^*(t) dt < \int_{s_{ij}^k}^{s_{ij}^{k+1} + \Phi_0} u_{ij}^*(t) dt
\]

if \( \text{sign}(D_{ij}(\tau_{ij})) = -1 \Rightarrow u_{ij}^*(t) < 0, t \in [s_{ij}^k, s_{ij}^{k+1}] \),

\[
\int_{s_{ij}^k}^{s_{ij}^{k+1} + \Phi_0} u_{ij}^*(t) dt < \int_{s_{ij}^k}^{s_{ij}^{k+1} + \Phi_0} u_{ij}^*(t) dt
\]

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

\[
\int_{s_{ij}^k}^{s_{ij}^{k+1}} u_{ij}^*(t) dt < \left| \text{sign}(D_{ij}(\tau_{ij})) \right| \Phi_0
\]

\[
= \int_{s_{ij}^k}^{s_{ij}^{k+1}} \left| \text{sign}(D_{ij}(\tau_{ij})) \right| dt + \int_{s_{ij}^k}^{s_{ij}^{k+1} + \Phi_0} 0 \ dt
\]

Thus, from (31), we can know if \( u_{ij}^* \) is actuated, it has the equivalent contribution of

\[
u_{ij}^*(t) = \begin{cases} 
\text{sign}(D_{ij}(\tau_{ij})), & s_{ij}^k < t < t_{ij}^{k+1} \\
0, & t_{ij}^k < t < s_{ij}^k 
\end{cases}
\]

where \( s_{ij}^k + \frac{(\Phi_0)^2}{\Phi_0 + \Phi_0} \leq t_{ij}^k \leq s_{ij}^{k+1} < s_{ij}^{k+1} \). In particular, \( t_{ij}^{k+1} = s_{ij}^k + \frac{(\Phi_0)^2}{\Phi_0 + \Phi_0} \) implies \( t_{ij}^{k+1} = s_{ij}^{k+1} \). ■
C. Proof of Corollary 2

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

$$\dot{V}(t) \geq D_{ij}(t) - d_i + d_j \{ t - t_{ij} \} (c)$$

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 et al., “Catching two European birds with one renewable stone: Mitigating climate change and Eurozone crisis by an energy transition,” Renew. Sustain. Energy Rev., vol. 39, pp. 1015–1028, Oct. 2014.

[2] J. Wang, R. El Kontar, X. Jin, and J. King, “Electrifying high-efficiency future communities: Impact on energy, emissions, and grid,” Adv. Appl. Energy, vol. 6, Jun. 2022, Art. no. 100095.

[3] J. Wang and X. Lu, “Sustainable and resilient distribution systems with networked microgrids,” Proc. IEEE, vol. 108, no. 2, pp. 238–241, Feb. 2020.

[4] A. Gholami and A. Sun, “Stability of multimicrogrids: New certificates, distributed control, and Braess’s paradox,” IEEE Trans. Control Netw. Syst., vol. 9, no. 1, pp. 308–319, Mar. 2022.

[5] P. Ge, F. Teng, C. Konstantinou, and S. Hu, “A resilience-oriented centralised-to-decentralised framework for networked microgrids management,” Appl. Energy, vol. 308, Feb. 2022, Art. no. 118234.

[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 Syst. Mag., 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,” Int. J. Robust 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 Trans. Power Syst., 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 Trans. Ind. Electron., vol. 69, no. 11, pp. 11560–11568, Nov. 2022.

[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 Trans. Smart Grid, vol. 12, no. 5, pp. 4494–4505, Sep. 2021.

[11] P. Danzi, M. Angelichino, C. Stefanovici, T. Dragicevic, and P. Popovski, “Software-defined microgrid control for resilience against denial-of-service attacks,” IEEE Trans. Smart Grid, vol. 10, no. 5, pp. 5258–5268, Sep. 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 Trans. Ind. Informat., vol. 15, no. 7, pp. 4066–4075, Jul. 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 Trans., vol. 127, pp. 197–205, Aug. 2022.