Resilient Distributed Self-Triggered Control of Networked Systems under Hybrid DoS Attacks

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

Abstract—This paper addresses a consensus control problem for networked systems subject to hybrid denial of service (DoS) attacks, which could simultaneously act on measurement, communication and control actuation channels. A novel notation, Persistency-of-Data-Flow (PoDF), is proposed to characterise all these potential vulnerabilities. Then, a distributed resilient control scheme is proposed in line with an edge-based self-triggered framework. Under such self-triggered framework and PoDF, the global consensus of the networked control systems in the presence of hybrid DoS attacks is proved based on the worst effects of the attack, and the bounded convergence time is derived analytically. To mitigate the conservativeness introduced by the global worst case analysis, a self-adaptive scheme is designed from a local perspective. Finally, the effectiveness of the proposed distributed self-triggered hybrid-DoS resilient control is verified by numerical simulations, and a case study with regard to the power network is carried out for further validation.

Index Terms—denial of service (DoS), resilient control, distributed control, self-triggered control, networked systems

I. INTRODUCTION

RECENT years have witnessed increasing attention towards cyber-physical systems (CPSs). CPSs are systems that involve connections of communication, computation and physical units. In the context of cyber-physical integrated systems where cyber-space implementation has direct effects on the physical-layer operation, cybersecurity has attracted much attention [1]. The major cyberattacks can be classified into denial-of-service (DoS) attacks and deception attacks [2]. DoS attacks cause the data loss by blocking the data flow, while deception attacks affect the trustworthiness of data by manipulating the transmitted data. In this paper, we are concerned with DoS attacks, which require less prior knowledge about the control system [3].

The resilience of CPSs under DoS has been investigated widely for both centralised control scheme [4], [5], [6] and distributed control scheme [7], [8], [9], [10]. In many large-scale and naturally distributed systems, such as power systems or unmanned aerial vehicles, distributed or networked control has been widely applied due to the sparse distribution of the agents. The distributed systems rely on neighbouring information exchange, which can be exploited by cyber attackers.

For this reason, resilient control under DoS over distributed communication channels have attracted growing investigation through many methods, such as game theory [3], LQG control [9] and model predictive control [11].

Event-based control [12], as a notion of reducing communication and computation burden, has been conducted extensively. The aperiodic control strategy in the event-based control leads to high dependence on aperiodic and limited information accessibility. To tackle this security issue, research on event/self-triggered control has been initiated to increase the resilience of control system against DoS attacks [13], [14], [15], [16], [17]. A general model [18], based on frequency and duration constraints of DoS attacks, has been proposed and has been applied widely to mitigate different types of DoS attacks (including trivial, periodic, random, and protocol-aware jamming attacks [19], [20], [21], [22]). Based on this model, the sufficient condition of stability with DoS attacks has been analysed through Lyapunov function and then the optimal event-based feedback control can be designed [18], [23], [24], [25], where updating sequence of the controller is optimized to ensure secure or resilient control performance.

In addition, from such general model of DoS attacks, the direct effect on distributed communication can be described by a notion of persistency-of-communication (PoC) [22], [26], which is further used in control design.

It is noteworthy that the existing research work mainly focuses on DoS attacks over communication links of a distributed system. However, many practical large-scale systems are constructed into a hierarchical or modular structure, where the controller and the sensor of each agent in the network are deployed following a subnetwork arrangement. On this occasion, as with the neighbouring communication links, measurement and control actuation of the subnetwork are also vulnerable to cyberattacks. For example, power grids involve multiple local electric generators, which are controlled in a distributed manner. Meanwhile, each electric generator system involves multilayer controllers and sensors that also involve data transmission [27]. As such, based on IEC-61850 [28], [29] and IEEE 2030.5 [30], all these three channels of the information flow could be blocked through malicious interception, e.g., fake gateway authorisation or IP address spoofing attack. Thus, the existing model of DoS attacks in the networked systems, such as PoC, cannot depict the hybrid-DoS effects on such distributed or hierarchical systems or be used to analyse the system dynamics.

In this context, the cooperation of DoS attacks on different channels or links may lead to complicated and undesired system dynamics. Therefore, this paper, in the spirit of self-
triggered control [12], [31], proposes an enhanced control method that is capable to address hybrid DoS attacks on local measurement, neighbouring communication and also control actuation channels. More specifically, the DoS existing in different channels is characterised by the Persistency-of-Data-Flow (PoDF) as a generalization from PoC. Based on the PoD, the control flow is analysed from an edge-based perspective and divided into three phases: local state update from sensors to controllers; edge-based control update in controllers; control actuation from controllers to subsystems. Then, a distributed self-triggered control is constructed. The main contributions are:

1) The Persistency-of-Data-Flow (PoDF), as a generalization from PoC, is proposed to enable the comprehensive characterization of all potential vulnerabilities within different data flow channels for networked systems, and therefore facilitates the dynamic performance analysis from a sequential logic.

2) An adaptive self-triggered control scheme is proposed to guarantee the global consensus of networked systems in the presence of hybrid-DoS attacks, and as a consequence, asynchronised data collection. In addition, the bounded convergence time is derived analytically.

3) A self-adaptive scheme is devised by utilising locally designed global stability criteria to mitigate the conservativeness of the algorithms designed from a global perspective.

The remainder of this paper is organized as follows. In Section II, the self-triggered consensus concept and the model of DoS attacks are provided. Section III introduces the adaptive distributed self-triggered consensus controller that is proved to be resilient against the hybrid DoS. The conservativeness of the algorithm is studied and a mitigation scheme is proposed in Section IV. Simulation results are presented in Section V and Section VI concludes this paper.

II. PRELIMINARIES

A. Primary Distributed Self-Triggered Control System

A consensus network is represented by an undirected graph $\mathcal{G} = \{\mathcal{I}, \mathcal{E}\}$, where $\mathcal{I} = \{1, 2, \ldots, n\}$ denotes the node set and $\mathcal{E} = \mathcal{I} \times \mathcal{I}$ denotes the edge set. For each node $i$, we define its neighbours by the set $\mathcal{N}_i$ with $d_i = |\mathcal{N}_i|$ denoting the cardinality of $\mathcal{N}_i$. In this paper, the graph $\mathcal{G}$ is assumed to be connected.

The self-triggered control has been applied in the consensus network by ternary controllers [32] and edge-based approach [22]. In summary, the hybrid dynamics are described by state 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 $d := \sum_{i=1}^{n} d_i$.

Then, the system dynamics satisfy:

\[
\begin{align*}
\dot{x}_i &= \sum_{j \in \mathcal{N}_i} u_{ij} \\
\dot{u}_{ij} &= 0 \\
\dot{\theta}_{ij} &= -1
\end{align*}
\]  

where $i \in \mathcal{I}$, $j \in \mathcal{N}_i$, and the control of each edge is updated only when its clock variable reaches zero. Define a set denoting the edges whose control should be update:

\[
\mathcal{F}(\theta, t) = \{(i, j) : j \in \mathcal{N}_i \land \theta_{ij}(t^-) = 0\}
\]

where $\theta_{ij}(t^-) = \lim_{\tau \rightarrow t^-} \theta_{ij}(\tau)$. Then, the update law of edge-based control under (1) is

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

and

\[
\begin{align*}
D_{ij}(t) &= \max \left\{ \frac{|D_{ij}(t)|}{2(d_i + d_j)}, \frac{\varepsilon}{2(d_i + d_j)} \right\} \\
\phi_{ij}(z) &= \begin{cases} 
\text{sign}(z), & \text{if } |z| \geq \varepsilon \\
0, & \text{otherwise}
\end{cases}
\end{align*}
\]

where $\varepsilon > 0$ is a user designed sensitivity parameter.

B. Denial-of-Service Attacks

To model DoS attacks, let us first define $\{h_n\}_{n \in \mathbb{N}}$ $(h_0 \geq 0)$ as the sequence of active DoS attack instance, when the DoS status exhibits a transition from 0 (inactive attack/successful transmission) to 1 (active attack/unsuccessful transmission). Then, the $n$th DoS time-interval is expressed as

\[
H_n := \{h_n\} \cup [h_n, h_n + \tau_n]
\]

where $\tau_n \in \mathbb{R}_{\geq 0}$ represents the length of $n$th DoS attack. Particularly, $\tau_n = 0$ means an impulse DoS attack at time $h_n$.

Give any time interval $[t_1, t_2]$ with $0 \leq t_1 < t_2$,

\[
\Xi(t_1, t_2) := \bigcup_{n \in \mathbb{N}} H_n \cap [t_1, t_2]
\]

where $\setminus$ denotes relative complement, and $\Xi(t_1, t_2)$ and $\Theta(t_1, t_2)$ are the under-attack and healthy subsets of $[t_1, t_2]$, respectively.

Let $n(t_1, t_2)$ denote the incidence of DoS inactive/active transitions within the time interval $[t_1, t_2]$. The following assumptions on the frequency and duration of DoS attacks are introduced [22], [24].

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

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

Assumption 2 (DoS Duration): There exist $\kappa \in \mathbb{R}_{\geq 0}$ and $\tau^d \in \mathbb{R}_{\geq 0}$ such that

\[
|\Xi(t_1, t_2)| \leq \kappa + \frac{t_2 - t_1}{\tau^d}
\]
III. RESILIENT CONSENSUS CONTROL AGAINST HYBRID
DOs ATTACKS

The schematic of the problem is shown in Fig. 1, where the data flow in the networked systems could be interrupted. In addition to the neighbouring communication attacks, DoS acting on data flows of local sensing and control actuation are also considered. In this section, we design a DoS-resilient control strategy for global consensus to mitigate the joint impacts of hybrid DoS attacks in the networked systems.

A. Hybrid-DoS Resilient Consensus Control

Through a notion of PoC, the effects of DoS on communication links on the consensus have been explicitly described [22], and the distributed control protocol (3) is based on the hypothesis that the controller can have access to both local state $x_i(t)$ and neighbouring state $x_j(t)$ at the triggered time. However, local measurement and control actuation commands could also suffer from DoS attacks in practice. To ensure the fully cyber-resilient consensus, we design an enhanced adaptive self-triggered control protocol from (3) to achieve resilience under hybrid DoS attacks (the corresponding stability criteria will be discussed later in Section III-B and Section IV):

$$
\begin{align*}
\dot{x}_i(t) &= x_i(t^-) \quad \forall i \in \mathcal{I} \\
\dot{u}_{ij}(t) &= \begin{cases} 
\text{sign}_{\varepsilon}(D_{ij}(\bar{t})) , & (i,j) \in \mathcal{J}(\theta,t) \land t \in \Theta_{ij}(0,t) \\
0, & (i,j) \in \mathcal{J}(\theta,t) \land t \in \Xi_{ij}(0,t) \\
\varepsilon f_{ij}(x(\bar{t})) , & (i,j) \in \mathcal{J}(\theta,t) \land t \in \Theta_{ij}(0,t) \\
\varepsilon \frac{1}{2(d_i + d_j)} , & (i,j) \in \mathcal{J}(\theta,t) \land t \in \Xi_{ij}(0,t) \\
\varepsilon t_{ij}(t^-) , & \text{otherwise}
\end{cases}
\end{align*}
$$

(12)

and for $i \in \mathcal{I}, j \in \mathcal{N}_i$, the map $f_{ij} : \mathbb{R}^2 \to \mathbb{R}_{>0}$ is defined as:

$$f_{ij}(x(\bar{t})) = \max \left\{ \frac{|D_{ij}(\bar{t})|}{2(d_i + d_j)}, \frac{\varepsilon_{ij}}{2(d_i + d_j)} \right\}
$$

(13)

which contributes to the sequence of communication-triggering attempts $\{t_{ij}^k\}_{k \geq 0}$ satisfying:

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

(14)

where $d_{\max} = \max_{i \in \mathcal{I}} d_i$. This ensures the adaptive self-triggered control (12) to be Zeno-free. It is worth noting that the proposed edge-based control involves individual clock rates $R_{ij}$ and the consensus error bound $\varepsilon_{ij}$ for each edge, which turns out to be useful in the context of consensus performance as will be discussed in Section IV.

The item $D_{ij}(\bar{t})$ of (12) is designed to mitigate the cooperative impacts of hybrid DoS:

$$D_{ij}(\bar{t}) = x_j(\bar{t}_j) - x_i(\bar{t}_i)
$$

(15)

where “$\bar{t}$” denotes latest time instant when the state is available.

For the sake of further analysis, the secure consensus is defined:

**Definition 1 (Secure Consensus):** Given the system (1), 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 hybrid DoS attacks if for any initial condition, $x(t)$ converges in finite time to a point belonging to the set

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

(16)

where $\delta = \varepsilon(n-1)$.

In the following, the distributed control strategy will be analysed, followed by the convergence analysis in line with (16).

B. Convergence Analysis

To model hybrid DoS attacks in a unified form, the PoC 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 $\mu \in \{\mathcal{I} \cup \mathcal{E}\}$ serving for the distributed control, if hybrid DoS sequences satisfy Assumption 1 and Assumption 2 respectively with coefficients $\tau_{\mu}^*, \tau_{\mu}^d$, such that

$$\phi_{\mu}(\tau_{\mu}^f, \tau_{\mu}^d, \Delta_{\mu}^*) := \frac{1}{\tau_{\mu}^d} + \frac{\Delta_{\mu}^*}{\tau_{\mu}^f} < 1
$$

(17)

where $\Delta_{\mu}^* := \min \Delta_{\mu}$. Then, for any unsuccessful data transmission attempt $t_{\mu}^k$, at least one successful transmission occurs within the time interval $[t_{\mu}^k, t_{\mu}^k + \Phi_{\mu}]$ with

$$\Phi_{\mu} := \frac{\kappa_{\mu} + (\eta_{\mu} + 1)\Delta_{\mu}^*}{1 - \phi_{\mu}(\tau_{\mu}^f, \tau_{\mu}^d, \Delta_{\mu}^*)}
$$

(18)

**Proof:** The proof is similar to that in the Appendix A of [22], thus omitted here.

**Remark 1:** Proposition 1 describes the impact of hybrid DoS attacks on each data flow channel. The parameter $\Delta_{\mu}^*$ denotes the minimum time interval between two sequential attempts of data flow, which is different for the three different

1 For any communication channel $(i,j) \in \mathcal{E}: j \in \mathcal{N}_i$, $\mu$ is expressed as $ij$; for any local measurement channel from sensors $i \in \mathcal{I}$, $\mu$ is expressed as $i0$.
types of data transmissions. In practice, $\Delta^{*}$ can be know a priori, though conservatively, based on the specification of the system. More specifically, $\Delta^{*}$, $\Delta^{*0}$ depend on the performance of each distributed control system, while $\Delta_{ij}$ is determined by (14).

Assumption 3: 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 $\tau^{f}_i \approx \tau^{f}_0$, $\tau^{d}_i \approx \tau^{d}_0 \Rightarrow \Phi_i \approx \Phi_{i0}$ and $\Phi_i \leq \Phi_{ij}$, $\Phi_{i0} \leq \Phi_{ij}$.

Now, the behaviour of the control system (12) is analysed. In the first instance, let us assume uniform clock rate and consensus error bound, such that $R_{ij} = R$, $\varepsilon_{ij} = \varepsilon$, $\forall i \in \mathcal{I}$. After the controller $i$ updates the associated input $u_{ij}$ related to its neighbour $j$ by (12), 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: $\{t^k_{ij} : k \in \mathbb{N}\}$ and $\{s^k_{ij} : k \in \mathbb{N}\}$. The sequence $t^k_{ij}$ denotes the time instants at which $(i, j) \in \mathcal{J}(\theta, t)$ satisfies, while the sequence $s^k_{ij}$ denotes the corresponding time instants at which transmission attempts of control actuation from (12) are successful. Then, two sequences have the property of $0 \leq s^k_{ij} - t^k_{ij} \leq \Phi_{i0}$.

**Theorem 1:** Consider the distributed control system (1), (12) subject to hybrid DoS attacks. If Assumptions 1-3 hold and

$$
\begin{align*}
\varepsilon &> 2d_{\text{max}}(\Phi_{i0}^{\text{max}} + 2\Phi_{i0}^{\text{max}}) \\
R &> \frac{\varepsilon}{2[\varepsilon - 2d_{\text{max}}(\Phi_{i0}^{\text{max}} + 2\Phi_{i0}^{\text{max}})]}
\end{align*}
$$

(19)

with $\Phi_{i0}^{\text{max}} = \max_{i \in \mathcal{I}} \Phi_i$, $\Phi_{i0}^{\text{max}} = \max_{i \in \mathcal{I}} \Phi_{i0}$, then $x(t)$ reaches consensus in finite time as described in (16).

**Proof:** Consider any time $t$, there exists two successive time instants of successful control actuation that satisfy $s^k_{ij} \leq t < s^{k+1}_{ij}$. During the time period $[s^k_{ij}, s^{k+1}_{ij})$, the control input that is updated through (12) at the time instant $t^k_{ij}$ will be applied. For each $(i, j) \in \mathcal{E} : j \in \mathcal{N}_i$, we have the following inequality:

$$
t - t^k_{ij} \leq \frac{f_{ij}(x(t^k_{ij}))}{R} + 2\Phi_{i0}
$$

(20)

Then if $D_{ij}(t^k_{ij}) \geq \varepsilon$,

$$
\begin{align*}
D_{ij}(t) &= x_j(t) - x_i(t) \\
&\geq (a1) \ [x_j(t^k_{ij}) - d_{ij}(t - t^k_{ij})] - [x_i(t^k_{ij}) + d_i(t - t^k_{ij})] \\
&= D_{ij}(t^k_{ij}) - (d_i + d_j)(t - t^k_{ij}) \\
&\geq D_{ij}(t^k_{ij}) - d_i\Phi_i - d_j\Phi_j \\
&\geq (a2) \ [x_j(t^k_{ij}) - d_{ij}(t - t^k_{ij})] - (d_i + d_j)(t - t^k_{ij})
\end{align*}
$$

(21)

where (a1) derives from deterministic neighbours and control inputs, and (a2), (a3) are from Proposition 1 and (20) respectively, then (21) can be expressed as

$$
D_{ij}(t) \geq D_{ij}(t^k_{ij}) - (d_{ij} + d_{ij})(t - t^k_{ij}) - d_i(\Phi_i + 2\Phi_{i0}) - d_j(\Phi_j + 2\Phi_{i0})
$$

(22)

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

$$
D_{ij}(t) \leq D_{ij}(t^k_{ij}) - (d_{ij} + d_{ij})(t - t^k_{ij}) - d_i(\Phi_i + 2\Phi_{i0}) - d_j(\Phi_j + 2\Phi_{i0})
$$

(23)

Define error terms as

$$
e_i = x_i - \sum_{i=1}^{n} x_i
$$

(24)

and $e = [e_i]_{N \times 1}$. Consider a candidate Lyapunov function

$$
V(t) = \frac{1}{2}e^T e
$$

(25)

Define $S := |D_{ij}(t^k_{ij})| \geq \varepsilon \land t^k_{ij} \in \Theta_{ij}(0, t)$, then the derivative of $V(t)$ under the controller (12):

$$
\dot{V}(t) = \sum_{i=1}^{n} e_i \dot{e}_i
$$

(26)

where (b) derives by applying (19) in Theorem 1. As a result, (26) shows convergence in finite time. 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 (Bounded Convergence Time):** Consider $T_*$ as the convergence time of the distributed control system (1), (12). It holds that

$$
T_* \leq \frac{2\varepsilon(d_{\text{max}} + d_{\text{min}}) + 8Rd_{\text{max}}d_{\text{min}}(\Phi_{i0}^{\text{max}} + 2\Phi_{i0}^{\text{max}})}{\varepsilon d_{\text{min}}[\varepsilon(1 - \frac{1}{2\pi}) - 2d_{\text{max}}(\Phi_{i0}^{\text{max}} + 2\Phi_{i0}^{\text{max}})]} V(0)
$$

(27)

where $\Phi_{i0}^{\text{max}} = \max_{i \in \mathcal{I}, j \in \mathcal{N}_i} \Phi_{ij}$, $d_{\text{min}} = \min_{i \in \mathcal{I}} d_i$. 


Proof: Consider the Lyapunov function based stability analysis (26), 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 $\rho = \frac{1}{2} \left[ \varepsilon (1 - \frac{1}{2\pi}) - 2d_{\max}(\Phi_{T,ij}^{\max} + 2\Phi_{i0}) \right]$ by at least $(\varepsilon/4Rd_{\max})$ units of time (as inferred from (14)) under the enhanced adaptive controller (12).

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 $u_{ij}^*(s_{ij}^k) = u_{ij}(t_{ij}^k)$ occurs at $s_{ij}^k \in \left[ t_{ij}^k, t_{ij}^k + \Phi_{i0} \right]$. The time-duration of $u_{ij}^*(s_{ij}^k)$ contributing to the consensus is determined by the next successful control actuation attempt, which can be defined as $s_{ij}^{k+1} \in \left[ t_{ij}^k, t_{ij}^k + \Phi_{i0} \right]$. We assume $u_{ij}^*(s_{ij}^k)$ will be lasting for at least $(\varepsilon/4Rd_{\min} + \Delta t)$ 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. Therefore, the convergence time

$$T_* \leq \frac{\varepsilon/4Rd_{\min} + \Phi_{ij} + \Phi_{i0} + \varepsilon/4Rd_{\max} + \Delta t}{\rho(\varepsilon/4Rd_{\max} + \Delta t)} V(0) \leq \frac{\varepsilon/4Rd_{\max} + \Phi_{ij} + 2\Phi_{i0} + \varepsilon/4Rd_{\max} V(0)}{\rho(\varepsilon/4Rd_{\max})} \leq \frac{2(\varepsilon/4Rd_{\min} + \varepsilon/4Rd_{\max} + \Phi_{T,ij}^{\max} + 2\Phi_{i0}^{\max})}{\varepsilon(1 - \frac{1}{2\pi}) - 2d_{\max}(\Phi_{T,ij}^{\max} + 2\Phi_{i0}^{\max})} V(0)$$

$$= \frac{\varepsilon d_{\min} (\varepsilon(1 - \frac{1}{2\pi}) - 2d_{\max}(\Phi_{T,ij}^{\max} + 2\Phi_{i0}^{\max}))}{\rho(\varepsilon/4Rd_{\max})} V(0)$$

(28)

IV. CONSERVATIVENESS MITIGATION UNDER HYBRID DO S ATTACKS

The global consensus criteria (19) given in Theorem 1 are inferred from the global worst case analysis in terms of PoDF (uniform bounds across all the agents), thereby being conservative and could lead to degraded consensus accuracy.

In this section, under the procedure of hybrid-DoS resilient control protocol summarised in Table I, less conservative criteria are derived from a local perspective (Theorem 2) to further improve the control performance.

Theorem 2: Consider the distributed system (1) subject to hybrid DoS attacks and the edge-based control (12). If each subsystem can individually choose its parameters $\varepsilon_{ij}$ and $R_{ij}$, such that

$$\begin{cases} \varepsilon_{ij} > d_i(\Phi_i + 2\Phi_{i0}) + d_j(\Phi_j + 2\Phi_{i0}) \\ R_{ij} > \frac{\varepsilon_{ij}}{2[\varepsilon_{ij} - d_i(\Phi_i + 2\Phi_{i0}) - d_j(\Phi_j + 2\Phi_{i0})]} \end{cases}$$

(29)

with $i \in \mathcal{I}, j \in \mathcal{N}_i$, then the global consensus (16) can be guaranteed.

TABLE I

| HYBRID-DO S RESILIENT DISTRIBUTED CONSENSUS CONTROL |
|----------------------------------------------------|
| 1: initialization: for all $i \in \mathcal{I}$ and $j \in \mathcal{N}_i$, set $\theta_{ij}(0^-) = 0$, $u_{ij}(0^-) = 0$, $u_{ij}^*(0^-) = 0$; |
| local state update from sensors to controllers |
| 2: for all $i \in \mathcal{I}$ do |
| 3: if $t \in \Theta_i(0, t)$ then |
| 4: $i$ updates $x_i(t) = x_i(t)$; |
| 5: end if |
| 6: end for |
| edge-based control update in controllers |
| 7: for all $i \in \mathcal{I}$ do |
| 8: for all $j \in \mathcal{N}_i$ do |
| 9: while $\theta_{ij}(t) > 0$ do |
| 10: $i$ applies the control $u_i(t) = \sum_{j \in \mathcal{N}_i} u_{ij}(t)$; |
| 11: end while |
| 12: if $\theta_{ij}(t) \leq 0 \wedge t \in \Theta_{ij}(0, t)$ then |
| 13: $i$ updates $u_{ij}(t) = \text{sign}(D_{ij}(t))$; |
| 14: $i$ updates $\theta_{ij}(t) = f_i(x_i(t))$; |
| 15: else if $\theta_{ij}(t) \leq 0 \wedge t \in \Xi_{ij}(0, t)$ then |
| 16: $i$ updates $u_{ij}(t) = 0$; |
| 17: $i$ updates $\theta_{ij}(t) = \frac{\varepsilon_{ij}}{2[\varepsilon_{ij} - d_{ij}]}$; |
| 18: end if |
| 19: end for |
| 20: end for |
| control actuation |
| 21: for all $i \in \mathcal{I}$ do |
| 22: if $u_i(t)$ is updated $\wedge t \in \Theta_{i0}(0, t)$ then |
| 23: $u_i^*(t) = u_i(t)$; |
| 24: end if |
| 25: end for |

† $u_i(t)$ denotes the desired control output, while $u_i^*(t)$ denotes the actual control input of the subsystem, $u_i(t) = u_{ij}^*(t)$ if the actuation channel is not attacked.

Proof: From the proof of Theorem 1, the inequality (22) and (23) can be replaced by

$$\begin{align} D_{ij}(t) &\geq D_{ij}(t_{ij}^k)(1 - \frac{1}{2R_{ij}}) - d_i(\Phi_i + 2\Phi_{i0}) \\
&\quad - d_j(\Phi_j + 2\Phi_{i0}), \text{ if } D_{ij}(t_{ij}^k) \geq \varepsilon_{ij} \\
D_{ij}(t) &\leq D_{ij}(t_{ij}^k)(1 - \frac{1}{2R_{ij}}) + d_i(\Phi_i + 2\Phi_{i0}) \\
&\quad + d_j(\Phi_j + 2\Phi_{i0}), \text{ if } D_{ij}(t_{ij}^k) \leq -\varepsilon_{ij} \end{align}$$

(30)

Then, (26) can be replaced by

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

(31)

which shows the convergence using (29) in Theorem 2. Thus, the secure consensus (16) is achieved.

It is obvious that $\Phi_i \leq \Phi_{T,ij}^{\max}, \Phi_{i0} \leq \Phi_{i0}^{\max}, \forall i \in \mathcal{I}$, thus the condition (29) is less conservative than (19).

Furthermore, although Proposition 1 gives bounded time interval $\mu_{\Phi}$ that can be utilized to design parameters, the time to achieve a successful data flow would not be $\Phi_{\mu}$.
all the time under DoS. 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 \( t^k_{ij} \), we define the following time instants:

\[
t^k_{ij}, t^k_{ij} := t^k_{ij} - \bar{t}^k, \quad t^k_{ij} := t^k_{ij} - \bar{t}^k, \quad t^0_{ij} := s^k_{ij} - t^k_{ij} \tag{32}
\]

where \( t^k_{ij}, t^k_{ij} \) are available at \( t^k_{ij} \) whereas \( t^0_{ij} \) is not known until \( t = s^k_{ij} \). To estimate \( t^0_{ij} \), let us consider an unsuccessful control actuation attempt at \( \hat{s}_{ij} \in [t^k_{ij}, s^k_{ij}) \) and \( t^0_{ij} \), the estimate of \( t^0_{ij} \).

As we know that the next attempt will be made at \( \hat{s}_{ij} + \Delta^u_0 \), we keep updating \( t^0_{ij} \) via \( t^0_{ij} = \hat{s}_{ij} + \Delta^u_0 - t^k_{ij} \) until the next successful attempt. As such, there always exists a time instant \( \bar{t} < s^k_{ij} \), such that for all \( t \in [\bar{t}, s^k_{ij}) \), \( t^k_{ij} = t^0_{ij} \). It implies that \( t^0_{ij} \) is known prior to \( s^k_{ij} \).

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

\[
u'_{ij}(t) = \text{sign}_\varepsilon(D_{ij}(t^k_{ij})), \quad \frac{\varrho_{ij}^k}{\sqrt{\varrho_{ij}^k + \Phi_{00}}}, \quad s^k_{ij} \leq t < s^{k+1}_{ij} \tag{33}\]

\[
\iff u_{ij}(t) = \text{sign}_\varepsilon(D_{ij}(t^k_{ij})), \quad s^k_{ij} \leq t < s^{k+1}_{ij}
\]

where \( \varrho_{ij}^k = \frac{\varrho_{ij}^k}{R^k_{ij}}, \) and \( s^k_{ij} + \frac{(\varrho_{ij}^k)^2}{\varrho_{ij}^k + \Phi_{00}} \leq s^{k+1}_{ij} \).

**Proof:** By the inequality \( s^{k+1}_{ij} - t^{k+1}_{ij} = t^{k+1}_{ij} - \Phi_{00} \) and \( t^{k+1}_{ij} - s^k_{ij} = \varrho_j^k \), if \( \text{sign}_\varepsilon(D_{ij}(t^k_{ij})) = 1 \Rightarrow u'_{ij}(t) > 0, t \in [s^k_{ij}, s^{k+1}_{ij}] \), we obtain

\[
\int_{s^k_{ij}}^{s^{k+1}_{ij}} u'_{ij}(t)dt = \int_{s^k_{ij}}^{s^{k+1}_{ij} + \Phi_{00}} u'_{ij}(t)dt 
\leq \int_{s^k_{ij}}^{s^{k+1}_{ij} + \Phi_{00}} u_{ij}(t)dt \tag{34}\]

if \( \text{sign}_\varepsilon(D_{ij}(t^k_{ij})) = -1 \Rightarrow u'_{ij}(t) < 0, t \in [s^k_{ij}, s^{k+1}_{ij}] \), we obtain

\[
\int_{s^k_{ij}}^{s^{k+1}_{ij}} u'_{ij}(t)dt = \int_{s^k_{ij}}^{s^{k+1}_{ij} + \Phi_{00}} u'_{ij}(t)dt 
\geq \int_{s^k_{ij}}^{s^{k+1}_{ij} + \Phi_{00}} u_{ij}(t)dt \tag{35}\]

Combining (34) and (35), the contribution of control actuation during \([s^k_{ij}, s^{k+1}_{ij})\) is limited:

\[
\int_{s^k_{ij}}^{s^{k+1}_{ij}} |u'_{ij}(t)|dt \leq \int_{s^k_{ij}}^{s^{k+1}_{ij} + \Phi_{00}} |u_{ij}(t)|dt = \text{sign}_\varepsilon(D_{ij}(t_{ij}^k)) \int_{s^k_{ij}}^{t_{ij}^k} \varrho_{ij}^k dt + \int_{s^k_{ij}}^{s^{k+1}_{ij}} 0 \ dt \tag{36}\]

Thus, from (36), we can know if \( u'_{ij} \) is actuated, it has the equivalent contribution of

\[
u_{ij}(t) = \begin{cases} 
\text{sign}_\varepsilon(D_{ij}(t_{ij}^k)), & t^k_{ij} < t < t^{k+1}_{ij} \\
0, & t^{k+1}_{ij} < t < s^k_{ij} \tag{37}\end{cases}\]

where \( s^k_{ij} + \frac{(\varrho_{ij}^k)^2}{\varrho_{ij}^k + \Phi_{00}} \leq t^{k+1}_{ij} \). In particular, \( t^{k+1}_{ij} = s^k_{ij} + \frac{(\varrho_{ij}^k)^2}{\varrho_{ij}^k + \Phi_{00}} \) implies \( t^{k+1}_{ij} = s^{k+1}_{ij} \).

Although the consensus error bound \( \varepsilon_{ij} \) guaranteed in Theorem 2 is less conservative than (19), it still relies on the PoDF conditions, which is inevitably conservative. Next, we show that a tighter consensus error bound can be achieved if a 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 (1) subject to hybrid DoS attacks and the edge-based control (12) with control input \( u'_{ij} \) in Proposition 2, if \( \varepsilon_{ij} \) and \( R_{ij} \) can be adapted after each successful communication attempt, such that

\[
\varepsilon_{ij} > \Gamma_{ij}R_{ij} \geq \frac{\varepsilon_{ij}}{2(k^* - \Gamma_{ij}^2)} \tag{38}\]

where \( \Gamma_{ij}^2 = d_i(t_{ij,i} + t_{ij}) + d_j(t_{ij,i} + t_{ij}) + t_{ij,i} + t_{ij} \) with \( t_{ij,i}, t_{ij} \) defined in (32), then the secure consensus condition (16) can be preserved.

**Proof:** If \( D_{ij}(t_{ij}^k) \geq \varepsilon_{ij}^k \), (21) in Theorem 1 can be modified as the following

\[
D_{ij}(t) \geq D_{ij}(t_{ij}^k) - (d_i + d_j)(t - t_{ij}^k) \tag{39}\]

\[
\geq D_{ij}(t_{ij}^k) - d_i(t_{ij,i} + t_{ij}) - d_j(t_{ij,i} + t_{ij}) - 0 \times \Phi_{00} = D_{ij}(t_{ij}^k)(1 - \frac{1}{2R_{ij}^k}) 
- d_i(t_{ij,i} + t_{ij}) - d_j(t_{ij,i} + t_{ij}) \tag{39}\]

where (c) comes from Proposition 2. Then followed by the similar process as (22)-(26), we obtain \( V(t) < 0 \) remains guaranteed with (38). Similarly, secure consensus (16) is achieved.

After the \( k \)th successful communication attempt of edge \((i, j) \in E \); \( j \in N_i \), \( \Gamma_{ij} \) is already known before the control actuation attempt. Then we can choose appropriate \( \varepsilon_{ij}^k, R_{ij} \) to satisfy (38), and the corresponding clock variable \( \varrho_j^k \) and control variable \( u'_{ij} \) can be obtained from (12) and (33) respectively. To make the proposed self-adaptive scheme clear, we summarise it in Table II.

**Remark 2:** The conditions shown in (38) are equivalent to \( \varepsilon_{ij}^k > 1 + \frac{1}{2R_{ij}} > 0.5 \), which explicitly shows the relationship between two designed parameters. The selection of \( \varepsilon_{ij}^k, R_{ij} \) is subject to a trade-off between consensus accuracy and computation burden. More specifically, smaller \( \varepsilon_{ij}^k \) leads to more accurate consensus performance but requires larger \( R_{ij} \), which means more frequent communication between agents. Hence, the parameter selection in practice should consider
TABLE II
SELF-ADAPTIVE SCHEME FOR HYBRID-DoS RESILIENT DISTRIBUTED CONSENSUS CONTROL

| Step | Description |
|------|-------------|
| 1:   | for all \((i, j) \in E\) do |
| 2:   | for any communication attempt \(k\) do |
| 3:   | if attempt is unsuccessful |
| 4:   | apply (12) and Table I to the unsuccessful solution; |
| 5:   | else if attempt is successful |
| 6:   | design \(\epsilon_{ij}^k, R_{ij}^k\) using (38); |
| 7:   | calculate \(\theta_{ij}^k\) as (12) and apply \(u_{ij}^k = u_{ij}^{k'}\) as (33); |
| 8:   | end if |
| 9:   | end for |
| 10:  | end for |

![Figure 2](image2.png)

Fig. 2. Evolution of the states \(x\) in absence of DoS under (12) and Table I both the communication capability and accuracy requirement of application.

V. RESULTS

In the section, two numerical examples including a case study on power networks are given to show the effectiveness of the proposed hybrid-DoS resilient control.

A. Numerical Test

A random connected undirected graph with \(n = 50\) nodes and \(d_i = 4\) is considered. In this graph, the initial state of each node is initialised randomly with \([0, 1]\). The simulation results in absence of DoS are shown in Fig. 2.

We randomly generate the hybrid DoS attacks, whose \(\tau_f, \tau_d\) are depicted in Fig. 3, such that \(\Phi_{\max} = \Phi_{\max}^0 = 0.0099, \tau_f \approx \tau_f^0 < \tau_f^0\) to satisfy Assumption 3. To meet the requirements (19) as in Theorem 1, set \(\varepsilon = 0.2376, R = 1\). Under such parameter design, the consensus can be achieved with undesired performance, as shown in Fig. 4, where quite large \(\delta\) defined in Definition 1 shows conservative consensus results. To reach acceptable consensus performance, \(\varepsilon\) needs to be set relatively smaller than that satisfying Theorem 1. If the global consensus of (19) does not satisfy by setting \(\varepsilon = 0.001, R = 1\), the consensus cannot be reached as Fig. 5. However, if the proposed self-adaptive scheme as Corollary 2 is applied, Fig. 6 summarizes the consensus performance under conservativeness mitigation. From Fig. 6, the consensus is reached in relatively small errors rapidly and then consensus errors gradually narrow down. The self-adaptive scheme for the self-triggered control guarantees the consensus with limited errors through (38), though considering the unforeseeable DoS effects of the next control actuation by using Proposition 2 causes longer convergence time compared to that shown in Fig. 2.

Then, we also evaluate the DoS effects of local and neighbouring channels on the consensus respectively. In particular, we change the DoS attacks on local levels and neighbouring communication channels separately compared to that shown in Fig. 3, and discuss the consensus performance. As shown in Fig. 7, if the negative effects of DoS attacks on neighbour-
ing communication channels are weakened with $\Phi_{IJ} = 0.0411$, the convergence speed becomes fast compared to that in Fig. 6 ($\Phi_{IJ} = 0.1210$). In addition, the DoS attacks on local levels have the similar phenomenon, but Fig. 8 ($\Phi_{I} = \Phi_{0} = 0.0030$) shows that the increasing cybersecurity of local levels has more contributions to convergence because the unforeseeable DoS effects, which are considered as the worst scenario $\Phi_{I0}$ and mitigated by Proposition 2, can be reduced.

**B. Distributed Frequency Regulation of Power Grids**

Microgrid (MG), as a typical operational scenario in power grids [33], [34], [35], could suffer from DoS attacks on both local generators or multi-generator coordination, which is depicted in Fig. 9. The dynamics of distributed generators are detailed in [34], [36], where frequency regulation is formulated as a consensus problem as defined in (1) (see details of problem formulation in Appendix A).

The proposed hybrid-DoS resilient distributed control method is tested with a 50-Hz, 220-V (single-phase RMS value) islanded MG system as shown in Fig. 10, the parameters of which are detailed in Appendix B. In the simulation, the test system is initialized before 1 second, when only primary controller is enabled, so the deviation of frequency exists; the load change, a typical event in the power networks, occurs at 5 second and 9 second respectively. In addition, DoS attacks on local and neighbouring sides are depicted in Fig. 11.

Confronted with such hybrid DoS attacks, the proposed resilient distributed self-triggered control can regulate the MG well, as shown in Fig. 12, where frequency tracking and accurate power sharing are guaranteed. To emphasise the effects of DoS attacks on the local side, in the same scenario,
the method in [22], which only considers DoS on neighbouring communication, is applied. As shown in Fig. 13, the consensus of local frequencies cannot be reached due to the presence of local DoS, which cannot be tackled by the method in [22].

**VI. CONCLUSION**

In this paper, we propose a hybrid-DoS resilient distributed self-triggered control method of networked systems. Hybrid DoS attacks on different channels of data flow are considered: DoS attacks on local measurement, neighbouring communication 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 self-adaptive scheme which classifies effects of DoS attacks into foreseeable and unforeseeable parts. Through numerical and power network examples, the effectiveness of such hybrid-DoS resilient strategy is illustrated with individual analysis of DoS attacks on local or neighbouring data transmissions.

However, this paper only investigates the networked systems that only have first-order local dynamics, and it is interesting
to conduct the research on the system involving higher-order dynamics. 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

Problem Formulation of Microgrids

The droop-based frequency control can be formulated as [37], [38]

\[
\omega_{ni} = \omega_i + m_{p_i} P_i
\]

(40)

where \( \omega_{ni} \) is the nominal set point for frequency regulation; \( \omega_i \) is the angular frequency of the \( i \)th generator; \( m_{p_i} \) and \( P_i \) are respectively frequency droop coefficient and active power output of the \( i \)th generator.

The primary control through (40) can not eliminate the frequency deviations from the reference, and the secondary control is employed to achieve frequency regulation and accurate active power sharing, i.e.,

\[
\lim_{t \to \infty} \left| \omega_i - \omega_j \right| = 0, \quad \lim_{t \to \infty} \omega_i = \omega_{\text{ref}}
\]

(41)

\[
\lim_{t \to \infty} \left| \frac{P_i}{P_{\text{max},i}} - \frac{P_j}{P_{\text{max},j}} \right| = 0
\]

(42)

where \( P_{\text{max},i} \) denotes the active power ratings of the \( i \)th generator, and (42) is equivalent to \( \lim_{t \to \infty} \left| m_{p_i} P_i - m_{p_j} P_j \right| = 0 \) by approximately setting frequency droop coefficients.

To formulate the control problem, we differentiate (40) and choose the changing rates of frequency and active power output as control variables

\[
\dot{\omega}_{ni} = \dot{\omega}_i + m_{p_i} \dot{P}_i = u_{\omega_i} + u_{P_i}
\]

(43)

from which we describe the frequency and active power dynamics by

\[
\dot{x}_{\omega} = u_{\omega}, \quad \dot{x}_{P} = u_P
\]

(44)

where \( x_{\omega} = [\omega_1, \ldots, \omega_n]^T \), \( x_P = [m_{p_1} P_1, \ldots, m_{p_n} P_n]^T \), \( u_{\omega} = [u_{\omega_1}, \ldots, u_{\omega_n}]^T \) and \( u_P = [u_{P_1}, \ldots, u_{P_n}]^T \).

Appendix B

Parameters of MG Test System

| Parameters of the MG Test System |
|----------------------------------|
| DG1 | DG2 | DG3 & DG4 |
| DG power ratings | 40kW, 30kVar | 27kW, 20kVar | 20kW, 15kVar |
| \( m_P \) | 6.28 \times 10^{-5} | 9.42 \times 10^{-5} | 12.56 \times 10^{-5} |
| \( n_Q \) | 0.5 \times 10^{-3} | 0.75 \times 10^{-3} | 1 \times 10^{-3} |
| \( R_f \) | 0.1 \Omega | 0.1 \Omega | 0.1 \Omega |
| \( L_f \) | 1.35 mH | 1.35 mH | 1.35 mH |
| \( C_f \) | 47\mu F | 47\mu F | 47\mu F |
| DGs | | |
| \( R_e \) | 0.02 \Omega | 0.02 \Omega | 0.02 \Omega |
| \( L_c \) | 2 mH | 2 mH | 2 mH |
| \( K_{P_e} \) | 0.05 | 0.05 | 0.1 |
| \( K_{P_i} \) | 390 | 390 | 420 |
| \( K_{P_c} \) | 10.5 | 10.5 | 15 |
| \( K_{I_c} \) | 1.6 \times 10^4 | 1.6 \times 10^4 | 2 \times 10^3 |

Lines

| Lines | DG1 | DG2 | DG3 & DG4 |
|-------|-----|-----|-----------|
| Load1 | R = 0.23 \Omega, L = 318 \mu H | | |
| Load2 | R = 0.35 \Omega, L = 1847 \mu H | | |
| Load3 | R = 0.23 \Omega, L = 318 \mu H | | |
| Load4 | R = 0.23 \Omega, L = 318 \mu H | | |

RL Loads

| RL Loads | DG1 | DG2 | DG3 & DG4 |
|----------|-----|-----|-----------|
| Load1 | R = 4 \Omega, L = 9.6 mH | | |
| Load2 | R = 8 \Omega, L = 12.8 mH | | |
| Load3 | R = 12 \Omega, L = 25.6 mH | | |
| Load4 | R = 12 \Omega, L = 25.6 mH | | |

References

[1] 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.

[2] A. Teixeira, L. Shames, H. Sandberg, and K. H. Johansson, “A secure control framework for resource-limited adversaries,” Automatica, vol. 51, pp. 135–148, Jan. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0005109814004488

[3] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, “Resilient Control of Networked Control System Under DoS Attacks: A Unified Game Approach,” IEEE Transactions on Industrial Informatics, vol. 12, no. 5, pp. 1786–1794, Oct. 2016.

[4] Q. Sun, K. Zhang, and Y. Shi, “Resilient Model Predictive Control of Cyber–Physical Systems Under DoS Attacks,” IEEE Transactions on Industrial Informatics, vol. 16, no. 7, pp. 4920–4927, Jul. 2020.

[5] Y. Sun and G. Yang, “Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks,” International Journal of Robust and Nonlinear Control, vol. 29, no. 14, pp. 4797–4811, Sep. 2019. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/rnc.4654

[6] S. Feng and P. Tesi, “Resilient control under Denial-of-Service: Robust design,” Automatica, vol. 79, pp. 42–51, May 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0005109817300419

[7] Z. Feng, G. Wen, and G. Hu, “Distributed secure coordinated control for multiagent systems under adversarial attacks,” IEEE Transactions on Cybernetics, vol. 47, no. 5, pp. 1273–1284, 2016.

[8] Q. Zhu and T. Basar, “Game-Theoretic Methods for Robustness, Security, and Resilience of Cyber-Physical Control Systems: Games-in-Games Principle for Optimal Cross-Layer Resilient Control Systems,” IEEE Control Systems Magazine, vol. 35, no. 1, pp. 46–65, Feb. 2015.

[9] H. Zhang, P. Cheng, L. Shi, and J. Chen, “Optimal Denial-of-Service Attack Scheduling With Energy Constraint,” IEEE Transactions on Automatic Control, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.

[10] B. Chen, D. W. Ho, G. Hu, and L. Yu, “Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks,” IEEE transactions on cybernetics, vol. 48, no. 6, pp. 1862–1876, 2017.

[11] M. Zhu and S. Martinez, “On the Performance Analysis of Resilient Networked Control Systems Under Replay Attacks,” IEEE Transactions on Automatic Control, vol. 59, no. 3, pp. 804–808, Mar. 2014.
