IEEE Control Systems Letters paper presented at
2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

# Data-driven Event-triggered Bipartite Consensus for Multi-agent Systems Preventing DoS Attacks

Huarong Zhao, Jinjun Shan, Li Peng, Hongnian Yu

***Abstract*— This paper considers event-triggered bipartite consensus issues for discrete-time nonlinear networked multi-agent systems with antagonistic interactions and denial-of-service (DoS) attacks. Firstly, a pseudo partial derivative technology is applied to obtain an equivalent dynamic linearization model of the controlled system. The signed graph theory is employed to analyze the coopetition relationships among agents. Next, a distributed combined measurement error function is formulated to transform the bipartite consensus issue into a consensus issue. Then, an output predictive compensation scheme is proposed to offset the influence of DoS attacks. Furthermore, a dead-zone operator is designed to improve the flexibility of the proposed event-triggered mechanism. Additionally, a data-driven event-triggered resilient bipartite consensus scheme is formulated. Then, the convergence of the proposed method is strictly proved by using the Lyapunov theory and the contraction mapping principle, which indicates that the bipartite consensus error could be cut to a small region around zero. Finally, hardware tasks are conducted to verify the effectiveness of the proposed method.**

## I. Introduction

With information theory and technology development, cooperative control of networked multi-agent systems (NMASs) has received considerable attention in recent years. Massive applications exist for NMASs, for instance, satellite formation, intelligent transport systems, and so forth. However, most agents are often based on microprocessors or weak data-processing computers in practical industrial processing. The communication limitations and energy efficiency issues must be addressed, especially for larger-scale NMASs. Fortunately, the event-triggered (ET) scheme [1] is one of the useful schemes for the above issues, effectively reducing the computation and communication burden of NMASs with satisfactory control performance. The ET control was first introduced into NMASs by Dimarogonas et al. [2], which has inspired many useful researches. For example, Zhao et al. [3] designed a fully distributed edge-based ET method, Liang et al. [4] studied a neural-network-based ET method, and some meaningful results can be found in [5].

Nevertheless, most previous ET algorithms for NMASs may not properly function when attackers invade some agents or communication channels. So far, few results focus on ET consensus control for NMASs under the cyber-attack influence. Moreover, the openness of NMASs makes them vulnerable and makes it easier to be attacked. Generally, cyber-attacks mainly include denial-of-service (DoS) attacks, false data injection attacks, and deception attacks. Zhang et al. [6] investigated the intermittently random DoS attack issue for linear NMASs and formulated a resilient ET controller. Nonlinear NMASs subjected to DoS attacks to perform ET consensus control were studied by Shang et al. [7]. Besides, Guo et al. [8] proposed an ET cluster consensus method for heterogeneous NMASs with DoS attacks. Moreover, more details about cyber-attacks can be found in [9], [10].

The efforts mentioned above usually assume that the dynamic models of controlled plants are available. However, nonlinearity and uncertainty are inevitable in practical systems. The errors of modeling or identification are ubiquitous and cause the aforementioned model-based approaches to be hardly applied to practical NMASs. To address this problem, data-driven control approaches have attracted much attention from scholars, including iterative learning, reinforcement learning, model-free adaptive control (MFAC), and so forth. It is noteworthy that MFAC is a helpful approach to cope with the issue of discrete-time nonlinear systems with unknown dynamics models, which was studied for a single nonlinear system by Hou et al. [11]. After that, the cyber-attack and ET issues for a single plant were studied by Qiu et al. [12] and Lin et al. [13], respectively. An output-dependent perturbation issue was investigated by Corradini [14]. It is noticed that the results for NMASs based on MFAC are still open, although Bu et al. [15] proposed an MFAC framework for NMASs, the communication delay was investigated by Zhang et al. [16], and a distributed MFAC strategy for NMASs with DoS attacks was designed by Ma et al. [17]. Notably, ET and DoS attack issues were considered in [13] and [17], respectively. However, the method in [13] is only suitable for a single controlled system, and [17] did not consider the communication bandwidth issues of NMASs. Hence, designing a data-driven ET mechanism for NMASs under cyber attacks is meaningful work.

Furthermore, the research above on NMASs only considered the cooperative interactions among agents. However, cooperative and competitive are coexistent. For example, in a game, a player needs to collaborate with his teammates

This work was supported by the Fundamental Research Funds for the Central Universities (JUSRP123061), 111 project (B23008), the Natural Science Research Project of Higher Education in Jiangsu Province under Grant (18KJB413009), and a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC). (Corresponding author: Jinjun Shan)

Huarong Zhao and Li Peng are with Engineering Research Center of Internet of Things Applications Ministry of Education, Jiangnan University, Wuxi, Jiangsu 214122, China. (e-mail: hrzhao@jiangnan.edu.cn; pengli@jiangnan.edu.cn).

Jinjun Shan is with the Department of Earth and Space Science and Engineering, York University, Toronto, ON M3J 1P3, Canada (e-mail: jjshan@yorku.ca).

Hongnian Yu is with School of Computing, Engineering and the Built Environment, Edinburgh Napier University, EH10 5DT, Edinburgh, UK (e-mail: H.Yu@napier.ac.uk).

and antagonize others from the opposite team. Therefore, it is unreasonable to ignore the competitive relationships among agents when designing an algorithm for NMASs. Recently, a signed graph was studied for analyzing the relationships among agents by Altafini [18], and a bipartite consensus algorithm was proposed, where the agents are divided into two groups with opposite tracking objects. After that, several meaningful results were investigated. A bipartite consensus scheme was proposed for multi-robot systems with data quantization in [19]. A bipartite consensus method for NMASs was studied in [20]. Moreover, several efforts were made for data-driven bipartite consensus [21]–[23]. However, in MFAC framework, the relevant study of competitive relationship among MASs is still in its infancy.

This article considers nonlinear NMASs under coopetition interactions and successive DoS attacks to realize the ET bipartite consensus tasks. The main contributions of this paper are: (i) Propose an output predictive compensation scheme. Compared with the method in [17], the proposed output predictive compensation scheme can effectively offset the effects of successive DoS attacks; (ii) Establish a dead-zone-based operator ET strategy. Compared with the method in [13], the proposed ET strategy can adjust the number of ET to balance the performances and costs; (iii) Propose a data-driven ET resilient bipartite consensus (ET-RBC) method. Compared with the methods in [7]–[9], the proposed ET-RBC further considers the antagonistic interactions among agents and does not require the dynamics models.

The remainder of this paper is listed: Section II presents the signed graph theory and controlled systems. The proposed ET-RBC and analyses of its convergence property rigorously are given in Section III. The hardware tests and conclusions are given in Sections IV and V, respectively.

## II. Preliminary and Problem Formulation

### A. Signed Graph Theory

This paper considers a signed graph $\bar{G} = (\bar{V}, E, A)$ to describe the communication topology of NMASs, where $\bar{V} = \{0\} \cup V$ with $V = \{1, \cdots, N\}$, $E = \{(i,j)|i,j \in V\} \subseteq V \times V$, and $A = [a_{ij}] \in \mathbb{R}^{N\times N}$ with $a_{ij} \in \{-1, 0, 1\}$ denote the set of nodes, the set of edges, and the weighted adjacency matrix, respectively. The neighbor set of node $i$ is expressed by $N_i = \{j \in V|(j,i) \in E\}$, and the degree matrix of $\bar{G}$ is expressed by $D = \text{diag}\{d_1, \cdots, d_N\}$ with $d_i = \sum_{j\in N_i} |a_{ij}|$. $L = -A + D$ is the Laplacian matrix of $\bar{G}$. The virtual leader is expressed by node 0. Here, matrix $B = \text{diag}\{b_1, \cdots, b_N\}$ with $b_i \in \{0, 1\}$ is employed to describe the connection relationships between the virtual leader and each agent. If the virtual leader is directly connected with agent $i$, $b_i = 1$; otherwise, $b_i = 0$. In addition, $\bar{G}$ is also called as structurally balanced, where nodes of $\bar{G}$ are divided into two subsets $V_1$ and $V_2$, satisfying: (i) $V_1 \cup V_2 = V$ and $V_1 \cap V_2 = \emptyset$; (ii) If $\forall i, j \in V_z$ with $z \in \{1, 2\}$, $a_{ij} \in \{0, 1\}$; (iii) If $\forall i \in V_z$ and $j \in V_q$ with $z \neq q(z, q \in \{1, 2\})$, $a_{ij} \in \{-1, 0\}$. If $(j,i) \notin E$ or $i = j$, $a_{ij} = 0$. Moreover, $s = \text{diag}(s_1, \cdots, s_N)$ is the grouping matrix. If agent $i \in V_1$, $s_i = 1$. Otherwise, $s_i = -1$.

### B. System Descriptions

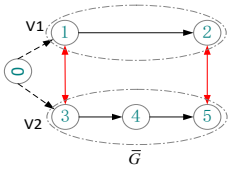



Fig. 1. Communication topologies of NMASs.

Consider the nonlinear NMASs, which consist of $N$ agents and a virtual leader, where the control input $u_i(k) \in \mathbb{R}$ and the control output $y_i(k) \in \mathbb{R}$ satisfy

$$y_i(k+1) = f_i(y_i(k), \cdots, y_i(k-n_y), u_i(k), \cdots, u_i(k-n_u)) \quad (1)$$

where $n_y \in \mathbb{Z}^+$, $n_u \in \mathbb{Z}^+$, and $f_i(\cdot)$ represents an unknown nonlinear function. All agents are connected by applying the internet, and all components are synchronous. The communication topology of NMASs satisfies the definition of graph $\bar{G} = (\bar{V}, E, A)$, which is defined in Section II-A, as shown in Fig. 1, where the data flow along the path with the arrows. The red arrow indicates that the connected agents' interactions are antagonistic with the negative weight, "$-1$", while the black one denotes the collaborative interactions with positive weight, "1". Moreover, constraints of the NMASs are presented below, which are critical requirements of MFAC theories.

*Assumption 1:* The partial derivative of $f_i(\cdot)$ concerning $u_i(k)$ exists and is continuous.

*Assumption 2:* The generalized Lipschitz condition applies to Eq. (1). Let $\Delta u_i(k) = u_i(k) - u_i(k-1) \neq 0$ and $\Delta y_i(k+1) = y_i(k+1) - y_i(k)$. If $\Delta u_i(k) \neq 0$, $|\Delta y_i(k+1)| \leq r|\Delta u_i(k)|$ with $r \in \mathbb{R}^+$.

*Remark 1:* Assumption 1 is a weak requirement when studying nonlinear systems. Assumption 2 implicates that both $u_i(k)$ and $y_i(k)$ of a practical plant are bounded, which is reasonable from the viewpoint of energy conservation [11].

*Lemma 1 ( [11]):* If Eq. (1) satisfies Assumptions 1 and 2, an equivalent dynamic linearization model can be structured:

$$\Delta y_i(k+1) = M_i(k) \Delta u_i(k) \quad (2)$$

where $M_i(k)$ is called as the pseudo-partial-derivative (PPD) parameter in the MFAC theory to describe the relationship between the input and output, which is time-varying. Moreover, there exits a constant $r$ leading to $|M_i(k)| \leq r$.

*Assumption 3 ( [24]):* $\bar{G}$ is strongly connected, where $L + B$ is an irreducible matrix with positive diagonal elements.

### C. The DoS Attack Descriptions

The DoS attack is a typical network attack that locks the communication channel and prevents agents from exchanging information. As same as several results [12], [17], the

success probability of the DoS attack is described as

$$\begin{cases} \text{Prob}\{\Lambda_i(k)=0\} = \text{E}\{\Lambda_i(k)\} = w \\ \text{Prob}\{\Lambda_i(k)=1\} = 1-\text{E}\{\Lambda_i(k)\} = 1-w \end{cases} \tag{3}$$

where $w \in (0,1)$, $\text{E}\{\Lambda_i(k)-w\}=0$, and $\text{E}\{(\Lambda_i(k)-w)^2\}=\sigma$ with $\sigma>0$. Here, a DoS attack model is established as

$$y_{attack_i}(k) = \Lambda_i(k) y_i(k)$$

where if agent $i$ is subjected to DoS attack, $\Lambda_i(k)=0$; otherwise, $\Lambda_i(k)=1$.

*Assumption 4 ( [17]):* The time of successive DoS attacks has a maximum upper bound $\bar{\Gamma} \in \mathbb{Z}^+$, that is, $0 \le \Gamma \le \bar{\Gamma}$.

To mitigate the effects of the attacks, an output compensation scheme is formulated as

$$y_{comp_i}(k) = (1-\Lambda_i(k)) y_i(k^* + \Gamma | k^*)$$

A signal $y_{ai}(k)$ consisting of the DoS attack and the output compensation is designed as

$$\begin{aligned} y_{ai}(k) &= y_{attack_i}(k) + y_{comp_i}(k) \\ &= \Lambda_i(k) y_i(k) + (1-\Lambda_i(k)) y_i(k^* + \Gamma | k^*) \end{aligned} \tag{4}$$

where $k^*$ denotes the last time instant that agent $i$ successfully escaped the DoS attack, $\Gamma$ stands for the times of the successive attacks, and $y_i(k^*+\Gamma|k^*)$ is designed later on.

The bipartite consensus error is defined as $e_i(k) = s_i y_r(k) - y_i(k)$, and this paper aims to guarantee that the NMASs realizes

$$\lim_{k\to\infty} e_i(k) = \lim_{k\to\infty} (s_i y_r(k) - y_i(k)) \le \upsilon, \ i \in V \tag{5}$$

where $y_r(k)$ denotes the ouput of the virtual leader, $\upsilon$ is an acceptable constant, and $s_i$ is given in Section II-A.

*Remark 2:* Since $\upsilon$ is not equal to zero, the NMASs finally realize bounded bipartite consensus. To facilitate the expression, we briefly name bounded bipartite consensus as bipartite consensus.

## III. ET-RBC Development and Analysis

Figure 2 shows an event generator and a compensator designed to realize ET control and mitigate the effects of the DoS attack, respectively, where all components of the controlled systems are synchronous.

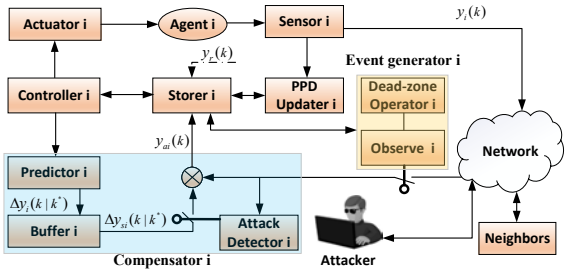



Fig. 2. The diagram of the proposed ET-RBC.

The output of controller $i$ will remind the same states during no ET processes and will update the states at the ET instant. The attack detector will monitor the information at the ET instant. If agent $i$ doesn't obtain the information from the communication network at the ET instant, attack detector $i$ will turn on the switch to make the compensator $i$ work and start to predict the missed data for agent $i$.

### A. Event-triggered PPD Estimation Mechanism

To relieve the computational burden of the controlled plants, an ET PPD estimation law is designed as

$$\hat{M}_i(k) = \begin{cases} \hat{M}_i(k-1) + \frac{\eta \Delta u_i(k-1)}{u+\Delta u_i^2(k-1)} (\Delta y_i(k) \\ \quad -\hat{M}_i(k-1)\Delta u_i(k-1)), & k=k_i \\ \hat{M}_i(k_i), & k_i < k < k_{i+1} \end{cases} \tag{6}$$

where $\hat{M}_i(k)$ is the estimation of $M_i(k)$, $k_i$ is the time-stamp of the last ET instant, $0<\eta<1$, and $u>0$. Besides, to enhance the estimate ability of Eq. (6), a reset law is defined:

$$\begin{aligned} \hat{M}_i(k) = \hat{M}_i(1), \text{ if } |\hat{M}_i(k)| \le \delta \text{ or } |\Delta u_i(k-1)| \le \delta \\ \text{or } \text{sign}(\hat{M}_i(k)) \ne \text{sign}(\hat{M}_i(1)) \end{aligned} \tag{7}$$

where $\hat{M}_i(1)$ is the initial condition of $\hat{M}_i(k)$. $\delta$ is a constant, which is often set as $10^{-3}$ or $10^{-4}$.

*Theorem 1:* If $\hat{M}_i(k)$ is adjusted by laws (6) and (7), there exist constants $\hat{r}$ and $\tilde{r}$, ensuring $|\hat{M}_i(k)| \le \hat{r}$ and $|\tilde{M}_i(k)| \le \tilde{r}$ with $\tilde{M}_i(k) = \hat{M}_i(k) - M_i(k)$.

*Proof:* **Case 1:** $k = k_i$. Here, Eq. (6) can be written as

$$\begin{aligned} \hat{M}_i(k) = \hat{M}_i(k-1) + (\Delta y_i(k) - \hat{M}_i(k-1)\Delta u_i(k-1)) \\ \times \eta \Delta u_i(k-1) / (u + \Delta u_i^2(k-1)) \end{aligned} \tag{8}$$

Then, according to Theorem 2 in [15], we obtain that $\hat{M}_i(k)$ and $\tilde{M}_i(k)$ are bounded.

**Case 2:** $k_i < k < k_{i+1}$. Here, Eq. (6) becomes that

$$\hat{M}_i(k) = \hat{M}_i(k_i) \tag{9}$$

The boundedness of $\hat{M}_i(k_i)$ ensures the boundedness of $\hat{M}_i(k)$. Moreover, since $M_i(k)$ is bounded, $\tilde{M}_i(k)$ is also bounded, and there exist constants $\hat{r}$ and $\tilde{r}$, satisfying $|\hat{M}_i(k)| \le \hat{r}$ and $|\tilde{M}_i(k)| \le \tilde{r}$, respectively. ■

### B. Output Predictive Compensation Mechanism

In this part, a gain predictive method is developed:

$$\Delta y_i(k^* + \Gamma | k^*) = \hat{M}_i(k^*) \Delta u_i(k^* + \Gamma - 1 | k^*) \tag{10}$$

$$\begin{aligned} y_i(k^* + \Gamma | k^*) = y_i(k^* + \Gamma - 1 | k^*) \\ + \Delta y_i(k^* + \Gamma | k^*) \end{aligned} \tag{11}$$

$$\Delta u_i(k^* + \Gamma | k^*) = H_i(k^*)(y_r(k^*+1) - y_i(k^* | k^*)) \tag{12}$$

where $H_i(k^*) = \rho_i \hat{M}_i(k^*) / (\lambda + \hat{M}_i^2(k^*))$, $0<\rho_i<1$, $\lambda>0$, $k^*+\Gamma = k \ge k^*$, $\Gamma$ stands for the number of the successive attacks, and $k^*$ represents the last time instant that the agent successfully escapes the DoS attack.

From Eqs. (10)-(12), an increment iterative compensation method is developed as

$$\begin{aligned} \Delta y_{si}(k^* + \Gamma | k^*) = \Delta y_{si}(k^* + \Gamma - 1 | k^*) \\ + \Delta y_i(k^* + \Gamma | k^*) \end{aligned} \tag{13}$$

where $\Delta y_{si}(k^*+1|k^*) = \Delta y_i(k^*+1|k^*)$.

*Theorem 2:* Using Eq. (11), Eq. (13), and Assumption 2, it yields that $\Delta y_{si}(k|k^*)$ is bounded for $k = k^* + \Gamma > k^*$.

*Proof:* According to Eqs. (11), (13), and (15), we have

$$\begin{aligned}\Delta y_{si}(k|k^*) &= \Delta y_i(k^*+\Gamma|k^*) + \Delta y_{si}(k^*+\Gamma-1|k^*) \\ &= y_i(k^*+\Gamma|k^*) - y_i(k^*|k^*)\end{aligned} \tag{14}$$

From Assumption 2, it is known that $y_i(k^*+\Gamma|k^*)$ and $y_i(k^*|k^*)$ are bounded. Thus, it is known that $\Delta y_{si}(k|k^*)$ is bounded for $k > k^*$. ∎

After that, the output predictive compensation approach is proposed as

$$y_i(k^*|k) = \Delta y_{si}(k^*+\Gamma|k^*) + y_i(k^*-1) \tag{15}$$

where $y_i(k^*-1)$ is the output of agent $i$ at $k = k^*-1$. From Eq. (15), it is noted that historical data can be used to predict the lost data. Then, according to Assumption 2, Eq. (15), and Theorem 2, we obtain a bounded variate $r_i(k^*|k)$ leading to

$$y_i(k) = y_i(k^*|k) + r_i(k^*|k) \tag{16}$$

Substituting Eq. (16) into Eq. (4), it yields that

$$y_{ai}(k) = y_i(k) - (1-\Lambda_i(k))\Delta_i(k) \tag{17}$$

where $\Delta_i(k) = \Delta y_{si}(k-1|k^*) + y_i(k^*-1) - y_i(k-1|k^*) + r_i(k^*|k) \leq \bar{\Delta}$ since of Theorem 2.

### C. Observer-based event-triggered mechanism

Here, an observer is designed:

$$\hat{y}_{ai}(k+1) = \hat{y}_{ai}(k) + \hat{M}_i(k)\Delta u_i(k) + x\breve{\varepsilon}_{yi}(k) \tag{18}$$

where $\breve{\varepsilon}_{yi}(k) = \hat{y}_{ai}(k) - y_{ai}(k)$, $\hat{M}_p(k)$ is defined in Eq. (6), and $y_{ai}(k)$ is defined in Eq. (4). $\hat{y}_{ai}(k)$ and $x$ are the output and the feedback gain of the observer, respectively. The observer error and the input gain error are formulated:

$$\varepsilon_{yi}(k) = \hat{y}_{ai}(k) - \breve{y}_i(k) \tag{19}$$

$$\varepsilon_{\Delta i}(k) = \Delta u_i(k) - \Delta\breve{u}_i(k) \tag{20}$$

where $\breve{y}_i(k) = y_i(k_i)$ and $\Delta\breve{u}_i(k) = \Delta u_i(k_i)$, $k_i \leq k < k_{i+1}$. Then, an ET condition is developed:

$$\Theta(|\varepsilon_{\Delta i}(k)|) > \sqrt{\frac{\theta(1-4(1+x)^2)}{4\hat{r}^2}}|\varepsilon_{yi}(k)| \text{ or } k-k_i \geq r_k \tag{21}$$

where $\theta \in (0,1)$, $r_k \in \mathbb{Z}^+$, $x \in (-1.5,\ -0.5)$, and $\hat{r}$ is the upper bound of $\hat{M}_i(k)$, obtained by experiments. Moreover, $\Theta(\cdot)$ stands for the dead-zone operator structured:

$$\Theta(|\varepsilon_{\Delta i}(k)|) = \begin{cases} |\varepsilon_{\Delta i}(k)|, & |\varepsilon_{yi}(k)| > \tau \\ 0, & \text{otherwise} \end{cases} \tag{22}$$

where $\tau$ is the bound of $\varepsilon_{yi}(k)$, which is derived later on.

*Remark 3:* Eq. (21) includes two different ET conditions. The second condition, $k-k_i \geq r_k$, is rarely developed, where the operator can adjust $r_k$ to monitor whether there are faults in the controlled plant. Moreover, from Eq. (22), it is noted that during the process that $|\varepsilon_{yi}(k)| \leqslant \tau$, whatever happened the event will not be triggered. The parameter $\tau$ of the dead-zone operator can be adjusted to reduce the number of ET to balance the product features and costs and can overcome a Zeno-like behavior of discrete-time systems [25].

*Theorem 3:* If system (1) is restrained by Assumptions 1-2, $M_i(k)$ is obtained by laws (6)-(7), and the ET conditions obey Eqs. (21)-(22), the observer error $\varepsilon_{yi}(k)$ is bounded.

*Proof:* According to Eqs. (2), (18), and (19), it yields

$$\begin{aligned}\varepsilon_{yi}(k+1) = (1+x)\varepsilon_{yi}(k) + \hat{M}_i(k)\varepsilon_{\Delta i}(k) \\ + x(\breve{y}_i(k) - y_{ai}(k))\end{aligned} \tag{23}$$

Then, a Lyapunov function is structured as

$$V_i(k+1) = \varepsilon_{yi}^2(k+1) \tag{24}$$

and analyze the two different situations below.

**Case 1:** $k = k_i$. Here, applying Eq. (20), it yields that $\varepsilon_{\Delta i}(k)=0$ and $\breve{y}_i(k)=y_i(k)$. Applying Eqs. (17), (18), and (23), it yields

$$\begin{aligned}\varepsilon_{yi}(k+1) = (1+x)\varepsilon_{yi}(k) + x(w-\Lambda_i(k))\Delta_i(k) \\ + x(1-w)\Delta_i(k)\end{aligned} \tag{25}$$

Using Eq. (3), Eq (17), Eq. (25), and Young's inequality, the expectation of $\Delta V_i(k+1) = V_i(k+1) - V_i(k)$ is obtained:

$$\begin{aligned}\mathrm{E}\{\Delta V_i(k+1)\} \leq -(1-2(1+x)^2)\varepsilon_{yi}^2(k) \\ + 2x^2(1-w)^2\bar{\Delta}^2 + x^2\sigma^2\bar{\Delta}^2\end{aligned} \tag{26}$$

If $|\varepsilon_{yi}(k)| > \sqrt{(\sigma+2(1-w)^2)x^2\bar{\Delta}^2/(1-2(1+x)^2)} = \tau$, we have $\mathrm{E}\{\Delta V_i(k+1)\} < 0$, and we obtain that

$$-(\sqrt{2}+2)/2 < x < (\sqrt{2}-2)/2 \tag{27}$$

**Case 2:** $k_i < k < k_{i+1}$. Here, Eq. (25) becomes

$$\begin{aligned}\varepsilon_{yi}(k+1) \leq (1+x)\varepsilon_{yi}(k) + \hat{M}_i(k)\varepsilon_{\Delta i}(k) + x\Omega \\ + x(w-\Lambda_i(k))\Delta_i(k) + x(1-w)\Delta_i(k)\end{aligned} \tag{28}$$

where $\Omega \geq |y_i(k_i) - y_i(k)|$. Eq. (26) becomes

$$\begin{aligned}\mathrm{E}\{\Delta V_i(k+1)\} \leq -(1-4(1+x)^2)\varepsilon_{yi}^2(k) \\ + 4\hat{r}^2\varepsilon_{\Delta i}^2(k) + H_1\end{aligned} \tag{29}$$

where $H_1 \geq 4x^2\Omega^2 4x^2 + (1-w)^2\bar{\Delta}^2 + x^2\sigma^2\bar{\Delta}^2$. According to Eq. (21), Eq. (29) can be rewritten as

$$\begin{aligned}&\mathrm{E}\{\Delta V_i(k+1)\} \\ &\quad\leq -(1-\theta)(1-4(1+x)^2)V_i(k) + H_1\end{aligned} \tag{30}$$

According to $\theta \in (0,1)$ and $x \in (-1.5,\ -0.5)$, we can obtain that $0 < (1-\theta)(1-4(1+x)^2) < 1$. Thus, applying Eq. (30) yields that $\varepsilon_{yi}(k)$ is bounded. ∎

*Remark 4:* From Eq. (29), it is found that if $|\varepsilon_{yi}(k)| > \sqrt{(\sigma+2(1-w)^2)x^2\bar{\Delta}^2/(1-2(1+x)^2)} = \tau$, it yields that $\mathrm{E}\{\Delta V_i(k+1)\} < 0$, that is, if the observer error $\varepsilon_{yi}(k)$ exceeds $\tau$, $\varepsilon_{yi}(k)$ will be declined to less than $\tau$. Hence, the operator can adjust $\tau$ to obtain a corresponding $\varepsilon_{yi}(k)$.

### D. ET-RBC Controller Design

A distributed combined measurement error function of agent $i$ is structured:

$$\begin{aligned}\zeta_i(k) = &\sum_{j\in N_i}((a_{ij})\hat{y}_{aj}(k) - |a_{ij}|\hat{y}_{ai}(k)) \\ &+ b_i(s_i y_r(k) - \hat{y}_{ai}(k))\end{aligned} \tag{31}$$

where $s_i$ and $b_i$ are presented in Section II-A, and $\hat{y}_{ai}(k)$ is defined in Eq. (18). Then, the ET-RBC controller is structured:

$$\Delta u_i(k) = \begin{cases} \rho_i \hat{M}_i(k)\zeta_i(k)/(\lambda + \hat{M}_i^2(k)), k = k_i \\ \Delta u_i(k_i), \qquad\qquad\qquad k_i < k < k_{i+1} \end{cases} \tag{32}$$

where $u_i(k) = \Delta u_i(k) + u_i(k-1)$, $0 < \rho_i \leq 1$, $\lambda > r^2/4$, $\hat{M}_i(k)$ is designed in Eq. (6), and $r$ is the controlled system inherent property discussed in Assumption 2.

*Remark 5:* It is noted that Eq. (31) successfully transfers the bipartite consensus issues to traditional consensus issues. Moreover, only local information from the network is employed, so Eq. (32) is a distributed ET scheme that can reduce computation costs.

*Lemma 2 ( [18]):* If $J(\phi)$ stands for a time-varying irreducible substochastic matrix with positive diagonal entries, $0 < \|J(\phi)J(\phi-1)\cdots J(1)\| \leq U < 1$ holds for all $\phi \in \mathbb{Z}^+$.

*Theorem 4:* When NMASs (1) are subjected to the DoS attacks, restricted by Assumptions 1-4 and ET conditions (21)-(22), and governed by the proposed ET-RBC (32) with the output compensation method (10)-(15) to conduct bipartite consensus tasks, the bipartite consensus error of the NMASs is bounded under the condition $\rho_i < 1/(d_i + b_i)$.

*Proof:* The following cases should be analyzed to prove the boundedness of the bipartite consensus error.

**Case 1:** $k_i < k < k_{i+1}$. Here, from Eqs. (18) and (19), it is found that the observer error increases since $\hat{y}_{ai}(k)$ increases during the no ET processes. If the observer error increases to exceed $\tau$, the controlled system will enter the ET processes. Hence, only the case $k = k_i$ needs to be analyzed.

**Case 2:** $k = k_i$. Here, let $\hat{e}_{ai}(k) = s_i y_r(k) - \hat{y}_{ai}(k)$. Then, applying Eq. (18) yields

$$\hat{e}_{ai}(k+1) = \hat{e}_{ai}(k) - \hat{M}_i(k)\Delta u_i(k) - x\breve{\varepsilon}_{yi}(k) \tag{33}$$

Meanwhile, Eq. (31) becomes

$$\zeta_i(k) = \sum_{j\in N_i}(a_{ij}\hat{e}_{ai}(k) - |a_{ij}|\hat{e}_{aj}(k)) + b_i\hat{e}_{ai}(k) \tag{34}$$

Then, let $\hat{e}_a(k) = [\hat{e}_{a1}(k), ..., \hat{e}_{aN}(k)]^T$, $\zeta(k) = [\zeta_1(k), ..., \zeta_N(k)]^T$, and $\breve{\varepsilon}_y(k) = [\breve{\varepsilon}_{y1}(k), ..., \breve{\varepsilon}_{yN}(k)]^T$. From Eqs. (2) and (34), Eq. (33) becomes

$$\begin{aligned}\hat{e}_a(k+1) &= \hat{e}_a(k) - \rho H(k)(L+B)\hat{e}_a(k) - x\breve{\varepsilon}_y(k) \\ &= (I - \rho\Psi(k))\hat{e}_a(k) - x\breve{\varepsilon}_y(k)\end{aligned} \tag{35}$$

where $H(k)$=diag$(H_1(k), ..., H_N(k))$, $\rho$=diag$(\rho_1, ..., \rho_N)$, $0 < H_i(k) = \hat{M}_i(k)\hat{M}_i(k)/(\lambda + \hat{M}_i^2(k)) < 1$, and $\Psi(k)$=$H(k)(L+B)$. Then, from Eqs. (17), (19), we have

$$\breve{\varepsilon}_{yi}(k) = \varepsilon_{yi}(k) + (1 - \Lambda_i(k))\Delta_i(k) \tag{36}$$

**Case 2.1:** ET and DoS attacks. Here, $\Lambda_i(k) = 0$. Applying Eq. (36) yields that $\breve{\varepsilon}_{yi}(k)$=$\varepsilon_{yi}(k) + \Delta_i(k)$. $\breve{\varepsilon}_{yi}(k)$ is bounded since $|\varepsilon_{yi}(k)| \leqslant \tau$ and $|\Delta_i(k)| \leqslant \bar{\Delta}$.

**Case 2.2:** ET and no DoS attacks. Here, $\Lambda_i(k) = 1$. Applying Eq. (36) yields that $\breve{\varepsilon}_{yi}(k)$=$\varepsilon_{yi}(k)$, and $\breve{\varepsilon}_{yi}(k)$ is bounded since $|\varepsilon_{yi}(k)| \leq \tau$.

To sum up, there exists a constant $\Omega$ satisfying $\|x\breve{\varepsilon}_y(k)\| \leq \Omega \in \mathbb{R}^+$. Moreover, since the graph $\bar{G}$ of the controlled NMASs is strongly connected, $\rho_i < 1/(d_i + b_i)$, and $0 < H_i(k) < 1$, we obtain that $I - \rho\Psi(k)$ satisfies the condition of Lemma 2 that $I - \rho\Psi(k)$ is an irreducible substochasitc matrix. Hence, taking norm from both sides of Eq. (35) and according to Lemma 2, we obtain that

$$\lim_{k\to\infty} ||\hat{e}_a(k+1)|| \leqslant \Omega/(1-U) \tag{37}$$

where the details about Eq. (37) can be found in Theorems 3 and 4 of references [15], [21]. According to Eq. (5) and $\hat{e}_{ai}(k) = s_i y_r(k) - \hat{y}_{ai}(k)$, we obtain that

$$e_i(k) = \hat{e}_{ai}(k) + \varepsilon_{yi}(k) \tag{38}$$

Then, from Theorem 3, Eq. (37), and Eq. (38), we obtain that the bipartite consensus error $e_i(k)$ is bounded. ■

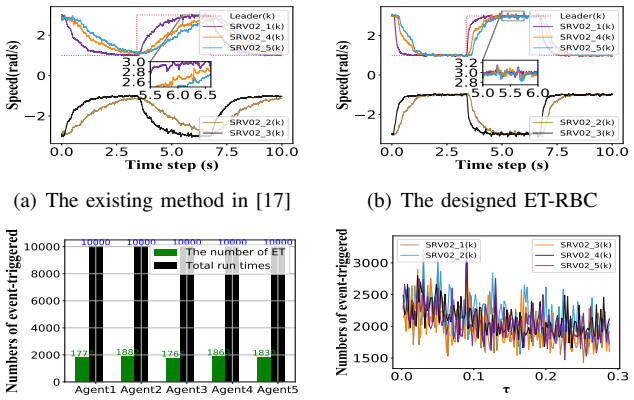
*Remark 6:* From Eq. (38), it is found that the upper bound of $e_i(k)$ is affected by $\hat{e}_{ai}(k)$ and $\varepsilon_{yi}(k)$. $\lim_{k\to\infty} ||\hat{e}_a(k)|| \leqslant \Omega/(1-U)$, where $\Omega/(1-U)$ is a constant. $\lim_{k\to\infty} |\varepsilon_{yi}(k)| \leqslant \tau$, where the operator can adjust $\tau$. Hence, the upper bound of $e_i(k)$ can be adjusted by the operator.

## IV. Experimental Results

In this section, a hardware platform consisting of five Quanser SRV02 units, three Q2-USB data acquisition devices, and five VoltPAQ-X1 amplifiers, as shown in Fig. 3, is established to verify the effectiveness of the proposed ET-RBC. Here, Quanser's QUARC and MATLAB/Simulink are employed as the code editor for the proposed ET-RBC, where the sampling time is 1ms, and the SRV02 units are connected as shown in Fig. 1. Moreover, the initial conditions are configured as $y_1(1) = y_4(1) = y_5(1) = 3$ rad/s and $y_2(1) = y_3(1) = -3$ rad/s. Furthermore, the parameters are configured as $\hat{M}_i(1) = 2$, $x = -1$, $\sigma = 0.5$, $\bar{\Delta} = 0.5$ $\rho_i = 0.2$, $\eta = 0.6$, $u = 0.5$, $\lambda = 1$, $\delta$=$10^{-3}$, $\theta = 0.01$, $\hat{r} = 35$, and $w = 0.8$. The objective speed is configured as $y_r(k) = 2 - (-1)^{\text{round}(3k/10000)}$ rad/s.

The performances of five SRV02 units shown in Fig. 4(a) are worse than that of five SRV02 units shown in Fig. 4(b). It demonstrates that the DoS attacks affect the performance of the existing MFAC [20]. However, the proposed ET-RBC effectively mitigates the effects of the DoS attacks. Moreover, the numbers of ET of SRV02 units are 1777, 1882, 1766, 1863, and 1839, which means that the proposed ET-RBC reduces about 81.7% communication energy for governing the SRV02 units under DoS attacks to perform bipartite consensus tasks. Besides, from the configurations of the parameters, it is obtained that the definitional domain of $\tau$ is [0, 0.29]. Then, the results are shown in Fig. 4(d). Here, as $\tau$ increases, the number of ET decreases, that is, the operator can adjust $\tau$ to balance the performances and costs.


Fig. 3. Experimental system with five SRV02.




(a) The existing method in [17]

(b) The designed ET-RBC

(c) Numbers of event-triggered

(d) Different values of $\tau$

Fig. 4. Performances of five SRV02 with DoS attacks.

## V. Conclusions

This paper has developed a data-driven ET resilient bipartite consensus approach for nonlinear NMASs under DoS attacks and coopetition interactions. Sufficient conditions of the designed method have been derived. The hardware tests have been conducted, where the proposed scheme effectively reduces communication resources and offsets the effects of DoS attacks. Moreover, the operator can flexibly adjust the number of ET to balance the performances and costs. In future studies, the reduction of the effects of unknown disturbances and time delays will be further considered.

## References


[1] F. Yang, X. Liang, and X. Guan, "Resilient distributed economic dispatch of a cyber-power system under dos attack," *Frontiers of Information Technology & Electronic Engineering*, vol. 22, no. 1, pp. 40–50, 2021.

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

[3] H. Zhao, X. Meng, and S. Wu, "Distributed edge-based event-triggered coordination control for multi-agent systems," *Automatica*, vol. 132, p. 109797, 2021.

[4] H. Liang, G. Liu, H. Zhang, and T. Huang, "Neural-network-based event-triggered adaptive control of nonaffine nonlinear multiagent systems with dynamic uncertainties," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 5, pp. 2239–2250, 2020.

[5] L. Ding, Q.-L. Han, X. Ge, and X.-M. Zhang, "An overview of recent advances in event-triggered consensus of multiagent systems," *IEEE Transactions on Cybernetics*, vol. 48, no. 4, pp. 1110–1123, 2017.

[6] T.-Y. Zhang and D. Ye, "Distributed event-triggered control for multi-agent systems under intermittently random denial-of-service attacks," *Information Sciences*, vol. 542, pp. 380–390, 2021.

[7] Y. Shang, C.-L. Liu, and K.-C. Cao, "Event-triggered consensus control of second-order nonlinear multi-agent systems under denial-of-service attacks," *Transactions of the Institute of Measurement and Control*, vol. 43, no. 10, pp. 2272–2281, 2021.

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

[9] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 319–333, 2021.

[10] Y. Xie, S. Ding, F. Yang, L. Wang, and X. Xie, "Probabilistic-constrained distributed set-membership estimation over sensor networks: A dynamic periodic event-triggered approach," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 6, pp. 4444–4457, 2022.

[11] Z. Hou and S. Xiong, "On model-free adaptive control and its stability analysis," *IEEE Transactions on Automatic Control*, vol. 64, no. 11, pp. 4555–4569, 2019.

[12] X. Qiu, Y. Wang, X. Xie, and H. Zhang, "Resilient model-free adaptive control for cyber-physical systems against jamming attack," *Neurocomputing*, vol. 413, pp. 422–430, 2020.

[13] N. Lin, R. Chi, and B. Huang, "Event-triggered model-free adaptive control," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 6, pp. 3358–3369, 2019.

[14] M. L. Corradini, "A robust sliding-mode based data-driven model-free adaptive controller," *IEEE Control Systems Letters*, vol. 6, pp. 421–427, 2021.

[15] X. Bu, Z. Hou, and H. Zhang, "Data-driven multiagent systems consensus tracking using model free adaptive control," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 5, pp. 1514–1524, 2017.

[16] J. Zhang, S.-C. Chai, B.-H. Zhang, and G.-P. Liu, "Distributed data-driven tracking control for networked nonlinear mimo multi-agent systems subject to communication delays," *Neurocomputing*, vol. 425, pp. 62–70, 2021.

[17] Y.-S. Ma, W.-W. Che, C. Deng, and Z.-G. Wu, "Distributed model-free adaptive control for learning nonlinear mass under dos attacks," *IEEE Transactions on Neural Networks and Learning Systems*, DOI 10.1109/TNNLS.2021.3104978, 2021.

[18] C. Altafini, "Consensus problems on networks with antagonistic interactions," *IEEE Transactions on Automatic Control*, vol. 58, no. 4, pp. 935–946, 2012.

[19] T.-F. Ding, M.-F. Ge, C.-H. Xiong, J. H. Park, and M. Li, "Second-order bipartite consensus for networked robotic systems with quantized-data interactions and time-varying transmission delays," *ISA Transactions*, vol. 108, pp. 178–187, 2021.

[20] Y. Chen, Z. Zuo, and Y. Wang, "Bipartite consensus for a network of wave pdes over a signed directed graph," *Automatica*, vol. 129, p. 109640, 2021.

[21] J. Liang, X. Bu, L. Cui, and Z. Hou, "Event-triggered asymmetric bipartite consensus tracking for nonlinear multi-agent systems based on model-free adaptive control," *IEEE/CAA Journal of Automatica Sinica*, DOI 10.1109/JAS.2022.106070, 2022.

[22] D. Liu, Z.-P. Zhou, and T.-S. Li, "Data-driven bipartite consensus tracking for nonlinear multiagent systems with prescribed performance," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, DOI 10.1109/TSMC.2022.3230504, 2023.

[23] H. Zhao, J. Shan, L. Peng, and H. Yu, "Learning-based robust bipartite consensus control for a class of multiagent systems," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 4, pp. 4068–4076, 2022.

[24] S. Yang, J.-X. Xu, and X. Li, "Iterative learning control with input sharing for multi-agent consensus tracking," *Systems & Control Letters*, vol. 94, pp. 97–106, 2016.

[25] D. Zhao, T. Dong, and W. Hu, "Event-triggered consensus of discrete time second-order multi-agent network," *International Journal of Control, Automation, and Systems*, vol. 16, no. 1, pp. 87–96, 2018.