SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

August 2026, Vol. 69, Iss. 8, 182204:1–182204:18
https://doi.org/10.1007/s11432-025-4895-2

Enhancing performance and cybersecurity resilience in ICSs 4.0: a reinforcement learning-driven intelligent control framework

Xiao CAI[1], Yanbin SUN[1*], Kaibo SHI[2], Chongwu DONG[1*], Huaicheng YAN[3] & Zhihong TIAN[1]

[1]*Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China*
[2]*School of Information Science and Engineering, Chengdu University, Chengdu 610106, China*
[3]*School of Information Science and Engineering, East China University of Science and Technology, Shanghai 200237, China*

Received 21 January 2025/Revised 23 June 2025/Accepted 4 July 2025/Published online 4 June 2026

Abstract Industrial control systems (ICSs) 4.0 increasingly rely on networked communications, making them vulnerable to cyber threats such as distributed denial-of-service (DDoS) attacks. These attacks can disrupt control signals and severely degrade system performance. This paper focuses on designing an adaptive control framework that jointly improves communication efficiency and ensures resilient system operation under such adversarial conditions. First, a reinforcement learning-supervised intelligent sampling (RLSIS) strategy is designed to dynamically adjust data transmission frequencies based on system state, reducing redundant communication while maintaining responsiveness. Additionally, a data quantization scheme is further integrated to compress transmitted data and alleviate network congestion. To defend against DDoS attacks, a hybrid detection mechanism and a controller restart strategy are developed to ensure timely recovery and sustained operation under attack conditions. These mechanisms ensure robust recovery of control signals, enabling uninterrupted system operation in critical applications. In addition, the stability of the proposed system is rigorously analyzed using the Lyapunov stability theory, providing a solid theoretical foundation for practical implementation. Finally, experimental validation is conducted using an industrial network-based unmanned marine vehicle (UMV) system under realistic conditions. The results demonstrate significant improvements in communication efficiency, control accuracy, and cybersecurity resilience, underscoring the potential of the proposed methods to advance ICSs 4.0 and offer effective solutions for complex industrial environments.

Keywords industrial control systems 4.0, Lyapunov-Krasovskii function, reinforcement learning, unmanned marine vehicle, cyber-attacks

Citation Cai X, Sun Y B, Shi K B, et al. Enhancing performance and cybersecurity resilience in ICSs 4.0: a reinforcement learning-driven intelligent control framework. Sci China Inf Sci, 2026, 69(8): 182204, https://doi.org/10.1007/s11432-025-4895-2

1 Introduction

Industrial control systems (ICSs) form the backbone of modern industrial production, enabling real-time monitoring, regulation, and optimization of critical processes to ensure stable and efficient operation of industrial equipment [1]. Traditional ICS architectures are predominantly centralized, with programmable logic controllers, distributed control systems, and industrial sensors serving as core hardware components. These systems operate as closed control networks, relying on proprietary communication protocols and physical isolation from external networks to ensure high reliability and robust security [2]. While this traditional design effectively minimizes external threats, it imposes significant limitations on scalability, interoperability, and adaptability. Consequently, conventional ICS architectures struggle to address the rapidly evolving demands of Industry 4.0, where flexibility, interconnectedness, and real-time data integration are critical [3].

In traditional ICSs, hardware and software operate based on fixed logic rules, executing pre-programmed control tasks [4]. While this architecture is highly effective for applications such as equipment operation, production line control, and field data acquisition, its limitations have become increasingly evident in modern industrial contexts. The lack of adaptability and flexibility restricts traditional ICSs from meeting the growing demands for real-time data analysis, dynamic optimization, and remote management [5]. Furthermore, these systems' isolated and closed nature significantly limits interconnectivity, making it challenging to address the complexities of dynamic production environments and the rapidly evolving requirements of competitive markets [6].

* Corresponding author (email: sunyanbin@gzhu.edu.cn, dongchongw@gzhu.edu.cn)

The advent of Industry 4.0 has driven the evolution of ICSs toward greater openness, intelligence, and interconnectivity, culminating in the emergence of ICSs 4.0. This next-generation system integrates advanced technologies into traditional industrial control frameworks, including the Internet of Things (IoT), artificial intelligence (AI), cloud computing, and big data analytics. This integration enables comprehensive digitization and automation of industrial processes [7]. ICSs 4.0 significantly enhances system flexibility and adaptability, allowing real-time adjustments to production processes to meet the dynamic demands of complex industrial environments [8]. Unlike the traditional model of physical isolation, ICSs 4.0 fosters seamless connectivity among diverse devices and subsystems, promoting the integration of information, control, and data flows [9]. By emphasizing real-time data acquisition, communication, and decision-making, ICSs 4.0 supports highly interconnected and automated industrial ecosystems. These advancements improve operational efficiency, enhance system responsiveness, and effectively address the challenges of modern industrial environments.

ICSs 4.0 increasingly rely on periodic sampling and high-frequency data transmission to maintain real-time performance and system reliability [10]. While effective in maintaining tight feedback control, this rigid communication scheme often leads to excessive data transmission during periods of system stability, where frequent updates provide little marginal value [11]. The resulting communication redundancy consumes valuable bandwidth resources and increases network congestion, posing serious challenges to the scalability, responsiveness, and energy efficiency of ICS networks [12]. To overcome these limitations, there is a pressing need for intelligent transmission strategies that can adapt to dynamic system conditions (transmitting only when needed) while still ensuring timely and accurate control actions.

Reinforcement learning (RL), with its ability to learn optimal decision policies through trial-and-error interaction with dynamic environments, offers a promising pathway toward adaptive sampling in ICSs [13]. Techniques such as Q-learning [14], deep Q-learning [15], and policy gradient methods [16] have demonstrated success in solving real-time optimization problems in uncertain control scenarios. For instance, Wang et al. [17] employed RL to improve tracking accuracy in unmanned surface vehicles without relying on precise system models, while other studies [18] have shown its effectiveness in handling unknown nonlinearities . In particular, recent advances have applied Q-learning to event-triggered control frameworks, enabling data-driven adaptive dynamic programming strategies that balance performance with communication efficiency in networked environments. These learning-based schemes allow the controller to intelligently decide when to sample and transmit, which is highly beneficial for bandwidth-constrained systems. However, most existing RL-based control strategies primarily focus on improving performance metrics such as tracking error or convergence speed, without considering the significant impact of real-time communication constraints. In addition, RL-driven adaptive sampling is rarely coupled with data compression mechanisms, such as quantization, which are essential for further reducing communication volume and network load.

To address this gap, this paper proposes an RL-supervised intelligent sampling (RLSIS) strategy that dynamically adjusts the sampling interval based on real-time variations in system state and network conditions [19]. By selectively transmitting critical information while suppressing unnecessary data during steady states, the RLSIS effectively reduces communication frequency without compromising control responsiveness. Furthermore, a data quantization mechanism is integrated into the framework to compress signal content, thereby minimizing data redundancy and alleviating bandwidth pressure [20,21]. This dual-layer design (targeting both transmission timing and data volume) enables finer-grained control over communication resources while preserving system stability and control accuracy. Compared to conventional fixed-rate sampling schemes, the proposed approach offers a more practical and scalable solution for modern ICSs operating in dynamic, resource-constrained, and security-sensitive environments.

The increasing reliance on communication networks exposes ICSs 4.0 to significant cybersecurity risks, as interconnected systems become more vulnerable to malicious intrusions [22–24]. Among these threats, distributed denial-of-service (DDoS) attacks are particularly challenging [25]. These attacks exploit multiple distributed sources to overwhelm communication networks with malicious requests, resulting in severe network congestion, delayed transmission of control signals, and potential system instability [26]. Such disruptions can lead to substantial operational consequences, including production stoppages, process errors, and safety-critical incidents [27]. While existing research primarily focuses on control strategies to manage systems during DDoS attacks, comprehensive mitigation solutions are often lacking [28], leaving critical vulnerabilities exposed [29]. To address these challenges, this paper proposes a hybrid detection mechanism and a controller restart strategy. These methods are designed to ensure robust recovery of control signals, enabling continuous and reliable system operation even under persistent attacks. By mitigating the adverse effects of DDoS attacks, the proposed approaches significantly enhance the cybersecurity resilience of ICSs 4.0, making them more robust for critical industrial applications. This controller-level solution also compensates for the limitations of existing passive or filter-based approaches, enabling active functional recovery even under severe resource exhaustion scenarios.

In summary, this paper addresses the critical challenges of communication efficiency, real-time control, and cybersecurity in ICSs 4.0. The proposed framework integrates an RLSIS strategy, a data quantization mechanism, and robust defenses against DDoS attacks, significantly enhancing the efficiency, stability, and security of ICSs 4.0 in complex and dynamic environments. The major contributions of this work are as follows.

(1) A dynamic RLSIS strategy is developed to optimize sampling frequency. This is complemented by an integrated data quantization mechanism that minimizes transmitted data while preserving critical information, thereby improving communication efficiency in bandwidth-constrained industrial networks.

(2) A hybrid detection and controller restart strategy is proposed to ensure timely recovery of control signals. This mechanism leverages behavioral anomalies in control signals to trigger lightweight recovery actions, ensuring timely and resilient restoration of control functionality during adversarial network conditions.

(3) Stability constraints for the proposed system are rigorously derived using Lyapunov-Krasovskii functionals (LKFs). Additionally, an explicit controller form is provided, offering theoretical guarantees for robust performance under adversarial conditions.

(4) Extensive simulations using an industrial network-based unmanned marine vehicle (UMV) system validate the proposed strategies. The results demonstrate significant improvements in communication efficiency, control accuracy, and resilience against cyber-attacks, highlighting the practical applicability of the framework.

Notations. $\mathbb{R}^n$ represents n-dimensional Euclidean space and $\mathbb{R}^{m\times n}$ represents the set of all $m\times n$ real matrices. $Q>0$ means Q is a positive definite and symmetric matrix. Define A^{-1} as the inverse of A and A^{T} as the transpose of A, respectively. I is an identity matrix of appropriate dimensions. $L_2[0,+\infty)$ refers to the space of square-summable infinite vector sequences. $\mathrm{He}\{Q\}=Q+Q^{\mathsf{T}}$ and $\mathrm{diag}\{\cdots\}_n$ denotes the block diagonal matrix.

2 Preliminaries

2.1 ICSs 4.0 model and UMV model

In this paper, the dynamics of the ICSs 4.0 model are described as follows:

$$\dot{x}(t)=\tilde{A}x(t)+\tilde{B}u(t)+\tilde{D}\omega(t), \tag{1}$$

where $x(t)$ is the system state vector, $u(t)$ represents the control input that may be subject to potential attacks, and $\omega(t)$ denotes external disturbances. The matrices $\tilde{A}$, $\tilde{B}$, and $\tilde{D}$ are constant system matrices defining the dynamics of the ICSs. Specifically, $\tilde{A}$ characterizes the internal behavior of the system, $\tilde{B}$ determines how the control input influences the system dynamics, and $\tilde{D}$, reflects the impact of external disturbances.

This subsection establishes the dynamic model of a UMV system within the context of an ICSs 4.0 framework [12,23]. The UMV is selected as a representative example due to its close alignment with the core characteristics of modern ICSs: it operates as a networked cyber-physical system where sensing, computation, and actuation are tightly integrated over an industrial communication network. This structure makes the UMV particularly suitable for examining key challenges in ICSs 4.0, such as maintaining control performance under communication constraints and ensuring resilience against cyber threats. Moreover, the UMV's continuous interaction with uncertain environments and its reliance on timely, high-fidelity data exchange reflect typical control demands in real-world industrial settings. As such, modeling the UMV system provides a meaningful testbed for evaluating the effectiveness of the proposed intelligent sampling strategy, data quantization scheme, and controller recovery mechanism. The mathematical formulation of the UMV's dynamics (capturing its motion in three degrees of freedom: surge, sway, and yaw) is given as follows (see Figure 1):

$$\mathcal{M}\dot{v}+\mathcal{N}v+\mathcal{G}\eta=u(t)+\omega(t),\ \dot{\eta}=P(\Phi(t))v, \tag{2}$$

where $v=[v_1(t)\ v_2(t)\ v_3(t)]^{\mathsf{T}}$ represents the body-fixed velocity vector, with v_1, v_2 and v_3 denoting the surge, sway, and yaw velocities, respectively. $\eta=[x_p(t)\ y_p(t)\ \Phi(t)]^{\mathsf{T}}$ is the earth-fixed orientation vector, where $x_p(t)$ and $y_p(t)$ represent the positional coordinates, and $\Phi(t)$ is the orientation angle. $u(t)=[u_1(t)\ u_2(t)\ u_3(t)]^{\mathsf{T}}$ denotes the control vector, with $u_1(t)$ and $u_2(t)$ being the surge and sway forces, respectively, and $u_3(t)$ representing the yaw moment generated by the thruster system. $\omega(t)$ represents external disturbances induced by environmental factors such as waves, winds, and currents. Moreover, $\mathcal{M}=\mathcal{M}^{\mathsf{T}}>0$ represents the inertia matrix, and $\mathcal{N}$ is the damping matrix. $\mathcal{G}=\mathrm{diag}\{g_{11},g_{22},g_{33}\}$ is the mooring matrix, and $P(\Phi(t))$ is the rotation matrix that transforms

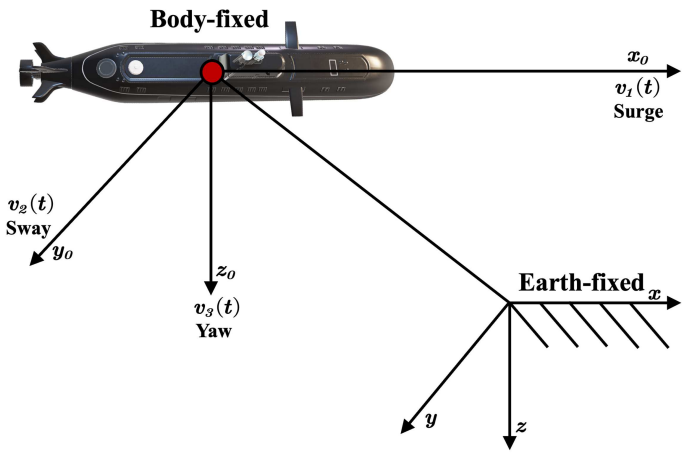

Figure 1 (Color online) Earth-fixed frame and body-fixed reference frame.

body-fixed velocities into the earth-fixed frame

$$P(\Phi(t)) = \begin{bmatrix} \cos(\Phi(t)) & -\sin(\Phi(t)) & 0 \\ \sin(\Phi(t)) & \cos(\Phi(t)) & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

By defining $A = -\mathcal{M}^{-1}\mathcal{N}$, $B = -\mathcal{M}^{-1}\mathcal{G}$, and $D = -\mathcal{M}^{-1}$, the dynamics of the UMV system can be reformulated as

$$\dot{v} = Av + B\eta + D(u(t) + \omega(t)), \tag{3}$$

where A, B, and D are system matrices encapsulating the effects of inertia, damping, and external inputs on the velocity dynamics of the UMV. This reformulation simplifies the system model, making it suitable for further analysis and control design. It aligns with the state-space representations commonly employed in ICSs, facilitating the application of advanced control strategies.

Then, we can define the $x(t) = [v^{\mathsf{T}}\ \eta^{\mathsf{T}}]^{\mathsf{T}}$, and assume that $\Phi(t)$ is sufficiently small. Under this assumption, $P(\Phi(t)) \approx I$ can be approximated using $\cos(\Phi(t)) \approx 1$ and $\sin(\Phi(t)) \approx 0$. By combining (2) and (3), the system dynamics can be reformulated as

$$\dot{x}(t) = \bar{A}x(t) + \bar{B}u(t) + \bar{B}\omega(t), \tag{4}$$

where $\bar{A} = [A, B; I, 0]$, $\bar{B} = \big[D; 0\big]$.

2.2 Quantitative control for RL supervision

To address the issue of bandwidth resource wastage in networked UMV systems caused by traditional fixed-frequency sampling methods, this paper proposes an RLSIS strategy. As illustrated in Figure 2, the proposed UMV control system dynamically adjusts sampling intervals based on variations in the system state, eliminating the reliance on conventional fixed sampling frequencies. This adaptive mechanism conserves communication bandwidth by reducing redundant sampling during stable periods while increasing the sampling frequency during rapid state transitions. This approach enhances control accuracy and ensures overall system stability, effectively addressing the challenges of dynamic and resource-constrained environments.

As detailed in Algorithm 1, the RLSIS algorithm leverages the self-learning and adaptive capabilities of RL to optimize the sampling strategy dynamically. The algorithm fine-tunes sampling intervals by continuously analyzing historical data and real-time feedback to achieve an optimal balance between communication efficiency and control performance. This adaptability is particularly critical for UMV systems operating in complex and dynamic marine environments, where fluctuating conditions demand a flexible and robust control framework. The adaptive nature of the RLSIS strategy provides dual benefits: it significantly reduces network load by minimizing redundant sampling during stable periods, and it ensures high control precision and system reliability by increasing sampling frequency during rapid state transitions. These attributes make the RLSIS strategy a practical and effective solution for resource-constrained industrial networks, addressing the challenges of dynamic operation and limited bandwidth in real-world applications.

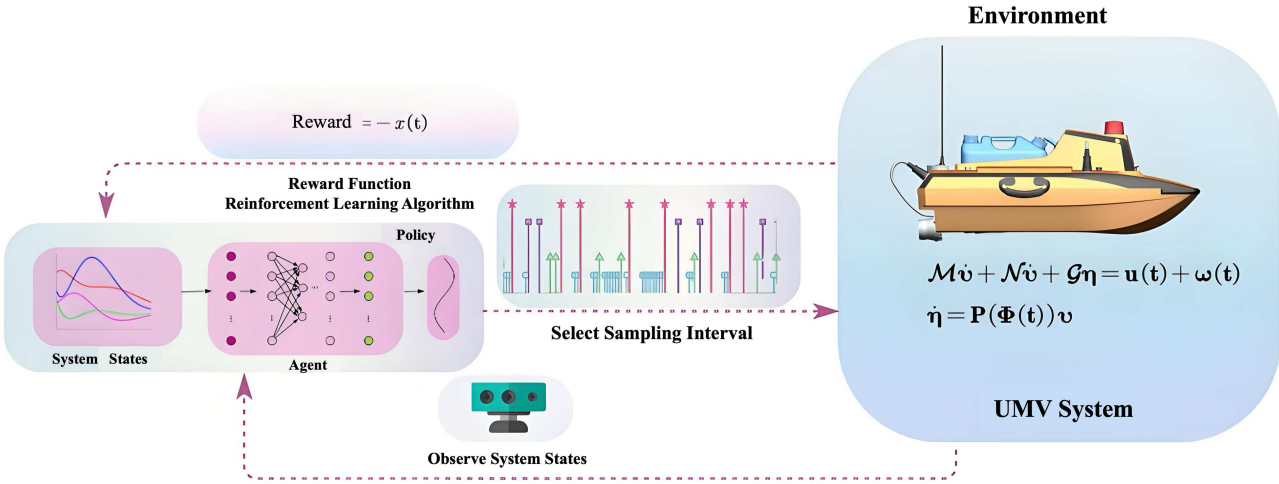

Figure 2 (Color online) Intelligently optimized UMV system framework.

Algorithm 1 Reinforcement learning spervised intelligent sampling algorithm.

Input: Learning rate α, discount factor γ_q, exploration probability ϵ, set of sampling intervals d_values, initial sampling interval d, minimum sampling interval h, number of actions $num\_actions$.

begin
- Initialize Q-table Q to zeros;
- Set initial system state $s \leftarrow 1$;
- Initialize time counter $time\_counter \leftarrow 0$;
- **while** $t_k h \geqslant 0$ **do**
  - **if** $time\_counter == 0$ **then**
    - **if** $random\ value < \epsilon$ **then**
      - $a \leftarrow$ randomly;
      - Select from$\{1, 2, \ldots, num_actions\}$;
    - **else**
      - $a \leftarrow \arg\max(Q(s, :))$;
    - Set sampling interval $d \leftarrow d\_values(a)$;
    - Update $time\_counter \leftarrow d/h$;
  - Apply selected sampling interval d to update system dynamics;
  - **if** $d \geqslant 0$ **then**
    - Compute reward based on system performance: $reward \leftarrow -x(t)$;
    - Update Q-table: $Q(s,a) \leftarrow Q(s,a)+\alpha\Big(reward + \gamma_q \max(Q(s,:)) - Q(s,a)\Big)$;
    - Decrease $time\_counter$ by 1;

Remark 1. The proposed algorithm adopts an RL framework to dynamically determine sampling intervals by balancing exploration and exploitation, thereby optimizing real-time control performance under varying system conditions. At each decision step, the agent either explores by selecting random actions with probability ε, promoting the discovery of new sampling strategies, or exploits its current knowledge by choosing the action with the highest estimated Q-value, thereby reinforcing previously successful decisions. The Q-values are iteratively updated based on system performance feedback using a temporal-difference learning rule, which enables the agent to refine its sampling policy over time. This online learning mechanism improves bandwidth efficiency by adjusting sampling frequency according to system state variability, reducing redundant data transmission during steady-state periods without compromising responsiveness during dynamic phases. The algorithm is model-free and does not rely on prior knowledge of system dynamics, making it highly adaptable to complex or uncertain environments. Besides, it maintains real-time operation through lightweight computations, ensuring seamless integration into embedded industrial control systems. By combining adaptability, bandwidth awareness, and real-time capability, the proposed RL-based strategy is well-suited for networked control applications such as UMV systems, where maintaining efficient communication and reliable performance is critical in dynamic and resource-constrained industrial settings.

Remark 2. To ensure the practical deployability of the proposed RLSIS algorithm in real-time industrial scenarios, its computational complexity and data security considerations have been carefully addressed. The algorithm adopts a compact design by restricting the action space to a small set of discrete sampling intervals, which effectively limits the size of the Q-table and simplifies the decision-making process. Meanwhile, the system state is abstracted into low-dimensional representations such as quantized tracking error levels, avoiding the use of high-dimensional or sensitive raw data that may involve personal information. Moreover, instead of updating the Q-values at every time step, the

algorithm performs updates only when a new sampling interval is selected, thereby reducing computational frequency and resource consumption. These strategies collectively ensure that the learning process remains lightweight and compatible with industrial controllers that often operate under limited computational capacity. Then, the proposed method enhances data protection by operating entirely within the local controller environment. It neither transmits nor stores raw sensor data externally, which minimizes the risk of privacy breaches or data misuse. Furthermore, the control decisions rely solely on real-time control signals rather than large historical datasets, further reducing the attack surface. This architecture also offers resilience against cyberthreats, as it avoids continuous external communications that are vulnerable to interception or injection.

Then, we define $t-t_k = d(t)$, and $d_1 \leqslant d(t) \leqslant d_2$, $\dot{d}(t) = 1$ except $t = t_k$. This implies that the value of $x(t-d(t))$ remains constant at $x(t_k)$ until the next successful sampling instance. Utilizing this definition, the control input can be expressed as

$$u(t) = -Kx(t - d(t)). \tag{5}$$

This paper introduces a data quantization mechanism as a complementary solution to enhance the efficiency of the proposed RL-based adaptive sampling strategy. While the adaptive sampling strategy dynamically adjusts the frequency of data transmission to minimize redundant communication, the data quantization mechanism reduces the size of transmitted information at each sampling instance. Together, these mechanisms address two critical dimensions of communication efficiency: adaptive sampling optimizes the timing of data transmission, while data quantization ensures that only the most essential and relevant information is sent. This integrated approach effectively reduces network load, optimizes bandwidth utilization, and improves overall resource efficiency without compromising system performance. Such a synergistic combination provides a robust and scalable solution for optimizing communication efficiency in networked UMV systems, particularly in bandwidth-constrained environments. To implement this framework, the data quantization mechanism is defined as

$$\mathbb{Q} = \{\pm q_i, q_i = \epsilon_i q_0, i = \pm 1, \pm 2, \dots\} \cup \{\pm q_0\} \cup \{0\}, \tag{6}$$

where the value of $0 < \epsilon_i < 1$ determines the data quantization density. A logarithmic quantizer is employed for the quantization process, defined as

$$\mathbb{Q}(x_n) = \begin{cases} q_i, & \dfrac{1}{1+\sigma} q_i < x_n \leqslant \dfrac{1}{1-\sigma} q_i, \\ 0, & x_n = 0, \\ -\mathbb{Q}(-x_n), & x_n < 0, \end{cases} \tag{7}$$

where $\sigma = \frac{(1-\epsilon_i)}{(1+\epsilon_i)} \in (0,1)$ represents the sector bound. Using this quantization process, the relationship between the quantized value and the original signal is expressed as $\mathbb{Q}(x_n) = (I + \Delta)x_n$ with $-\sigma < \Delta < \sigma$. The quantized control signal is then defined as

$$\mathbb{Q}(u(t)) = \hat{K}x(t - d(t)), \tag{8}$$

where $\hat{K} = (I + \Delta)K$, and $\Delta = \mathrm{diag}\{\Delta_1, \Delta_2, \dots, \Delta_i\}$ represents the quantization error matrix. This formulation incorporates the effects of quantization errors while ensuring the stability and accuracy of the control system.

2.3 DDoS attack detection model and restart control

Building on the previous discussion and incorporating the impact of aperiodic DDoS attacks, which impair the availability of the communication link by disrupting the transmission of control and feedback signals, the controller is designed as follows:

$$\mathbb{Q}(u(t)) = \begin{cases} \hat{K}x(t - d(t)), & t \in \bar{\mathcal{D}}^{\mathsf{T}}_{i,\ell}, \\ 0, & t \in \bar{\mathcal{D}}_{j,\ell}, \end{cases} \tag{9}$$

where $\mu(t) = d(t) + \sigma(t)$, $\sigma(t)$ is the time delay caused by DDoS attacks. An aperiodic DDoS attack model is proposed to address the challenges posed by a non-ideal network environment.

As illustrated in Figure 3, the aperiodic DDoS attack is assumed to occur regularly, following these specific occurrence rules

$$\mathcal{T}_{DDoS}(t) = \begin{cases} 0, & t \in [\mathcal{D}_{i,\ell}, \mathcal{D}_{j,\ell}), \\ 1, & t \in [\mathcal{D}_{j,\ell}, \mathcal{D}_{i,\ell+1}), \end{cases} \tag{10}$$

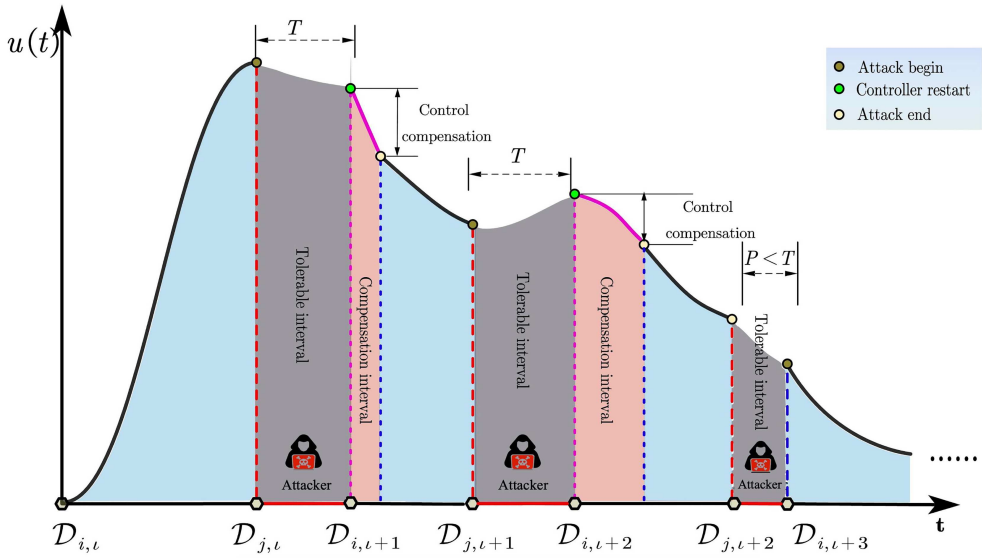

Figure 3 (Color online) DDoS attacks detection and restart control technology.

where $\mathcal{D}_{i,\ell} = (\ell-1)T_P$, $\mathcal{D}_{j,\ell} = (\ell-1)T_P + T_A^\ell$. Here, $\ell \in \mathbb{N}_+$ represents the current DDoS attack period, $T_P > 0$ denotes the total duration of a DDoS attack cycle, and $T_A^\ell > 0$ corresponds to the inactive period of the attack during the ℓ-th cycle. Additionally, $T_A^\ell \in [T_A^{\min}, T_A^{\max}]$, where $T_A^{\min} = \min_{\ell\in\mathbb{N}_+}\{T_A^\ell\}$, $T_A^{\max} = \max_{\ell\in\mathbb{N}_+}\{T_A^\ell\}$. In this model, $\mathcal{T}_{DDoS}(t) = 1$ indicates an active DDoS attack, while $\mathcal{T}_{DDoS}(t) = 0$ signifies an inactive period. This formulation captures the intermittent and aperiodic nature of DDoS attacks, providing a realistic representation that facilitates the development of robust control strategies to mitigate their impact effectively.

To address the issue of controller resource exhaustion caused by DDoS attacks, a lightweight supervised detection and recovery framework is proposed as detailed in Algorithm 2. Rather than relying on intrusive packet-level monitoring, the method infers potential cyberattacks by analyzing behavioral anomalies in the controller's output trajectory. Once sustained degradation is detected, an internal restart strategy is triggered to clear malicious buildup and restore normal control functionality. This integrated design ensures that detection and response are jointly realized within the control loop, enabling timely, minimal-intrusion recovery without introducing additional communication overhead. The framework is both computationally efficient and operationally responsive, making it particularly suitable for real-time industrial environments vulnerable to cyber-induced disruptions.

Algorithm 2 Restart control technology and attack detection algorithm.

Input: Real-time controller output $u(t)$; attack duration T; initial detect instant $\tilde{\mathcal{D}}_{j,\ell}$; attack end time $\tilde{\mathcal{D}}_{i,\ell+1}$.

```
begin
    for t = D̃_{j,ℓ} : D̃_{j,ℓ+1} do
        Calculate u(t);
        if u(t) == 0 then
            P = P + 1;
            if P > T then
                The UMV system is under attack;
                Restart controller;
                P = 0;
                D̃_{i,ℓ+1} = t;
                D̃_{j,ℓ} = t − T;
                set[D̄_{j,ℓ}, D̄_{i,ℓ+1}]=[D̃_{j,ℓ}, D̃_{i,ℓ+1}) and output;
```

Remark 3. DDoS attacks exploit vulnerabilities in the controller's communication stack, launching massive volumes of half-open TCP connections, malformed packets, or excessive request floods that overload the system's processing capabilities. These attacks result in the exhaustion of key computational resources (such as memory, CPU time, and socket buffers) ultimately impeding the controller's ability to process valid control commands. Unlike conventional control faults, which degrade model accuracy or introduce parametric uncertainty, DDoS attacks lead to non-functional degradation at the software and operating system level. To mitigate this type of disruption, a controller restart mechanism is proposed. Upon detecting sustained abnormal behavior, the mechanism forcibly

reinitializes the controller, thereby flushing residual malicious connections and releasing consumed system resources. This reset not only clears attack-induced interference but also restores the normal processing capacity of the controller. The restart operation is guided by a supervised anomaly detection strategy that monitors output signal deviation to avoid unnecessary or frequent reboots. This combination ensures targeted and minimal-intrusion recovery during active attacks, prevents long-term performance deterioration, and provides a lightweight solution that does not introduce significant computational burden. As a result, the restart mechanism serves as a cyber-aware recovery strategy that complements conventional control design by offering robust, real-time mitigation for resource exhaustion threats caused by cyberattacks.

Based on the supervised restart mechanism and the data quantization mechanism, the dynamics of the UMV system under DDoS attacks can be expressed as

$$\begin{cases} \dot{x}(t) = \bar{A}x(t) - \bar{B}\hat{K}x(t-d(t)) + \bar{B}\omega(t), & t \in \bar{\mathcal{D}}_{i,\ell}^{\mathsf{T}}, \\ \dot{x}(t) = \bar{A}x(t) + \bar{B}\omega(t), & t \in \bar{\mathcal{D}}_{j,\ell}. \end{cases} \tag{11}$$

The following lemmas are necessary for deriving the main results in the subsequent section.

Lemma 1 ([30])**.** Consider a differentiable function $x \in \mathbb{R}^n$ and integers $\alpha_2 > \alpha_1 > 0$. For $F = \left[\begin{smallmatrix} F_{11} & F_{12} \\ * & F_{22} \end{smallmatrix}\right] > 0$, if there exist symmetric matrices L, $J > 0$, along with matrices $N_j (j = 1, 2, 3)$ of appropriate dimensions, such that

$$\hat{F} = \begin{bmatrix} F_{11} & F_{12} - L \\ * & F_{22} - J \end{bmatrix} > 0,$$

and the following inequality holds:

$$\int_{\alpha_1}^{\alpha_2} \begin{bmatrix} x(s) \\ \dot{x}(s) \end{bmatrix}^{\mathsf{T}} E \begin{bmatrix} x(s) \\ \dot{x}(s) \end{bmatrix} ds \geqslant \varsigma_1^{\mathsf{T}}(t) \sum_{n=1}^{3} \Omega_n \varsigma_1(t),$$

where

$$\begin{aligned}
\zeta_1(t) =& \ \mathrm{col}\left\{ x(\alpha_2),\ x(\alpha_1), \frac{1}{\beta}\int_{\alpha_1}^{\alpha_2} x(s)ds,\ \frac{2}{\beta^2}\int_{\alpha_1}^{\alpha_2}\int_{s}^{\alpha_2} x(u)duds \right\}, \\
\Omega_1 =& \ \beta\rho_1^{\mathsf{T}}\hat{F}\rho_1 + \mathrm{He}\left\{\rho_1^{\mathsf{T}}\hat{F}\rho_2 + 3\rho_4^{\mathsf{T}}\hat{F}\rho_5\right\} + \rho_3^{\mathsf{T}}\begin{bmatrix} 0 \\ I_n \end{bmatrix}^{\mathsf{T}} \frac{\hat{F}}{\beta}\begin{bmatrix} 0 \\ I_n \end{bmatrix}\rho_3 + 3\beta\rho_4^{\mathsf{T}}U\rho_4 \\
& + \rho_6^{\mathsf{T}}\begin{bmatrix} 0 \\ I_n \end{bmatrix}^{\mathsf{T}} \frac{3\hat{E}}{\beta}\begin{bmatrix} 0 \\ I_n \end{bmatrix}\rho_6, \\
\Omega_2 =& \ \left(\sigma_1^{\mathsf{T}}L\sigma_1 - \sigma_2^{\mathsf{T}}L\sigma_2\right), \\
\Omega_3 =& \ \mathrm{He}\{N_1\rho_3 + N_2\rho_6 + N_3\rho_7\} - \sum_{j=1}^{j=3} \frac{\beta}{2j-1} N_j E^{-1} N_j, \\
\rho_1 =& \ \mathrm{col}\{\sigma_3, 0\},\ \rho_2 = \mathrm{col}\{0, \rho_3\},\ \rho_3 = \sigma_1 - \sigma_2,\ \rho_4 = \mathrm{col}\{\sigma_3 - \sigma_4, 0\}, \\
\rho_5 =& \ \mathrm{col}\{0, \rho_6\},\ \beta = \alpha_2 - \alpha_1,\ \rho_6 = \sigma_1 + \sigma_2 - 2v_3,\ \rho_7 = \sigma_1 - \sigma_2 + 6\sigma_3 - 6\sigma_4, \\
\sigma_i =& \ \left[\, 0_{n\times(i-1)n}\ I_n\ 0_{n\times(4-i)n} \,\right],\ i = 1, 2, \ldots, 4.
\end{aligned}$$

Lemma 2 ([31])**.** Given a $\psi \in [c_1, c_2]$, any matrices $U \in \mathbb{R}^{n\times n}$ and $E \in \mathbb{R}^{n\times n}$ and $\left[\begin{smallmatrix} U & E \\ E^{\mathsf{T}} & U \end{smallmatrix}\right] \geqslant 0$, the following inequality holds:

$$-(c_2 - c_1)\int_{c_2}^{c_1} \dot{x}(s)^{\mathsf{T}} U \dot{x}(s)\, ds \leqslant \xi(t)^{\mathsf{T}}\Sigma\xi(t),\ \xi(t) = \mathrm{col}\{x(c_1), x(\psi), x(c_2)\},$$

where

$$\Sigma = \begin{bmatrix} -U & U - E & E \\ (U-E)^{\mathsf{T}} & -2U + \mathrm{He}\{E\} & U - E \\ E^{\mathsf{T}} & (U-E)^{\mathsf{T}} & -U \end{bmatrix}.$$

3 Main results

Theorem 1. Given scalars γ, d, and the controller gain matrix K, the UMV (11) is asymptotically stable under DDoS attacks if there exist real symmetric matrices $P > 0$, $Q > 0$, $R_1 > 0$, S_1, $Z_1 > 0$ and $Z > 0$, as well as arbitrary matrices M, N of appropriate dimensions, such that the following LMIs are satisfied

$$\begin{bmatrix} Z_1 & N \\ * & Z_1 \end{bmatrix} > 0, \tag{12}$$

$$\begin{bmatrix} R_{11} & R_{12} - S_1 \\ * & R_{22} - Z_1 \end{bmatrix} > 0, \tag{13}$$

$$\Psi(g_i, \vartheta) < 0, \tag{14}$$

where

$$\begin{aligned}
&\Psi(g_i,\vartheta) = \mathrm{He}\{g_1^{\mathsf{T}} P g_1 + \Lambda_1 \Lambda_2\} + g_1^{\mathsf{T}} Q g_1 - g_4^{\mathsf{T}} Q g_4 - \gamma^2 g_6^{\mathsf{T}} I g_6 \\
&\qquad + d^2 \vartheta_1^{\mathsf{T}} R_1 \vartheta_1 + g_1^{\mathsf{T}} C^{\mathsf{T}} C g_1 - \vartheta_2^{\mathsf{T}} R_2 \vartheta_2 - d\vartheta_4^{\mathsf{T}} S_1 \vartheta_4 + \vartheta_3^{\mathsf{T}} Z \vartheta_3, \\
&\vartheta_1 = \mathrm{col}\{g_1, g_2\},\ \vartheta_2 = \mathrm{col}\{g_5, \vartheta_4\},\ \vartheta_4 = g_1 - g_4,\ \Lambda_1 = \mathrm{col}\{M, M, 0, 0, 0, 0\}, \\
&\Lambda_2 = [A, -I, BK, 0, 0, D],\ \vartheta_3 = \mathrm{col}\{g_1, g_3, g_4\},\ g_i = \left[0_{n\times(i-1)n}\ I_n\ 0_{n\times(6-i)n}\right], \\
&\zeta(t) = \mathrm{col}\left\{x(t),\ \dot{x}(t), x(t-d(t)),\ x(t-d),\ \int_{t-d}^{t} x(s)ds, \omega(t)\right\},\ i = 1, 2, \ldots, 6.
\end{aligned}$$

For the system described in (11), the following candidate LKFs are proposed, motivated by their ability to explicitly account for time-delay effects and historical state information

$$V(t) = V_1(t) + V_2(t), \tag{15}$$

where

$$\begin{aligned}
V_1(t) =&\ x^{\mathsf{T}}(t) P x(t), \\
V_2(t) =&\ d\int_{t-d}^{t}\int_{\theta}^{t} \delta_1^{\mathsf{T}}(s) R_1 \delta_1(s) ds d\theta.
\end{aligned}$$

Next, we calculate the time derivative of the $V(t)$. The following expressions are obtained:

$$\frac{\partial V(t)}{\partial t} = L_1 + L_2, \tag{16}$$

where

$$\begin{aligned}
L_1 =&\ 2x^{\mathsf{T}}(t) P \dot{x}(t), \\
L_2 =&\ d^2 \delta_1^{\mathsf{T}}(t) R_1 \delta_1(t) - d\int_{t-d}^{t} \delta_1^{\mathsf{T}}(s) R_1 \delta_1(s) ds.
\end{aligned}$$

The Lemmas and Jensen's inequality are employed to estimate the integral term $-d\int t - d^t \delta 1^{\mathsf{T}}(s) R_1 \delta_1(s) ds$ in L_3, where the Jensen inequality provides a tight and computable upper bound for the integral, facilitating the derivation of less conservative stability conditions in the subsequent analysis

$$-d\int_{t-d}^{t} \delta_1^{\mathsf{T}}(s) R_1 \delta_1(s) ds \leqslant -\delta_2(t)^{\mathsf{T}} R_2 \delta_2(t) - d\delta_3(t)^{\mathsf{T}} S_1 \delta_3(t) + \delta_4(t)^{\mathsf{T}} Z \delta_4(t), \tag{17}$$

where

$$R_1 = \begin{bmatrix} R_{11} & R_{12} \\ * & R_{22} \end{bmatrix},\ R_2 = \begin{bmatrix} R_{11} & R_{12} - S_1 \\ * & R_{22} - Z_1 \end{bmatrix},$$

$$Z = \begin{bmatrix} -Z_1 & Z_1 - N & N \\ * & -2Z_1 + \mathrm{He}\{N\} & Z_1 - N \\ * & * & -Z_1 \end{bmatrix},$$

$$\begin{aligned} \delta_1(t) &= \mathrm{col}\{x(t), \dot{x}(t)\},\ \delta_3(t) = x(t) - x(t-d), \\ \delta_2(t) &= \mathrm{col}\left\{\int_{t-d}^{t} x(s)ds,\ x(t) - x(t-d)\right\}, \\ \delta_4(t) &= \mathrm{col}\{x(t),\ x(t-d(t)),\ x(t-d)\}. \end{aligned}$$

According to the UMV system (11), the following zero equality holds:

$$\begin{aligned} 0 &= \mathbb{E}\left\{2[x(t) + \dot{x}(t)]^{\mathsf{T}} M[Ax(t) + \rho(t) \times BKx(t - d(t)) + D\omega(t) - \dot{x}(t)]\right\} \\ &= 2\zeta^{\mathsf{T}}(t)\Lambda_1\Lambda_2\zeta(t). \end{aligned} \tag{18}$$

Thus, $\frac{\partial V(t)}{\partial t}$ can be expressed as the sum of its components

$$\frac{\partial V(t)}{\partial t} = L_1 + L_2 = \xi^{\mathsf{T}}(t)\Psi(g_i, \vartheta)\xi(t). \tag{19}$$

Finally, based on the results in (9)–(16), the following inequality is established:

$$\frac{\partial V(t)}{\partial t} = \xi^{\mathsf{T}}(t)\Psi(g_i, \vartheta)\xi(t) < 0. \tag{20}$$

When the condition in (12)–(14) are satisfied, they ensure that $\frac{\partial V(t)}{\partial t} < 0$, thereby guaranteeing the asymptotic stability of the systems described in (11). These LMIs conditions serve as sufficient criteria to ensure the negative definiteness of the Lyapunov derivative, thereby facilitating stability verification in a computationally tractable manner, completing the proof.

Remark 4. In this paper, Lemma 1 is employed to estimate the integral term $-d\int_{t-d}^{t}\delta_1^{\mathsf{T}}(s)R_1\delta_1(s)ds$ introducing a structured matrix decomposition to facilitate the analysis. This estimation yields two significant terms $-d\delta_3(t)^{\mathsf{T}}S_1\delta_3(t)$, which contributes negative definiteness linked to the intermediate state variable, and $\delta_4(t)^{\mathsf{T}}Z\delta_4(t)$, which accounts for additional quadratic terms. These terms are derived using a matrix separation method, where the matrix $\left[\begin{smallmatrix} R_{11} & R_{12} \\ * & R_{22} \end{smallmatrix}\right]$ is decomposed into three components involving auxiliary matrices S_1 and Z_1. This decomposition enables systematic and computationally efficient handling of the integral term, simplifying its integration into the LKFs framework. Additionally, Lemma 2 is combined with advanced integral inequalities to introduce further negative-definite terms, reducing the conservativeness of the derived LMI conditions. These refinements enhance the feasibility of the proposed control framework, ensuring that the stability criteria are robust and practically applicable. This methodology is particularly effective for systems subject to time delays and external disturbances, including those operating under the influence of DDoS attacks, providing a reliable approach to maintain stability in complex and adverse conditions.

Remark 5. This paper presents a comprehensive framework that effectively integrates RLSIS, data quantization, and a robust cybersecurity defense mechanism to address the multifaceted challenges in ICSs 4.0. The RLSIS strategy optimizes bandwidth utilization by dynamically adjusting sampling intervals based on system state variations and network conditions, while the data quantization mechanism reduces the volume of transmitted data without compromising control accuracy. Furthermore, the hybrid detection mechanism and controller restart strategy provide a robust defense against DDoS attacks, enabling timely recovery of control signals and ensuring uninterrupted system operation. The synergy among these components enhances communication efficiency, improves control performance, and significantly strengthens system resilience under adverse network conditions. These innovations position the proposed framework as an adaptable and reliable solution for resource-constrained, high-stakes industrial environments, where efficiency, reliability, and security are paramount.

Theorem 2. Given scalars γ, d, and ρ, the UMV system described in (11) is asymptotically stable under DDoS attacks if there exist real symmetric matrices $\tilde{P} > 0$, $\tilde{Q} > 0$, $\tilde{R}_1 > 0$, $\tilde{S}_1$ and $\tilde{Z}_1 > 0$, as well as arbitrary matrices

$\hat{M}$, $\tilde{N}$ with appropriate dimensions, such that the following LMIs are satisfied:

$$\begin{bmatrix} \tilde{Z}_1 & \tilde{N} \\ * & \tilde{Z}_1 \end{bmatrix} > 0, \tag{21}$$

$$\begin{bmatrix} \tilde{R}_{11} & \tilde{R}_{12} - \tilde{S}_1 \\ * & \tilde{R}_{22} - \tilde{Z}_1 \end{bmatrix} > 0, \tag{22}$$

$$\tilde{\Psi}(g_i, \vartheta) < 0, \tag{23}$$

where

$$\begin{aligned} \tilde{\Psi}(g_i, \vartheta) = \mathrm{He}\{g_1^{\mathsf{T}} \tilde{P} g_1 + \tilde{\Lambda}_1 \tilde{\Lambda}_2\} + g_1^{\mathsf{T}} \tilde{Q} g_1 - g_4^{\mathsf{T}} \tilde{Q} g_4, + d^2 \vartheta_1^{\mathsf{T}} \tilde{R}_1 \vartheta_1 \\ - \gamma^2 g_6^{\mathsf{T}} I g_6 - \vartheta_2^{\mathsf{T}} \tilde{R}_2 \vartheta_2, - d \vartheta_4^{\mathsf{T}} \tilde{S}_1 \vartheta_4 + \vartheta_3^{\mathsf{T}} \tilde{Z} \vartheta_3, \\ \vartheta_4 = g_1 - g_4,\ \tilde{\Lambda}_1 = \mathrm{col}\{I, I, 0, 0, 0, 0\}, \tilde{\Lambda}_2 = [A\hat{M}, -\hat{M}, B\hat{K}, 0, 0, D], \\ \tilde{C} = C\hat{M} g_1,\ \vartheta_1 = \mathrm{col}\{g_1, g_2\},\ \vartheta_2 = \mathrm{col}\{g_5, \vartheta_4\},\ \vartheta_3 = \mathrm{col}\{g_1, g_3, g_4\}. \end{aligned}$$

Proof. Let $\hat{M} = M^{-1}$, $\Pi_n = \mathrm{diag}\{\overbrace{\hat{M}, \ldots, \hat{M}}^{n}\}$, and define the following matrix transformations:

$$\begin{aligned} &\tilde{Q} = \hat{M}^{\mathsf{T}} Q \hat{M},\ \tilde{S}_1 = \hat{M}^{\mathsf{T}} S_1 \hat{M},\ \tilde{Z}_1 = \hat{M}^{\mathsf{T}} Z_1 \hat{M},\ \tilde{N} = \hat{M}^{\mathsf{T}} N \hat{M}, \\ &\tilde{R}_1 = \Pi_2^{\mathsf{T}} R_1 \Pi_2,\ \tilde{R}_2 = \Pi_2^{\mathsf{T}} R_2 \Pi_2,\ \tilde{Z} = \Pi_3^{\mathsf{T}} Z \Pi_3,\ \tilde{P} = \hat{M}^{\mathsf{T}} P \hat{M},\ \Gamma = \mathrm{diag}\{\Pi_n, I\}. \end{aligned}$$

By pre-multiplying and post-multiplying both sides of the LMI conditions (12)–(14) with Π_n^{T} and Π_n, the transformed LMIs (21)–(23) are obtained. These transformations maintain equivalence between the original and transformed conditions, ensuring consistency in stability and performance criteria. Furthermore, by defining $K\hat{M} = \hat{K}$, the controller gain matrices are designed as $K = \hat{K}\hat{M}^{-1}$, preserving the stability and performance properties derived from the LMIs. With this, the proof of Theorem 2 is completed.

Remark 6. Although the Lyapunov-based stability analysis in this paper is tailored to the proposed RLSIS and restart control framework, the employed method (based on LKFs and LMIs) is generalizable to other classes of networked control systems. Specifically, this framework can be extended to systems with bounded delays, unknown disturbances, or event-triggered mechanisms with different scheduling rules. Therefore, the analytical approach presented here lays a theoretical foundation that can be adapted to a broader range of resilient control strategies under adversarial conditions.

4 Illustrative example

In this section, the performance of the proposed RLSIS scheme is evaluated using the UMV system described in [12]. The evaluation aims to assess the scheme's effectiveness in enhancing communication efficiency, maintaining control accuracy, and improving the system's resilience to external disturbances and network attacks. The following system matrices characterize the dynamics of the UMV system

$$\mathcal{M} = \begin{bmatrix} 1.0852 & 0 & 0 \\ 0 & 2.0275 & -0.4087 \\ 0 & -0.4087 & 0.2153 \end{bmatrix},\ \mathcal{G} = \begin{bmatrix} 0.0389 & 0 & 0 \\ 0 & 0.0266 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

$$\mathcal{N} = \begin{bmatrix} 0.0865 & 0 & 0 \\ 0 & 0.0762 & 0.1510 \\ 0 & 0.0151 & 0.0031 \end{bmatrix},\ \bar{A} = \begin{bmatrix} a & b \\ I_{3\times 3} & \mathbf{0}_{3\times 3} \end{bmatrix},\ \bar{B} = \begin{bmatrix} c \\ \mathbf{0}_{3\times 3} \end{bmatrix}.$$

Then, one has

$$a = \begin{bmatrix} -0.0797 & 0 & 0 \\ 0 & -0.0818 & -0.1224 \\ 0 & -0.2254 & -0.2468 \end{bmatrix},\ b = \begin{bmatrix} -0.0358 & 0 & 0 & 0 \\ -0.1224 & 0 & -0.0208 & 0 \\ -0.2468 & 0 & -0.0394 & 0 \end{bmatrix},\ c = \begin{bmatrix} 0.9215 & 0 & 0 \\ 0 & 0.7802 & 1.4811 \\ 0 & 1.4811 & 7.4562 \end{bmatrix}.$$

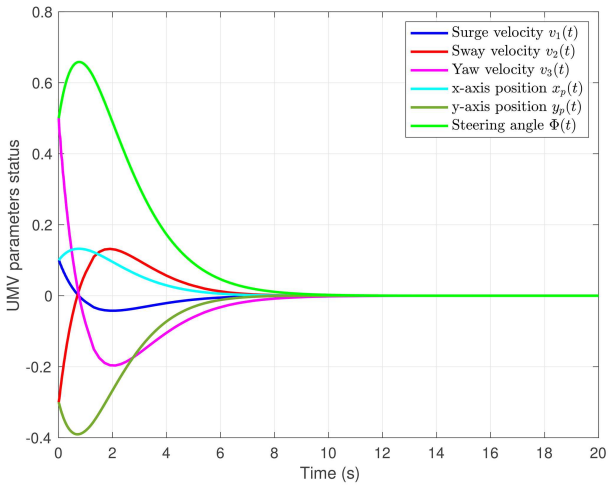

Figure 4 (Color online) System response under RLSIS supervision.

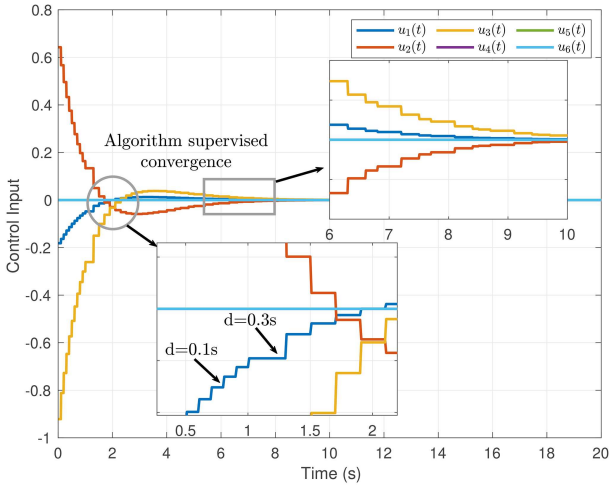

Figure 5 (Color online) Controller response under RLSIS supervision.

Consider the external disturbance $\omega(t) = [\omega_1(t), \omega_2(t), \omega_3(t)]^{\mathsf{T}}$, where $\omega_1(t) = \sin(t)\mathrm{e}^{-0.04t}$, $\omega_2(t) = \cos(t)\mathrm{e}^{-0.05t}$ and $\omega_3(t) = -\sin(t)\mathrm{e}^{-0.06t}$. These disturbances model time-varying external forces with exponential decay, simulating environmental effects such as waves, wind, and currents. By solving the LMIs presented in Theorem 2, the optimal controller gain $K = [k_1\ k_2]$ is obtained as

$$k_1 = \begin{bmatrix} -1.3850 & 0 & 0 \\ 0 & -2.7114 & 0.7948 \\ 0 & 0.5612 & -0.3159 \end{bmatrix},\ k_2 = \begin{bmatrix} -0.5863 & 0 & 0 \\ 0 & -1.1318 & 0.2968 \\ 0 & 0.2258 & -0.1339 \end{bmatrix}.$$

4.1 System performance evaluation under RLSIS

The RLSIS scheme is implemented with driven threshold parameters set as $\lambda_1 = \lambda_2 = 1$, $\alpha = 0.55$, $\gamma_q = 0.8$, and $\varepsilon = 0.05$. Under these configurations, the system's state responses and controller outputs are depicted in Figures 4 and 5. As shown, the system states converge and stabilize over time, even in the presence of external disturbances and network-induced challenges. These results demonstrate the effectiveness of the proposed controller and the RLSIS scheme in maintaining system stability. The ability to dynamically adjust sampling thresholds ensures efficient communication and control accuracy, underscoring the robustness of the designed control framework under varying environmental and operational conditions. The stabilized state responses further validate the theoretical findings, highlighting the practical applicability of the proposed strategies in real-world scenarios. The effectiveness of the RLSIS strategy is further illustrated through its dynamic adjustment of the sampling interval. As shown in Figure 6, during periods of significant system fluctuations, the sampling interval decreases, enabling the controller to respond more frequently and enhance control accuracy. Conversely, the sampling interval increases as the system stabilizes, reducing communication bandwidth usage and conserving network resources. This adaptive process is governed by RL, where the system state acts as the input, and the sampling interval is treated as the action. The adjustment is optimized by minimizing a cost function that balances control error and network bandwidth utilization. By dynamically adapting the sampling interval to real-time system conditions, the RLSIS strategy achieves efficient resource utilization and precise control performance, effectively addressing the challenges of dynamic, resource-constrained environments.

The experimental results demonstrate that the proposed method effectively balances control system performance and communication resource consumption, highlighting its strong practicality and engineering applicability. Additionally, it offers an efficient solution for unmanned ship control systems operating in complex and dynamic environments. Table 1 presents the dynamic performance indicators (DPIs) of the UMV systems across various scenarios (C1 to C5), where C1–C4 correspond to the periodic sampling strategy [32] and C5 represents the RLSIS sampling strategy. This comparison highlights the differences in control performance between traditional periodic sampling and the proposed intelligent non-periodic approach. The considered DPIs include the integral of absolute error (IAE), the integral of time-weighted absolute error (ITAE), and the integral of squared error (ISE), defined as $\mathrm{IAE} = \int_0^t |x(v)|dv$, $\mathrm{ISE} = \int_0^t |x(v)|^2 dv$, $\mathrm{ITAE} = \int_0^t |tx(v)|dv$. These metrics quantitatively evaluate the system's

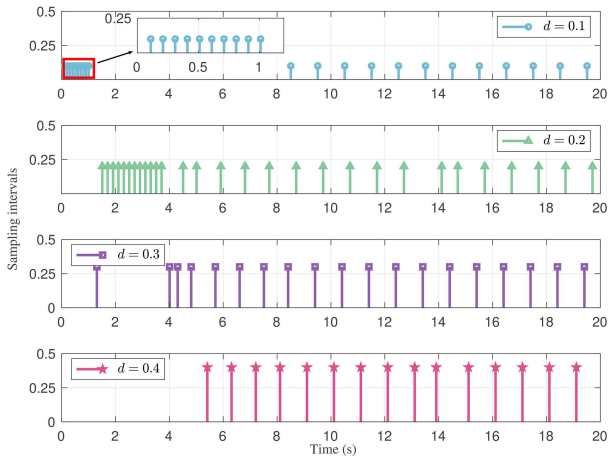

Figure 6 (Color online) Intelligent sampling under RLSIS supervision.

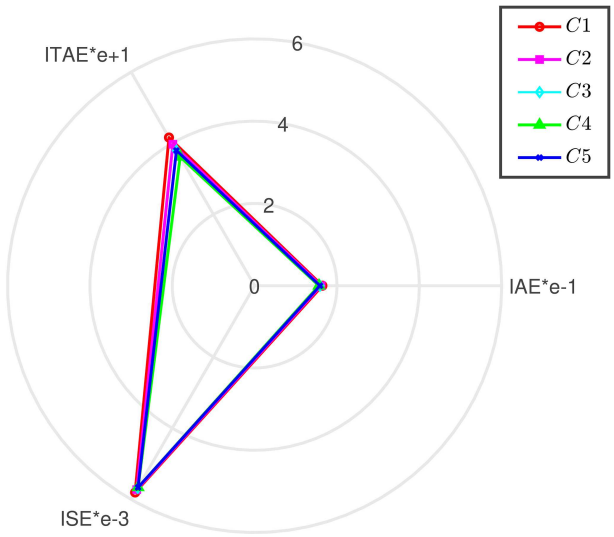

Figure 7 (Color online) System dynamic performance indicator evaluation.

Table 1 DPIs of UMV system under different cases ($\times 10^{-4}$).

DPIs	C1	C2	C3	C4	C5
IAE	1645.6	1614.7	1586.5	1562.5	1586.3
ITAE	4159.1	3970.4	3790.7	3616.4	3796.1
ISE	58.03	57.24	56.75	56.58	56.62

transient performance, measuring control accuracy, stability, and responsiveness over time [33, 34]. As shown in Table 1, scenarios C1 to C4 correspond to fixed sampling intervals ranging from 0.1 to 0.4 s, while C5 represents the RLSIS-based adaptive sampling strategy. The results clearly indicate that the RLSIS strategy (C5) outperforms fixed sampling strategies (C1–C4) across all DPIs, demonstrating its capability to dynamically adjust the sampling interval for optimal control performance and communication efficiency. These findings validate the effectiveness and robustness of the proposed approach in addressing the challenges posed by resource-constrained and dynamic environments.

The data in Table 1 clearly show that the C5 outperforms fixed sampling intervals across all three DPIs. Specifically, the IAE for C5 is reduced to 0.15863, significantly lower than 0.16456 for C1 and 0.16147 for C2, indicating improved accuracy in minimizing absolute deviations from the desired trajectory. Similarly, C5 achieves an ITAE value of 0.37961, compared to 0.41591 for C1 and 0.39704 for C2, reflecting its superior ability to mitigate time-weighted errors, ensuring timely and precise transient response corrections. The ISE for C5 is minimized to 0.005662, demonstrating consistent improvement in cumulative error energy, leading to smoother and more stable control performance. These results validate the effectiveness of the RLSIS-based adaptive sampling strategy in enhancing the UMV system's dynamic performance. By dynamically adjusting the sampling interval based on real-time system state, the RLSIS strategy reduces communication overhead while maintaining or improving control accuracy. Its ability to minimize absolute, squared, and time-weighted errors highlights its robustness and practical utility, particularly in complex and resource-constrained environments.

To further illustrate these results, Figure 7 presents a radar chart depicting the DPIs for the various cases. The axes are scaled to emphasize relative differences among the methods. Notably, case C5, which adopts the RLSIS-based adaptive sampling strategy, forms the smallest enclosed area on the chart, indicating superior performance across all indicators compared to fixed sampling strategies. While fixed sampling strategies show improved DPIs as the interval decreases (consistent with the expectation that finer sampling enhances control accuracy), this comes at the cost of increased communication. In contrast, C5 dynamically adjusts the sampling interval based on real-time system variations, achieving a better balance between control performance and communication efficiency. This result confirms the effectiveness of the RLSIS strategy in addressing the inherent trade-off in dynamic systems, and highlights its advantage in achieving reliable control with reduced communication load.

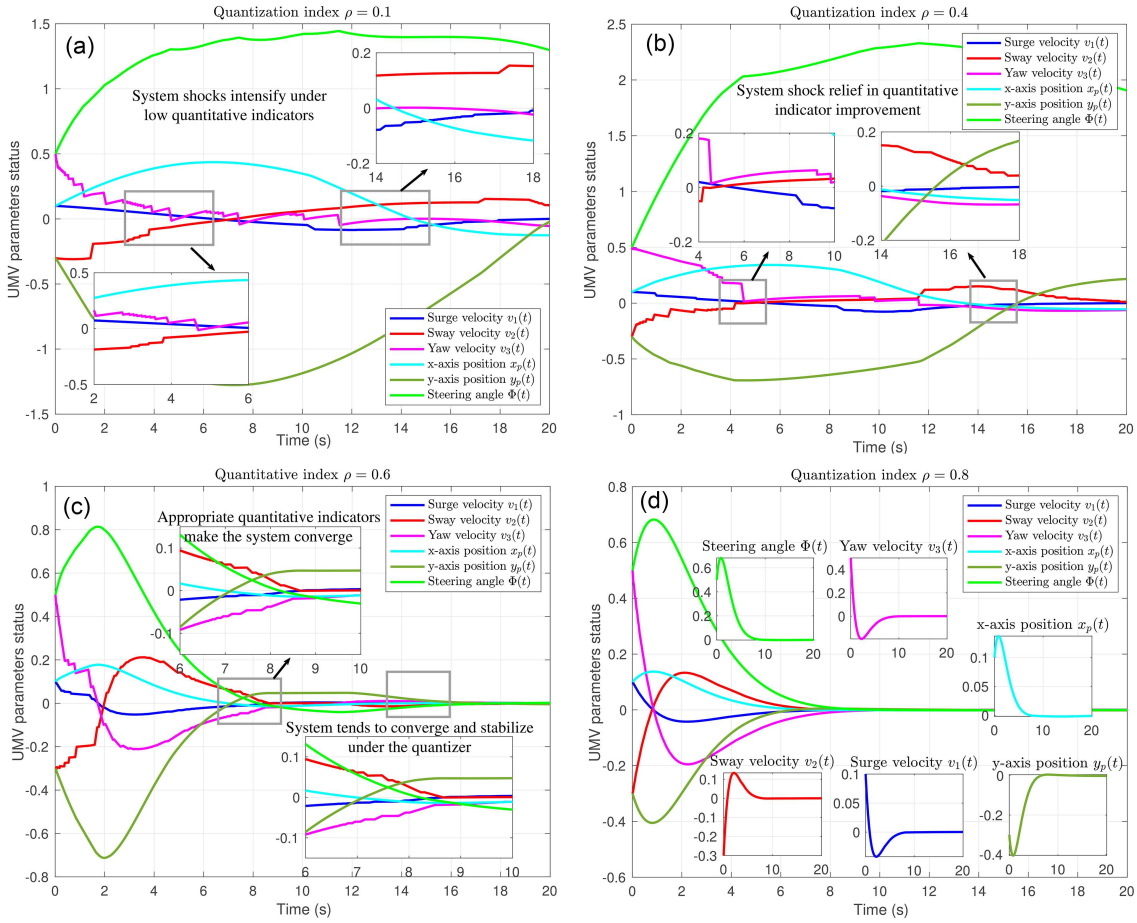

Figure 8 (Color online) System response under the quantization mechanism. (a) Quantitative index $\rho = 0.1$; (b) quantization index $\rho = 0.4$; (c) quantization index $\rho = 0.6$; (d) quantization index $\rho = 0.8$.

4.2 Intelligent controller under quantized mechanism

As depicted in Figure 8, the system state response demonstrates notable differences in dynamic behavior at the initial stage under varying quantization parameters ρ. For smaller values of ρ, the state response exhibits smoother transitions with relatively smaller oscillation amplitudes, indicating that the impact of quantization error is minimal. This enables the system to converge more rapidly to its equilibrium state. Conversely, larger ρ values result in significantly increased fluctuation amplitudes during the initial stage, with some state variables displaying transient and pronounced oscillations. This behavior reflects the introduction of greater quantization errors, which reduce the quality of the system's dynamic response. Despite these initial fluctuations, the system ultimately converges to a stable state over time. This trade-off highlights the dual impact of the quantization mechanism: smaller quantization intervals improve control accuracy by minimizing signal dispersion but require higher data transmission, while larger intervals conserve bandwidth at the expense of increased quantization errors and reduced precision. These findings emphasize the critical role of selecting an appropriate quantization parameter ρ to effectively balance communication efficiency and control performance.

The impact of the quantization mechanism on the controller's response behavior is illustrated in Figure 9. When the quantization parameter ρ is small, the controller output $u(t)$ remains smooth and continuous, indicating that the controller can adjust control signals accurately and compensate for state deviations effectively. However, as ρ increases, the output becomes more discretized and exhibits noticeable jitter, especially during the initial transient phase. This is because larger quantization intervals reduce the controller's ability to respond to subtle state changes, resulting in step-like control signals and increased quantization error. As the system approaches steady-state, state variations diminish, and the jitter in the control output gradually subsides, leading to a smoother control signal. This behavior reflects the inherent trade-off of quantization: while larger ρ values reduce communication and computation costs, they may temporarily compromise control precision during dynamic transitions. Nevertheless, once stability is reached, the quantization mechanism significantly lowers communication overhead without degrading overall system

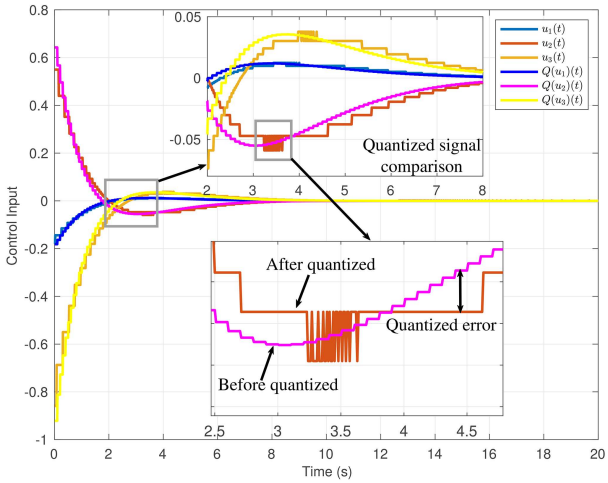

Figure 9 (Color online) Controller responses with and without data quantization.

performance. These results highlight the importance of selecting an appropriate ρ to balance communication efficiency and control accuracy, especially in systems that must handle both transient dynamics and long-term stability.

Figure 9 compares the controller's performance with and without data quantization. In the figure, $Q(u_i)(t)$ $(i = 1, 2, 3)$ represent control signals under quantization, while $u_i(t)$ $(i = 1, 2, 3)$ correspond to outputs from normal sampling without quantization. The results clearly show the impact of quantization on signal transmission, especially during periods of rapid system changes. In the quantized case (solid lines), the control signals display a noticeable "staircase" pattern, particularly during the time interval t from 2.5 to 4.5 s. This effect arises from discretization, where signal values are mapped to finite levels, resulting in stepwise transitions and reduced signal granularity. The zoomed-in portion of the figure highlights how this approximation leads to a loss of detail and limits the controller's ability to fine-tune responses in real time. Despite this reduction in signal precision during transients, quantization significantly lowers communication load and data transmission requirements. These results underscore the trade-off between control accuracy and communication efficiency: while quantization introduces approximation errors, it enhances network resource utilization. Therefore, careful selection of quantization parameters is essential to achieve an appropriate balance, particularly in systems where both control performance and bandwidth constraints are critical.

Despite the presence of quantization-induced errors, the overall system response remains stable and ultimately converges to the desired equilibrium. In the uncompressed case, the control signals are smoother and more continuous, allowing for precise tracking of system states with minimal deviation. In contrast, the compressed case exhibits slight reductions in precision due to discretization, particularly during transient periods. Nevertheless, the system retains stability and achieves satisfactory performance under quantization constraints. These observations further illustrate the trade-off between communication efficiency and control accuracy. While data quantization significantly reduces transmission load (an important benefit for networked systems operating under bandwidth limitations), it inevitably leads to reduced signal fidelity. This effect is most evident when rapid and fine-grained control adjustments are needed. Therefore, optimizing the quantization algorithm and carefully tuning the associated parameters are essential to mitigate performance degradation. When appropriately configured, quantization can minimize communication cost without compromising system stability, confirming its practicality for resource-constrained environments where both efficiency and accuracy are critical.

4.3 System resilience with restart control under attacks

This experiment analyzes the impact of DDoS attacks on system performance and demonstrates the benefits of incorporating a controller restart mechanism. The subplots of Figures 10–13 show the system's response under DDoS attacks without the restart mechanism. During attack periods, the state responses display pronounced oscillations and significant deviations from equilibrium. Communication between the controller and the system is severely disrupted, causing the controller output signals to become highly discontinuous and intermittent. This disruption prevents the controller from maintaining continuous control, limiting its ability to compensate for disturbances in real-time. As a result, the system experiences prolonged instability and a noticeable decline in performance. The controller fails to execute necessary control actions effectively, and the system state does not converge to

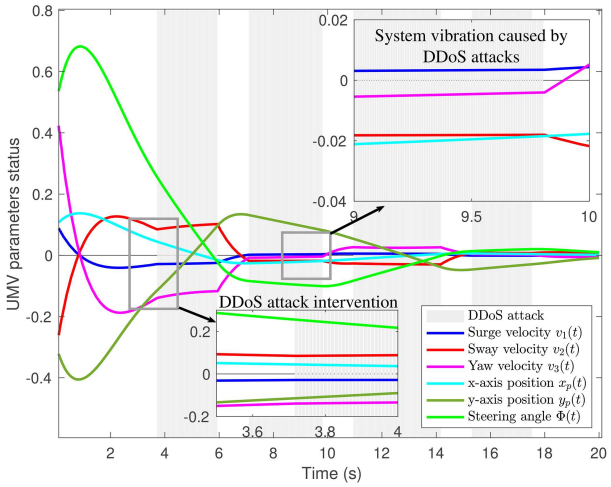

Figure 10 (Color online) System responses under DDoS attacks.

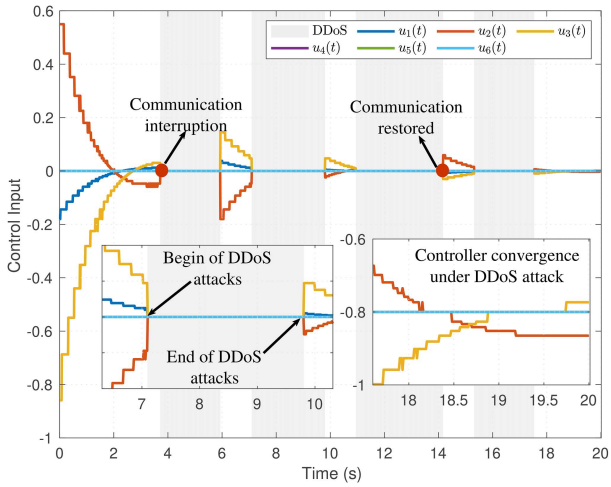

Figure 11 (Color online) Controller responses under DDoS attacks.

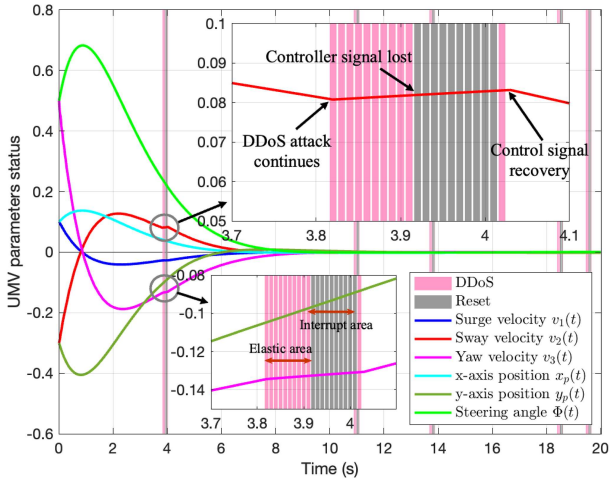

Figure 12 (Color online) System responses under DDoS attacks by controller reset technology.

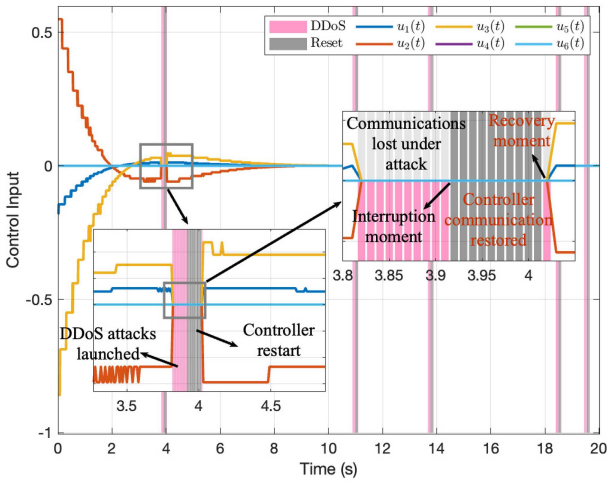

Figure 13 (Color online) Controller responses under DDoS attacks by controller reset technology.

equilibrium. These results underscore the controller's limitations in mitigating the effects of DDoS attacks without a robust defence mechanism.

In contrast, the bottom subplots of Figures 12 and 13 demonstrate the notable improvements achieved through the incorporation of the controller restart mechanism. Although the system initially undergoes similar perturbations when the DDoS attack begins, the state trajectories with the restart mechanism exhibit faster oscillation damping and a more rapid return to equilibrium after the attack ends. The zoomed-in view in the bottom-right subplot provides further insight into this process. Once the attack is detected, the restart mechanism is activated, clearing memory resources occupied during the attack and resetting the controller's internal computational state. This reset enables the recovery of control signal generation, resulting in smoother and more continuous outputs following each restart. By restoring reliable control and communication pathways, the restart mechanism allows the system to re-stabilize more efficiently, thereby reducing both the duration and severity of performance degradation. These results highlight the restart mechanism's effectiveness in mitigating the impact of DDoS attacks, enhancing system resilience and maintaining robust operation even under adverse network conditions.

A comparison of the two cases highlights both the severe impact of DDoS attacks on system performance and the effectiveness of the controller restart mechanism in mitigating these effects. Without the restart mechanism, disrupted control signals result in prolonged deviations in the system state and a diminished ability to counteract disturbances in real time, leading to substantial performance degradation. In contrast, the use of the restart mechanism significantly improves system robustness and resilience. By detecting the attack and resetting the

controller's internal state, the mechanism enables rapid recovery from communication failures and facilitates a timely return to normal operation. This approach effectively mitigates the adverse effects of DDoS attacks, preserving system stability while minimizing both the duration and severity of the disruption.

These findings underscore the critical importance of incorporating adaptive recovery strategies (such as the controller restart mechanism) into networked control systems operating under adversarial conditions. For applications like UMV systems, where reliable and consistent performance is essential, the restart mechanism offers an efficient and practical means to mitigate the disruptive impact of DDoS attacks. By enabling rapid recovery of stability and functionality after communication breakdowns, this strategy significantly enhances the control system's robustness and cybersecurity resilience. Furthermore, it ensures reliable operation even in bandwidth-constrained and hostile environments, making it a valuable tool for safeguarding high-stakes industrial systems.

5 Conclusion

This study has addressed the critical challenges of communication efficiency, control performance, and cybersecurity in ICSs 4.0 operating under complex environmental conditions. An RLSIS strategy was developed to optimize data transmission frequency dynamically, effectively reducing bandwidth consumption while maintaining the responsiveness required for industrial processes. Additionally, a data quantization scheme was introduced to minimize redundancy and alleviate network congestion, ensuring efficient operation in bandwidth-constrained environments. To enhance cybersecurity, a hybrid detection mechanism and a controller restart strategy were proposed to mitigate the impact of DDoS attacks. These mechanisms provided robust recovery of control signals, ensuring uninterrupted system operation under adverse network conditions. The stability of the proposed methods was rigorously analyzed using the Lyapunov stability theory, offering theoretical guarantees of system performance and resilience. Finally, the proposed strategies were experimentally validated on an industrial network-based UMV system under realistic conditions. The results demonstrated significant improvements in communication efficiency, control accuracy, and resilience against cybersecurity threats, confirming the practical applicability of the methods. These findings underscore the potential of the proposed approaches to advance ICSs 4.0, offering robust and adaptive solutions for dynamic and high-stakes industrial environments. In future work, the proposed centralized framework can be extended to support decentralized or hybrid architectures, enabling scalable and resilient deployment in Industry 4.0/5.0 scenarios.

Acknowledgements This work was supported by Key R&D Program of Shandong Province (Grant No. 2025CXGC010901), National Natural Science Foundation of China (Grant Nos. 62402129, 62272119, 62372126, 62372129, U2436208, U2468204), Guangdong Basic and Applied Basic Research Foundation (Grant Nos. 2026A1515010143, 2020A1515010450, 2021A1515012307), Guangdong S&T Program (Grant No. 2024B0101010002), Guangdong Higher Education Innovation Group (Grant No. 2020KCXTD007), Guangzhou Higher Education Innovation Group (Grant No. 202032854), Guangzhou Basic and Applied Basic Research Fund (Grant Nos. 2025A04J3446, 2024A04J9969), and Guangdong Provincial Key Laboratory of Industrial Control System Security Project (Grant No. 2024B1212020010).

References

1 Monmasson E, Cirstea M N. FPGA design methodology for industrial control systems: a review. IEEE Trans Ind Electron, 2007, 54: 1824–1842
2 Xia Y Q. Cloud-based control systems: towards the control architecture in cloud computing era. Sci China Inf Sci, 2024, 67: 206201
3 Humayed A, Lin J, Li F, et al. Cyber-physical systems security: a survey. IEEE Int Things J, 2017, 4: 1802–1831
4 Zhang P. Advanced Industrial Control Technology. Norwich: William Andrew, 2010. 1–50
5 Yang T, Hao W, Yang Q, et al. Cloud-edge coordinated traffic anomaly detection for industrial cyber-physical systems. Expert Syst Appl, 2023, 230: 120668
6 Kriaa S, Pietre-Cambacedes L, Bouissou M, et al. A survey of approaches combining safety and security for industrial control systems. Rel Eng Syst Saf, 2015, 139: 156–178
7 Zheng T, Ardolino M, Bacchetti A, et al. The applications of Industry 4.0 technologies in manufacturing context: a systematic literature review. Int J Prod Res, 2021, 59: 1922–1954
8 Liu P, Eti S, Yuksel S, et al. Analyzing energy transition for Industry 4.0 driven hybrid energy system selection with advanced neural network-used multi-criteria decision-making technique. Renew Energy, 2024, 232: 121081
9 Chen Y, Lu Y, Bulysheva L, et al. Applications of blockchain in Industry 4.0: a review. Inf Syst Front, 2024, 26: 1715–1729
10 Hao L Y, Zhang Y Q, Shen C, et al. Fault-tolerant control for unmanned marine vehicles via quantized integral sliding mode output feedback technique. IEEE Trans Intell Transp Syst, 2023, 24: 5014–5023
11 Chen H, Zong G, Gao F, et al. Probabilistic event-triggered policy for extended dissipative finite-time control of MJSs under cyber-attacks and actuator failures. IEEE Trans Automat Contr, 2023, 68: 7803–7810
12 Qi W, Yin H, Park J H, et al. Intelligent finite-time protocol-based stabilization for networked UMV systems with DoS attacks. IEEE Trans Intell Transp Syst, 2024, 25: 16734–16744
13 Cui W, Jiang Y, Zhang B. Reinforcement learning for optimal primary frequency control: a Lyapunov approach. IEEE Trans Power Syst, 2022, 38: 1676–1688
14 Ming Z, Zhang H, Yan Y, et al. Adaptive optimal control via Q-learning for Ito fuzzy stochastic nonlinear continuous-time systems with Stackelberg game. IEEE Trans Fuzzy Syst, 2024, 32: 2029–2038
15 Evangelidis A, Dimitriou N, Charalampous P, et al. Efficient deep Q-learning for industrial equipment calibration in elevator manufacturing. IEEE Trans Ind Inf, 2024, 20: 12220–12230
16 Wang Y, Fang W, Ding Y, et al. Computation offloading optimization for UAV-assisted mobile edge computing: a deep deterministic policy gradient approach. Wireless Netw, 2021, 27: 2991–3006

17 Wang N, Gao Y, Zhang X. Data-driven performance-prescribed reinforcement learning control of an unmanned surface vehicle. IEEE Trans Neural Netw Learn Syst, 2021, 32: 5456–5467
18 Wang T, Zong G, Zhao X, et al. Data-driven-based sliding-mode dynamic event-triggered control of unknown nonlinear systems via reinforcement learning. Neurocomputing, 2024, 601: 128176
19 Xu Y, Wu Z G, Che W W, et al. Reinforcement learning-based unknown reference tracking control of HMASs with nonidentical communication delays. Sci China Inf Sci, 2023, 66: 170203
20 Cai X, Shi K, Sun Y, et al. Stability analysis of networked control systems under DoS attacks and security controller design with mini-batch machine learning supervision. IEEE Trans Inf Forensic Secur, 2023, 19: 3857–3865
21 Cai X, Shi K, Sun Y, et al. Intelligent event-triggered control supervised by mini-batch machine learning and data compression mechanism for T-S fuzzy NCSs under DoS attacks. IEEE Trans Fuzzy Syst, 2023, 32: 804–815
22 Conti M, Donadel D, Turrin F. A survey on industrial control system testbeds and datasets for security research. IEEE Commun Surv Tutor, 2021, 23: 2248–2294
23 Ye Z, Zhang D, Wu Z G, et al. A3C-based intelligent event-triggering control of networked nonlinear unmanned marine vehicles subject to hybrid attacks. IEEE Trans Intell Transp Syst, 2021, 23: 12921–12934
24 Xu J, Ma X, Liu J, et al. Automatically identifying imperfections and attacks in practical quantum key distribution systems via machine learning. Sci China Inf Sci, 2024, 67: 202501
25 Ma Y, Nie Z, Hu S, et al. Fault detection filter and controller co-design for unmanned surface vehicles under DoS attacks. IEEE Trans Intell Transp Syst, 2020, 22: 1422–1434
26 Dong J, Ye Z, Zhang D. Finite-time security control of networked unmanned marine vehicle systems subject to DoS attack. IEEE Trans Intell Veh, 2024, 9: 3464–3477
27 Hu S, Yue D, Han Q L, et al. Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. IEEE Trans Cybern, 2020, 50: 1952–1964
28 Shi K, Cai X, She K, et al. Stability analysis and security-based event-triggered mechanism design for T-S fuzzy NCS with traffic congestion via DoS attack and its application. IEEE Trans Fuzzy Syst, 2023, 31: 3639–3651
29 Song L, Tong S. Finite-time resilient integral sliding-mode control for fuzzy impulsive stochastic system under denial-of-service attacks. IEEE Trans Fuzzy Syst, 2024, 32: 2930–2939
30 Xiong D, Zhang C K, Wan X, et al. Stability and stabilization of T-S fuzzy systems under sampled-data control via a matrix-separation-based inequality. IEEE Trans Fuzzy Syst, 2024, 32: 4312–4323
31 Kazemy A, Lam J, Zhang X M. Event-triggered output feedback synchronization of master-slave neural networks under deception attacks. IEEE Trans Neural Netw Learn Syst, 2020, 33: 952–961
32 Li T F, Lu J, Zhu J. Periodic sampled-data-based dynamic model control of switched linear systems. J Franklin Inst, 2022, 359: 8539–8552
33 Shen Y, Yao W, Wen J, et al. Adaptive wide-area power oscillation damper design for photovoltaic plant considering delay compensation. IET Gener Transm Distrib, 2017, 11: 4511–4519
34 Yao W, Jiang L, Wen J Y, et al. Wide-area damping controller for power system interarea oscillations: a networked predictive control approach. IEEE Trans Contr Syst Technol, 2014, 23: 27–36