# Input-retention Strategies for Secure Synchronization of Piecewise Markov Neural Networks under Hybrid Cyber-attacks

Yuting Cao, Shanshan Zhao, Shiping Wen, *Senior Member, IEEE*, and Tingwen Huang, *Fellow, IEEE*

***Abstract*—How to achieve synchronization control for Piecewise Homogeneous Markov Delayed Neural Networks (PHMDNNs) under hybrid cyber-attacks is the primary focus of this research. Firstly, a Piecewise Homogeneous Markov Process (PHMP) is employed to model the mode transitions of system parameters and controllers, accurately capturing the dynamic characteristics of practical systems and providing a solid foundation for subsequent controller design. In response to the challenges arising from hybrid cyber-attacks, a novel controller is developed based on an input retention strategy. This ensures system stability under hybrid cyber-attacks, effectively avoiding the instability issues caused by traditional zero-input strategies and enhancing control robustness. To further optimize system performance, an improved Resilient Adaptive Event-triggered Mechanism (RAETM) is proposed. By optimizing triggering conditions and thresholds, the mechanism reduces communication overhead while strengthening system security, making it well-suited for networked control systems. In addition, a generalized common Lyapunov functional is constructed by incorporating sampling instants, time delays, and Markov jump parameters. Sufficient conditions for system synchronization and stability are derived, providing a simplified analytical framework. Finally, the effectiveness and superiority of the proposed approach are confirmed through simulation results, showcasing its robust performance against hybrid cyber-attacks and its ability to achieve secure synchronization.**

***Index Terms*—Delayed Neural Networks, Piecewise Homogeneous Markov Process, hybrid cyber-attacks, Resilient Adaptive Event-triggered Mechanism, input retention strategy, secure synchronization control.**

## I. Introduction

In the last few decades, Neural Networks (NNs) have seen remarkable advancements, extending their applications to biomedicine, chemical production, and aerospace. However, in practice, NNs often exhibit undesirable behaviors, including parameter mutations and state delays. These issues typically arise from external disturbances, component failures, or unpredictable factors, leading to instability, oscillations, or even chaotic dynamics [1, 2]. To model the dynamics of NNs with parameter mutations and state delays more accurately, Markov Delayed Neural Networks (MDNNs) were first introduced in [3], where parameter mutations are modeled as a Homogeneous Markov Process (HMP) with a fixed Mode Transmission Rate (MTR). As a result, MDNNs have drawn increasing research attention in areas such as stability analysis [2], state estimation [4], and synchronization control [5–8]. Among these, synchronization control plays a crucial role in applications such as image processing, signal transmission, and secure communications. However, parameter mutations and state delays can significantly degrade synchronization performance and even cause its failure. Thus, investigating synchronization control for MDNNs is of great theoretical and practical significance.

It is worth mentioning that most studies on the synchronization control problem of MDNNs [9] share a common assumption: the mode transitions of system parameters and the controller are driven by the same HMP with a constant MTR [10]. Nevertheless, this assumption may not be valid in real-world applications. In many cases, the mode transitions of system parameters and the controller may be semi-dependent, as the physical plant and the controller are often deployed in distinct working environments. Semi-dependence implies that the mode transitions of system parameters are influenced not only by their own dynamics but also by those of the controller. This renders the traditional HMP framework inadequate for such scenarios. Fortunately, PHMP, a special type of non-homogeneous Markov process with time-varying MTRs, provides a powerful modeling tool for capturing semi-dependent dynamics. Consequently, PHMP has received significant attention in recent years for analyzing and synthesizing various systems. For instance, the asynchronous filtering design problem for PHMJSs with quantization is addressed in [11], the output feedback control issue of PHMJSs is studied in [12], and the mean stabilization of positive PHMJSs is investigated

Shanshan Zhao's work was supported in part by the China Scholarship Council. *(Corresponding author: Tingwen Huang.)*

Y. Cao and T. Huang are with Faculty of Computer Science and Control Engineering, Shenzhen University of Advanced Technology, Shenzhen 518055, China (caoyuting@suat-sz.edu.cn; huangtingwen@suat-sz.edu.cn). S. Zhao and S. Wen are with the Australian AI Institute, Faculty of Engineering and Information Technology, The University of Technology Sydney, Sydney, NSW 2007, Australia (e-mail: shanshan.zhao@student.uts.edu.au; shiping.wen@uts.edu.au).

Table I: Notations and their meanings

| Symbol | Meaning | Symbol | Meaning |
|---|---|---|---|
| $\mathbb{N}$ | Set of non-negative integers. | $E\{\cdot\}$ | Mathematical expectation. |
| $S_n^+$ | Set of symmetric matrices. | $col\{\cdots\}$ | Column vector. |
| $\mathbb{R}^n$ | $n$-dimensional Euclidean space. | $diag\{\cdots\}$ | Diagonal matrix. |
| $\mathbb{R}^{n\times n}$ | $n\times n$-dimensional real matrix space. | $\lambda_{\max}(P)$ | Largest eigenvalue of matrix $P$. |
| $\Pr\{\alpha\}$ | Probability of occurrence of event $\alpha$. | $\lambda_{\min}(P)$ | Smallest eigenvalue of matrix $P$. |
| $\Pr\{\alpha\|\beta\}$ | Probability of occurrence of $\alpha$ conditional on $\beta$. | $P>0$ ($P<0$) | Positive (negative) definite matrix. |
| $\|\cdot\|$ | Euclidean norm. | $P^T$ | Transposition of matrix $P$. |
| $sym\{Y\}$ | Symmetric part of $Y$: $Y+Y^T$. | $P^{-1}$ | Inverse of matrix $P$. |
| $\Omega$ | Event-triggering weight matrix. | $*$ | Symmetric term in a symmetric matrix. |
| $\Xi$ | Attack-modified state term. | | |

in [13]. Although significant advancements have been made, the synchronization control of PHMDNNs remains largely unexplored. Bridging this gap serves as the primary motivation for this study.

With the integration of wireless communication technologies, MDNNs often rely on networked environments for synchronization control. While this enhances flexibility and scalability, it also introduces vulnerabilities to hybrid cyber-attacks [14, 15], including Denial of Service (DoS) and deception attacks. These attacks disrupt communication channels and inject false information, posing significant challenges to system stability and security. Existing studies have made efforts to address hybrid cyber-attacks on networked systems, such as exponential synchronization under stochastic hybrid cyber-attacks [16], security filtering design under DoS and deception attacks [17], and event-triggered control for Markov systems with hybrid cyber-attacks [18]. However, most of these works focus on modeling attacks from the attacker's perspective, overlooking practical defensive strategies. This paper adopts a defense-oriented approach, proposing a novel periodic fluctuation model for non-periodic DoS attacks, which provides a more realistic and practical representation from the defender's perspective. Furthermore, most existing works assume that the control input vanishes when communication is disrupted, adopting a zero-input strategy. However, this assumption often leads to system performance degradation, as the absence of control input can cause instability and desynchronization in practical applications. To mitigate this issue, this paper considers an input retention strategy, which preserves the latest available control input during communication outages. By maintaining system actuation even under attack conditions, this strategy enhances robustness against hybrid cyber-attacks and improves synchronization resilience. Despite significant progress, the security synchronization control of MDNNs under hybrid cyber-attacks, particularly in the PHMP framework, has received limited attention. This forms the second motivation of this study.

Moreover, due to the challenges posed by cyber-attacks, parameter mutations, and state delays, it is essential to design a safer, more efficient, and cost-effective control strategy for NNs, particularly under limited network resources, such as sensor energy, communication bandwidth, and processor capacity. To address these challenges, Resilient Adaptive Event-triggered Mechanisms (RAETMs) have gained significant attention in recent years for their ability to reduce redundant signal transmission and optimize resource utilization [19, 20]. RAETMs adjust the trigger threshold dynamically based on the system's error state, ensuring timely responses to disturbances while avoiding excessive communication. Compared with traditional event-triggered mechanisms [21], RAETMs introduce resilience by incorporating adaptive strategies that can adjust the triggering condition in real time, enhancing the system's robustness under uncertain environments such as hybrid cyber-attacks [22–24]. For instance, [22] explores an adaptive event-triggered law for improving networked control systems under cyber-attacks, and [24] designs a resilient mechanism that optimizes communication by dynamically tuning the trigger threshold based on real-time state feedback. These studies demonstrate the potential of RAETMs in addressing both safety and efficiency challenges in networked environments. However, most existing RAETMs focus on static or overly simplified adaptive laws, which may limit their performance under complex system dynamics. In this paper, we propose an improved RAETM that optimizes the triggering condition by refining both the trigger threshold and error state dynamics. This enhanced mechanism reduces communication burden while maintaining system stability and synchronization under hybrid cyber-attacks.

Building on the above analysis, this study focuses on the security synchronization control of PHMDNNs under hybrid cyber-attacks. The primary contributions of this work can be outlined as follows:

- A novel controller design is developed by leveraging the PHMP framework, which accurately captures mode-dependent transitions of system parameters. To enhance robustness against hybrid cyber-attacks, an input retention strategy is introduced, effectively mitigating instability caused by conventional zero-input strategies under DoS attacks.

- A refined RAETM is proposed, improving both triggering conditions and threshold adaptation. This mechanism significantly reduces communication overhead while strengthening system security, effectively addressing the challenges posed by hybrid cyber-attacks.
- A generalized common Lyapunov functional is constructed, incorporating sampling instants, time delays, and Markov jump parameters. This framework simplifies the theoretical analysis and provides rigorous sufficient conditions for synchronization and stability under hybrid cyber-attacks.

To ensure clarity and consistency, the notations used in this paper are systematically summarized in Table I.

## II. Preliminaries

Consider the following PHMDNNs:

$$\begin{aligned}\dot{m}(t) =& -B_{\alpha(t)}m(t) + B_{1\alpha(t)}f(m(t)) \\ &+ B_{2\alpha(t)}f(m(t-d(t)))\end{aligned} \tag{1}$$

Here, $m(t) \in \mathbb{R}^n$ represents the system state vector, while $d(t) \in [0, d]$ corresponds to the time-varying delay, satisfying $0 < \dot{d}(t) \leq \mu$. The matrices $B_\alpha(t), B_{1\alpha}(t), B_{2\alpha}(t) \in \mathbb{R}^{n\times n}$ are known, and the neuron activation function $f(m(t)) \in \mathbb{R}^n$ is defined as $f(m(t)) = col\{f_1(m_1(t)), \ldots, f_n(m_n(t))\}$, where $f_l(0) = 0$. Moreover, for known constants $\varpi_l^-, \varpi_l^+ (l = 1, 2, \ldots, n)$, the following inequality holds:

$$\varpi_l^- \leq \frac{f_l(m_1) - f_l(m_2)}{m_1 - m_2} \leq \varpi_l^+, \forall m_1 \neq m_2. \tag{2}$$

The process $\{\alpha(t), t \geq 0\}$ is a continuous-time PHMP that takes values from the finite set $\Pi_1 = \{1, 2, ..., N\}$. Its mode transition probability is governed by the time-varying MTR matrix $P^{\beta(t+\Delta)} = \left[p_{mn}^{\beta(t+\Delta)}\right]_{N\times N}$, which can be expressed as:

$$\begin{aligned}&\Pr\{\alpha(t+\Delta) = n | \alpha(t) = m\} \\ &= \begin{cases} p_{mn}^{\beta(t+\Delta)}\Delta + o(\Delta), & \text{if} m \neq n, \\ 1 + p_{mm}^{\beta(t+\Delta)}\Delta + o(\Delta), & \text{if} m = n. \end{cases}\end{aligned} \tag{3}$$

Here, $\Delta > 0$, and the term $o(\Delta)$ satisfies $\lim_{\Delta\to 0} \frac{o(\Delta)}{\Delta} = 0$. The non-diagonal elements $p_{mn}^{\beta(t+\Delta)} \geq 0$ $(\forall m \neq n)$ represent the MTR from mode $m$ at time $t$ to mode $n$ at time $t + \Delta$. For the diagonal elements, the following condition must hold: $p_{mm}^{\beta(t+\Delta)} = -\sum_{n=1, m\neq n}^{N} p_{mn}^{\beta(t+\Delta)}$.

Similar to the process $\{\alpha(t), t \geq 0\}$, the process $\{\beta(t), t \geq 0\}$ represents a continuous-time HMP, which assumes values from the finite set $\Pi_2 = \{1, 2, ..., M\}$. The mode transition probability, governed by the constant MTR matrix $\bar{P} = [\rho_{kl}]_{M\times M}$, is expressed as:

$$\begin{aligned}&\Pr\{\beta(t+\Delta) = l | \beta(t) = k\} \\ &= \begin{cases} \rho_{kl}\Delta + o(\Delta), & k \neq l, \\ 1 + \rho_{kk}\Delta + o(\Delta), & k = l. \end{cases}\end{aligned} \tag{4}$$

Here, $\Delta > 0$, and the term $o(\Delta)$ satisfies $\lim_{\Delta\to 0} \frac{o(\Delta)}{\Delta} = 0$. The coefficient $\rho_{kl} \geq 0$ $(\forall k \neq l)$ denotes the MTR from mode $k$ at time $t$ to mode $l$ at time $t+\Delta$, while the diagonal elements satisfy the condition: $\rho_{kk} = -\sum_{l=1, k\neq l}^{M} \rho_{kl}$. The high-level signal $\{\beta(t), t \geq 0\}$ dictates the switching MTR matrix of the low-level signal $\{\alpha(t), t \geq 0\}$, which, in turn, determines the switching dynamics or topology structure modes.

In this study, the system described by (1) is referred to as the master system, while its corresponding slave system is defined as:

$$\begin{aligned}\dot{s}(t) =& -B_{\alpha(t)}s(t) + B_{1\alpha(t)}f(s(t)) \\ &+ B_{2\alpha(t)}f(s(t-d(t))) + u(t)\end{aligned} \tag{5}$$

Here, the matrices $B_{\alpha(t)}$, $B_{1\alpha(t)}$, and $B_{2\alpha(t)}$ are those specified in the master system (1), and $u(t) \in \mathbb{R}^n$ represents the control input. Let the synchronization error between the master and slave systems be defined as $z(t) = s(t) - m(t)$. Accordingly, the error dynamics can be expressed as:

$$\begin{aligned}\dot{z}(t) =& -B_{\alpha(t)}z(t) + B_{1\alpha(t)}w(z(t)) \\ &+ B_{2\alpha(t)}w(z(t-d(t))) + u(t)\end{aligned} \tag{6}$$

The term $w(z(t))$ is defined as $w(z(t)) = f(s(t)) - f(m(t))$, and the control input $u(t)$ is formulated as:

$$u(t) = -K_{\alpha(t),\beta(t)}z(t) \tag{7}$$

Here, $K_{\alpha(t),\beta(t)}$ denotes the controller gains, which depend on the modes $\alpha(t)$ and $\beta(t)$, and will be determined in subsequent sections.

## III. Problems and Methods

Consider aperiodic DoS attacks based on the concept of cyclic fluctuation of time series, where $T > 0$ and $T_{off}^n$ $(n = 1, 2, 3, \cdots)$ is a variable parameter within each cycle. The attack sequence $A_{Dos}(t)$ is defined as:

$$A_{Dos}(t) = \begin{cases} 0, t \in \mathrm{H}_1^n \\ 1, t \in \mathrm{H}_2^n \end{cases} \tag{8}$$

where $\mathrm{H}_1^n \triangleq \left[nT, nT + T_{off}^n\right)$ denotes the time interval during which the attack signals are inactive, allowing communications, and $\mathrm{H}_2^n \triangleq \left[nT + T_{off}^n, (n+1)T\right)$ denotes the time interval during which the attack signals are active, disrupting communications.

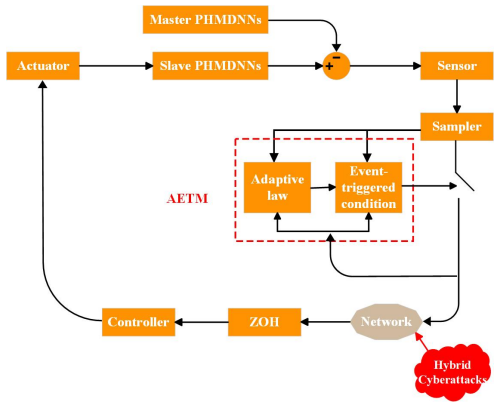


Figure 1: Framework of system under hybrid cyber-attacks.

Since aperiodic DoS attacks disrupt communication by intermittently denying transmission, traditional ETMs struggle to maintain system stability. To address this challenge, this paper introduces a RAETM, which dynamically adjusts the triggering threshold to enhance robustness and reduce unnecessary transmissions under DoS attacks. During the operation of the RAETM, the next triggering instant $t_{k+1}^n h$ is determined as follows:

$$t_{k+1}^n h = \begin{cases} t_k^n h + \min\limits_{j \in N} \Phi(jh), & t_k^n h + jh \in \mathrm{H}_1^n \\ t_{\mathrm{last}}^n h, & t_k^n h + jh \in \mathrm{H}_2^n \end{cases} \tag{9}$$

where $\Phi(jh) = \{jh | e^T(t_k^n + jh)\Omega e(t_k^n + jh) \geq \delta(t_k^n + jh) z^T(t_k^n)\Omega z(t_k^n)\}$, $0 < h < T$, $n$, $j \in N$, and $k$ is the trigger number occurring in the $n$th attack operation cycle, and $t_{k_{last}}^n h$ denotes the last triggered instant of the last DoS attacks dormant period $\mathrm{H}_1^n$. The triggering threshold is adaptively designed based on the state variations: $\delta\left(t_k^n h + jh\right) = a_1[1 - \frac{2}{\pi}\arctan(a_2(\frac{\|z(t_k^n h + jh)\| - \|z(t_k^n h)\|}{\|z(t_k^n h)\|} - \sigma))]$, and for the last triggering instant in each period: $\delta\left((n+1)T\right) = a_1[1 - \frac{2}{\pi}\arctan(a_2(\frac{\|z(t_{k_{last}}^n h + jh)\| - \|z(t_{k_{last}}^n h)\|}{\|z(t_{k_{last}}^n h)\|} - \sigma))]$, where $\sigma \in [0, 1]$ is a sensitivity parameter that adjusts the system's responsiveness to state variations, $a_1 \in (0, 1]$ is a scaling factor controlling the maximum threshold value, and $a_2 \in (0, 10]$ is a sensitivity adjustment parameter that amplifies the effect of state variations on the threshold. This adaptive mechanism allows the threshold to dynamically decrease when the state variation is large, ensuring a prompt reaction and enhanced control performance. Conversely, smaller variations lead to a higher threshold, effectively reducing redundant triggers and conserving communication resources.

**Remark 1.** *The proposed event-triggered threshold $\delta\left(t_k^n h + jh\right)$ is designed to achieve an effective balance between system responsiveness and communication efficiency, especially under hybrid cyber-attacks like DoS. Here, $\sigma$ defines the system's sensitivity to state variations, allowing the threshold to decrease during large changes for quicker response and increase during smaller changes to reduce unnecessary triggering. Parameters $a_1$ and $a_2$ are included to adjust the scaling and sensitivity of the threshold, providing flexibility to suit different system requirements. This design enables the system to respond effectively to critical disturbances while reducing communication overhead during stable periods. The absence of dependency on historical data simplifies implementation and enhances real-time adaptability. In summary, the proposed event-triggered threshold provides a robust, efficient, and practical solution for ensuring stability and efficiency under hybrid cyber-attacks.*

To counteract the impact of DoS attacks, the control input (7) is adjusted through an input retention strategy:

$$u(t) = \begin{cases} -K_{\alpha(t),\beta(t)}^1 z\left(t_k^n h\right), t \in \widehat{\mathrm{H}_1^n} \\ -K_{\alpha(t),\beta(t)}^2 z\left(t_{k_{last}}^n h\right), t \in \mathrm{H}_2^n \end{cases} \tag{10}$$

where, $\widehat{\mathrm{H}_1^n} = \left[t_k^n h, t_{k+1}^n h\right) \cap \mathrm{H}_1^n$.

**Remark 2.** *This paper proposes an RAETM to address the challenges of single-channel DoS attacks in networked control systems. When DoS attacks occur, the communication channel is blocked, preventing the transmission of control signals. However, the sampler and the event-triggering device remain operational, allowing local sampling signals to be generated. To mitigate the impact of DoS attacks, a trigger signal retention strategy is employed. During DoS attacks, the triggering instant $t_{k+1}^n h$ is set to the last triggered signal $t_{k_{last}}^n h$ stored in the buffer during the attack's dormant period. This ensures that when the communication channel recovers, the retained trigger signal can be directly utilized to restore control actions, thereby maintaining system stability and avoiding disruptions caused by signal unavailability.*

**Remark 3.** *As illustrated in Fig. 1, the control strategy during DoS attacks incorporates the keep-input strategy to ensure system robustness. Specifically, when the communication channel is blocked due to DoS attacks, the ZOH mechanism is employed to maintain the last control input $t_{k_{last}}^n h$ from the dormant period of the attack. This approach ensures that the system operates continuously and reliably during the communication interruption, while providing flexibility and adaptability to handle transitions between active and dormant communication states.*

Signals transmitted over communication networks are prone to spoofing attacks. To increase the success rate and concealment of such attacks, attackers often inject malicious signals in a randomized fashion. To characterize this behavior, a random variable $\wp(k)$, following a Bernoulli distribution with $E\{\wp(k)\} = \wp$, is utilized.

Specifically, $\wp(k) = 1$ signifies the occurrence of an attack, while $\wp(k) = 0$ indicates that the sampled data is transmitted without interference.

Let the deception attack signal be represented by a nonlinear function $\tilde{z}(t)$, which is randomly introduced into the control input signal. Considering the energy limitation of the attack, the attack signal is bounded. Accordingly, the following assumption is established:

**Assumption 1.** *[25] For the attack signal $\tilde{z}(t)$, there exists a constant matrix $L$ such that:*

$$\|\tilde{z}(t)\|^2 \leq \|Lz(t)\|^2. \tag{11}$$

As a result, the control input (10) is modified under the influence of hybrid cyber-attacks to:

$$u(t) = \begin{cases} -K^1_{\alpha(t),\beta(t)}\Xi(t^n_k h, k), t \in \widehat{\mathrm{H}^n_1} \\ -K^2_{\alpha(t),\beta(t)} z\left(t^n_{k_{last}} h\right), t \in \mathrm{H}^n_2 \end{cases} \tag{12}$$

where, $\Xi(t^n_k h, k) = \wp(k)\,\tilde{z}(t^n_k h) + (1-\wp(k))\,z(t^n_k h)$.

**Remark 4.** *When the DoS attacks take place, a large number of signals flood into the network communication channel, resulting in the triggering signals not being able to be transmitted normally, so it is pointless to consider deception attacks within $\mathrm{H}^n_2$. Meanwhile, as shown in Fig. 2, for the hybrid cyber-attacks, this paper adopts the input hold strategy, i.e., when the DoS attacks take place, the control signals from the last trigger moment $t^n_{k_{last}} h$ of the last DoS attack dormant period are used to control the system.*

Based on the preceding analysis, the system (6) can be expressed as:

$$\dot{z}(t) = \begin{cases} \Theta(t) - \Gamma_1(t), t \in \widehat{\mathrm{H}^n_1} \\ \Theta(t) - \Gamma_2(t), t \in \mathrm{H}^n_2 \end{cases} \tag{13}$$

where, $\Theta(t) = -B_{\alpha(t)}z(t) + B_{1\alpha(t)}w(z(t)) + B_{2\alpha(t)}w(z(t-d(t)))$, $\Gamma_1(t) = K^1_{\alpha(t),\beta(t)}\Xi(t^n_k h, k)$, $\Gamma_2(t) = K^2_{\alpha(t),\beta(t)} z\left(t^n_{k_{last}} h\right)$ and the initial value $z(\theta) = \zeta(\theta)$, $\theta \in [-d, 0]$. This state-space formulation characterizes the system's response under adversarial conditions, capturing both DoS-induced input losses and deception-induced perturbations. However, while this formulation provides a comprehensive dynamical description, it does not inherently guarantee synchronization stability. Therefore, a rigorous stability analysis is required to formally establish sufficient conditions for ensuring robust synchronization under hybrid cyber-attacks. The next section presents a Lyapunov-based framework that systematically addresses these challenges.

## IV. Main Results

The presence of hybrid cyber-attacks introduces significant challenges in ensuring synchronization stability, due to the stochasticity and adversarial nature of these disturbances. To systematically address these challenges, this section develops a comprehensive stability analysis framework using Lyapunov theory, providing a rigorous foundation for guaranteeing the resilience of the proposed control strategy. In preparation for subsequent analysis, the following vectors and functions are specified:

$$\begin{aligned}
\iota^T_1(t) &= \Big[\ z^T(t) \quad \dot{z}^T(t) \quad z^T(t-d) \quad z^T(t-d(t)) \\
&\quad w^T(z(t)) \quad w^T(z(t-d(t))) \quad \left(\tfrac{1}{d(t)}\int^t_{t-d(t)} z(s)\,ds\right)^T \\
&\quad \left(\tfrac{1}{d-d(t)}\int^{t-d(t)}_{t-d} z(s)\,ds\right)^T \quad z^T(t^n_k h + jh)\ \Big], \\
\mathrm{I}^T_1(t) &= \Big[\ \iota^T_1(t) \quad z^T(t^n_k h) \quad \tilde{z}^T(t^n_k h)\ \Big], \\
\mathrm{I}^T_2(t) &= \Big[\ \iota^T_1(t) \quad z^T\left(t^n_{k_{last}} h\right)\ \Big], \\
e_i &= col\left\{0, \cdots, 0, \underbrace{I}_{o_1}, 0, \cdots, 0\right\}, (o_1 = 1, 2, \cdots, 11), \\
\tilde{e}_i &= col\left\{0, \cdots, 0, \underbrace{I}_{o_2}, 0, \cdots, 0\right\}, (o_2 = 1, 2, \cdots, 10).
\end{aligned}$$

**Theorem 1.** *For given constants $\gamma_1$, $\gamma_2$, $\eta_i$, $h$, $a_1$, $a_2$, $\sigma$, $\mu \in (0,1)$, and the deception attack parameter $\wp$, as well as the DoS attack parameters $k_1 > 0$, $\chi > 0$, and $T$, the following condition must be satisfied:*

$$\bar{\gamma}_k = k_1\bar{\Pi}_{1k} - k_2\bar{\Pi}_{2k} > 0, \tag{14}$$

*where $\bar{\Pi}_k = \bar{\Pi}_{1k} + \bar{\Pi}_{2k}$, $\bar{\Pi}_{1k} = \left(kT + T^k_{off}\right) - kT$, $\bar{\Pi}_{2k} = (k+1)T - \left(kT + T^k_{off}\right)$, and $k = 1, 2, 3, \ldots$. Suppose there exist scalars $d > 0$, $\psi > 0$, symmetric matrices $P_{m,k} > 0$, $S_c > 0$ $(c = 1, 2, 3)$, $\Omega > 0$, $H > 0$, $W > 0$, and a block matrix $V = \begin{bmatrix} V_1 & V_2 \\ * & V_3 \end{bmatrix} > 0$, along with given matrices $L_1$, $L_2$, $L$, $Q$, $M_1$, $M_2$, $X^1_{m,k}$, $Y^1_{m,k}$, $X^2_{m,k}$, and $Y^2_{m,k}$. If the following inequalities hold:*

$$\Xi_{m,k} + \Xi_1 + h\Xi_2 < 0, \Xi_{m,k} + \Xi_1 + h\Xi_3 < 0, \tag{15}$$

$$\Theta_{m,k} + \Theta_1 + h\Theta_2 < 0, \Theta_{m,k} + \Theta_1 + h\Theta_3 < 0, \tag{16}$$

*where,*

$$\begin{aligned}
\Xi_{m,k} =& k_1 e^T_1 P_{m,k} e_1 + sym\left\{e^T_1 P_{m,k} e_2\right\} \\
&+ e^T_1\left[\sum_{l\in\Pi_2}\rho_{kl}P_{m,k} + \sum_{n\in\Pi_1} p^k_{mn}P_{n,k}\right]e_1 \\
&+ e^T_1 S_1 e_1 - e^{-k_1 d}e^T_3 S_1 e_3 + e^T_1 S_2 e_1 \\
&- (1-\mu)\,e^{-k_1 d}e^T_4 S_2 e_4 + e^T_5 S_3 e_5 \\
&- (1-\mu)\,e^{-k_1 d}e^T_6 S_3 e_6 - e^{-k_1 d}\varpi^T_1\psi\varpi_1 \\
&+ \delta_{\min}e^T_{10}\Omega e_{10} - (e_9 - e_{10})^T\Omega(e_9 - e_{10}) \\
&+ e^T_{11}L^T L e_{11} - e^T_{10} I e_{10} + d^2 e^T_2 H_1 e_2 \\
&- sym\left\{(e_5 - L_1 e_1)^T M_1 (e_5 - L_2 e_1)\right\}
\end{aligned}$$

$$
\begin{aligned}
&- sym\left\{(e_6 - L_1e_4)^T M_2 (e_6 - L_2e_4)\right\} \\
&sym\left\{\left[e_1^T + \gamma_1 e_2^T + \gamma_2[\wp e_{11} + (1-\wp)e_{10}]^T\right]\right. \\
&\left.\phi_{m,k}^1\right\}, \\
\varpi_1 =& col\{e_1 - e_4, e_1 + e_4 - 2e_7, e_4 - e_3, \\
&e_4 + e_3 - 2e_8\}, \\
\phi_{m,k}^1 =& - Y_{m,k}^1 e_2 - Y_{m,k}^1 B_m e_1 + Y_{m,k}^1 B_{1m} e_5 \\
&+ Y_{m,k}^1 B_{2m} e_6 - X_{m,k}^1 [\wp e_{11} + (1-\wp)e_{10}], \\
\bar{H} =& \begin{bmatrix} H & 0 \\ 0 & 3H \end{bmatrix}, \psi = \begin{bmatrix} \bar{H} & Q \\ Q^T & \bar{H} \end{bmatrix}, \Xi_2 = e_9^T V_4 e_9, \\
\Xi_1 =& -\frac{1}{h}(e_1 - e_9)^T V_1 (e_1 - e_9) - 2(e_1 - e_9)^T V_2 e_9 \\
&- \begin{bmatrix} e_1 \\ e_9 \end{bmatrix}^T W \begin{bmatrix} e_1 \\ e_9 \end{bmatrix}, \\
\Xi_3 =& \begin{bmatrix} e_2 \\ e_9 \end{bmatrix}^T V \begin{bmatrix} e_2 \\ e_9 \end{bmatrix} + 2\begin{bmatrix} e_1 \\ e_9 \end{bmatrix}^T W \begin{bmatrix} e_2 \\ 0 \end{bmatrix}, \\
\Theta_{m,k} =& - k_1 \tilde{e}_1^T P_{m,k} \tilde{e}_1 + 2\tilde{e}_1^T P_{m,k} \tilde{e}_2 + \tilde{e}_5^T S_3 \tilde{e}_5 \\
&+ \tilde{e}_1^T \left[\sum_{l\in\Pi_2} \rho_{kl} P_{m,k} + \sum_{n\in\Pi_1} p_{mn}^k P_{n,k}\right] \tilde{e}_1 \\
&+ \tilde{e}_1^T S_1 \tilde{e}_1 - e^{-k_1 d} \tilde{e}_3^T S_1 \tilde{e}_3 + \tilde{e}_1^T S_2 \tilde{e}_1 \\
&- (1-\mu) e^{-k_1 d} \tilde{e}_4^T S_2 \tilde{e}_4 + d^2 \tilde{e}_2^T H_1 \tilde{e}_2 \\
&- (1-\mu) e^{-k_1 d} \tilde{e}_6^T S_3 \tilde{e}_6 - e^{-k_1 d} \varpi_2^T \psi_1 \varpi_2 \\
&- sym\left\{(\tilde{e}_5 - L_1\tilde{e}_1)^T M_1 (\tilde{e}_5 - L_2\tilde{e}_1)\right\} \\
&- sym\left\{(\tilde{e}_6 - L_1\tilde{e}_4)^T M_2 (\tilde{e}_6 - L_2\tilde{e}_4)\right\} \\
&+ \delta_{\min} \tilde{e}_{10}^T \Omega \tilde{e}_{10} - (\tilde{e}_9 - \tilde{e}_{10})^T \Omega (\tilde{e}_9 - \tilde{e}_{10}) \\
&+ sym\left\{\left(\tilde{e}_1^T + \gamma_1 \tilde{e}_2^T + \gamma_2 \tilde{e}_{10}^T\right)\phi_{m,k}^2\right\}, \\
\varpi_2 =& col\{\tilde{e}_1 - \tilde{e}_4, \tilde{e}_1 + \tilde{e}_4 - 2\tilde{e}_7, \tilde{e}_4 - \tilde{e}_3, \\
&\tilde{e}_4 + \tilde{e}_3 - 2\tilde{e}_8\}, \\
\phi_{m,k}^2 =& - Y_{m,k}^2 \tilde{e}_2 - Y_{m,k}^2 B_m \tilde{e}_1 + Y_{m,k}^2 B_{1m} \tilde{e}_5 \\
&+ Y_{m,k}^2 B_{2m} \tilde{e}_6 - X_{m,k}^2 \tilde{e}_{10}, \\
\Theta_1 =& - \frac{1}{h}(\tilde{e}_1 - \tilde{e}_9)^T V_1 (\tilde{e}_1 - \tilde{e}_9) - 2(\tilde{e}_1 - \tilde{e}_9)^T V_2 \tilde{e}_9 \\
&- \begin{bmatrix} \tilde{e}_1 \\ \tilde{e}_9 \end{bmatrix}^T W \begin{bmatrix} \tilde{e}_1 \\ \tilde{e}_9 \end{bmatrix}, \Theta_2 = \tilde{e}_9^T V_4 \tilde{e}_9, \\
\Theta_3 =& \begin{bmatrix} \tilde{e}_2 \\ \tilde{e}_9 \end{bmatrix}^T V \begin{bmatrix} \tilde{e}_2 \\ \tilde{e}_9 \end{bmatrix} + 2\begin{bmatrix} \tilde{e}_1 \\ \tilde{e}_9 \end{bmatrix}^T W \begin{bmatrix} \tilde{e}_2 \\ 0 \end{bmatrix}.
\end{aligned}
$$

*As a result, the error system (13) is exponentially mean square stable under hybrid cyber-attacks, with the controller gains given by* $K_{m,k}^1 = \left(Y_{m,k}^1\right)^{-1} X_{m,k}^1$ *and* $K_{m,k}^2 = \left(Y_{m,k}^2\right)^{-1} X_{m,k}^2$.

**Proof**. To begin with, let $\alpha(t) = m$, $\beta(t) = k$ ($m \in \Pi_1$, $k \in \Pi_2$), and the following Lyapunov-Krasovskii functional is taken into account:

$$\bar{V}(z(t), m, k) = V(z(t), m, k) + \nu(z(t), m, k), \tag{17}$$

where $\nu(z(t), m, k) = e^{-k_1 t} v(z(t), m, k)$ and

$$
\begin{aligned}
V(z(t), m, k) =& \sum_{k=1}^{3} V_k(z(t), m, k), \qquad (18)\\
V_1(z(t), m, k) =& z^T(t) P_{m,k} z(t), \\
V_2(z(t), m, k) =& \int_{t-d}^{t} e^{-k_1(t-s)} z^T(s) S_1 z(s) ds \\
&+ \int_{t-d(t)}^{t} e^{-k_1(t-s)} z^T(s) S_2 z(s) ds \\
&+ \int_{t-d(t)}^{t} e^{-k_1(t-s)} w^T(z(s)) S_3 w(z(s)) ds, \\
V_3(z(t), m, k) =& d\times \\
&\int_{t-d}^{t}\int_{u}^{t} e^{-k_1(t-s)} \dot{z}^T(s) H \dot{z}(s) ds du, \\
v(z(t), m, k) =& \sum_{c=1}^{2} v_c(z(t), m, k), \qquad (19)\\
v_1(z(t), m, k) =& [(t_k^n h + (j+1)h) - t] \times \\
&\int_{t_k^n h + jh}^{t} \begin{bmatrix} \dot{z}(s) \\ z(t_k^n h + jh) \end{bmatrix}^T V \begin{bmatrix} \dot{z}(s) \\ z(t_k^n h + jh) \end{bmatrix} ds, \\
v_2(z(t), m, k) =& [(t_k^n h + (j+1)h) - t] \times \\
&\begin{bmatrix} z(t) \\ z(t_k^n h + jh) \end{bmatrix}^T W \begin{bmatrix} z(t) \\ z(t_k^n h + jh) \end{bmatrix}.
\end{aligned}
$$

When $t \in \widehat{\mathrm{H}_1^n}$, by utilizing the weak infinitesimal generator $L$ of the Markov process along the Lyapunov-Krasovskii functional, the following results can be derived:

$$
\begin{aligned}
LV_1(z(t), m, k) =& 2z^T(t) P_{m,k} \dot{z}(t) \\
&+ z^T(t) \left[\sum_{l\in\Pi_2} \rho_{kl} P_{m,k} + \sum_{n\in\Pi_1} p_{mn}^k P_{n,k}\right] z(t), \qquad (20)\\
LV_2(z(t), m, k) \le& -k_1 V_2(z(t), m, k) \\
&+ z^T(t) S_1 z(t) - e^{-k_1 d} z^T(t-d) S_1 z(t-d) \\
&+ z^T(t) S_2 z(t) + w^T(z(t)) S_3 w(z(t)) \\
&- (1-\mu) e^{-k_1 d} w^T(z(t-d(t))) S_3 w^T(z(t-d(t))) \\
&- (1-\mu) e^{-k_1 d} z^T(t-d(t)) S_2 z(t-d(t)), \qquad (21)\\
LV_3(z(t), m, k) \le& -k_1 V_3(z(t), m, k) \\
&+ d^2 \dot{z}^T(t) H_1 \dot{z}(t) - d e^{-k_1 d} \int_{t-d}^{t} \dot{z}^T(s) H_1 \dot{z}(s) ds. \qquad (22)
\end{aligned}
$$

By applying Corollary 4 from [26] and Theorem 1 from [27], the integral terms in (22) can be bounded by

the following inequalities:

$$-de^{-k_1 d}\int_{t-d}^{t}\dot{z}^T(s)H_1\dot{z}(s)ds \le -e^{-k_1 d}\mathrm{I}_1^T(t)\varpi_1^T\psi\varpi_1\mathrm{I}_1(t). \quad (23)$$

From (2), it follows that:

$$-\left(w(z(t))-L_1z(t)\right)^T M_1\left(w(z(t))-L_2z(t)\right)\ge 0, \quad (24)$$

$$-\left(w(z(t-d(t)))-L_1z(t-d(t))\right)^T M_2\times \left(w(z(t-d(t)))-L_2z(t-d(t))\right)\ge 0. \quad (25)$$

For scalars $\gamma_1$ and $\gamma_2$ and matrix $Y^1_{m,k}$, the coming equation is valid:

$$0=\mathrm{I}_1^T(t)\,sym\left\{\left[e_1^T+\gamma_1 e_2^T+\gamma_2[\wp e_{11}+(1-\wp)e_{10}]^T\right]\phi^1_{m,k}\right\}\mathrm{I}_1(t), \quad (26)$$

where, $X^1_{m,k}=Y^1_{m,k}K^1_{m,k}$.

Based on (20)-(26), Assumption 1, and the RAETM (9), the following conclusion can be drawn:

$$LV(w(t),m,k)-k_1V(w(t),m,k) \le \mathrm{I}_1^T(t)\Xi_{m,k}\mathrm{I}_1(t). \quad (27)$$

The expression for the derivative of $v(z(t),m,k)$ is as follows:

$$\dot{v}_1(z(t),m,k)= -\int_{t_kh+jh}^{t}\begin{bmatrix}\dot{z}(s)\\ z(t_kh+jh)\end{bmatrix}^T V\begin{bmatrix}\dot{z}(s)\\ z(t_kh+jh)\end{bmatrix}ds + [(t_kh+(j+1)h)-t]\times \left[\begin{bmatrix}\dot{z}(t)\\ z(t_kh+jh)\end{bmatrix}^T V\begin{bmatrix}\dot{z}(t)\\ z(t_kh+jh)\end{bmatrix}\right], \quad (28)$$

$$\dot{v}_2(z(t),m,k)= -\begin{bmatrix}z(t)\\ z(t_kh+jh)\end{bmatrix}^T W\begin{bmatrix}z(t)\\ z(t_kh+jh)\end{bmatrix} + 2[(t_kh+(j+1)h)-t]\times \begin{bmatrix}z(t)\\ z(t_kh+jh)\end{bmatrix}^T W\begin{bmatrix}\dot{z}(t)\\ 0\end{bmatrix}. \quad (29)$$

Through the application of Jensen's inequality and by summarizing the aforementioned inequalities, we finally obtain:

$$\dot{v}(z(t),m,k)\le I_1^T(t)\{\Xi_1+(t-(t_kh+jh))\Xi_2 +((t_kh+(j+1)h)-t)\Xi_3\}I_1(t). \quad (30)$$

Based on (27) and (30), the following inequality can be derived:

$$L\bar{V}(z(t),m,k)+k_1\bar{V}(z(t),m,k)\le \mathrm{I}_1^T(t)\left\{\frac{t-(t_kh+jh)}{h}(\Xi_{m,k}+\Xi_1+h\Xi_2) +\frac{(t_kh+(j+1)h)-t}{h}(\Xi_{m,k}+\Xi_1+h\Xi_3)\right\}\mathrm{I}_1(t). \quad (31)$$

From LMIs (15), we have $L\bar{V}(z(t),m,k)+k_1\bar{V}(z(t),m,k)\le 0$. Afterwards, when $t\in\widehat{\mathrm{H}_1^n}$, the following inequality is gained:

$$L\bar{V}(z(t),\alpha(t),\beta(t))\le -k_1\bar{V}(z(t),\alpha(t),\beta(t)). \quad (32)$$

Inequality (31) characterizes the dynamic property of the system in the absence of DoS attacks. When transitioning to conditions with DoS attacks, and for $t\in\mathrm{H}_2^n$, the term $\bar{V}(z(t),m,k)$ can be directly derived as follows:

$$L\bar{V}(z(t),m,k)-k_1\bar{V}(z(t),m,k)\le \mathrm{I}_2^T(t)\left\{\frac{t-(t_kh+jh)}{h}(\Theta_{m,k}+\Theta_1+h\Theta_2) +\frac{(t_kh+(j+1)h)-t}{h}(\Theta_{m,k}+\Theta_1+h\Theta_3)\right\}\mathrm{I}_2(t). \quad (33)$$

To establish the relationship between $\bar{V}(z(t),\alpha(t),\beta(t))$ and $\bar{V}(z(0),\alpha(0),\beta(0))$, assume $k_1+k_2=\chi>0$. Accordingly, for $t\in\mathrm{H}_2^n$, the following inequality can be derived from LMIs (16):

$$L\bar{V}(z(t),\alpha(t),\beta(t))\le k_2\bar{V}(z(t),\alpha(t),\beta(t)). \quad (34)$$

From (32) and (34), and using Dynkin's formula, we derive the following results. When the system state satisfies $t\in\mathrm{H}_1^n$, the expected value of the Lyapunov function is given by:

$$\mathbb{E}\bar{V}(z(t),\alpha(t),\beta(t)) \le e^{-k_1(t-nT)}\mathbb{E}\bar{V}(z(nT),\alpha(nT),\beta(nT)). \quad (35)$$

Similarly, when $t\in\mathrm{H}_2^n$, we obtain:

$$\mathbb{E}\bar{V}(z(t),\alpha(t),\beta(t))\le e^{k_2\left[t-\left(nT+T^n_{off}\right)\right]}\times \mathbb{E}\bar{V}\left(z(nT+T^n_{off}),\alpha(nT+T^n_{off}),\beta(nT+T^n_{off})\right). \quad (36)$$

Next, based on (35) and (36), the following inequalities are derived. When $t\in\mathrm{H}_1^n$, we have:

$$\mathbb{E}\bar{V}\left(z(nT+T^n_{off}),\alpha(nT+T^n_{off}),\beta(nT+T^n_{off})\right) \le e^{-k_1\left[(nT+T^n_{off})-nT\right]}\times\mathbb{E}\bar{V}\left(r(nT),\alpha(nT),\beta(nT)\right). \quad (37)$$

Similarly, when $t \in \mathrm{H}_2^n$, we obtain:

$$\begin{aligned}&\mathbb{E}\bar{V}\big(z((n+1)T),\alpha((n+1)T),\beta((n+1)T)\big)\\&\leq e^{k_2\left[(n+1)T-(nT+T_{off}^n)\right]_\times}\\&\mathbb{E}\bar{V}\big(z(nT+T_{off}^n),\alpha(nT+T_{off}^n),\beta(nT+T_{off}^n)\big).\end{aligned} \tag{38}$$

For $t \in [nT, nT+T_{off}^n)$, (35), (36), (37) and (38) imply that:

$$\begin{aligned}&\mathbb{E}\bar{V}\left(z\left(t\right),\alpha\left(t\right),\beta\left(t\right)\right)\\&\leq e^{-k_1(t-nT)}\mathbb{E}\bar{V}\left(z\left(nT\right),\alpha\left(nT\right),\beta\left(nT\right)\right)\\&\vdots\\&\leq e^{-\sum\limits_{k=1}^{n-1}\bar{\gamma}_k}\mathbb{E}\bar{V}\left(z\left(0\right),\alpha\left(0\right),\beta\left(0\right)\right).\end{aligned} \tag{39}$$

For $t \in [nT+T_{off}^n, (n+1)T)$, the following expression can be derived:

$$\begin{aligned}&\mathbb{E}\bar{V}\left(z\left(t\right),\alpha\left(t\right),\beta\left(t\right)\right)\\&\leq e^{-\sum\limits_{k=1}^{n}\bar{\gamma}_k}\mathbb{E}\bar{V}\left(z\left(0\right),\alpha\left(0\right),\beta\left(0\right)\right).\end{aligned} \tag{40}$$

Using (39) and (40) with $\bar{\gamma}_k > 0$, and considering (2), for $t \in \mathrm{H}_1^n \cup \mathrm{H}_2^n$, the following is obtained:

$$\begin{aligned}&\mathbb{E}\bar{V}\left(z\left(t\right),\alpha\left(t\right),\beta\left(t\right)\right)\\&\leq \mathbb{E}\bar{V}\left(z\left(0\right),\alpha\left(0\right),\beta\left(0\right)\right)\\&= \mathbb{E}V\left(z\left(0\right),\alpha\left(0\right),\beta\left(0\right)\right)\\&\leq \lambda_{\max}\left(P_{m,k}\right)\left\|z\left(0\right)\right\|^2\\&+\lambda_{\max}\left(S_1\right)\frac{1-e^{-dk_1}}{k_1}\sup_{-d\leq\xi\leq 0}\left\|z\left(\xi\right)\right\|^2\\&+\lambda_{\max}\left(S_2\right)\frac{1-e^{-dk_1}}{k_1}\sup_{-d\leq\xi\leq 0}\left\|z\left(\xi\right)\right\|^2\\&+\lambda_{\max}\left(S_3\right)\varpi_l^+\frac{1-e^{-dk_1}}{k_1}\sup_{-d\leq\xi\leq 0}\left\|z\left(\xi\right)\right\|^2\\&+\lambda_{\max}\left(H\right)\frac{d^2k_1-d+de^{-dk_1}}{k_1^2}\sup_{-d\leq\xi\leq 0}\left\|\dot{z}\left(\xi\right)\right\|^2\\&\leq \kappa_1\sup_{-d\leq\xi\leq 0}\left\|z\left(\xi\right)\right\|^2+\kappa_2\sup_{-d\leq\xi\leq 0}\left\|\dot{z}\left(\xi\right)\right\|^2,\end{aligned} \tag{41}$$

where, $\kappa_1 = \lambda_{\max}\left(P_{m,k}\right) + \lambda_{\max}\left(S_1\right)\frac{1-e^{-dk_1}}{k_1} + \lambda_{\max}\left(S_2\right)\frac{1-e^{-dk_1}}{k_1} + \lambda_{\max}\left(S_3\right)\varpi_l^+\frac{1-e^{-dk_1}}{k_1}$ and $\kappa_2 = \lambda_{\max}\left(H\right)\frac{d^2k_1-d+de^{-dk_1}}{k_1^2}$.

By combining the definition of $\bar{V}\left(z\left(t\right),\alpha\left(t\right),\beta\left(t\right)\right)$, it is evident that:

$$\mathbb{E}\|z\left(t\right)\|^2 \leq \varepsilon e^{-k_1 t}\sup_{-d\leq\xi\leq 0}\left\{\left\|z\left(\xi\right)\right\|^2,\left\|\dot{z}\left(\xi\right)\right\|^2\right\}, \tag{42}$$

where, $\varepsilon = \frac{\kappa_1+\kappa_2}{\lambda_{\min}(P_{m,k})}$. According to Definition 1 in [28], the error system (6) is exponentially mean square stable, ensuring synchronization between the master and slave systems.

**Remark 5.** *In existing studies, most research adopts the zero-input strategy for DoS attacks and constructs switching Lyapunov functionals to handle the dormant and active periods of DoS attacks [29]. However, this approach often introduces more constraints and increases conservativeness. To address these issues, this paper proposes a single Lyapunov functional for different periods of DoS attacks, aiming to reduce constraints and conservativeness while maintaining system stability. Furthermore, the loop functional is incorporated into the single Lyapunov functional to account for additional state information at the sampled instant. Specifically, the constructed loop functional $v(t)$ fully considers the state information at the current instant $z\left(t\right)$ and the sampled instant $z\left(t_kh+jh\right)$. Notably, the matrices in $v\left(z\left(t\right),m,k\right)$ are not required to be positive definite, as the condition $v_c\left(t_kh+jh\right) = v_c\left(t_kh+\left(j+1\right)h\right) = 0$, $c = 1, 2$, satisfies the cyclic functional property proposed in [30].*

## V. Numerical Examples

**Example 1.** *Consider the PHMDNNs (6) with the following parameter setup:*

$$\textbf{\textit{Mode 1:}}\ B_1=\begin{bmatrix}1&0\\0&1\end{bmatrix},\ B_{11}=\begin{bmatrix}2&-0.4\\-5&3\end{bmatrix},\ B_{21}=\begin{bmatrix}-1.5&-0.1\\0.2&-2.5\end{bmatrix}$$

$$\textbf{\textit{Mode 2:}}\ B_2=\begin{bmatrix}0.8&0\\0&0.8\end{bmatrix},\ B_{12}=\begin{bmatrix}2&-0.11\\-2&3.2\end{bmatrix},\ B_{22}=\begin{bmatrix}-1.6&-0.1\\-0.18&-2.4\end{bmatrix}.$$

*Let* $w\left(z\left(t\right)\right) = 0.5\left(|z(t)+1| - |z(t)-1|\right)$, $m(0) = col\{0.25, 0.35\}$ *and* $s(0) = col\{-0.3, -0.4\}$, *and* $L_1 = diag\{0, 0\}$, $L_2 = diag\{0.5, 0.5\}$. *Set the DoS attacks parameters to* $k_1 = 0.2$, $\gamma = 0.4$, $T = 1$, *we can calculate* $\mathrm{T}_{off}^{\min} = 0.5$ *by Theorem1. Set the deception attacks parameters to* $\wp = 0.4$, $\tilde{z}\left(t\right) = col\{tanh(-0.06z_1(t)), tanh(-0.06z_2(t))\}$. *When* $q = 3$, *set the weight of the HTS as* $b_1 = 0.5$, $b_2 = 0.3$, $b_3 = 0.2$. *Set event trigger parameters as* $a_1 = 1$, $a_2 = 1$, $\sigma = 0.1$. *Other parameters are defined that* $h = 0.1$, $d = 0.1$, $\eta_1 = 0.5$, $\eta_2 = 0.3$, $\eta_3 = 0.2$, $\gamma_1 = \gamma_2 = 0.2$ *and* $\mu = 0.1$.

*The MTR matrices of* $\{\alpha\left(t\right), t \geq 0\}$ *for each modes in* $\Pi_1 = 1, 2, 3$ *are given as:*

$$P_1=\begin{bmatrix}-4.5&4.5\\3.75&-3.75\end{bmatrix}, P_2=\begin{bmatrix}-2.75&2.75\\3&-3\end{bmatrix},$$

$$P_3=\begin{bmatrix}-4&4\\1.5&-1.5\end{bmatrix},$$

*and the MTR matrix of* $\{\beta(t), t \geq 0\}$ *is as follows:*

$$\bar{P} = \begin{bmatrix} -4.5 & 2 & 2.5 \\ 4.5 & -7.5 & 3 \\ 1 & 2 & -3 \end{bmatrix}.$$

*Then, applying Theorem1, we can get:*

$$K_{11}^1 = \begin{bmatrix} 3.1059 & 0.3164 \\ 0.1408 & 3.2075 \end{bmatrix},$$
$$K_{21}^1 = \begin{bmatrix} 0.3036 & -0.1341 \\ -0.0896 & 0.5039 \end{bmatrix},$$
$$K_{12}^1 = \begin{bmatrix} 0.3126 & 0.0346 \\ 0.0164 & 0.3167 \end{bmatrix},$$
$$K_{22}^1 = \begin{bmatrix} 0.3079 & -0.1307 \\ -0.0884 & 0.5080 \end{bmatrix},$$
$$K_{13}^1 = \begin{bmatrix} 0.3199 & 0.0348 \\ 0.0138 & 0.3359 \end{bmatrix},$$
$$K_{23}^1 = \begin{bmatrix} 0.2916 & -0.1395 \\ -0.0914 & 0.4935 \end{bmatrix},$$
$$K_{11}^2 = \begin{bmatrix} 0.2924 & -0.0851 \\ -0.1112 & 0.6664 \end{bmatrix},$$
$$K_{21}^2 = \begin{bmatrix} 0.3171 & -0.0791 \\ -0.1002 & 0.5795 \end{bmatrix},$$
$$K_{12}^2 = \begin{bmatrix} 0.2938 & -0.0818 \\ -0.1100 & 0.6685 \end{bmatrix},$$
$$K_{22}^2 = \begin{bmatrix} 0.3219 & -0.0793 \\ -0.0995 & 0.5833 \end{bmatrix},$$
$$K_{13}^2 = \begin{bmatrix} 0.2976 & -0.0845 \\ -0.1115 & 0.6704 \end{bmatrix},$$
$$K_{23}^2 = \begin{bmatrix} 0.3060 & -0.0766 \\ -0.0989 & 0.5680 \end{bmatrix},$$
$$\Omega = \begin{bmatrix} 13.9920 & 0.0058 \\ 0.0058 & 13.9300 \end{bmatrix}.$$

*Figs. 2–7 illustrate the simulation results of the proposed method under hybrid cyber-attacks, demonstrating its effectiveness in maintaining system synchronization and stability. Fig. 2 presents the master-slave synchronization of the error system with control input during hybrid cyber-attacks. The results confirm that the proposed method ensures synchronization between the master and slave systems even in the presence of severe attack disturbances, highlighting its robustness and adaptability. Fig. 3 shows the state responses of the error system without control input under hybrid cyber-attacks. It is evident that in the absence of control input, the system experiences severe synchronization degradation, with significant deviations occurring during attack periods. This comparison underscores the critical role of the proposed control strategy in maintaining synchronization and stability. Fig. 4 and Fig. 6 analyze the release intervals of the event-triggered mechanism, which dynamically adjusts in response to system state variations. This self-adaptive mechanism increases the triggering frequency when the system encounters severe disturbances and reduces it when stability is restored, effectively minimizing unnecessary communication overhead. Fig. 5 further illustrates the control input* $u(t)$*, which adapts dynamically to mitigate attack-induced fluctuations, ensuring system stability. Fig. 7 visualizes the hybrid cyber-attacks, including deception attacks, revealing that such attacks predominantly occur during the dormant phases of DoS attacks. By leveraging the adaptive event-triggering mechanism, the system strategically increases triggering frequency during these phases, enabling faster stabilization and synchronization.*

*Overall, the simulation results validate the proposed method's superiority in handling complex attack scenarios. Compared to conventional event-triggered strategies, the proposed approach achieves faster recovery, enhanced robustness against cyber-attacks, and optimized communication efficiency.*

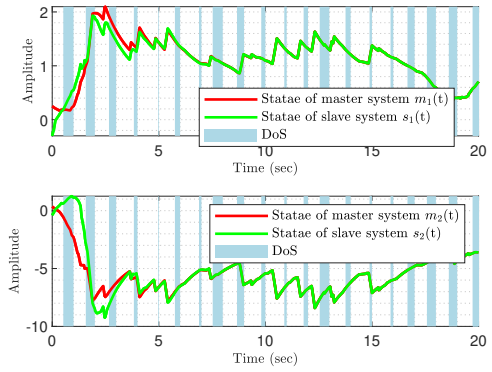


Figure 2: Master-slave synchronization of the error system with control input.

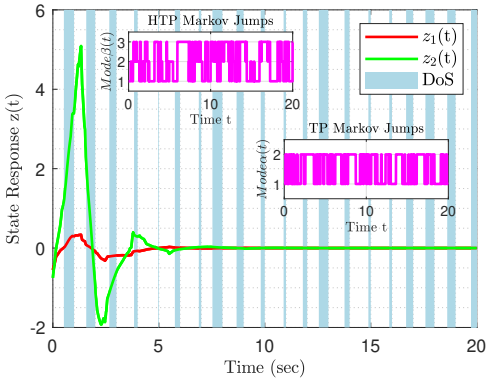


Figure 3: Synchronization errors for the PHMDNNs with control input.

*The combined results demonstrate the superiority of the proposed method. The adaptive event-triggered mechanism increases triggering frequency during dormant periods of hybrid cyber-attacks, enabling rapid stabilization and synchronization while effectively reducing unnecessary communication. These advantages validate*

*the robustness and efficiency of the proposed method in addressing complex attack scenarios.*

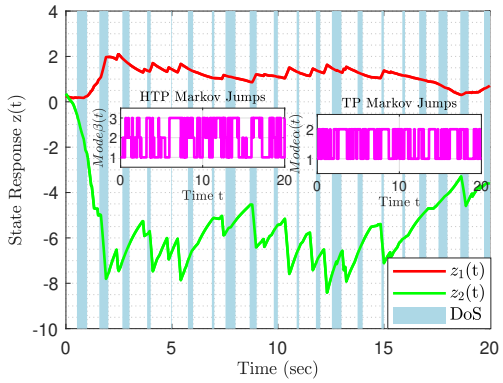


Figure 4: Synchronization errors for the PHMDNNs without control input.

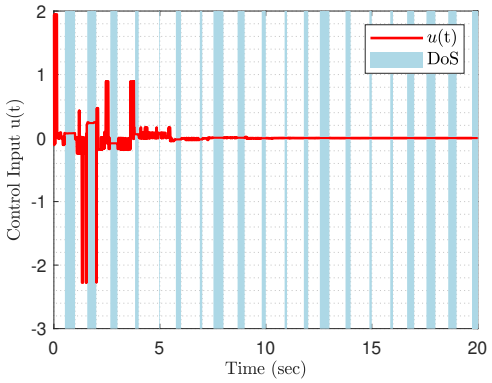


Figure 5: Control input $u(t)$.

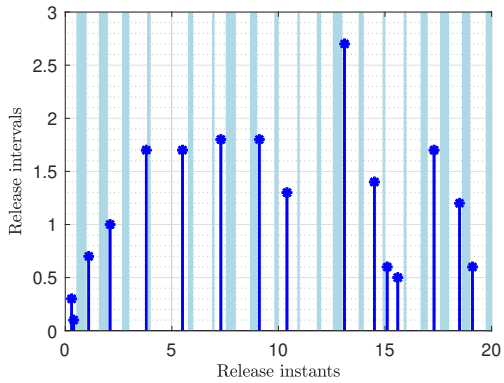


Figure 6: Release time intervals.

**Example 2.** *This example is designed to compare the proposed input-retention strategy with the zero-input strategy under hybrid cyber-attacks. The objective is to highlight the advantages of the proposed method in maintaining synchronization and stability while improving communication efficiency in complex attack scenarios.*

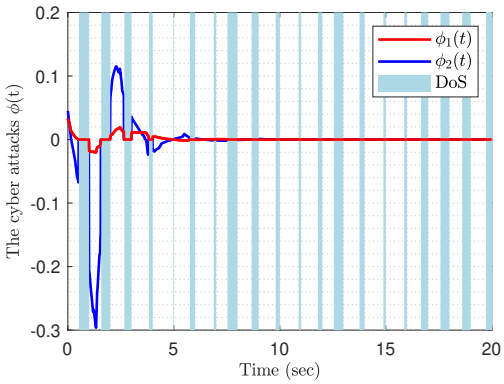


Figure 7: The hybrid cyber-attacks.

*Figs. 8–10 compare the system performance under the zero-input strategy and the proposed input-retention strategy (Figs. 2–7) when subjected to hybrid cyber-attacks. The simulation results clearly illustrate the limitations of the zero-input strategy and the improvements brought by the proposed method, particularly in synchronization accuracy, attack resilience, and communication efficiency.*

*Fig. 8 depicts the synchronization errors of the error system under the zero-input strategy. During attack periods, the system fails to maintain synchronization, and large deviations are observed. These errors indicate that, without control input, the system cannot counteract disturbances introduced by hybrid cyber-attacks. In contrast, the proposed input-retention strategy (Fig. 2) demonstrates rapid synchronization recovery and stability, even under severe attack conditions. This improvement stems from the ability of input retention to maintain control action during DoS-induced communication disruptions, effectively preventing abrupt synchronization failures.*

*Fig. 9 illustrates the event-triggering intervals under the zero-input strategy. The lack of an adaptive event-triggering mechanism results in inefficient communication scheduling, leading to redundant transmissions and poor synchronization performance. Without a dynamic adaptation mechanism, the triggering intervals remain largely constant, failing to account for varying attack intensities. In contrast, the proposed approach (Fig. 6) dynamically regulates the triggering intervals based on the system state, achieving an optimal balance between communication efficiency and synchronization performance. This self-adaptive triggering significantly reduces unnecessary transmissions while ensuring stable synchronization.*

*Fig. 10 visualizes the hybrid cyber-attacks and their effects on the zero-input strategy. It is evident that, during*

*the dormant phases of DoS attacks, the zero-input strategy struggles to recover synchronization, causing severe instability. In particular, the absence of control input leads to prolonged desynchronization, as the system is unable to respond effectively during these periods. Conversely, the proposed input-retention strategy (Fig. 7) increases triggering frequency during these phases, allowing the system to counteract attacks effectively and regain stability in a shorter time. This proactive adjustment ensures that the system remains resilient against cyber-attacks and minimizes long-term performance degradation.*

*In summary, the simulation results validate the advantages of the proposed input-retention strategy over conventional zero-input approaches. By integrating an adaptive event-triggering mechanism with robust control inputs, the proposed method significantly improves synchronization accuracy, enhances resilience to hybrid cyber-attacks, and optimizes communication efficiency. These findings underscore the practical feasibility of the proposed method for real-world networked control systems.*

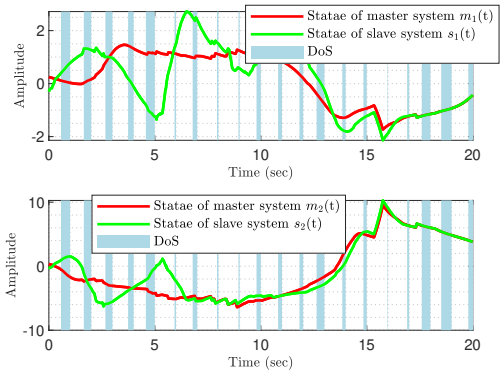


Figure 8: Master-slave synchronization of the error system with control input.

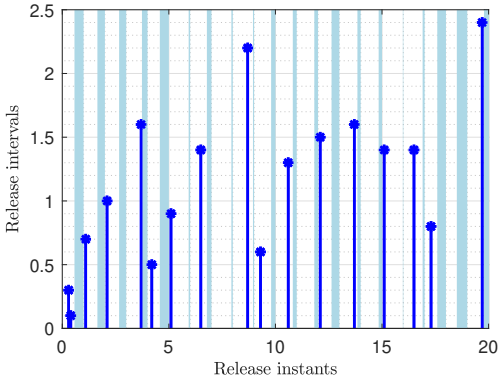


Figure 9: Release time intervals.

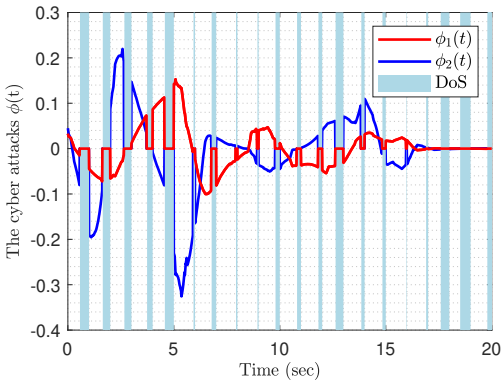


Figure 10: The hybrid cyber-attacks.

## VI. Conclusions

In this paper, an input-retention strategy based on an AETM is proposed to address the synchronization control of PHMDNNs under hybrid cyber-attacks. The proposed method integrates robust control with a dynamic event-triggered mechanism, ensuring system synchronization, stability, and communication efficiency. Theoretical analysis and numerical simulations demonstrate that our approach achieves faster convergence, reduced communication overhead, and improved robustness against cyber-attacks compared to conventional zero-input strategies. These contributions highlight the practical significance of our framework in modern cyber-physical systems.

Future research may explore several promising directions. First, adaptive event-triggered optimization methods can be introduced to dynamically adjust triggering thresholds based on real-time system states and attack intensities. Second, integrating machine learning techniques, such as DRL, can facilitate intelligent event-triggered mechanisms and proactive cyber-attack detection. Finally, extending this framework to multi-agent systems and decentralized control architectures could further broaden its applicability in large-scale networked environments. Additionally, investigating hybrid control strategies that integrate event-triggered and time-triggered mechanisms could enhance robustness against varying network conditions. Furthermore, applying the proposed method to real-world scenarios such as power grids and industrial IoT systems would provide valuable insights into its practical feasibility.

## References

[1] Z. Wang, Y. Liu, l. Yu, and X. Liu, "Exponential stability of delayed recurrent neural networks with markovian jumping parameters," *Physics Letters A*, vol. 356, pp. 346–352, 08 2006.

[2] Z. Wu, P. Shi, H. Su, and J. Chu, "Stability analysis for discrete-time markovian jump neural networks with mixed time-delays," *Expert Systems with Applications*, vol. 39, no. 6, pp. 6174–6181, 2012.

[3] Z. Wang, Y. Liu, L. Yu, and X. Liu, "Exponential stability of delayed recurrent neural networks with markovian jumping parameters," *Physics Letters A*, vol. 356, no. 4, pp. 346–352, 2006.
[4] Q. Li, Q. Zhu, S. Zhong, X. Wang, and J. Cheng, "State estimation for uncertain markovian jump neural networks with mixed delays," *Neurocomputing*, vol. 182, pp. 82–93, 2016.
[5] Z. Li, Z. Chen, T. Fang, and H. Shen, "Extended dissipativity-based synchronization of markov jump neural networks subject to partially known transition and mode detection information," *Neurocomputing*, vol. 517, pp. 201–212, 2023.
[6] D. Zhang, J. Cheng, J. Cao, and D. Zhang, "Finite-time synchronization control for semi-markov jump neural networks with mode-dependent stochastic parametric uncertainties," *Applied Mathematics and Computation*, vol. 344-345, pp. 230–242, 2019.
[7] Q. Ma, S. Xu, and Y. Zou, "Stability and synchronization for markovian jump neural networks with partly unknown transition probabilities," *Neurocomputing*, vol. 74, no. 17, pp. 3404–3411, 2011.
[8] X. Yang, Z. Feng, J. Feng, and J. Cao, "Synchronization of discrete-time neural networks with delays and markov jump topologies based on tracker information," *Neural Networks*, vol. 85, pp. 157–164, 2017.
[9] Y. Shen, Z.-G. Wu, P. Shi, H. Su, and T. Huang, "Asynchronous filtering for markov jump neural networks with quantized outputs," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 2, pp. 433–443, 2018.
[10] P. Shi and F. Li, "A survey on markovian jump systems: modeling and design," *International Journal of Control, Automation and Systems*, vol. 13, pp. 1–16, 2015.
[11] C. Gong, G. Zhu, and P. Shi, "Secure and asynchronous filtering for piecewise homogeneous markov jump systems with quantization and round-robin communication," *Information Sciences*, vol. 640, p. 119032, 2023.
[12] Y. Men and J. Sun, "Output feedback control of piecewise homogeneous semi-markov jump systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 70, no. 2, pp. 546–550, 2022.
[13] L. Wang, Z.-G. Wu, and Y. Shen, "Asynchronous mean stabilization of positive jump systems with piecewise-homogeneous markov chain," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 10, pp. 3266–3270, 2021.
[14] J. Liu, Y. Gu, L. Zha, Y. Liu, and J. Cao, "Event-triggered $h\infty$ load frequency control for multiarea power systems under hybrid cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1665–1678, 2019.
[15] Z. Lian, P. Shi, C. C. Lim, and X. Yuan, "Fuzzy-model-based lateral control for networked autonomous vehicle systems under hybrid cyber-attacks," *IEEE Transactions on Cybernetics*, vol. 53, no. 4, pp. 2600–2609, 2022.
[16] T. Wu, S. Gorbachev, H.-K. Lam, J. H. Park, L. Xiong, and J. Cao, "Adaptive event-triggered space-time sampled-data synchronization for fuzzy coupled rdnns under hybrid random cyberattacks," *IEEE Transactions on Fuzzy Systems*, vol. 31, no. 6, pp. 1855–1869, 2023.
[17] Y. Deng, H. Lu, and W. Zhou, "Security event-triggered filtering for delayed neural networks under denial-of-service attack and randomly occurring deception attacks," *Neural Processing Letters*, pp. 5273–5298, Dec 2022.
[18] X. Gao, F. Deng, P. Zeng, and H. Zhang, "Adaptive neural event-triggered control of networked markov jump systems under hybrid cyberattacks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 3, pp. 1502–1512, 2023.
[19] K. Zhang, R. Su, H. Zhang, and Y. Tian, "Adaptive resilient event-triggered control design of autonomous vehicles with an iterative single critic learning framework," *IEEE transactions on neural networks and learning systems*, vol. 32, no. 12, pp. 5502–5511, 2021.
[20] N. Zhao, P. Shi, W. Xing, and C. P. Lim, "Resilient adaptive event-triggered fuzzy tracking control and filtering for nonlinear networked systems under denial-of-service attacks," *IEEE Transactions on Fuzzy Systems*, vol. 30, no. 8, pp. 3191–3201, 2021.
[21] W. P. Heemels, K. H. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *2012 ieee 51st ieee conference on decision and control (cdc)*. IEEE, 2012, pp. 3270–3285.
[22] A. Wang, M. Fei, Y. Song, C. Peng, D. Du, and Q. Sun, "Secure adaptive event-triggered control for cyber-physical power systems under denial-of-service attacks," *IEEE Transactions on Cybernetics*, pp. 1–12, Jan 2023.
[23] R. Zhang, D. Zeng, J. H. Park, Y. Liu, and X. Xie, "Adaptive event-triggered synchronization of reaction-diffusion neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 8, pp. 3723–3735, Aug 2021.
[24] W. Qi, G. Zong, and W. X. Zheng, "Adaptive event-triggered smc for stochastic switching systems with semi-markov process and application to boost converter circuit model," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 2, pp. 786–796, Feb 2021.
[25] X. Sun, Z. Gu, F. Yang, and S. Yan, "Memory-event-trigger-based secure control of cloud-aided active suspension systems against deception attacks," *Information Sciences*, vol. 543, pp. 1–17, 2021.
[26] A. Seuret and G. Frederic, "Wirtinger-based integral inequality: Application to time-delay systems," *Automatica*, vol. 49, no. 9, pp. 2860–2866, 2013.
[27] P. G. Park, J. Ko, and C. Jeong, "Reciprocally convex approach to stability of systems with time-varying delays," *Automatica*, vol. 47, no. 1, pp. 235–238, 2011.
[28] N. Akbari, A. Sadr, A. Kazemy, and M. Faraji-Niri, "Exponential synchronization of a complex dynamical network with piecewise-homogeneous markovian jump structure and coupling delay," in *2019 6th International Conference on Control, Instrumentation and Automation (ICCIA)*, 2019, pp. 1–6.
[29] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic dos jamming attacks," *IEEE Transactions on Cybernetics*, vol. 49, no. 12, pp. 4271–4281, 2019.
[30] A. Seuret, "Brief paper: A novel stability analysis of linear systems under asynchronous samplings," *Automatica*, vol. 48, pp. 177–182, 01 2012.