This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI: 10.1109/JIOT.2026.3690405, IEEE Internet of Things Journal

PID-Based Secure Cluster Synchronization of Discrete-Time Nonlinear IoT Networks Under Stochastic Replay Attacks

Yunjie Chen, Zidong Wang, Yurong Liu, and Weihao Song

***Abstract*—Large-scale Internet of Things (IoT) systems are characterized by massive numbers of interconnected devices, heterogeneous dynamics, and complex interaction structures, which can be effectively modeled using complex networks. In many IoT applications, secure cluster synchronization is essential for coordinated and reliable operation, yet it is highly vulnerable to cyber-attacks, particularly replay attacks that maliciously reuse previously transmitted but valid data. This paper investigates the secure cluster synchronization problem for discrete-time nonlinear complex networks representing IoT systems under stochastic replay attacks. A probabilistic replay attack model with bounded consecutive attack duration is introduced to capture the random and intermittent characteristics of realistic attack behaviors. To mitigate the adverse impact of replayed information, a PID-based cluster synchronization control strategy is developed, where proportional, integral, and derivative actions are jointly exploited to enhance robustness against outdated and compromised signals. By constructing an appropriate Lyapunov functional and employing stochastic analysis techniques, sufficient conditions are derived to guarantee asymptotic mean-square cluster synchronization. A systematic controller synthesis procedure is further provided. Numerical simulations demonstrate the effectiveness and improved resilience of the proposed approach compared with conventional proportional control schemes.**

***Index Terms*—Internet of Things; Secure synchronization; Cluster synchronization; PID control; Replay attacks; Discrete-time nonlinear systems; Cyber-physical security.**

I. Introduction

Complex networks (CNs) [1] consist of a large number of dynamically interacting nodes connected through structured topologies, where nodes represent individual components and edges characterize their interaction relationships. Due to their ability to capture large-scale interconnectivity, heterogeneous node dynamics, and complex interaction patterns, CNs have been widely employed to model real-world systems with similar characteristics, including power grids [32], biological neural networks [19], social networks [4], cyber-physical systems [51], and transportation networks [14]. In recent years, such modeling paradigms have also become increasingly relevant for Internet of Things (IoT) systems, which are composed of massive numbers of heterogeneous devices interconnected through communication networks.

From a system-theoretic perspective, CNs provide an effective and widely accepted representation framework for IoT networks, enabling rigorous analysis of their large-scale dynamical behaviors. Owing to the tight coupling among nodes and the large-scale nature of IoT-oriented CNs, the analysis of network dynamics has attracted significant research interest. Representative research topics include stability analysis [6], [7], [16], [25], synchronization [40], [42], [53], and state estimation [18], [41], [50]. Among these topics, synchronization plays a fundamental role in coordinating the behaviors of distributed IoT devices and ensuring reliable operation of large-scale IoT systems.

Synchronization aims to drive network nodes toward collective behaviors through appropriately designed control strategies. Various synchronization patterns have been extensively investigated, including complete synchronization [28], [52], phase synchronization [31], [49], lag synchronization [43], [44], [48], projective synchronization [13], [26], [54], and cluster synchronization [5], [22], [24], [45]. Among these synchronization modes, cluster synchronization is particularly relevant to IoT applications, as IoT devices are often organized into functional, geographical, or task-driven groups that require intra-cluster coordination while maintaining inter-cluster independence. Such clustered behaviors naturally arise in smart grids, industrial IoT, and intelligent transportation systems.

In general, cluster synchronization refers to the phenomenon in which nodes within the same cluster achieve synchronization, whereas synchronization across different clusters is not required. In IoT networks, cluster synchronization is rarely achieved through intrinsic coupling alone and typically requires external control intervention. To this end, various control strategies have been developed, including pinning control [46], adaptive control [39], and intermittent control [27], to steer network nodes toward desired clustered behaviors. These methods have significantly advanced synchronization theory and provided useful tools for group-based coordination in networked systems. However, despite the widespread deployment

This work was supported in part by the National Natural Science Foundation of China under Grants 62173292, 62203016, and 62376242, the Yangzhou University International Academic Exchange Fund of China, the Royal Society of the UK, and the Alexander von Humboldt Foundation of Germany. *(Corresponding author: Yurong Liu.)*

Yunjie Chen and Yurong Liu are with the Department of Mathematics, Yangzhou University, Yangzhou 225002, China (e-mails: yunjie573725746@outlook.com; yrliu@yzu.edu.cn).

Zidong Wang is with the Department of Computer Science, Brunel University of London, Uxbridge, Middlesex, UB8 3PH, U.K. (e-mail: Zidong.Wang@brunel.ac.uk).

Weihao Song is with the School of Advanced Manufacturing and Robotics, Peking University, Beijing 100871, China, and also with the Department of Computer Science, Brunel University of London, Uxbridge, Middlesex, UB8 3PH, U.K. (e-mail: Weihao.Song@brunel.ac.uk).

of PID controllers in industrial and embedded IoT devices, PID-based cluster synchronization control for CNs has not yet been systematically investigated. Given its simple structure, low computational burden, and clear physical interpretation, PID control is particularly attractive for resource-constrained IoT applications, making its study both theoretically meaningful and practically relevant.

In most existing studies on synchronization control of CNs, it is commonly assumed that transmitted information is reliable. However, in practical IoT environments, communication channels are often subject to disturbances, uncertainties, and malicious cyber-attacks, which may result in discrepancies between transmitted and received signals. Network attacks are generally categorized into deception attacks, denial-of-service (DoS) attacks, and replay attacks. Deception attacks manipulate transmitted data by injecting malicious signals [2], [3], [38], [47], DoS attacks disrupt communication availability [10], [23], [34], and replay attacks resend previously intercepted valid data to mislead the system [9], [17], [30]. Among these threats, replay attacks are particularly dangerous for IoT systems because they are difficult to detect and can continuously inject outdated but legitimate information into the control loop.

Due to their stealthy nature, replay attacks may mislead controllers over extended periods, thereby degrading synchronization performance or even causing instability. Consequently, developing effective synchronization control strategies resilient to replay attacks is of significant importance for secure IoT operation. Existing research has primarily focused on designing attack detection mechanisms [17], [29], [33], often overlooking the potential of leveraging inherent control structures to actively counter such threats. PID controllers, which integrate proportional, integral, and derivative actions, are well known for their ability to enhance robustness by exploiting both current and historical information. Compared with proportional-only controllers, PID-based strategies can better eliminate steady-state errors, suppress oscillations, and improve transient performance [8], [15], [20], [21], [35], making them well suited for IoT environments subject to cyber disturbances.

Although considerable progress has been made in state estimation under replay attacks [11], [12], [17], the synchronization control problem of CNs representing IoT systems under replay attacks has not been fully addressed. In particular, PID-based secure cluster synchronization for discrete-time nonlinear CNs remains largely open. This problem is challenging due to several fundamental issues: 1) how to establish an appropriate mathematical model to describe the dynamic behavior of replay attacks in complex systems, especially their randomness and persistence? 2) how to construct an analytical framework for PID-based synchronization control of CNs under replay attacks? and 3) how to design PID controllers that ensure mean-square stability in the presence of such attacks? The objective of this paper is to provide effective solutions to these challenges.

The main contributions of this paper are summarized as follows.

1) A secure cluster synchronization framework is established for discrete-time nonlinear CNs subject to replay attacks, where the attack behavior is explicitly characterized by both stochastic occurrence and bounded persistence. This modeling approach captures essential practical features of replay attacks that are not addressed in conventional synchronization studies.
2) A PID-based cluster synchronization control strategy is developed, integrating proportional, integral, and derivative actions to exploit both instantaneous and historical information. By embedding PID dynamics into the cluster synchronization setting, the proposed approach enhances robustness against replay-induced outdated information and extends existing proportional-control-based secure synchronization methods.
3) A rigorous analytical framework is constructed to derive sufficient conditions ensuring ultimate mean-square cluster synchronization in the presence of replay attacks. The obtained results provide theoretical guarantees on synchronization performance and robustness, thereby bridging secure control analysis and cluster synchronization theory for nonlinear CNs.

The remainder of this paper is organized as follows. Section II introduces the system dynamics and formulates the PID controller design problem for CNs under replay attacks. Section III presents the main analytical results on PID-based cluster synchronization. Section IV demonstrates the effectiveness of the proposed approach through numerical simulations, and Section V concludes the paper.

Notations: Let $\mathbb{R}^n$ and $\mathbb{R}^{m\times n}$ denote the n-dimensional Euclidean space and the set of $m \times n$ real matrices, respectively. The transpose and inverse of a matrix A are denoted by A^T and A^{-1}, respectively. $\mathbb{P}\{X\}$ represents the occurrence probability of event X, and $\mathbb{E}\{x\}$ denotes the expectation of a random variable x. For $y \in \mathbb{R}^n$, $\|y\|_2 = \sqrt{y^T y}$ denotes the 2-norm of y. The symbol $\otimes$ denotes the Kronecker product.

II. Preliminaries and Problem Formulation

A. System Dynamics

Consider a class of nonlinear CNs governed by the following dynamics:

$$x_{i,k+1} = h_i(x_{i,k}) + \sum_{j=1}^{N} \ell_{ij}\Gamma x_{j,k} + u_{i,k}, \tag{1}$$

for $i \in \digamma \triangleq \{1, 2, \ldots, N\}$, where $x_{i,k} \in \mathbb{R}^{n_x}$ and $u_{i,k} \in \mathbb{R}^{n_x}$ denote, respectively, the state vector and the control input of node i. The inner-coupling matrix $\Gamma \geq 0$ represents the connections between the different elements of the subsystem. For each node i, the local dynamics is described by a nonlinear vector-valued function $h_i(\cdot)$. The following assumption is imposed on the nonlinear function $h_i(\cdot)$.

Assumption 1: For any node $i \in \digamma$, the nonlinear function $h_i : \mathbb{R}^{n_x} \to \mathbb{R}^{n_x}$ is continuous and satisfies

$$\begin{aligned}[h_i(\psi_1) - h_i(\psi_2) - \chi_{i1}(\psi_1 - \psi_2)]^T \\ \times [h_i(\psi_1) - h_i(\psi_2) - \chi_{i2}(\psi_1 - \psi_2)] \leq 0,\end{aligned}$$

for $\psi_1, \psi_2 \in \mathbb{R}^{n_x}$, where χ_{i1}, χ_{i2} are known constant matrices.

Now, the N nodes in the network are partitioned into s disjoint and nonempty clusters, denoted by $\mathcal{F}_1 = \{1, 2, \ldots, n_1\}$, $\mathcal{F}_2 = \{n_1 + 1, \ldots, n_1 + n_2\}$, $\cdots$, $\mathcal{F}_s = \{\sum_{\rho=1}^{s-1} n_\rho + 1, \ldots, \sum_{\rho=1}^{s} n_\rho\}$, where $\sum_{\rho=1}^{s} n_\rho = N$. It follows that $\bigcup_{\rho=1}^{s} \mathcal{F}_\rho = \mathcal{F}$. The notation $\bar{i}$ is used to denote the cluster index to which node i belongs, namely, $i \in \mathcal{F}_{\bar{i}}$. Clearly, for any two nodes i and j belonging to the same cluster, it holds that $\bar{i} = \bar{j}$. Furthermore, nodes within the same cluster are assumed to share identical local dynamics, that is, $h_{\bar{i}}(\cdot) = h_{\bar{j}}(\cdot)$ for $\bar{i} = \bar{j}$.

For the CN (1) with s clusters, the network topology is characterized by the coupling configuration matrix $\mathcal{L} \triangleq [\ell_{ij}]_{N\times N}$, which describes both the coupling strengths and the topological structure of the network. The matrix $\mathcal{L}$ satisfies $\ell_{ii} = -\sum_{j=1, j\neq i}^{N} \ell_{ij}$ and $\ell_{ij} \geq 0$ for $i \neq j$, and is not necessarily symmetric or irreducible. Its block form is given by

$$\mathcal{L} = \begin{bmatrix} L_{11} & L_{12} & \cdots & L_{1s} \\ L_{21} & L_{22} & \cdots & L_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ L_{s1} & L_{s2} & \cdots & L_{ss} \end{bmatrix}_{N\times N} \tag{2}$$

where each matrix block $L_{pq} \triangleq [\ell_{ij}]_{n_p\times n_q} \in \mathbb{R}^{n_p\times n_q}$ is a zero-row-sum matrix. Moreover, $\ell_{ij} > 0$ if there exists a connection between the node i and node j, and $\ell_{ij} = 0$ otherwise (for $i \neq j$).

For the mth cluster, the dynamics of the unforced target node is described by

$$\begin{cases} \sigma_{m,k+1} &= h_m(\sigma_{m,k}), \\ \sigma_{m,0} &= \bar{\sigma}_{m,0}, \end{cases} \tag{3}$$

where $\sigma_{m,k} \in \mathbb{R}^{n_x}$ denotes the state of the target node and $\bar{\sigma}_{m,0}$ is the corresponding initial condition. Clearly, for any $i \in \mathcal{F}_m$, it holds that $h_i(\cdot) = h_m(\cdot)$, whereas $h_i(\cdot) \neq h_m(\cdot)$ for $i \notin \mathcal{F}_m$.

Remark 1: As the network scale increases, achieving global synchronization often becomes impractical. In contrast, cluster synchronization enables synchronization within localized subnetworks, allowing each cluster to perform specialized functions or tasks. Compared with global synchronization, cluster synchronization offers advantages in terms of reduced communication costs and enhanced flexibility.

B. The Attacker Model

In an open communication environment, the transmitted data is highly susceptible to attacks, which may lead to the degradation of system performance. In this paper, we consider a replay attack model, which aims to replace the current control signal with previously intercepted control signal, thereby disrupting the synchronization of system. To capture the occurrence of attacks, we introduce a Bernoulli random variable γ_k to characterize the randomness of the attacks. The specific description of the variable γ_k is as follows:

$$\gamma_k = \begin{cases} 1, & \text{if the replay attack occurs,} \\ 0, & \text{otherwise,} \end{cases} \tag{4}$$

where γ_k satisfies the following statistical properties

$$\mathbb{P}\{\gamma_k = 1\} = \mathbb{E}\{\gamma_k\} = \overline{\gamma},\ \mathbb{P}\{\gamma_k = 0\} = 1 - \overline{\gamma}. \tag{5}$$

Here, $\overline{\gamma} \in (0, 1)$ is a known scalar representing the likelihood of a replay attack occurring.

The replay attack model can be mathematically represented by

$$u_{i,k} = \widetilde{u}_{i,k} + \gamma_k(-\widetilde{u}_{i,k} + \widetilde{u}_{i,k_d}), \tag{6}$$

where $u_{i,k}$ is the current control signal subject to replay attacks. The signal $u_{i,k}$ received by the actuator can be either the normal signal $\widetilde{u}_{i,k}$, which is generated and transmitted by the controller, or a historically recorded signal $\widetilde{u}_{i,k_d}$. This depends on whether a replay attack occurs and on the number of consecutive replay attacks $d_k = k - k_d$. The number of successive attacks are defined recursively as:

$$d_k = \gamma_k(d_{k-1} + 1). \tag{7}$$

As described in (4), when $\gamma_k = 0$, the communication channels operate normally, and the number of successive attacks is $d_k = 0$. On the other hand, when $\gamma_k = 1$, the communication channels are subject to replay attacks, causing the number of successive attacks to increase by one at each time step, until the attackers exhaust their energy budget. Considering that it is impossible for attackers to continue high-intensity attacks indefinitely, the number of consecutive attacks is assumed to satisfy

$$\kappa_1 \leq d_k \leq \kappa_2,$$

where κ_1 and κ_2 represent, respectively, the maximum and minimum values of d_k. And they are known positive scalars determined by the attacker's energy constraints. Constraining the number of attacks within reasonable upper and lower bounds helps improve the model realism and better capture real-world attack scenarios.

Remark 2: Traditional synchronization studies typically assume that the communication channels among network nodes are perfectly reliable. However, this idealized assumption rarely holds in practice, as communication links are often vulnerable to various malicious cyber-attacks. Incorporating such practical constraints enables the synchronization control framework to more accurately capture the dynamical behaviors of real-world networked systems. Therefore, investigating secure synchronization control for IoT networks under replay attacks is both theoretically significant and practically urgent. Research on secure synchronization control for IoT networks is not merely an extension of conventional synchronization theory, but a necessary step toward ensuring the reliable and resilient operation of practical networked systems.

Remark 3: Replay attacks is a kind of typical cyber-attacks in which adversaries intercept and record legitimate data packets previously transmitted in the network and subsequently retransmit them to the receiver in order to deceive the system and disrupt its normal operation. According to this definition, the attack process involves two stages: (1) the phase of data interception and storage, during which the attackers collect valid information, and (2) the phase of replay, in which

the current control signals are deleted and the previously captured data are retransmitted. Consequently, replay attacks cannot occur instantaneously, and it requires at least one sampling delay between data interception and retransmission. The earliest replay attack is usually at $k \geq 1$.

Remark 4: Existing studies on replay attacks [17] typically assume that the attack time-stamps are known in advance. However, in realistic networked environments, attackers rarely maintain persistent attacks indefinitely; instead, they tend to act in a random and intermittent fashion. To capture this practical feature, Bernoulli random variables are adopted in this paper to characterize the stochastic nature of attack occurrences, thus better reflecting the randomness inherent in real-world attack behaviors. Furthermore, the upper and lower bounds on duration of continuous attack are imposed to constrain the attack, which not only reflects the limited persistence of practical attacks but also facilitates the design of more realistic and effective defense strategies in the networked system.

C. Synchronization Error Dynamics

Define $e_{i,k} \triangleq x_{i,k} - \sigma_{\bar{i},k}$. The PID-based synchronization controller for node i is designed as

$$\widetilde{u}_{i,k} = K_i^P e_{i,k} + K_i^I \sum_{n=k-L}^{k-1} e_{i,n} + K_i^D (e_{i,k} - e_{i,k-1}), \quad (8)$$

where K_i^P, K_i^I, and K_i^D denote the PID controller gain parameters to be designed. The scalar L specifies the time length of the integral window. For convenience, (8) can be rewritten as

$$\begin{aligned}\widetilde{u}_{i,k} =&(K_i^P + K_i^D)e_{i,k} + K_i^I \sum_{n=k-L}^{k-2} e_{i,n} \\ &+ (K_i^I - K_i^D)e_{i,k-1}. \end{aligned} \quad (9)$$

By exploiting the zero-row-sum property of L_{pq}, we have

$$\begin{aligned}\sum_{j=1}^{N} \ell_{ij}\Gamma x_{j,k} &= \sum_{m=1}^{s} \sum_{j\in\mathcal{F}_m} \ell_{ij}\Gamma x_{j,k} \\ &= \sum_{m=1}^{s} \sum_{j\in\mathcal{F}_m} \ell_{ij}\Gamma (e_{j,k} + \sigma_{m,k}) \\ &= \sum_{m=1}^{s} \sum_{j\in\mathcal{F}_m} \ell_{ij}\Gamma e_{j,k} + \sum_{m=1}^{s} \sum_{j\in\mathcal{F}_m} \ell_{ij}\Gamma \sigma_{m,k} \\ &= \sum_{m=1}^{s} \sum_{j\in\mathcal{F}_m} \ell_{ij}\Gamma e_{j,k}.\end{aligned}$$

Accordingly, the cluster synchronization error dynamics of node i are obtained as

$$\begin{aligned}e_{i,k+1} =&\tilde{h}_i(e_{i,k}) + \sum_{j=1}^{N} \ell_{ij}\Gamma e_{j,k} + (1-\gamma_k) \\ &\times ((K_i^P + K_i^D)e_{i,k} + K_i^I \sum_{n=k-L}^{k-2} e_{i,n} \\ &+ (K_i^I - K_i^D)e_{i,k-1}) \\ &+ \gamma_k((K_i^P + K_i^D)e_{i,k_d} + K_i^I \sum_{n=k_d-L}^{k_d-2} e_{i,n} \\ &+ (K_i^I - K_i^D)e_{i,k_d-1}), \end{aligned} \quad (10)$$

where $\tilde{h}_i(e_{i,k}) = h_i(x_{i,k}) - h_{\bar{i}}(\sigma_{\bar{i},k})$. For ease of presentation, the following notations are introduced:

$$\begin{aligned} e_k &\triangleq \mathrm{col}_N\{e_{i,k}\}, \\ e_{k_d} &\triangleq \mathrm{col}_N\{e_{i,k_d}\}, \\ \tilde{H}(e_k) &\triangleq \mathrm{col}_N\{\tilde{h}_i(e_{i,k})\}, \\ \omega_k &\triangleq [e_{k-1}^T, \cdots, e_{k-L}^T]^T, \\ \omega_{k_d} &\triangleq [e_{k_d-1}^T, \cdots, e_{k_d-L}^T]^T, \\ \bar{K}_P &\triangleq \mathrm{diag}_N\{K_i^P\}, \\ \bar{K}_I &\triangleq \mathrm{diag}_N\{K_i^I\}, \\ \bar{K}_D &\triangleq \mathrm{diag}_N\{K_i^D\}, \\ M &\triangleq [\bar{K}_I - \bar{K}_D \quad \underbrace{\bar{K}_I \ \cdots \ \bar{K}_I}_{L-1}]. \end{aligned}$$

By employing the Kronecker product, the synchronization error dynamics (10) can be compactly rewritten as

$$\begin{cases} \begin{aligned} e_{k+1} =&\tilde{H}(e_k) + \Lambda e_k - \overrightarrow{\gamma}_k K e_k + \widetilde{\gamma} M \omega_k \\ &- \overrightarrow{\gamma}_k M \omega_k + \bar{\gamma} K e_{k_d} + \overrightarrow{\gamma}_k K e_{k_d} \\ &+ \bar{\gamma} M \omega_{k_d} + \overrightarrow{\gamma}_k M \omega_{k_d}, \\ e_l =&\phi_l, \quad l = -\max\{L, \kappa_2\} - L, \ldots, -1, 0, \end{aligned} \end{cases} \quad (11)$$

where

$$\begin{aligned} &\Lambda \triangleq (\mathcal{L} \otimes \Gamma) + \widetilde{\gamma} K, \quad K \triangleq \bar{K}_P + \bar{K}_D, \\ &\widetilde{\gamma} \triangleq 1 - \bar{\gamma}, \quad \overrightarrow{\gamma}_k \triangleq \gamma_k - \bar{\gamma}. \end{aligned}$$

Under replay attacks, the following definition of mean-square synchronization is adopted as the performance criterion for secure synchronization behavior.

Definition 1: The described CN is said to be asymptotically mean-square cluster synchronized if the N nodes can be partitioned into s disjoint and nonempty clusters $\mathcal{F}_1, \cdots, \mathcal{F}_s$, for any $i \in \mathcal{F}_l$ ($l \in \{1, 2, \cdots, s\}$), the following condition holds:

$$\lim_{k\to\infty} \mathbb{E}\{\|x_{i,k} - \sigma_{l,k}\|_2^2\} = 0.$$

In the context of secure control, an important objective is to maintain synchronization performance in the presence of malicious attacks or abnormal interference. In particular, the integral and derivative terms in the PID controller introduce additional state dynamics, which provide useful memory effects but also interact with stochastic replay attacks and nonlinear network dynamics, making the system analysis more challenging. The purpose of this paper is therefore to design a PID controller for nonlinear CNs under replay attacks such that the synchronization error dynamics (11) satisfies the above performance criterion.

III. Main results

In this section, the main results for achieving secure cluster synchronization under replay attacks are derived.

A. Synchronization Analysis

In the following theorem, the mean-square ultimate synchronization performance of the cluster synchronization error dynamics (11) is analyzed.

Theorem 1: Consider the given PID controller gain matrices $\bar{K}_P$, $\bar{K}_I$, $\bar{K}_D$. Assume that there exist positive definite matrices $P \in \mathbb{R}^{n_x N \times n_x N}$, $R_1 \in \mathbb{R}^{n_x N \times n_x N}$, $R_2 \in \mathbb{R}^{n_x NL \times n_x NL}$, and $Q_j \in \mathbb{R}^{n_x N \times n_x N} (j = 1, 2, \cdots, L)$ such that the following inequality holds:

$$\overline{\Pi} \triangleq \begin{bmatrix} \Pi_{11} & \Pi_{12} & \Pi_{13} & \Pi_{14} & \Pi_{15} \\ * & \Pi_{22} & \Pi_{23} & \Pi_{24} & \Pi_{25} \\ * & * & \Pi_{33} & 0 & 0 \\ * & * & * & \Pi_{44} & \Pi_{45} \\ * & * & * & * & \Pi_{55} \end{bmatrix} < 0, \tag{12}$$

where

$$\begin{aligned}
\Pi_{11} \triangleq& \Lambda^T P \Lambda + \hat{\gamma}^2 K^T P K - P + (1 + \kappa_2 - \kappa_1) R_1 - \hat{U}_1 \\
&+ \sum_{j=1}^{L} Q_j, \\
\Pi_{12} \triangleq& \Lambda^T P + \hat{U}_2, \quad \Pi_{22} \triangleq P - I, \\
\Pi_{13} \triangleq& \widetilde{\gamma} \Lambda^T P M + \hat{\gamma}^2 K^T P M, \quad \Pi_{23} \triangleq \widetilde{\gamma} P M, \\
\Pi_{14} \triangleq& \bar{\gamma} \Lambda^T P K - \hat{\gamma}^2 K^T P K, \\
\Pi_{15} \triangleq& \bar{\gamma} \Lambda^T P M - \hat{\gamma}^2 K^T P M, \\
\Pi_{24} \triangleq& \bar{\gamma} P K, \quad \Pi_{25} \triangleq \bar{\gamma} P M, \\
\Pi_{33} \triangleq& \widetilde{\gamma} M^T P M - Q + (1 + \kappa_2 - \kappa_1) R_2, \\
\Pi_{44} \triangleq& \bar{\gamma} K^T P K - R_1, \\
\Pi_{45} \triangleq& \bar{\gamma} K^T P M, \quad \Pi_{55} \triangleq \bar{\gamma} M^T P M - R_2, \\
\hat{U}_1 \triangleq& \text{diag}_N\{\bar{U}_i\}, \quad \hat{U}_2 \triangleq \text{diag}_N\{\tilde{U}_i\}, \\
\bar{U}_i \triangleq& (\chi_{i1}^T \chi_{i2} + \chi_{i2}^T \chi_{i1})/2, \quad \tilde{U}_i \triangleq (\chi_{i2} + \chi_{i1})^T/2, \\
Q \triangleq& \text{diag}\{Q_1, Q_2, \cdots, Q_L\}, \\
\hat{\gamma} \triangleq& \sqrt{\bar{\gamma}(1 - \bar{\gamma})}.
\end{aligned}$$

Then, under replay attacks, the CN (1) can asymptotically achieve mean-square synchronization.

Proof: Consider the following Lyapunov-like function:

$$V_k = \sum_{s=1}^{6} V_{s,k}, \tag{13}$$

where

$$\begin{aligned}
V_{1,k} &= e_k^T P e_k, \\
V_{2,k} &= \sum_{j=1}^{L} \sum_{\iota=k-j}^{k-1} e_\iota^T Q_j e_\iota, \\
V_{3,k} &= \sum_{\iota=k-d_k}^{k-1} e_\iota^T R_1 e_\iota, \\
V_{4,k} &= \sum_{t=k-\kappa_2+1}^{k-\kappa_1} \sum_{\iota=t}^{k-1} e_\iota^T R_1 e_\iota, \\
V_{5,k} &= \sum_{\iota=k-d_k}^{k-1} \omega_\iota^T R_2 \omega_\iota, \\
V_{6,k} &= \sum_{t=k-\kappa_2+1}^{k-\kappa_1} \sum_{\iota=t}^{k-1} \omega_\iota^T R_2 \omega_\iota.
\end{aligned}$$

Before calculating the mathematical expectation of the difference of $V_{s,k}$ $(s = 1, 2, \cdots, 6)$, we evaluate the corresponding conditional expectations and obtain

$$\begin{aligned}
\mathbb{E}\{\Delta V_{1,k} | V_k\} \triangleq& \mathbb{E}\{V_{1,k+1} | V_k\} - V_{1,k} \\
=& (\tilde{H}(e_k) + \Lambda e_k - \overrightarrow{\gamma}_k K e_k + \widetilde{\gamma} M \omega_k \\
&- \overrightarrow{\gamma}_k M \omega_k + \bar{\gamma} K e_{k_d} + \overrightarrow{\gamma}_k K e_{k_d} \\
&+ \bar{\gamma} M \omega_{k_d} + \overrightarrow{\gamma}_k M \omega_{k_d})^T P (\tilde{H}(e_k) + \Lambda e_k \\
&- \overrightarrow{\gamma}_k K e_k + \widetilde{\gamma} M \omega_k - \overrightarrow{\gamma}_k M \omega_k + \bar{\gamma} K e_{k_d} \\
&+ \overrightarrow{\gamma}_k K e_{k_d}) - e_k^T P e_k \\
=& e_k^T (\Lambda^T P \Lambda + \hat{\gamma}^2 K^T P K - P) e_k \\
&+ \tilde{H}^T(e_k) P \tilde{H}(e_k) + \bar{\gamma} e_{k_d}^T K^T P K e_{k_d} \\
&+ \widetilde{\gamma} \omega_k^T M^T P M \omega_k + \bar{\gamma} \omega_{k_d}^T M^T P M \omega_{k_d} \\
&+ 2 e_k^T \Lambda^T P \tilde{H}(e_k) + 2 \widetilde{\gamma} \tilde{H}^T(e_k) P M \omega_k \\
&+ 2 \bar{\gamma} \tilde{H}^T(e_k) P K e_{k_d} + 2 \bar{\gamma} \tilde{H}^T(e_k) P M \omega_{k_d} \\
&+ 2 e_k^T (\widetilde{\gamma} \Lambda^T P M + \hat{\gamma}^2 K^T P M) \omega_k \\
&+ 2 e_k^T (\bar{\gamma} \Lambda^T P K - \hat{\gamma}^2 K^T P K) e_{k_d} \\
&+ 2 e_k^T (\bar{\gamma} \Lambda^T P M - \hat{\gamma}^2 K^T P M) \omega_{k_d} \\
&+ 2 \bar{\gamma} e_{k_d}^T K^T P M \omega_{k_d},
\end{aligned} \tag{14}$$

$$\begin{aligned}
\mathbb{E}\{\Delta V_{2,k} | V_k\} \triangleq& \mathbb{E}\{V_{2,k+1} | V_k\} - V_{2,k} \\
=& \sum_{j=1}^{L} (e_k^T Q_j e_k - e_{k-j}^T Q_j e_{k-j}) \\
=& \sum_{j=1}^{L} e_k^T Q_j e_k - \omega_k^T Q \omega_k,
\end{aligned} \tag{15}$$

$$\begin{aligned}
\mathbb{E}\{\Delta V_{3,k} | V_k\} \triangleq& \mathbb{E}\{V_{3,k+1} | V_k\} - V_{3,k} \\
=& e_k^T R_1 e_k + \sum_{\iota=k-d_{k+1}+1}^{k-1} e_\iota^T R_1 e_\iota \\
&- e_{k_d}^T R_1 e_{k_d} - \sum_{\iota=k-d_k+1}^{k-1} e_\iota^T R_1 e_\iota \\
=& e_k^T R_1 e_k - e_{k_d}^T R_1 e_{k_d} + \sum_{\iota=k-d_{k+1}+1}^{k-d_k} e_\iota^T R_1 e_\iota \\
\leq& e_k^T R_1 e_k - e_{k_d}^T R_1 e_{k_d} + \sum_{\iota=k-\kappa_2+1}^{k-\kappa_1} e_\iota^T R_1 e_\iota,
\end{aligned} \tag{16}$$

$$\begin{aligned}
\mathbb{E}\{\Delta V_{4,k} | V_k\} \triangleq& \mathbb{E}\{V_{4,k+1} | V_k\} - V_{4,k} \\
=& \sum_{t=k-\kappa_2+1}^{k-\kappa_1} \left(\sum_{\iota=t}^{k} e_\iota^T R_1 e_\iota - \sum_{\iota=t}^{k-1} e_\iota^T R_1 e_\iota \right) \\
&+ \sum_{\iota=k-\kappa_1+1}^{k} e_\iota^T R_1 e_\iota - \sum_{\iota=k-\kappa_2+1}^{k} e_\iota^T R_1 e_\iota \\
=& (\kappa_2 - \kappa_1) e_k^T R_1 e_k - \sum_{\iota=k-\kappa_2+1}^{k-\kappa_1} e_\iota^T R_1 e_\iota.
\end{aligned} \tag{17}$$

Similarly, the conditional expectation of differences of $V_{5,k}$ and $V_{6,k}$ are calculated as:

$$\begin{aligned}\mathbb{E}\{\Delta V_{5,k}|V_k\} \triangleq&\mathbb{E}\{V_{5,k+1}|V_k\} - V_{5,k}\\ \leq&\omega_k^T R_2\omega_k - \omega_{k_d}^T R_2\omega_{k_d} + \sum_{\iota=k-\kappa_2+1}^{k-\kappa_1}\omega_\iota^T R_2\omega_\iota,\\ \mathbb{E}\{\Delta V_{6,k}|V_k\} \triangleq&\mathbb{E}\{V_{6,k+1}|V_k\} - V_{6,k}\\ =&(\kappa_2-\kappa_1)\omega_k^T R_2\omega_k - \sum_{\iota=k-\kappa_2+1}^{k-\kappa_1}\omega_\iota^T R_2\omega_\iota.\end{aligned}$$

By combining the above expressions with Assumption 1, the following inequality is derived:

$$\begin{aligned}\mathbb{E}\{\Delta V_k|V_k\} =&\sum_{s=1}^{6}\mathbb{E}\{\Delta V_{s,k}|V_k\}\\ \leq&e_k^T(\Lambda^T P\Lambda + \hat{\gamma}^2 K^T PK - P)e_k\\ &+\tilde{H}^T(e_k)P\tilde{H}(e_k) + \bar{\gamma}e_{k_d}^T K^T PKe_{k_d}\\ &+\widetilde{\gamma}\omega_k^T M^T PM\omega_k + \bar{\gamma}\omega_{k_d}^T M^T PM\omega_{k_d}\\ &+2e_k^T\Lambda^T P\tilde{H}(e_k) + 2\widetilde{\gamma}\tilde{H}^T(e_k)PM\omega_k\\ &+2\bar{\gamma}\tilde{H}^T(e_k)PKe_{k_d} + 2\bar{\gamma}\tilde{H}^T(e_k)PM\omega_{k_d}\\ &+2e_k^T(\widetilde{\gamma}\Lambda^T PM + \hat{\gamma}^2 K^T PM)\omega_k\\ &+2e_k^T(\bar{\gamma}\Lambda^T PK - \hat{\gamma}^2 K^T PK)e_{k_d}\\ &+2e_k^T(\bar{\gamma}\Lambda^T PM - \hat{\gamma}^2 K^T PM)\omega_{k_d}\\ &+2\bar{\gamma}e_{k_d}^T K^T PM\omega_{k_d} + \sum_{j=1}^{L}e_k^T Q_j e_k - \omega_k^T Q\omega_k\\ &+e_k^T R_1 e_k - e_{k_d}^T R_1 e_{k_d} + (\kappa_2-\kappa_1)e_k^T R_1 e_k\\ &+\omega_k^T R_2\omega_k - \omega_{k_d}^T R_2\omega_{k_d} + (\kappa_2-\kappa_1)\omega_k^T R_2\omega_k\\ \leq&\zeta_k^T\overline{\Pi}\zeta_k,\end{aligned}\tag{18}$$

where

$$\zeta_k \triangleq [e_k^T \quad \tilde{H}^T(e_k) \quad \omega_k^T \quad e_{k_d}^T \quad \omega_{k_d}^T]^T.$$

Taking inequality (12) into account, it can be concluded that there exists a sufficiently small positive scalar ϵ such that

$$\begin{aligned}\mathbb{E}\{\Delta V_k\} \leq&\mathbb{E}\{\zeta_k^T\tilde{\Pi}\zeta_k\}\\ \leq&-\epsilon\mathbb{E}\{\|e_k\|^2\}.\end{aligned}\tag{19}$$

From the definition of V_k in (13), it follows that

$$\begin{aligned}\mathbb{E}\{V_k\} \leq&c_1\mathbb{E}\{\|e_k\|^2\} + c_2\sum_{i=k-h}^{k-1}\mathbb{E}\{\|e_i\|^2\}\\ &+c_3\sum_{i=k-h}^{k-1}\mathbb{E}\{\|\omega_i\|^2\},\end{aligned}\tag{20}$$

where

$$\begin{aligned}&h \triangleq \max\{L,\kappa_2\}, \quad c_1 \triangleq \lambda_{\max}(P),\\ &c_2 \triangleq L\lambda_{\max}(Q_j) + (1+\kappa_2-\kappa_1)\lambda_{\max}(R_1),\\ &c_3 \triangleq (1+\kappa_2-\kappa_1)\lambda_{\max}(R_2).\end{aligned}$$

Next, for any $\lambda > 1$, it follows from (19) and (20) that

$$\begin{aligned}&\mathbb{E}\{\lambda^{k+1}V(k+1)\} - \mathbb{E}\{\lambda^k V_k\}\\ =&\lambda^{k+1}\mathbb{E}\{\Delta V_k\} + \lambda^{k+1}\mathbb{E}\{V_k\} - \lambda^k\mathbb{E}\{V_k\}\\ =&\lambda^{k+1}\mathbb{E}\{\Delta V_k\} + \lambda^k(\lambda-1)\mathbb{E}\{V_k\}\\ \leq&\lambda^{k+1}(-\epsilon\mathbb{E}\{\|e_k\|^2\}) + \lambda^k(\lambda-1)\\ &\times\left(c_1\mathbb{E}\{\|e_k\|^2\} + c_2\sum_{i=k-h}^{k-1}\mathbb{E}\{\|e_i\|^2\}\right.\\ &\left.+c_3\sum_{i=k-h}^{k-1}\mathbb{E}\{\|\omega_i\|^2\}\right)\\ =&\lambda^k\mu_1(\lambda)\mathbb{E}\{\|e_k\|^2\} + \lambda^k\mu_2(\lambda)\sum_{i=k-h}^{k-1}\mathbb{E}\{\|e_i\|^2\}\\ &+\lambda^k\mu_3(\lambda)\sum_{i=k-h}^{k-1}\mathbb{E}\{\|\omega_i\|^2\},\end{aligned}\tag{21}$$

where

$$\begin{aligned}&\mu_1(\lambda) \triangleq -\lambda\epsilon + (\lambda-1)c_1, \quad \mu_2(\lambda) \triangleq (\lambda-1)c_2,\\ &\mu_3(\lambda) \triangleq (\lambda-1)c_3.\end{aligned}$$

For any integer $\delta \geq h+1$, summing up both sides of (21) from 0 to $\delta-1$ with regard to k, we acquire

$$\begin{aligned}&\mathbb{E}\{\lambda^\delta V_\delta\} - \mathbb{E}\{V_0\}\\ \leq&\mu_1(\lambda)\sum_{k=0}^{\delta-1}\lambda^k\mathbb{E}\{\|e_k\|^2\} + \mu_2(\lambda)\sum_{k=0}^{\delta-1}\sum_{i=k-h}^{k-1}\lambda^k\mathbb{E}\{\|e_i\|^2\}\\ &+\mu_3(\lambda)\sum_{k=0}^{\delta-1}\sum_{i=k-h}^{k-1}\lambda^k\mathbb{E}\{\|\omega_i\|^2\}.\end{aligned}\tag{22}$$

Furthermore, the second and final terms in (22) are computed as

$$\begin{aligned}&\sum_{k=0}^{\delta-1}\sum_{i=k-h}^{k-1}\lambda^k\mathbb{E}\{\|e_i\|^2\}\\ =&\sum_{i=-h}^{\delta-2}\sum_{k=\max\{0,i+1\}}^{\min\{\delta-1,i+h\}}\lambda^k\mathbb{E}\{\|e_i\|^2\}\\ \leq&\left(\sum_{i=-h}^{-1}\sum_{k=0}^{i+h} + \sum_{i=0}^{\delta-h-1}\sum_{k=i+1}^{i+h} + \sum_{i=\delta-h}^{\delta-1}\sum_{k=i+1}^{\delta-1}\right)\lambda^k\mathbb{E}\{\|e_i\|^2\}\\ \leq&\sum_{i=-h}^{-1}h\lambda^{i+h}\mathbb{E}\{\|e_i\|^2\} + \sum_{i=0}^{\delta-1}h\lambda^{i+h}\mathbb{E}\{\|e_i\|^2\}\\ \leq&h\lambda^h\sum_{k=0}^{\delta-1}\lambda^k\mathbb{E}\{\|e_k\|^2\} + h^2\lambda^h\sup_{l\in[-h,0]}\mathbb{E}\{\|\phi_l\|^2\},\end{aligned}\tag{23}$$

and

$$\begin{aligned}&\sum_{k=0}^{\delta-1}\sum_{i=k-h}^{k-1}\lambda^k\mathbb{E}\{\|\omega_i\|^2\}\\ \leq&\sum_{i=-h}^{-1}h\lambda^{i+h}\mathbb{E}\{\|\omega_i\|^2\} + \sum_{i=0}^{L}h\lambda^{i+h}\mathbb{E}\{\|\omega_i\|^2\}\\ &+\sum_{i=L+1}^{\delta-1}h\lambda^{i+h}\mathbb{E}\{\|\omega_i\|^2\}\end{aligned}$$

$$
\begin{aligned}
=&h\lambda^h\sum_{i=-h}^{-1}\sum_{q=i-L}^{i-1}\lambda^i\mathbb{E}\{\|e_q\|^2\}+h\lambda^h\sum_{i=0}^{L}\sum_{q=i-L}^{i-1}\lambda^i\mathbb{E}\{\|e_q\|^2\}\\
&+h\lambda^h\sum_{i=L+1}^{\delta-1}\sum_{q=i-L}^{i-1}\lambda^i\mathbb{E}\{\|e_q\|^2\}\\
\le&h^2\lambda^h\left(h+\frac{(h+1)}{2}\lambda^h\right)\sup_{l\in[-h-L,0]}\mathbb{E}\{\|\phi_l\|^2\}\\
&+h^2\lambda^h\sum_{k=0}^{\delta-1}\lambda^k\mathbb{E}\{\|e_k\|^2\}. \qquad (24)
\end{aligned}
$$

Substituting (23) and (24) into (22), one has

$$
\begin{aligned}
&\mathbb{E}\{\lambda^\delta V_\delta\}-\mathbb{E}\{V_0\}\\
\le&\mu_4(\lambda)\sum_{k=0}^{\delta-1}\lambda^k\mathbb{E}\{\|e_k\|^2\}+\mu_5(\lambda)\sup_{l\in[-h-L,0]}\mathbb{E}\{\|\phi_l\|^2\}, \qquad (25)
\end{aligned}
$$

where

$$
\begin{aligned}
&\mu_4(\lambda)\triangleq\mu_1(\lambda)+h\lambda^h\mu_2(\lambda)+h^2\lambda^h\mu_3(\lambda),\\
&\mu_5(\lambda)\triangleq h^2\lambda^h\mu_2(\lambda)+h^2\lambda^h\left(h+\frac{(h+1)}{2}\lambda^h\right)\mu_3(\lambda).
\end{aligned}
$$

It is observed that, as $\lambda\to+\infty$, the function $\mu_4(\lambda)\to+\infty$. Meanwhile, we have $\mu_4(1)=-\epsilon<0$. Thus, there exists $1<\bar{\lambda}<+\infty$ such that $\mu_4(\bar{\lambda})=0$. Furthermore, we have

$$
\mathbb{E}\{\bar{\lambda}^\delta V_\delta\}\le\mu_5(\bar{\lambda})\sup_{l\in[-h-L,0]}\mathbb{E}\{\|\phi_l\|^2\}+\mathbb{E}\{V_0\}. \qquad (26)
$$

Based on (20), we obtain that

$$
\begin{aligned}
\mathbb{E}\{V_0\}\le&c_1\mathbb{E}\{\|e_0\|^2\}+c_2\sum_{i=-h}^{-1}\mathbb{E}\{\|e_i\|^2\}\\
&+c_3\sum_{i=-h}^{-1}\mathbb{E}\{\|\omega_i\|^2\}\\
\le&c_4\sup_{l\in[-h-L,0]}\mathbb{E}\{\|\phi_l\|^2\}, \qquad (27)
\end{aligned}
$$

where

$$
c_4\triangleq\max\{c_1,c_2,c_3\}(h+hL+1).
$$

Then, it follows from (26) and (27) that

$$
\mathbb{E}\{V_\delta\}\le\bar{\lambda}^{-\delta}(\mu_5(\bar{\lambda})+c_4)\sup_{l\in[-h-L,0]}\mathbb{E}\{\|\phi_l\|^2\}. \qquad (28)
$$

On the other hand, based on (13) and properties of positive definite matrices, we have

$$
\begin{aligned}
\mathbb{E}\{V_\delta\}\ge&\lambda_{\min}(P)\mathbb{E}\{\|e_\delta\|^2\}+L\lambda_{\min}(Q_j)\mathbb{E}\{\|e_{\delta-1}\|^2\}\\
&+\lambda_{\min}(R_1)(1+\kappa_2-\kappa_1)\sum_{i=\delta-\kappa_1}^{\delta-1}\mathbb{E}\{\|e_i\|^2\}\\
&+\lambda_{\min}(R_2)(1+\kappa_2-\kappa_1)\sum_{i=\delta-\kappa_1}^{\delta-1}\mathbb{E}\{\|\omega_i\|^2\}\\
>&c_5\mathbb{E}\{\|e_\delta\|^2\}, \qquad (29)
\end{aligned}
$$

where

$$
c_5\triangleq\lambda_{\min}(P).
$$

Combining (28) and (29) gives Moreover, we can know

$$
\begin{aligned}
\mathbb{E}\{\|e_\delta\|^2\}\le&\frac{1}{c_5}\mathbb{E}\{V_\delta\}\\
\le&a^\delta b\sup_{l\in[-h-L,0]}\mathbb{E}\{\|\phi_l\|^2\}, \qquad (30)
\end{aligned}
$$

where

$$
a\triangleq\bar{\lambda}^{-1}\in(0,1),\quad b\triangleq\frac{\mu_5(\bar{\lambda})+c_4}{c_5}>0.
$$

It is obvious that

$$
\lim_{\delta\to\infty}\mathbb{E}\left\{\|e_\delta\|_2^2\right\}=0, \qquad (31)
$$

which completes the proof. ■

B. PID Controller Design

This subsection addresses the design problem of PID controller gains for CNs under replay attacks.

Theorem 2: If there exist positive definite matrices $P_i\in\mathbb{R}^{n_x\times n_x}$, $R_1\in\mathbb{R}^{n_xN\times n_xN}$, $R_2\in\mathbb{R}^{n_xNL\times n_xNL}$, $Q_j\in\mathbb{R}^{n_xN\times n_xN}(j=1,2,\cdots,L)$, and matrices $\mathscr{K}^P$, $\mathscr{K}^I$ and $\mathscr{K}^D$ satisfying

$$
\begin{bmatrix}\tilde{\Pi}_{11}&\tilde{\Pi}_{12}&\tilde{\Pi}_{13}\\ *&-P&0\\ *&*&-P\end{bmatrix}<0, \qquad (32)
$$

where

$$
\begin{aligned}
&\tilde{\Pi}_{11}\triangleq\begin{bmatrix}\tilde{\Omega}_1&\hat{U}_2&0&0&0\\ *&-I&0&0&0\\ *&*&\tilde{\Omega}_2-Q&0&0\\ *&*&*&-R_1&0\\ *&*&*&0&-R_2\end{bmatrix},\\
&\tilde{\Pi}_{12}\triangleq\begin{bmatrix}\tilde{\Lambda}&P&(1-\bar{\gamma})\tilde{M}&\bar{\gamma}\tilde{K}&\bar{\gamma}\tilde{M}\end{bmatrix}^T,\\
&\tilde{\Pi}_{13}\triangleq\begin{bmatrix}\hat{\gamma}\tilde{K}&0&\hat{\gamma}\tilde{M}&-\hat{\gamma}\tilde{K}&-\hat{\gamma}\tilde{M}\end{bmatrix}^T,\\
&\tilde{\Omega}_1\triangleq-P+(1+\kappa_2-\kappa_1)R_1-\hat{U}_1+\sum_{j=1}^{L}Q_j,\\
&\tilde{\Omega}_2\triangleq(1+\kappa_2-\kappa_1)R_2,\quad\tilde{\Lambda}\triangleq P(L\otimes\Gamma)+\tilde{\gamma}\tilde{K},\\
&P\triangleq\text{diag}_N\{P_i\},\quad\tilde{K}\triangleq\mathscr{K}^P+\mathscr{K}^D,\\
&\tilde{M}\triangleq[\mathscr{K}^I-\mathscr{K}^D\quad\underbrace{\mathscr{K}^I\ \cdots\ \mathscr{K}^I}_{L-1}],
\end{aligned}
$$

then the CN (1) can asymptotically achieve mean-square synchronization under replay attacks, and the PID controller gains are given by $\bar{K}_P=P^{-1}\mathscr{K}^P$, $\bar{K}_I=P^{-1}\mathscr{K}^I$, $\bar{K}_D=P^{-1}\mathscr{K}^D$.

Proof: First, (12) is rewritten as follows:

$$
\overline{\Pi}=\tilde{\Pi}_{11}+\Omega^T\tilde{P}\Omega<0, \qquad (33)
$$

where

$$
\begin{aligned}
&\Omega\triangleq[{\Omega_1}^T\quad{\Omega_2}^T]^T,\quad\tilde{P}\triangleq\text{diag}\{P,P\},\\
&\Omega_1\triangleq\begin{bmatrix}\Lambda&I&(1-\bar{\gamma})M&\bar{\gamma}K&\bar{\gamma}M\end{bmatrix},\\
&\Omega_2\triangleq\begin{bmatrix}\hat{\gamma}K&0&\hat{\gamma}M&-\hat{\gamma}K&-\hat{\gamma}M\end{bmatrix}.
\end{aligned}
$$

By the Schur complement lemma, inequality (33) is ensured if

$$\begin{bmatrix} \tilde{\Pi}_{11} & \Omega^T \\ * & -\tilde{P}^{-1} \end{bmatrix} < 0. \tag{34}$$

Then, by pre- and post-multiplying (34) $\text{diag}\{I_{n_xN}, I_{n_xN}, I_{n_xNL}, I_{n_xN}, I_{n_xNL}, P, P\}$ and its transpose, we derive

$$\begin{bmatrix} \tilde{\Pi}_{11} & \Omega^T\tilde{P} \\ * & -\tilde{P} \end{bmatrix} < 0. \tag{35}$$

By letting $\mathscr{K}^P = P\bar{K}_P$, $\mathscr{K}^I = P\bar{K}_I$ and $\mathscr{K}^D = P\bar{K}_D$, it follows that the inequality (35) is equivalent to (32). The proof is complete. ■

Remark 5: Up to now, the secure cluster synchronization control problem for CNs under replay attacks has been investigated, and a unified framework for PID-based controller design has been established. The main difficulties arise from the interaction among controller parameters, network topology, and the stochastic characteristics of replay attacks. In Theorem 1, Lyapunov stability theory and stochastic analysis have been employed to guarantee mean-square synchronization under replay attacks. In Theorem 2, a systematic procedure has been provided to determine admissible PID controller gains, thereby completing the secure control design framework.

The subsequent analysis focuses on a special case in which $h_i(x_{i,k}) = A_i x_{i,k}$. Consequently, for $\bar{i} = \bar{j}$, we have $A_{\bar{i}} = A_{\bar{j}}$. In the following corollaries, we will analyze the ultimate synchronization performance for linear CNs subject to replay attacks and provide a solution to the design problem of the PID-based cluster controller gains.

Corollary 1: Consider the given PID controller gain matrices $\bar{K}_P$, $\bar{K}_I$, $\bar{K}_D$. If there exist positive definite matrices $P \in \mathbb{R}^{n_xN\times n_xN}$, $R_1 \in \mathbb{R}^{n_xN\times n_xN}$, $R_2 \in \mathbb{R}^{n_xNL\times n_xNL}$, and $Q_j \in \mathbb{R}^{n_xN\times n_xN}(j = 1, 2, \cdots, L)$ such that the following inequality holds:

$$\overline{\Xi} \triangleq \begin{bmatrix} \Xi_{11} & \Xi_{12} & \Xi_{13} & \Xi_{14} \\ * & \Pi_{33} & 0 & 0 \\ * & * & \Pi_{44} & \Pi_{45} \\ * & * & * & \Pi_{55} \end{bmatrix} < 0, \tag{36}$$

where

$$\begin{aligned}
\Xi_{11} &\triangleq \hat{\Lambda}^T P\hat{\Lambda} + \hat{\gamma}^2 K^T PK - P + (1+\kappa_2-\kappa_1)R_1 + \sum_{j=1}^{L} Q_j,\\
\Xi_{12} &\triangleq (1-\bar{\gamma})\hat{\Lambda}^T PM + \hat{\gamma}^2 K^T PM,\\
\Xi_{13} &\triangleq \bar{\gamma}\hat{\Lambda}^T PK - \hat{\gamma}^2 K^T PK,\\
\Xi_{14} &\triangleq \bar{\gamma}\hat{\Lambda}^T PM - \hat{\gamma}^2 K^T PM,\\
\hat{\Lambda} &\triangleq \widetilde{A} + (L\otimes\Gamma) + \tilde{\gamma}K, \quad \widetilde{A} \triangleq \text{diag}_N\{A_i\},
\end{aligned}$$

then, under the replay attacks, the CN (1) can asymptotically achieve mean-square synchronization.

Corollary 2: If there exist positive definite matrices $P_i \in \mathbb{R}^{n_x\times n_x}$, $R_1 \in \mathbb{R}^{n_xN\times n_xN}$, $R_2 \in \mathbb{R}^{n_xNL\times n_xNL}$, $Q_j \in \mathbb{R}^{n_xN\times n_xN}(j = 1, 2, \cdots, L)$, and matrices $\mathscr{K}^P$, $\mathscr{K}^I$ and $\mathscr{K}^D$ satisfying

$$\begin{bmatrix} \tilde{\Xi}_{11} & \tilde{\Xi}_{12} & \tilde{\Xi}_{13} \\ * & -P & 0 \\ * & * & -P \end{bmatrix} < 0, \tag{37}$$

where

$$\begin{aligned}
\tilde{\Xi}_{11} &\triangleq \begin{bmatrix} \tilde{\Theta}_1 & 0 & 0 & 0 \\ * & \tilde{\Omega}_2 - Q & 0 & 0 \\ * & * & -R_1 & 0 \\ * & * & 0 & -R_2 \end{bmatrix},\\
\tilde{\Xi}_{12} &\triangleq \begin{bmatrix} \bar{\Lambda} & (1-\bar{\gamma})\tilde{M} & \bar{\gamma}\tilde{K} & \bar{\gamma}\tilde{M} \end{bmatrix}^T,\\
\tilde{\Xi}_{13} &\triangleq \begin{bmatrix} \hat{\gamma}\tilde{K} & \hat{\gamma}\tilde{M} & -\hat{\gamma}\tilde{K} & -\hat{\gamma}\tilde{M} \end{bmatrix}^T,\\
\tilde{\Theta}_1 &\triangleq -P + (1+\kappa_2-\kappa_1)R_1 + \sum_{j=1}^{L} Q_j,\\
\bar{\Lambda} &\triangleq P\widetilde{A} + P(L\otimes\Gamma) + \tilde{\gamma}\tilde{K},\\
P &\triangleq \text{diag}_N\{P_i\}, \quad \tilde{K} \triangleq \mathscr{K}^P + \mathscr{K}^D,\\
\tilde{M} &\triangleq [\mathscr{K}^I - \mathscr{K}^D \quad \underbrace{\mathscr{K}^I \ \cdots \ \mathscr{K}^I}_{L-1}],
\end{aligned}$$

then the CN (1) can asymptotically achieve mean-square synchronization under replay attacks. Moreover, the PID controller gains can be determined by $\bar{K}_P = P^{-1}\mathscr{K}^P$, $\bar{K}_I = P^{-1}\mathscr{K}^I$, $\bar{K}_D = P^{-1}\mathscr{K}^D$.

Corollary 1 and Corollary 2 can be established by arguments analogous to those used in Theorem 1 and Theorem 2. Therefore, the detailed proofs are omitted for brevity.

Remark 6: In comparison with existing studies on secure synchronization of CNs, the distinguishing features of the present results can be summarized as follows:

1) A PID-based cluster synchronization control framework is investigated for discrete-time nonlinear CNs under replay attacks. By incorporating proportional, integral, and derivative actions, the controller enhances robustness against attack-induced outdated information. Moreover, cluster synchronization is enforced only within local subgroups, which reduces communication overhead and control energy consumption.
2) A replay attack model with stochastic occurrence and bounded persistence is introduced for the communication channel between the controller and the actuator. By combining Bernoulli random variables with time-varying attack duration, the model captures both the randomness and limited persistence of replay attacks, thereby reflecting practical attack behaviors more accurately than conventional static models.
3) The secure synchronization conditions are derived in the form of matrix inequalities, which explicitly incorporate both the PID dynamics and replay attack characteristics. This framework extends existing results on secure synchronization by accommodating clustered network topologies and PID-based control schemes within a unified analytical setup.

IV. Numerical Example

In this section, a numerical example is presented to verify the effectiveness of the proposed PID-based cluster synchronization controller.

The CN (1) consisting of five coupled nodes is divided into two clusters, namely, $\mathcal{F}_1 = \{1, 2\}$ and $\mathcal{F}_2 = \{3, 4, 5\}$. The coupling configuration matrix and the inner-coupling matrix are specified as

$$\mathcal{L} = \begin{bmatrix} -0.2 & 0.2 & -0.1 & 0 & 0.1 \\ 0.3 & -0.3 & -0.1 & 0.1 & 0 \\ 0.1 & -0.1 & -0.2 & 0.1 & 0.1 \\ 0 & 0 & 0.3 & -0.6 & 0.3 \\ -0.1 & 0.1 & 0.3 & 0.2 & -0.5 \end{bmatrix},$$

and $\Gamma = 2.82I$.

The nonlinear functions associated with the nodes in the two clusters are given by

$$h_1\left(\begin{bmatrix}\nu_1 \\ \nu_2\end{bmatrix}\right) = \begin{bmatrix}0.95\nu_1 + \tanh(0.2\nu_1) \\ 0.95\nu_2 + \tanh(0.2\nu_2)\end{bmatrix},$$

$$h_2\left(\begin{bmatrix}\nu_1 \\ \nu_2\end{bmatrix}\right) = \begin{bmatrix}0.95\nu_1 + \tanh(0.1\nu_1) \\ 0.95\nu_2 + \tanh(0.1\nu_2)\end{bmatrix}.$$

According to Assumption 1, the following matrices are obtained:

$$\chi_{11} = \begin{bmatrix}1.15 & 0 \\ 0 & 1.15\end{bmatrix}, \ \chi_{12} = \begin{bmatrix}0.95 & 0 \\ 0 & 0.95\end{bmatrix},$$
$$\chi_{21} = \begin{bmatrix}1.05 & 0 \\ 0 & 1.05\end{bmatrix}, \ \chi_{22} = \begin{bmatrix}0.95 & 0 \\ 0 & 0.95\end{bmatrix}.$$

The parameters in the replay attack model are selected as $\bar{\gamma} = 0.2$, $\kappa_1 = 1$, and $\kappa_2 = 3$. And the time length of the integral window is given as $L = 3$. The initial values of the target node states $\sigma_{m,k}$ $(m = 1, 2)$ and the node states $x_{i,k}$ $(i = 1, 2, 3, 4, 5)$ are chosen as

$$\bar{\sigma}_{1,0} = \begin{bmatrix}0.9 & -0.9\end{bmatrix}^T, \ \bar{\sigma}_{2,0} = \begin{bmatrix}0.8 & -0.8\end{bmatrix}^T,$$
$$x_{1,0} = \begin{bmatrix}0.1 & -0.1\end{bmatrix}^T, \ x_{2,0} = \begin{bmatrix}0.2 & -0.2\end{bmatrix}^T,$$
$$x_{3,0} = \begin{bmatrix}0.1 & -0.1\end{bmatrix}^T, \ x_{4,0} = \begin{bmatrix}0.2 & -0.2\end{bmatrix}^T,$$
$$x_{5,0} = \begin{bmatrix}0.3 & -0.3\end{bmatrix}^T.$$

The simulation results under replay attacks are illustrated in Figs. 1–8. Figs. 1 and 2 depict the trajectories of σ_k and x_k under the proportional cluster control strategy. Figs. 3 and 4 present the corresponding trajectories under the PID-based cluster control strategy. The synchronization error trajectories e_k under proportional cluster control are shown in Figs. 5 and 6, while those under PID-based cluster control are displayed in Figs. 7 and 8. It can be observed that the proportional cluster control strategy results in nonzero steady-state errors, whereas the PID-based cluster control strategy enables the discrete-time nonlinear CN to achieve secure synchronization under replay attacks.

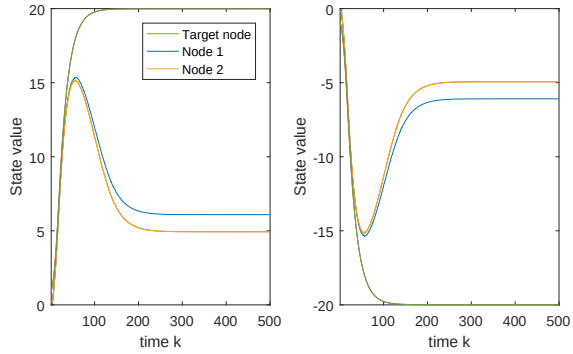


Fig. 1. Trajectories of the first state component and the second state component of nodes in cluster $\mathcal{F}_1$ under proportional control.

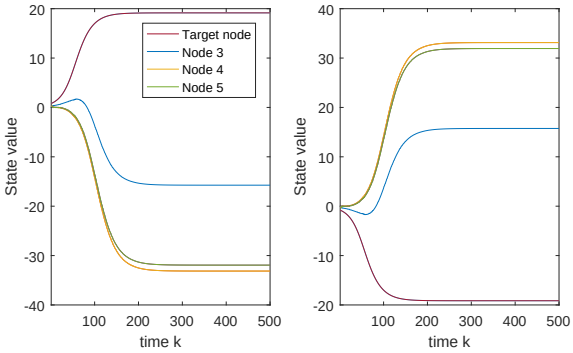


Fig. 2. Trajectories of the first state component and the second state component of nodes in cluster $\mathcal{F}_2$ under proportional control.

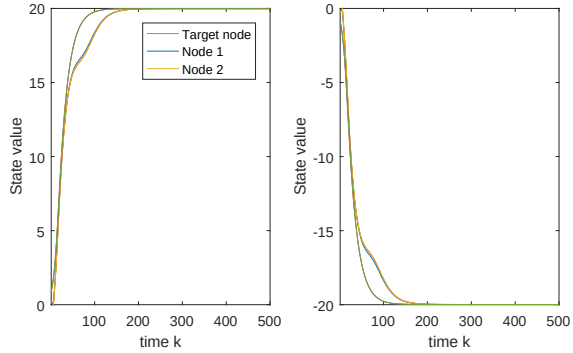


Fig. 3. Trajectories of the first state component and the second state component of nodes in cluster $\mathcal{F}_1$ under PID-based control.

V. Conclusion

In this paper, the cluster synchronization control problem has been investigated for a class of discrete-time nonlinear CNs subject to replay attacks. A replay attack model has been introduced by employing Bernoulli random variables together with bounded attack duration parameters, thereby characterizing both the randomness and persistence of replay attacks. To achieve reliable synchronization under such adverse conditions, a PID-based cluster synchronization control strategy has been developed. By incorporating proportional, integral, and derivative components, the controller makes

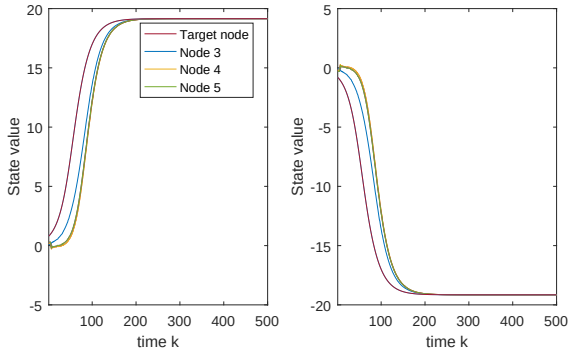


Fig. 4. Trajectories of the first state component and the second state component of nodes in cluster $\mathcal{F}_2$ under PID-based control.

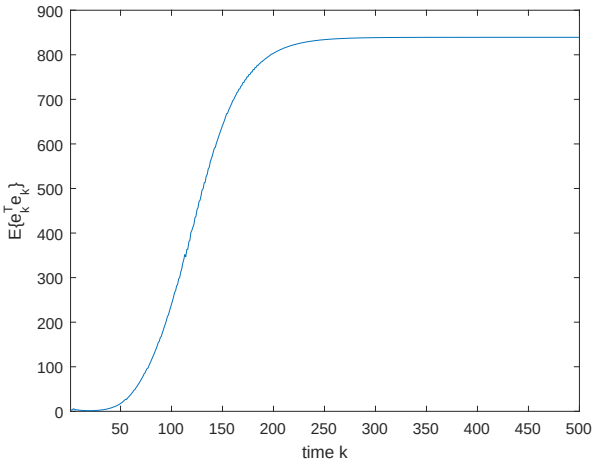


Fig. 5. Synchronization error of nodes in cluster $\mathcal{F}_1$ under proportional control.

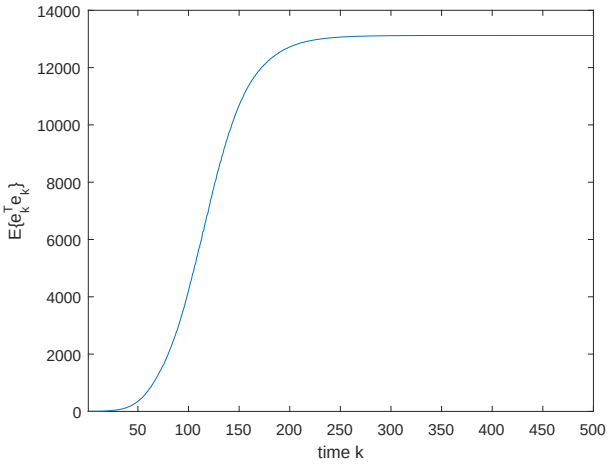


Fig. 6. Synchronization error of nodes in cluster $\mathcal{F}_2$ under proportional control.

use of both current and historical information to alleviate the detrimental effects of replay attacks. Moreover, sufficient conditions have been established to guarantee mean-square ultimate cluster synchronization through Lyapunov stability

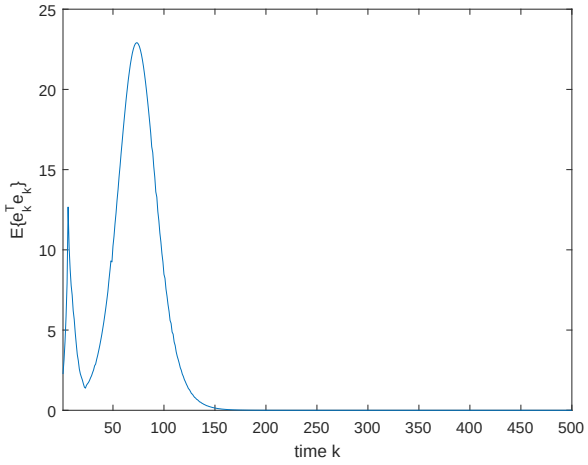


Fig. 7. Synchronization error of nodes in cluster $\mathcal{F}_1$ under PID-based control.

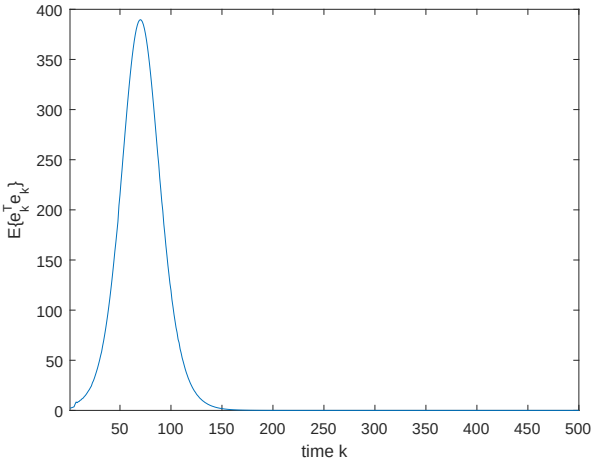


Fig. 8. Synchronization error of nodes in cluster $\mathcal{F}_2$ under PID-based control.

analysis and stochastic techniques. Based on these conditions, a systematic procedure for determining admissible PID controller gains has been provided. Numerical simulation results have demonstrated that the proposed control strategy is capable of maintaining satisfactory synchronization performance even in the presence of replay attacks.

In this paper, the network model under consideration is assumed to be available. In practical large-scale IoT networks, precise system models may be difficult to obtain. Therefore, developing data-driven-based [36], [37] privacy-preserving synchronization control methods to extend the current results without relying on accurate system models is an interesting topic for future research.

REFERENCES

[1] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez and D.-U. Hwang, Complex networks: structure and dynamics, *Physics Reports*, vol. 424, no. 4–5, pp. 175–308, 2006.

[2] R. Caballero-Águila and J. Linares-Pérez, Centralized fusion estimation in networked systems: addressing deception attacks and packet dropouts with a zero-order hold approach, *International Journal of Network Dynamics and Intelligence*, vol. 3, no. 4, art. no. 100021, 2024.

[3] R. Caballero-Águila, J. Hu and J. Linares-Pérez, Filtering and smoothing estimation algorithms from uncertain nonlinear observations with time-correlated additive noise and random deception attacks, *International Journal of Systems Science*, vol. 55, no. 10, pp. 2023–2035, 2024.

[4] J. Cai, X. Feng, H. Jiang and M. Shi, Node influence calculation of novel social networks, in *Proceedings of the 18th International Conference on Computer and Information Science(ICIS)*, Beijing, China, 2019, pp. 366–370.

[5] J. Cao and L. Li, Cluster synchronization in an array of hybrid coupled neural networks with delay, *Neural Networks*, vol. 22, no. 4, pp. 335–342, 2009.

[6] W.-H. Chen, X. Lu and D.-Y. Liang, Global exponential stability for discrete-time neural networks with variable delays, *Physics Letters. A*, vol. 358, no. 3, pp. 186–198, 2006.

[7] Y. Chen, S. Fei and Y. Li, Robust stabilization for uncertain saturated time-delay systems: a distributed-delay-dependent polytopic approach, *IEEE Transactions on Automatic Control*, vol. 62, no. 7, pp. 3455–3460, 2017.

[8] M.-C. Fang, Y.-Z. Zhuo and Z.-Y. Lee, The application of the self-tuning neural network PID controller on the ship roll reduction in random waves, *Ocean Engineering*, vol. 37, no. 7, pp. 529–538, 2010.

[9] G. Franzè, F. Tedesco and W. Lucia, Resilient control for cyber-physical systems subject to replay attacks, *IEEE Control Systems Letters*, vol. 3, no. 4, pp. 984–989, 2019.

[10] H. Fu, X. Meng and Y. Chen, Finite-time distributed filtering of time-varying switched stochastic systems with DoS attacks based on encoding–decoding scheme, *IEEE Systems Journal*, vol. 18, no. 1, pp. 268–277, 2024.

[11] H. Fu, Z. Wang, D. Zhao and B. Shen, Secure state estimation for a class of nonlinear systems over sensor networks with sensor resolution: tackling replay attacks, *IEEE Internet of Things Journal*, vol. 12, no. 13, pp. 25333–25345, 2025.

[12] H. Fu, Z. Wang, D. Zhao and B. Shen, Proportional-integral state estimation for a class of nonlinear complex networks with uncertain couplings: tackling adversarial replay attacks, *IEEE Transactions on Network Science and Engineering*, vol. 12, no. 5, pp. 4001–4012, 2025.

[13] D. Ghosh and S. Banerjee, Projective synchronization of time-varying delayed neural network with adaptive scaling factors, *Chaos, Solitons and Fractals*, vol. 53, pp. 1–9, 2013.

[14] J. Hong, R. Tamakloe, S. Lee and D. Park, Exploring the topological characteristics of complex public transportation networks: focus on variations in both single and integrated systems in the seoul metropolitan area, *Sustainability*, vol. 11, no. 19, art. no. 5404, 2019.

[15] N. Hou, D. Zhang, F. Yang, W. Li and Y. Sui, Security-guaranteed PID control for discrete-time systems subject to periodic Dos attacks, *Processes*, vol. 11, art. no. 1375, 2023.

[16] S. Hu and J. Wang, Global robust stability of a class of discrete-time interval neural networks, *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 53, no. 1, pp. 129–138, 2006.

[17] J. Huang, W. Yang, D. W. C. Ho, F. Li and Y. Tang, Security analysis of distributed consensus filtering under replay attacks, *IEEE Transactions on Cybernetics*, vol. 54, no. 6, pp. 3526–3539, 2024.

[18] C. Jia, J. Hu, X. Yi, H. Liu, J. Huang and Z. Cao, Recursive state estimation for a class of quantized coupled complex networks subject to missing measurements and amplify-and-forward relay, *Information Science*, vol. 630, pp. 53–73, 2023.

[19] K. Kaneko, Relevance of dynamic clustering to biological networks, *Physica D: Nonlinear Phenomena*, vol. 75, no. 1–3, pp. 55–73, 1994.

[20] F. Karray, W. Gueaieb and S. Al.-Sharhan, The hierarchical expert tuning of PID controllers using tools of soft computing, *IEEE Transactions on Cybernetics*, vol. 32, no. 1, pp. 77–90, 2002.

[21] M. Kumar, A. Kumar, and A. Altaf, Resilient PID control design for cyber–physical AC microgrid with multiple electric vehicle and heat pump, *Chaos, Solitons & Fractals*, vol. 205, art. no. 117881, 2026.

[22] J.-Y. Li, Z. Wang, R. Lu and Y. Xu, Cluster synchronization control for discrete-time complex dynamical networks: when data transmission meets constrained bit rate, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 5, pp. 2554–2568, 2023.

[23] X. Lin, Y. Hu, X. Zhang and K. Peng, Encoding-decoding-based distributed state estimation over sensor networks with limited sensing range under DoS attacks, *Neurocomputing*, vol. 611, art. no. 128713, 2025.

[24] D. Liu and D. Ye, Cluster synchronization of complex networks under denial-of-service attacks with distributed adaptive strategies, *IEEE Transactions on Control of Network Systems*, vol. 9, no. 1, pp. 334–343, 2021.

[25] M. Liu, D. W. C. Ho and Y. Niu, Stabilization of Markovian jump linear system over networks with random communication delay, *Automatica*, vol. 45, no. 2, pp. 416–421, 2009.

[26] P. Liu, M. Kong and Z. Zeng, Projective synchronization analysis of fractional-order neural networks with mixed time delays, *IEEE Transactions on Cybernetics*, vol. 52, no. 7, pp. 6798–6808, 2020.

[27] X. Liu and T. Chen, Cluster synchronization in directed networks via intermittent pinning control, *IEEE Transactions on Neural Networks*, vol. 22, no. 7, pp. 1009–1020, 2011.

[28] G. M. Mahmoud and E. E. Mahmoud, Complete synchronization of chaotic complex nonlinear systems with uncertain parameters, *Nonlinear Dynamics*, vol. 62, no. 4, pp. 875–882, 2010.

[29] S. Majumder, S. Ray, M. Dasgupta, P. Bhattacharya, T. R. Gadekallu and G. Srivastava, QuanFraud: quantum state verification scheme for fraud detection in IoT-assisted quantum-blockchain networks, *IEEE Transactions on Services Computing*, vol. 19, no. 1, pp. 616–627, 2026.

[30] Y. Mo, S. Weerakkody and B. Sinopoli, Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs, *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 93–109, 2015.

[31] V. Novicenko and I. Ratas, In-phase synchronization in complex oscillator networks by adaptive delayed feedback control, *Physical Review E*, vol. 98, art. no. 042302, 2019.

[32] G. A. Pagani and M. Aiello, The power grid as a complex network: a survey, *Computing Research Repository*, vol. 392, no. 11, pp. 2688–2700, 2013.

[33] K. Pang, L. Ma, H. Bai and S. Xue, Probability-guaranteed secure consensus control for time-varying stochastic multi-agent systems under mixed attacks, *Journal of the Franklin Institute*, vol. 359, pp. 2541–2563, 2022.

[34] C. Peng and H. Sun, Switching-like event-triggered control for networked control systems under malicious denial of service attacks, *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3943–3949, 2020.

[35] M. Sedighizadeh and A. Rezazadeh, A modified adaptive wavelet PID control based on reinforcement learning for wind energy conversion system control, *Advances in Electrical and Computer Engineering*, vol. 10, no. 2, pp. 153–159, 2010.

[36] H. Shen, C. Peng, H. Yan and S. Xu, Data-driven near optimization for fast sampling singularly perturbed systems, *IEEE Transactions on Automatic Control*, vol. 69, no. 7, pp. 4689–4694, 2024.

[37] H. Shen, Y. Wang, H. Yan and S. Xu, Data-driven single-loop policy iteration control of uncertain singularly perturbed systems, *IEEE Transactions on Automatic Control*, vol. 70, no. 12, pp. 8314–8320, 2025.

[38] W. Song, Z. Wang, Z. Li, J. Wang and Q.-L. Han, Nonlinear filtering with sample-based approximation under constrained communication: progress, insights and trends, *IEEE/CAA Journal of Automatica Sinica*, vol. 11, no. 7, pp. 1539–1556, 2024.

[39] H. Su, Z. Rong, M. Z. Q. Chen, X. Wang, G. Chen and H. Wang, Decentralized adaptive pinning control for cluster synchronization of complex dynamical networks, *IEEE Transactions on Cybernetics*, vol. 43, no. 1, pp. 394–399, 2013.

[40] Z. Tang, J.-H. Park, Y. Wang and J. Feng, Adaptively synchronize the derivative coupled complex networks with proportional delay, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 8, pp. 4969–4979, 2021.

[41] X. Wan, Y. Li, Y. Li and M. Wu, Finite-time H_∞ state estimation for two-time-scale complex networks under stochastic communication protocol, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 1, pp. 25–36, 2022.

[42] X. F. Wang and G. Chen, Synchronization in scale-free dynamical networks: robustness and fragility, *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 49, no. 1, pp. 54–62, 2022.

[43] S. Wen, Z. Zeng, T. Huang and Y. Zhang, Exponential adaptive lag synchronization of memristive neural networks via fuzzy method and applications in pseudorandom number generators, *IEEE Transactions on Fuzzy Systems*, vol. 22, no. 6, pp. 1704–1713, 2014.

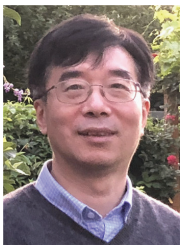
[44] S. Wen, Z. Zeng, T. Huang, Q. Meng and W. Yao, Lag synchronization of switched neural networks via neural activation function and applications in image encryption, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 26, no. 7, pp. 1493–1502, 2015.

[45] H. Wu, S. Liu and L. Wang. Cluster synchronization of complex dynamic networks under pinning control via a limited capacity communication channel, *Nonlinear Analysis: Hybrid Systems*, vol. 55, art. no. 101547, 2025.

[46] W. Wu, W. Zhou and T. Chen, Cluster synchronization of linearly coupled complex networks under pinning control, *IEEE Transactions*

on Circuits and Systems I: Regular Papers, vol. 56, no. 4, pp. 829–839, 2009.
[47] H. Xiao, D. Ding, H. Dong and G. Wei, Adaptive event-triggered state estimation for large-scale systems subject to deception attacks, *Science China Information Sciences*, vol. 65, art. no. 122207, 2022.
[48] H. Yang, L. Shu and S. Zhong, Pinning lag synchronization of complex dynamical networks with known state time-delay and unknown channel time-delay, *Nonlinear Dynamics*, vol. 89, no. 3, pp. 1793–1802, 2017.
[49] Z. Yao, P. Zhou, Z. Zhu and J. Ma, Phase synchronization between a light-dependent neuron and a thermosensitive neuron, *Neurocomputing*, vol. 423, pp. 518–534, 2021.
[50] L. Yu, Y. Liu, Y. Cui, N.-D. Alotaibi and F.-E. Alsaadi, Intermittent dynamic event-triggered state estimation for delayed complex networks based on partial nodes, *Neurocomputing*, vol. 459, pp. 59–69, 2021.
[51] Y. Yuan, X. Tang, W. Zhou, W. Pan, X. Li, H.-T. Zhang, H. Ding and J. Goncalves, Data driven discovery of cyber physical systems, *Nature Communications*, vol. 10, no. 1, pp. 1–9, 2019.
[52] D. Yue and H. Li, Synchronization stability of continuous/discrete complex dynamical networks with interval time-varying delays, *Neurocomputing*, vol. 73, pp. 809–819, 2010.
[53] G. Y. Zang, S. L. Shi and Y. C. Ma, Finite-time H_∞ synchronization of Markov jump complex dynamical networks with additive time-varying delays: an event-triggered control strategy, *Computational & Applied Mathematices*, vol. 42, art. no. 141, 2023.
[54] L. Zhang, X. Fu, Y. Wang, Y. Lei and X. Chen, Matrix projective synchronization for a class of discrete-time complex networks with commonality via controlling the crucial node, *Neurocomputing*, vol. 461, pp. 360–369, 2021.

Yunjie Chen was born in Jiangsu, China, in 1998, and received her B.S. degree in Mathematics and the M.S. degree in Mathematics from Yangzhou University, Yangzhou, China, in 2020 and 2023, respectively. Now she is pursuing the Ph.D. degree in Applied Mathematics at Yangzhou University, and her research interests include complex network systems, privacy protection and secure control.



Zidong Wang (Fellow, IEEE) received the B.Sc. degree in mathematics in 1986 from Suzhou University, Suzhou, China, and the M.Sc. degree in applied mathematics in 1990 and the Ph.D. degree in electrical engineering in 1994, both from Nanjing University of Science and Technology, Nanjing, China.

He is currently Professor of Dynamical Systems and Computing in the Department of Computer Science, Brunel University of London, U.K. From 1990 to 2002, he held teaching and research appointments in universities in China, Germany and the UK. Prof. Wang's research interests include dynamical systems, signal processing, bioinformatics, control theory and applications. He has published a number of papers in international journals. He is a holder of the Alexander von Humboldt Research Fellowship of Germany, the JSPS Research Fellowship of Japan, William Mong Visiting Research Fellowship of Hong Kong.

Prof. Wang serves (or has served) as the Editor-in-Chief for *International Journal of Systems Science*, the Editor-in-Chief for *Neurocomputing*, the Editor-in-Chief for *Systems Science & Control Engineering*, and an Associate Editor for 12 international journals including IEEE Transactions on Automatic Control, IEEE Transactions on Control Systems Technology, IEEE Transactions on Neural Networks, IEEE Transactions on Signal Processing, and IEEE Transactions on Systems, Man, and Cybernetics-Part C. He is a Member of the Academia European, a Member of the European Academy of Sciences and Arts, an Academician of the International Academy for Systems and Cybernetic Sciences, a Fellow of the IEEE, a Fellow of the Royal Statistical Society and a member of program committee for many international conferences.

Yurong Liu was born in Jiangsu, China, in 1964. He received the B.S. degree in Mathematics from Suzhou University, Suzhou, China, in 1986, the M.S. degree in Applied Mathematics from Nanjing University of Science and Technology, Nanjing, China, in 1989, and the Ph.D. degree in Applied Mathematics from Suzhou University, Suzhou, China, in 2001.

Dr. Liu is currently a professor with the Department of Mathematics, Yangzhou University, China. He also serves as an Associate Editor of Neurocomputing. So far, he has published more than 100 papers in refereed international journals. His current interests include stochastic control, neural networks, complex networks, nonlinear dynamics, time-delay systems, multi-agent systems, and chaotic dynamics.

Weihao Song (Member, IEEE) received the B.S. degree in flight vehicle design and engineering in 2016 and the Ph.D. degree in aeronautical and astronautical science and technology in 2021, both from Beijing Institute of Technology, Beijing, China.

From May 2019 to May 2020, he was a Visiting Scholar with the Department of Computer Science, Brunel University of London, Uxbridge, U.K. Since 2021, he has been a Postdoctoral Researcher at Peking University. He is also currently an Honorary Research Fellow with the Department of Computer Science, Brunel University of London. His research interests include Bayesian state estimation, distributed state estimation, nonlinear filtering, and networked control systems.