Electronic Research Archive

http://www.aimspress.com/journal/era

ERA, 33(8): 5022–5044.
DOI: 10.3934/era.2025225
Received: 09 July 2025
Revised: 08 August 2025
Accepted: 15 August 2025
Published: 26 August 2025

Research article

Observer-based networked control for stochastic nonlinear systems under false data injection attacks and limited bandwidth

Xinyi Bai*and Qinru Yang

School of Computer Science and Technology, Anhui University of Technology, Ma'anshan 243032, China

* **Correspondence:** Email: xybai@ahut.edu.cn.

Abstract: This paper investigates observer-based networked control for stochastic nonlinear systems under false data injection (FDI) attacks and limited communication bandwidth. To mitigate the impact of FDI attacks while reducing communication load, we propose an FDI attack-resilient periodic encoding–decoding scheme based on uniform quantization. We first establish a detectability criterion for the stochastic nonlinear system under this periodic encoding–decoding scheme. Then, we derive a condition to further guarantee the input-to-state stability of the resulting closed-loop system. The condition, which enables the determination of the desired observer and controller gains, involves a series of linear matrix inequalities that are straightforward to verify using available MATLAB numerical tools. Finally, we validate the effectiveness and robustness of the proposed controller design through a case study.

Keywords: stochastic nonlinear system; false data injection attack; observer-based network control; input-to-state stability; encoding–decoding scheme

1. Introduction

Networked control systems (NCSs) refer to distributed architectures where information among sensors, actuators, and controllers is transmitted via a shared communication network, as opposed to traditional direct connections [1, 2]. NCSs offer several advantages, including flexible system architecture, reduced wiring complexity, improved scalability, effective handling of system-level complexity, and support for remote monitoring and maintenance. Over the past few decades, networked control has been considered for various complex systems, including multi-agent systems and power systems, and the corresponding methods have been deployed in many fields, including industrial automation, smart grids, remote surgery, intelligent vehicles, and distributed robotics [3–7]. However, it should be noted that most of the existing references have been concerned with deterministic and linear system models. Considering that many actual dynamic systems are often subject to noisy disturbances [8–11] and nonlinear dynamics [12–15], the networked control of stochastic nonlinear systems (SNSs) has

attracted increasing research attention over the last several years [16–20].

As a consequence of the communication network's openness, NCSs are vulnerable to cyber–attacks. Malicious attackers can exploit network access points to manipulate system data without physical contact. Common attack types include denial-of-service [21–23], replay [24], man-in-the-middle [25], TCP/IP protocol [26, 27], and, notably, false data injection (FDI) attacks [28, 29]. The FDI attack refers to the attacker's manipulation of measurement or control data in a statistically deceptive manner [30, 31]. By dynamically adjusting the injected data to conform to the normal operation mode of the system, FDI attacks can often bypass the detection mechanisms and continue to act on the system, thus posing long-term potential threats and even systemic damage [32, 33]. A variety of strategies have been proposed to address FDI attacks in NCSs with different architectures in recent years. For example, Xu et al. [34] investigated FDI threats in power system state estimation and designed a robust moving target defense mechanism by perturbing system parameters. Liu et al. [35] examined the drive–response networked synchronization of chaotic neural networks under stochastic FDIs and presented a quantized event-driven controller design scheme, while in [36], Joby et al. focused on time-delay systems subject to input nonlinearities and scaling FDIs and developed a robust networked observer-based control strategy.

Another problem is the limitation of communication bandwidth. In NCSs, the limited network bandwidth constrains the rate and volume of sensor–actuator data transmission [37, 38]. To address this, encoding–decoding techniques have been introduced into NCSs to optimize bandwidth usage. Wang et al. [39] studied discrete-time MIMO linear systems with two-sided quantization bounds and proposed an exponential interval shaping control strategy based on finite data rate. Liu et al. [40] took the ultimate boundedness of periodic dynamic systems into account and provided networked observer-based control design methods under encoding–decoding mechanisms. Singh et al. [41] focused on the mismatch problem between input quantizers and decoders and proposed a sector condition framework based on the scattered pair $\{K, KL\}$, analyzing the stability of systems under quantization uncertainty. Zhou et al. [42] developed an encoding–decoding-based sliding-mode control scheme for jump systems under constrained bit rates, employing an adaptive quantizer to guarantee mean-square stability through per-sample encoding and decoding operations. Notably, the majority of existing studies on networked control with encoding–decoding do not account for FDI attacks. It is also worth noting that they employ encoding–decoding operations at every sampling instant, which leaves room for improvement in terms of network resource efficiency.

Motivated by the two observations presented above, this paper focuses on observer-based networked control for SNSs subject to FDI attacks and communication bandwidth constraints. The main contributions are summarized as follows:

1) An FDI attack-resilient periodic encoding–decoding scheme based on uniform quantization is designed. Compared with the encoding–decoding schemes in [39–42], the FDI attack-resilient periodic encoding–decoding scheme reduces the number of data transmissions to save network resources while considering FDI attacks.

2) A condition guaranteeing the detectability and the input-to-state stability (ISS) is established for the resulting closed-loop SNS. The condition, which enables the determination of the desired observer and controller gains, involves a series of linear matrix inequalities (LMIs) that are straightforward to verify using available MATLAB numerical tools.

2. Preliminaries

This section presents a detailed description of the SNS under consideration, the networked observer-based controller, and the FDI attack-resilient periodic encoding–decoding scheme, and then formulates the issue to be solved in this work.

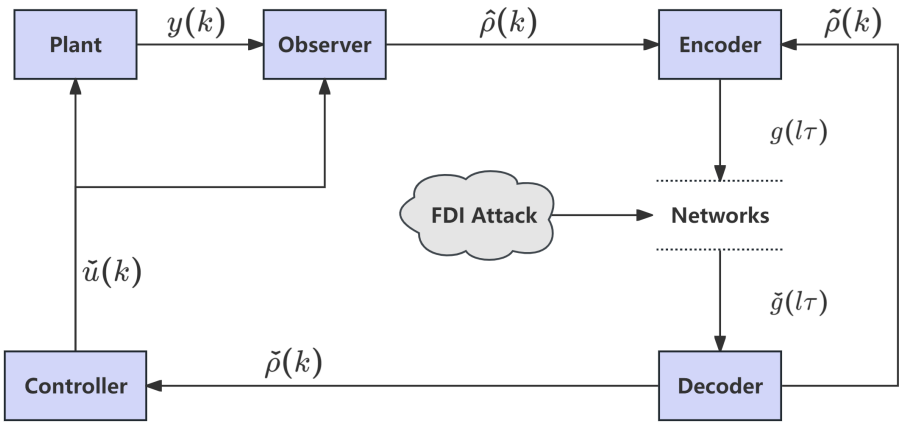

Figure 1. Control structure of the SNS subject to FDI attacks.

The control structure of the SNS subject to FDI attacks is detailed in Figure 1. In this paper, we use class $\mathcal{K}$ functions to represent functions that are continuous, strictly increasing, and vanish at zero; class $\mathcal{KL}$ functions to represent functions that are of class $\mathcal{K}$ in the first argument and decrease to zero in the second argument; and class $\mathcal{K}_\infty$ functions to represent class $\mathcal{K}$ functions that are unbounded. All other notations, unless explicitly stated otherwise, are consistent with those outlined in Refs. [43–45].

2.1. System description

In general, existing studies on SNSs can be classified into two categories: continuous-time SNSs [46–48] and discrete-time SNSs [49]. This paper focuses on the latter, where the plant model under consideration is given as follows:

$$\begin{cases} \rho(k+1) = A\rho(k) + f(\rho(k)) + E\rho(k)\omega(k) + Bu(k), \\ \quad y(k) = C\rho(k). \end{cases} \tag{2.1}$$

Here, $\rho(k) = [\rho_1(k) \ \dots \ \rho_n(k)]^\top \in \mathbb{R}^n$ represents the state of the SNS with $\rho_0 = \phi_0$ and $f(\cdot) : \mathbb{R}^n \to \mathbb{R}^n$ is a nonlinear function. Unlike those considered in Refs. [50–54], the function $f(\cdot)$ in this paper is required to meet $f(0) = 0$ and

$$[f(\epsilon_1) - f(\epsilon_2) - U_l(\epsilon_1 - \epsilon_2)]^T [f(\epsilon_1) - f(\epsilon_2) - U_r(\epsilon_1 - \epsilon_2)] \leq 0 \tag{2.2}$$

for any $\epsilon_1, \epsilon_2 \in \mathbb{R}^n$. The matrices A, B, C , E , U_l and U_r are real and known. The measurement output is denoted by $y(k) \in \mathbb{R}^m$, and the control input vector is given by $\check{u}(k) \in \mathbb{R}^n$. The stochastic disturbance $\omega(k) \in \mathbb{R}$ is a scalar Brownian motion as in [55].

2.2. Observer-based networked controller

To guarantee the ISS of the SNS, the controller is constructed as follows:

$$\begin{cases} \hat{\rho}(k+1) = A\hat{\rho}(k) + f(\hat{\rho}(k)) + L(y(k) - C\hat{\rho}(k)) + B\check{u}(k), \\ \quad \check{u}(k) = K\check{\rho}(k). \end{cases} \tag{2.3}$$

In this formulation, the estimated state $\hat{\rho}(k) = [\hat{\rho}_1(k) \ \dots \ \hat{\rho}_n(k)]^\top \in \mathbb{R}^n$ is initialized as $\hat{\rho}_0 = \hat{\varphi}_0$, where $\hat{\varphi}_0$ is known. The control input $\check{u}(k) \in \mathbb{R}^n$ is generated based on the estimate, and $\check{\rho}(k) = [\check{\rho}_1(k) \ \dots \ \check{\rho}_n(k)]^\top \in \mathbb{R}^n$ represents the decoded state. The observer–gain $L \in \mathbb{R}^{n\times m}$ and the controller–gain $K \in \mathbb{R}^{n\times n}$ are the matrices that need to be designed.

2.3. FDI Attack-resilient periodic encoding–decoding scheme

Considering the limited bandwidth and potential unreliability in the communication link, a quantization-based encoding–decoding strategy is adopted to achieve effective data transmission.

Let $\tau \in \mathbb{Z}_{>0}$ be a fixed positive integer that denotes the period parameter. At every coding moment $k = l\tau$ for $l = 1, 2, \dots$, the most recent decoded value $\check{\rho}_i(l\tau)$ for the ith node is unavailable. To tackle this issue, we define $\tilde{\rho}_i(l\tau)$ as an auxiliary state derived from $\check{\rho}_i(l\tau-1)$ and recursively update $\tilde{\rho}(k)$ using the rule:

$$\tilde{\rho}(k) = \begin{cases} 0, & k = 0, \\ A\check{\rho}(k-1) + f(\check{\rho}(k-1)) + \check{u}(k-1), & k = l\tau, \\ \check{\rho}(k), & \text{otherwise.} \end{cases} \tag{2.4}$$

Afterward, a uniform quantization is utilized to process the error

$$\xi(l\tau) \triangleq \hat{\rho}(l\tau) - \tilde{\rho}(l\tau)$$

between the estimated state and the auxiliary state. Define the error vector at time lh for node i as:

$$\xi_i(l\tau) = \hat{\rho}_i(l\tau) - \tilde{\rho}_i(l\tau).$$

Let the quantization threshold be $\varsigma(l\tau) > 0$ and the quantization level be $q \in \mathbb{Z}_{>0}$. Using the infinity norm as the boundary constraint, the total bounded region is defined as:

$$B_{\varsigma(l\tau)} = \{\xi \in \mathbb{R}^n : \|\xi\|_\infty \le \varsigma(l\tau)\}.$$

The set $B_{\varsigma(l\tau)}$ is uniformly partitioned into equally spaced q^n hyperrectangles. The interval for each component $i \in \{1, \dots, n\}$ is defined as:

$$\mathcal{I}_{s_i}(\varsigma(l\tau)) = \left[-\varsigma(l\tau) + \tfrac{2(s_i-1)\varsigma(l\tau)}{q}, \ -\varsigma(l\tau) + \tfrac{2s_i\varsigma(l\tau)}{q}\right], s_i \in \{1, \dots, q\}, \tag{2.5}$$

where the geometric center of (2.5) is

$$-\varsigma(l\tau) + \frac{(2s_i - 1)\varsigma(l\tau)}{q}.$$

The geometric center of the corresponding hyperrectangle is defined by:

$$\Theta_{\varsigma(l\tau)}(s_1,\ldots,s_n)=\left[-\varsigma(l\tau)+\frac{(2s_1-1)\varsigma(l\tau)}{q},\ \ldots,\ -\varsigma(l\tau)+\frac{(2s_n-1)\varsigma(l\tau)}{q}\right]^{\top}. \tag{2.6}$$

Therefore, for any $\xi\in B_{\varsigma(l\tau)}$, the Euclidean distance between ξ and its nearest center point satisfies the bound:

$$\|\xi-\Theta_{\varsigma(l\tau)}(s_1,\ldots,s_n)\|_2\le\frac{\sqrt{n}\varsigma(l\tau)}{q}. \tag{2.7}$$

This quantized representation enables the state to be encoded into a finite set of codewords with guaranteed precision. In the presence of an FDI attack, the encoder continues to operate normally, but the decoder, which has been compromised by malicious manipulation, fails to reconstruct the correct state. A specialized formulation of an FDI attack-resilient periodic encoding–decoding scheme is proposed to analyze detectability.

Coding: At each transmission instant $k=l\tau$, the encoder computes the quantization error vector $\xi(l\tau)$ and determines the corresponding subinterval indices as

$$(s_1,s_2,\ldots,s_n)\in\{1,\ldots,q\}^n$$

based on the predefined quantization grid. These indices indicate the coordinate-wise location of $\xi(l\tau)$ within the uniform partition of the bounded region $B_{\varsigma(l\tau)}$, and are assembled into a codeword:

$$g(l\tau)=(s_1,s_2,\ldots,s_n),$$

which is then transmitted over the communication channel.

Decoding: Upon reception, the decoder is expected to utilize the nominal quantization center $\Theta_{\varsigma(l\tau)}(s_1,\ldots,s_n)$ corresponding to the received indices. However, under the FDI attack, the decoder receives a manipulated codeword as

$$\breve{g}(l\tau)=(s_1,s_2,\ldots,s_n),$$

which corresponds to a falsified quantization center reconstructed as:

$$\breve{\Theta}_{\varsigma(l\tau)}(s_1,\ldots,s_n)=\Theta_{\varsigma(l\tau)}(s_1,\ldots,s_n)+\varepsilon(l\tau)\,a_f(l\tau), \tag{2.8}$$

where $\varepsilon(l\tau)\in\{0,1\}$ is a Bernoulli random variable indicating whether an attack occurs at the l-th coding instant [56]. The probability distribution governing the attack occurrence is given by:

$$\mathbb{P}(\varepsilon(l\tau)=1)=p,\quad \mathbb{P}(\varepsilon(l\tau)=0)=1-p,\quad 0\le p\le 1. \tag{2.9}$$

Here, $\varepsilon(l\tau)=1$ corresponds to an active attack, and the injected forged signal takes the form $a_f(l\tau)=\sigma(\tilde{\rho}(l\tau)-\hat{\rho}(l\tau))$, where $\sigma\in(0,1)$ denotes the injection intensity coefficient. Accordingly, the decoder updates its estimate using the rule:

$$\breve{\rho}(k)=\begin{cases}0, & k=0,\\ \tilde{\rho}(k)+\breve{\Theta}_{\varsigma(l\tau)}(s_1,\ldots,s_n), & k=l\tau,\\ A\tilde{\rho}(k-1)+f(\tilde{\rho}(k-1))+\tilde{u}(k-1), & \text{otherwise.}\end{cases} \tag{2.10}$$

2.4. Problem description

Define

$$\begin{aligned} e(\cdot) &= \rho(\cdot) - \hat{\rho}(\cdot), \\ z(\cdot) &= \rho(\cdot) - \check{\rho}(\cdot), \\ f(e(\cdot)) &= f(\rho(\cdot)) - f(\hat{\rho}(\cdot)). \end{aligned}$$

Then, based on Eqs (2.1) and (2.3), we have

$$\eta(k+1) = A_2\eta(k) + F(\eta(k)) + \check{E}\eta(k)w(k) + \check{B}Z(k), \tag{2.11}$$

where

$$\begin{aligned} &\eta(k) = \begin{bmatrix} \rho(k) \\ e(k) \end{bmatrix}, \quad F(\eta(k)) = \begin{bmatrix} f(\rho(k)) \\ f(e(k)) \end{bmatrix}, \quad \check{E} = \begin{bmatrix} E & 0 \\ E & 0 \end{bmatrix}, \\ &A_2 = \begin{bmatrix} A+BK & 0 \\ 0 & A-LC \end{bmatrix}, \quad \check{B} = \begin{bmatrix} BK & 0 \\ 0 & 0 \end{bmatrix}, \quad Z(k) = \begin{bmatrix} z(k) \\ 0 \end{bmatrix}. \end{aligned}$$

Next, we introduce two definitions.

Definition 1. *[57] We define the SNS described in* (2.1) *as detectable through a digital communication channel if, in the absence of control input* (*i.e.*, $u(k) = 0$)*, there exists a set of encoding and decoding functions ensuring that*

$$\lim_{k\to+\infty} \mathbb{E}\{\|\rho(k) - \check{\rho}(k)\|\} = 0. \tag{2.12}$$

Definition 2. *[58] We say that the closed-loop SNS in* (2.11) *exhibits ISS if there exist class $\mathcal{KL}$ and $\mathcal{K}$ functions, denoted by $\beta(\cdot,\cdot)$ and $\gamma(\cdot)$, respectively, such that for every initial state $\eta(0) \in \mathbb{R}^n$ and any bounded input sequence $\{Z(k)\}$, the following condition is satisfied:*

$$\mathbb{E}\{\|\eta(k)\|\} \le \beta\mathbb{E}\{(\|\eta(0)\|, k)\} + \gamma\left(\sup_{0\le t\le k} \|Z(t)\|\right), \quad \forall k \ge 0. \tag{2.13}$$

Remark 1. *In the context of this paper, the input signal $Z(k)$ represents the decoding error resulting from the quantization and limited communication in the encoder–decoder scheme. As such, it is treated as an external bounded input in the ISS analysis.*

This study focuses on the observer-based control of SNSs under FDI attacks and bandwidth constraints. The aim is to design appropriate gains of the observer-based controller (2.3) for a detectable SNS modeled by (2.1), ensuring the ISS of the closed-loop SNS (2.11) under the proposed FDI attack-resilient periodic encoding–decoding scheme.

3. Main results

We first establish a detectability criterion for the SNS (2.1) under the proposed FDI attack-resilient periodic encoding–decoding scheme. Then, we derive a condition to further guarantee the ISS of the closed-loop SNS (2.11).

3.1. Detectability analysis

This part focuses on the detectability of the SNS (2.1), which concerns the ability to asymptotically reconstruct the true system state from quantized codewords generated via the encoding–decoding process, despite limited communication bandwidth. To lay the foundation for the subsequent theoretical analysis, we first introduce several supporting lemmas.

Lemma 1. *Assume that $\delta_0 > 0$ is a given scalar. If there exists a matrix $R_1 > 0$ and a constant $\mu_1 > 0$ such that the LMI*

$$\Pi_1 = \begin{bmatrix} \check{E}^\top R_1 \check{E} - (1+\delta_0)R_1 - \mu_1 \check{U} & -\mu_1 \widetilde{U}^\top & \check{A}^\top R_1 \\ * & -2\mu_1 I & R_1 \\ * & * & -R_1 \end{bmatrix} < 0 \tag{3.1}$$

holds, then

$$\mathbb{E}\left[\|\rho(k+1) - \tilde{\rho}(k+1)\|_2\right] \le c_0 \mathbb{E}\left[\|\rho(k) - \tilde{\rho}(k)\|_2\right], \tag{3.2}$$

where the constants and matrices are given as

$$\check{A} = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}, \quad \check{E} = \begin{bmatrix} E & 0 \\ E & 0 \end{bmatrix}, \quad c_0 = \sqrt{\frac{(1+\delta_0)\lambda_{\max}(R_1)}{\lambda_{\min}(R_1)}},$$
$$\check{U} = \begin{bmatrix} U_l^\top U_r + U_r^\top U_l & 0 \\ 0 & U_l^\top U_r + U_r^\top U_l \end{bmatrix}, \quad \widetilde{U} = \begin{bmatrix} -(U_l + U_r) & 0 \\ 0 & -(U_l + U_r) \end{bmatrix},$$

and where $\rho(k)$ satisfies the original system dynamics, while $\tilde{\rho}(k)$ evolves as $\tilde{\rho}(k+1) = A\tilde{\rho}(k) + f(\tilde{\rho}(k)) + B\check{u}(k)$ for any instant k within the non-coding interval.

Proof. For any instant k within the non-coding interval, define

$$d(\cdot) = \rho(\cdot) - \tilde{\rho}(\cdot), \quad f(d(\cdot)) = f(\rho(\cdot)) - f(\tilde{\rho}(\cdot)).$$

In the absence of control input, we obtain from (2.1) that

$$d(k+1) = Ad(k) + f(d(k)) + E\rho(k)\omega(k). \tag{3.3}$$

To facilitate unified analysis, define the extended state vector

$$\vartheta(\cdot) = \begin{bmatrix} \rho(\cdot)^\top & d(\cdot)^\top \end{bmatrix}^\top.$$

Then, the associated system dynamics take the form:

$$\vartheta(k+1) = \check{A}\vartheta(k) + F(\vartheta(k)) + \check{E}\vartheta(k)\omega(k),$$

where $F(\vartheta(k)) = \begin{bmatrix} f(\rho(k)) \\ f(d(k)) \end{bmatrix}$.

Consider the Lyapunov function (LF):

$$V_1(\cdot) = \vartheta(\cdot)^\top R_1 \vartheta(\cdot).$$

Then,

$$\mathbb{E}\left\{\Delta V_1(k) - \delta_0 V_1(k)\right\} = \mathbb{E}\left\{V_1(k+1) - V_1(k)\right\} - \mathbb{E}\left\{\delta_0 V_1(k)\right\}$$

$$
\begin{aligned}
=&\vartheta(k)^\top(\check{A}^\top R_1\check{A}+\check{E}^\top R_1\check{E})\vartheta(k)+F(\vartheta(k))^\top R_1F(\vartheta(k))\\
&+2\vartheta(k)^\top\check{A}^\top R_1F(\vartheta(k))-(1+\delta_0)\vartheta(k)^\top R_1\vartheta(k).
\end{aligned}\tag{3.4}
$$

From (2.2), we have

$$
\begin{bmatrix}\vartheta(\cdot)\\ F(\vartheta(\cdot))\end{bmatrix}^\top\begin{bmatrix}\check{U} & \widetilde{U}^\top\\ * & 2I\end{bmatrix}\begin{bmatrix}\vartheta(\cdot)\\ F(\vartheta(\cdot))\end{bmatrix}\le 0.\tag{3.5}
$$

Combining (3.4) and (3.5) gives

$$
\begin{aligned}
\mathbb{E}\left\{\Delta V_1(k)-\delta_0V_1(k)\right\}\le&\vartheta(k)^\top(\check{A}^\top R_1\check{A}+\check{E}^\top R_1\check{E})\vartheta(k)+F(\vartheta(k))^\top R_1F(\vartheta(k))\\
&+2\vartheta(k)^\top\check{A}^\top R_1F(\vartheta(k))-(1+\delta_0)\vartheta(k)^\top R_1\vartheta(k)\\
&-\mu_1\begin{bmatrix}\vartheta(k)\\ F(\vartheta(k))\end{bmatrix}^\top\begin{bmatrix}\check{U} & \widetilde{U}^\top\\ * & 2I\end{bmatrix}\begin{bmatrix}\vartheta(k)\\ F(\vartheta(k))\end{bmatrix}\\
=&\widetilde{\vartheta}(k)^\top\check{\Pi}_1\widetilde{\vartheta}(k),
\end{aligned}\tag{3.6}
$$

where

$$
\widetilde{\vartheta}(k)=\begin{bmatrix}\vartheta(k)\\ F(\vartheta(k))\end{bmatrix},\quad \check{\Pi}_1=\begin{bmatrix}\check{A}^\top R_1\check{A}+\check{E}^\top R_1\check{E}-(1+\delta_0)R_1-\mu_1\check{U} & \check{A}^\top R_1-\mu_1\widetilde{U}^\top\\ * & R_1-2\mu_1I\end{bmatrix}.
$$

With the utilization of Schur's complement presented by S. Boyd [59], one can derive from (3.1) that $\Pi_1<0$ holds. From this and (3.6), we derive

$$
\mathbb{E}\left\{V_1(k+1)\right\}\le(1+\delta_0)\mathbb{E}\left\{V_1(k)\right\}.
$$

It can be inferred from how $V_1(k)$ is defined that

$$
\lambda_{\min}(R_1)\mathbb{E}\left\{\|\vartheta(k+1)\|_2^2\right\}\le\mathbb{E}\left\{V_1(k+1)\right\}\le(1+\delta_0)\lambda_{\max}(R_1)\mathbb{E}\left\{\|\vartheta(k)\|_2^2\right\},
$$

which implies

$$
\mathbb{E}\left\{\|\vartheta(k+1)\|_2\right\}\le\sqrt{\frac{(1+\delta_0)\lambda_{\max}(R_1)}{\lambda_{\min}(R_1)}}\mathbb{E}\left\{\|\vartheta(k)\|_2\right\}.\tag{3.7}
$$

Then

$$
\mathbb{E}\{\|\vartheta(k+1)\|_2\}\le c_0\mathbb{E}\{\|\vartheta(k)\|_2\},
$$

which directly implies (3.2). This concludes the proof. □

Lemma 2. *Let the scalar $\delta_1\in(0,1)$. If there exist matrices $R_2=diag\{R_0,R_0\}>0$ and Y, scalars $\mu_1>0$ and $c_1\in(0,1)$, and an integer $\tau\in\mathbb{Z}_{>0}$ such that the LMI*

$$
\Pi_2=\begin{bmatrix}\check{E}^\top R_2\check{E}-(1-\delta_1)R_2-\mu_2\check{U} & -\mu_2\widetilde{U}^\top & \check{A}_1^\top R_2-W\\ * & -2\mu_2I & R_2\\ * & * & -R_2\end{bmatrix}<0\tag{3.8}
$$

holds, then the following inequality is satisfied:

$$
\mathbb{E}\left[\|\rho(k+\tau)-\hat{\rho}(k+\tau)\|_2\right]\le c_1\mathbb{E}\left[\|\rho(k)-\hat{\rho}(k)\|_2\right],\tag{3.9}
$$

where

$$\check{A} = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}, \quad \check{E} = \begin{bmatrix} E & 0 \\ E & 0 \end{bmatrix}, \quad W = \begin{bmatrix} 0 & 0 \\ 0 & C^\top Y \end{bmatrix},$$

$$\check{U} = \begin{bmatrix} U_l^\top U_r + U_r^\top U_l & 0 \\ 0 & U_l^\top U_r + U_r^\top U_l \end{bmatrix}, \quad \widetilde{U} = \begin{bmatrix} -(U_l + U_r) & 0 \\ 0 & -(U_l + U_r) \end{bmatrix}.$$

Additionally, the observer–gain matrix can be selected as

$$L = R_0^{-1} Y^T. \tag{3.10}$$

Proof. In the absence of control input, the augmented dynamics described in (2.11) can be expressed as

$$\tilde{\eta}(k+1) = \begin{bmatrix} \rho(k+1)^\top & e(k+1)^\top \end{bmatrix}^\top = \check{A}_1 \tilde{\eta}(k) + F(\tilde{\eta}(k)) + \check{E}\tilde{\eta}(k)\omega(k),$$

where

$$\check{A}_1 = \begin{bmatrix} A & 0 \\ 0 & A - LC \end{bmatrix}, \quad \check{E} = \begin{bmatrix} E & 0 \\ E & 0 \end{bmatrix}, \quad F(\tilde{\eta}(k)) = \begin{bmatrix} f(\rho(k)) \\ f(e(k)) \end{bmatrix}.$$

Choose a LF:

$$V_2(\cdot) = \tilde{\eta}(\cdot)^\top R_2 \tilde{\eta}(\cdot).$$

We can write

$$\begin{aligned} \mathbb{E}\{\Delta V_2(k) + \delta_1 V_2(k)\} =& \mathbb{E}\{V_2(k+1) - V_2(k)\} + \mathbb{E}\{\delta_1 V_2(k)\} \\ =& \tilde{\eta}(k)^\top \check{A}_1^\top R_2 \check{A}_1 \tilde{\eta}(k) + \tilde{\eta}(k)^\top \check{E}^\top R_2 \check{E}\tilde{\eta}(k) + F(\tilde{\eta}(k))^\top R_2 F(\tilde{\eta}(k)) \\ &+ 2\tilde{\eta}(k)^\top \check{A}_1^\top R_2 F(\tilde{\eta}(k)) - (1-\delta_1)\tilde{\eta}(k)^\top R_2 \tilde{\eta}(k). \end{aligned} \tag{3.11}$$

It follows from (2.2) that

$$\begin{bmatrix} \tilde{\eta}(\cdot) \\ F(\tilde{\eta}(\cdot)) \end{bmatrix}^\top \begin{bmatrix} \check{U} & \widetilde{U}^\top \\ * & 2I \end{bmatrix} \begin{bmatrix} \tilde{\eta}(\cdot) \\ F(\tilde{\eta}(\cdot)) \end{bmatrix} \leq 0. \tag{3.12}$$

Then, by (3.11) and (3.12), we have

$$\begin{aligned} \mathbb{E}\{\Delta V_2(k) + \delta_1 V_2(k)\} \leq& \tilde{\eta}(k)^\top \check{A}_1^\top R_2 \check{A}_1 \tilde{\eta}(k) + \tilde{\eta}(k)^\top \check{E}^\top R_2 \check{E}\tilde{\eta}(k) + F(\tilde{\eta}(k))^\top R_2 F(\tilde{\eta}(k)) \\ &+ 2\tilde{\eta}(k)^\top \check{A}_1^\top R_2 F(\tilde{\eta}(k)) - (1-\delta_1)\tilde{\eta}(k)^\top R_2 \tilde{\eta}(k) \\ &- \mu_2 \begin{bmatrix} \tilde{\eta}(k) \\ F(\tilde{\eta}(k)) \end{bmatrix}^\top \begin{bmatrix} \check{U} & \widetilde{U}^\top \\ * & 2I \end{bmatrix} \begin{bmatrix} \tilde{\eta}(k) \\ F(\tilde{\eta}(k)) \end{bmatrix} \\ =& \check{\eta}(k)^\top \check{\Pi}_2 \check{\eta}(k), \end{aligned} \tag{3.13}$$

where

$$\check{\eta}(k) = \begin{bmatrix} \tilde{\eta}(k) \\ F(\tilde{\eta}(k)) \end{bmatrix}, \quad \check{\Pi}_2 = \begin{bmatrix} \check{A}_1^\top R_2 \check{A}_1 + \check{E}^\top R_2 \check{E} - (1-\delta_1)R_2 - \mu_2 \check{U} & \check{A}_1^\top R_2 - \mu_2 \widetilde{U}^\top \\ * & R_2 - 2\mu_2 I \end{bmatrix}.$$

We can derive from (3.10) that $\check{\Pi}_2 < 0$ holds. From this and (3.13), we derive

$$\mathbb{E}\{\Delta V_2(k) + \delta_1 V_2(k)\} \leq 0.$$

Observing the structure of $V_2(k)$, we get that

$$\mathbb{E}\{V_2(k+\tau)\} \leq (1-\delta_1)^{\tau}\mathbb{E}\{V_2(k)\}.$$

Therefore, we derive that

$$\lambda_{\min}\{R_2\}\mathbb{E}\{\|e(k+\tau)\|_2^2\} \leq (1-\delta_1)^{\tau}\mathbb{E}\{V_2(k)\} \leq (1-\delta_1)^{\tau}\lambda_{\max}\{R_2\}\mathbb{E}\{\|e(k)\|_2^2\}. \tag{3.14}$$

It follows from (3.14) that the estimation error satisfies

$$\mathbb{E}\{\|\rho(k+\tau)-\hat{\rho}(k+\tau)\|_2\} < c_1\mathbb{E}\{\|\rho(k)-\hat{\rho}(k)\|_2\}$$

with $c_1 = \sqrt{(1-\delta_1)^{\tau}\lambda_{\max}\{R_2\}/\lambda_{\min}\{R_2\}}$. Note that an appropriate integer $\tau \in \mathbb{Z}^+$ can always be chosen such that $0 < c_1 < 1$. This completes the proof. □

To proceed with the forthcoming analysis, several definitions are presented below:

$$\begin{aligned}
&\check{\varphi}_0 = \mathbb{E}\{\|\varphi_0\|_2\}, \quad \tilde{\varphi}_0 = \mathbb{E}\{\|\hat{\varphi}_0-\varphi_0\|_2\},\\
&\mathbb{E}\{\varsigma(\tau)\} = c_1\tilde{\varphi}_0 + c_0^{\tau}\check{\varphi}_0,\\
&\mathbb{E}\{\varsigma((l+1)\tau)\} = c_1^{j}(c_1 + \frac{c_0^{\tau}}{1-\sigma p} + \sigma p\cdot\frac{c_0^{\tau}}{1-\sigma p})\tilde{\varphi}_0 + \frac{c_0^{\tau}}{1-\sigma p}\cdot\frac{\sqrt{n}\varsigma(j\tau)}{q}.
\end{aligned} \tag{3.15}$$

Lemma 3. *If Lemmas 1 and 2 hold, then for the designed FDI attack-resilient periodic encoding–decoding scheme, the following inequality holds:*

$$\mathbb{E}\{\|\hat{\rho}(l\tau)-\tilde{\rho}(l\tau)\|_2\} \leq \mathbb{E}\{\varsigma(l\tau)\}, \quad l = 1,2,\ldots, \tag{3.16}$$

where $\hat{\rho}(l\tau)$ and $\tilde{\rho}(l\tau)$ denote the estimated and auxiliary states at coding instants, respectively.

Proof. We prove this result by mathematical induction. First, for $l = 1$, with Lemmas 1 and 2 we have

$$\begin{aligned}
\mathbb{E}\{\|\hat{\rho}(\tau)-\tilde{\rho}(\tau)\|_2\} &\leq \mathbb{E}\{\|\hat{\rho}(\tau)-\rho(\tau)\|_2\} + \mathbb{E}\{\|\rho(\tau)-\tilde{\rho}(\tau)\|_2\}\\
&\leq c_1\tilde{\varphi}_0 + c_0\mathbb{E}\{\|\rho(\tau-1)-\check{\rho}(\tau-1)\|_2\}\\
&\leq c_1\tilde{\varphi}_0 + c_0^{\tau}\mathbb{E}\{\|\rho(0)\|_2\}\\
&\leq c_1\tilde{\varphi}_0 + c_0^{\tau}\check{\varphi}_0\\
&= \mathbb{E}\{\varsigma(\tau)\},
\end{aligned}$$

which implies

$$\mathbb{E}\{\|\hat{\rho}(l\tau)-\tilde{\rho}(l\tau)\|_2\} \leq \mathbb{E}\{\varsigma(l\tau)\}.$$

Next, assuming that $\mathbb{E}\{\|\hat{\rho}(l\tau)-\tilde{\rho}(l\tau)\|_2\} \leq \mathbb{E}\{\varsigma(l\tau)\}$ for $l = 2,\ldots,j$, from (2.10), we can deduce

$$\begin{aligned}
\mathbb{E}\{\|\rho(j\tau)-\check{\rho}(j\tau)\|_2\} &\leq \mathbb{E}\{\|\rho(j\tau)-\hat{\rho}(j\tau)\|_2\} + \mathbb{E}\{\|\hat{\rho}(j\tau)-\check{\rho}(j\tau)\|_2\}\\
&\leq c_1^{j}\tilde{\varphi}_0 + \mathbb{E}\left\{\left\|\hat{\rho}(j\tau)-\tilde{\rho}(j\tau)-\check{\Theta}_{\varsigma(j\tau)}(s_1,\ldots,s_n)\right\|_2\right\}.
\end{aligned} \tag{3.17}$$

Under the designed encoding–decoding mechanism, we have

$$\mathbb{E}\left\{\left\|\hat{\rho}(j\tau)-\tilde{\rho}(j\tau)-\check{\Theta}_{\varsigma(j\tau)}(s_1,\ldots,s_n)\right\|_2\right\}$$

$$
\begin{aligned}
&\leq \mathbb{E}\left\{\left\|\hat{\rho}(j\tau)-\tilde{\rho}(j\tau)-\Theta_{\varsigma(j\tau)}(s_1,\ldots,s_n)-\sigma\varepsilon(j\tau)\cdot(\hat{\rho}(j\tau)-\tilde{\rho}(j\tau))\right\|_2\right\}\\
&\leq \mathbb{E}\left\{\left\|\hat{\rho}(j\tau)-\tilde{\rho}(j\tau)-\Theta_{\varsigma(j\tau)}(s_1,\ldots,s_n)\right\|_2\right\}+\mathbb{E}\left\{\|\sigma\varepsilon(j\tau)\cdot(\hat{\rho}(j\tau)-\tilde{\rho}(j\tau))\|_2\right\}\\
&\leq \frac{\sqrt{n}\varsigma(j\tau)}{q}+\sigma p\cdot\mathbb{E}\left\{\|\hat{\rho}(j\tau)-\rho(j\tau)\|_2\right\}+\sigma p\cdot\mathbb{E}\left\{\|\rho(j\tau)-\check{\rho}(j\tau)\|_2\right\}\\
&\leq \frac{\sqrt{n}\varsigma(j\tau)}{q}+\sigma p\cdot c_1^j\tilde{\varphi}_0++\sigma p\cdot\mathbb{E}\left\{\|\rho(j\tau)-\check{\rho}(j\tau)\|_2\right\},
\end{aligned}
\tag{3.18}
$$

where the first inequality follows from (2.8), the second uses the norm inequality $\|\epsilon_1+\epsilon_2\|^2 \leq \|\epsilon_1\|^2+\|\epsilon_2\|^2$, the third follows from (2.7) and (2.9), and the final inequality is derived from (3.9). When $l = j+1$, it can be inferred from (3.17) and (3.18) that

$$
\begin{aligned}
\mathbb{E}\left\{\|\hat{\rho}((j+1)\tau)-\tilde{\rho}((j+1)\tau)\|_2\right\} &\leq \mathbb{E}\left\{\|\hat{\rho}((j+1)\tau)-\rho((j+1)\tau)\|_2\right\}+\mathbb{E}\left\{\|\rho((j+1)\tau)-\tilde{\rho}((j+1)\tau)\|_2\right\}\\
&\leq c_1^{j+1}\tilde{\varphi}_0+c_0\mathbb{E}\left\{\|\rho(j\tau+\tau-1)-\check{\rho}(j\tau+\tau-1)\|_2\right\}\\
&\leq c_1^{j+1}\tilde{\varphi}_0+c_0^{\tau}\mathbb{E}\left\{\|\rho(j\tau)-\check{\rho}(j\tau)\|_2\right\}\\
&\leq c_1^{j+1}\tilde{\varphi}_0+\frac{c_0^{\tau}}{1-\sigma p}\left(c_1^j\tilde{\varphi}_0+\frac{\sqrt{n}\varsigma(j\tau)}{q}+\sigma p\cdot c_1^j\tilde{\varphi}_0\right)\\
&\leq c_1^j(c_1+\frac{c_0^{\tau}}{1-\sigma p}+\sigma p\cdot\frac{c_0^{\tau}}{1-\sigma p})\tilde{\varphi}_0+\frac{c_0^{\tau}}{1-\sigma p}\cdot\frac{\sqrt{n}\varsigma(j\tau)}{q}\\
&= \mathbb{E}\left\{\varsigma((j+1)\tau)\right\}.
\end{aligned}
$$

Therefore, (3.16) holds true. This completes the proof. □

Theorem 1. *Given positive integers q and τ, and scalars $\delta_0 > 0$, $\delta_1 \in (0,1)$, $\sigma \in (0,1)$ and $p \in [0,1]$, suppose that there exist matrices $R_1 > 0$, $R_2 > 0$, and Y, and scalars $\mu_1 > 0$, $\mu_2 > 0$ such that the LMIs* (3.1) *and* (3.8) *are satisfied. Then, the SNS in* (2.1) *is guaranteed to be detectable under FDI attacks if*

$$
\frac{c_0^{\tau}\sqrt{n}}{q(1-\sigma p)} < 1 \tag{3.19}
$$

holds, where $c_0 = \sqrt{(1+\delta_0)\lambda_{\max}(R_1)/\lambda_{\min}(R_1)}$.

Proof. From the definition of $\varsigma(l\tau)$ in (3.15) and (3.19) and noting that $0 < c_1 < 1$, it follows that

$$
\lim_{l\to+\infty}\mathbb{E}\left\{\varsigma(l\tau)\right\} = 0.
$$

Then, applying Lemma 3, we obtain

$$
\lim_{l\to+\infty}\mathbb{E}\left\{\|\hat{\rho}(l\tau)-\tilde{\rho}(l\tau)\|_2\right\} = 0.
$$

Combining (3.17) and (3.18), it further holds that

$$
\lim_{l\to+\infty}\mathbb{E}\left\{\|\rho(l\tau)-\check{\rho}(l\tau)\|_2\right\} = 0. \tag{3.20}
$$

For any instant k within the non-coding interval, Lemma 1, together with (2.4), yields

$$
\mathbb{E}\left\{\|\rho(k)-\check{\rho}(k)\|_2\right\} \leq c_0^{k-l\tau}\mathbb{E}\left\{\|\rho(l\tau)-\check{\rho}(l\tau)\|_2\right\}. \tag{3.21}
$$

By (3.20) and (3.21), we obtain

$$\lim_{k\to+\infty} \mathbb{E}\{\|\rho(k) - \check{\rho}(k)\|_2\} = 0. \tag{3.22}$$

According to Definition 1, the SNS exhibits detectability. This concludes the proof. □

Remark 2. *Based on the feasible solutions of* (3.1) *and* (3.8)*, an inequality involving the dimensionality of the system state, the quantization level q, the injection intensity σ, and the attack probability p is presented in* (3.19)*. When the inequality holds, the SNS in* (2.1) *is guaranteed to be detectable under FDI attacks; that is, the decoding results can be used to reconstruct the state of the SNS in* (2.1)*.*

3.2. ISS of the closed-loop SNS

Lemma 4. *The ISS of the closed-loop SNS in* (2.11) *is ensured if there exists an ISS-LF* $V : \mathbb{Z}_{\geq 0} \times \mathbb{R}^n \to \mathbb{R}_{\geq 0}$*, three class* $\mathcal{K}_\infty$ *functions* $\alpha_1(\cdot), \alpha_2(\cdot), \alpha_3(\cdot)$*, and a class* $\mathcal{K}$ *function* $\varpi(\cdot)$ *such that the following inequalities hold for all* $\eta(k) \in \mathbb{R}^n$*,* $Z(k) \in \mathbb{R}^p$*, and* $k \geq 0$*:*

$$\alpha_1(\mathbb{E}\{\|\eta(k)\|\}) \leq \mathbb{E}\{V(k, \eta(k))\} \leq \alpha_2(\mathbb{E}\{\|\eta(k)\|\}), \tag{3.23}$$

$$\mathbb{E}\{V(k+1, \eta(k+1))\} - \mathbb{E}\{V(k, \eta(k))\} \leq -\alpha_3(\mathbb{E}\{\|\eta(k)\|\}) + \varpi(\|Z(k)\|). \tag{3.24}$$

Proof. Applying inequality (3.24) recursively from $k = 0$ to $k = l$ yields

$$\mathbb{E}\{V(l+1, \rho(l+1))\} \leq \phi^{l+1}\mathbb{E}\{V(0, \eta(0))\} + \sum_{j=0}^{l} \phi^{l-j}\varpi(\|Z(j)\|).$$

Here, $\phi \in (0, 1)$ denotes a contraction rate associated with the decay of the LF $V(k, \eta(k))$ in inequality (3.24). This is ensured by the existence of a constant $c \in (0, 1)$ satisfying $\alpha_3(\mathbb{E}\{\|\eta(k)\|\}) \geq c\mathbb{E}\{V(k, \eta(k))\}$, from which ϕ is defined as $\phi = 1 - c$. Using (3.23), we have

$$\alpha_1(\mathbb{E}\{\|\eta(k)\|\}) \leq \mathbb{E}\{V(k, \eta(k))\} \leq \phi^k\alpha_2(\mathbb{E}\{\|\eta(0)\|\}) + \sum_{j=0}^{k-1} \phi^{k-1-j}\varpi(\|Z(j)\|),$$

which yields

$$\mathbb{E}\{\|\eta(k)\|\} \leq \alpha_1^{-1}\left(\phi^k\alpha_2(\mathbb{E}\{\|\eta(0)\|\}) + \sum_{j=0}^{k-1} \phi^{k-1-j}\varpi(\|Z(j)\|)\right).$$

Invoking the monotonicity and sub additivity properties of class $\mathcal{K}_\infty$ functions, we obtain

$$\mathbb{E}\{\|\eta(k)\|\} \leq \underbrace{\alpha_1^{-1}\left(\phi^k\alpha_2(\mathbb{E}\{\|\eta(0)\|\})\right)}_{\beta(\mathbb{E}\{\|\eta(0)\|\},k)} + \underbrace{\alpha_1^{-1}\left(\sum_{j=0}^{k-1} \phi^{k-1-j}\varpi(\|Z(j)\|)\right)}_{\gamma(\cdot)}.$$

To estimate the summation term, we first observe that

$$\varpi(\|Z(j)\|) \leq \sup_{0\leq i\leq k-1} \varpi(\|Z(i)\|), \quad \forall\, j \in [0, k-1],$$

so the entire sum can be upper bounded as

$$\sum_{j=0}^{k-1} \phi^{k-1-j} \varpi(\|Z(j)\|) \leq \left(\sum_{j=0}^{k-1} \phi^{k-1-j} \right) \cdot \sup_{0 \leq i \leq k-1} \varpi(\|Z(i)\|).$$

Notice that the inner sum is a geometric series as

$$\sum_{j=0}^{k-1} \phi^{k-1-j} = \sum_{m=0}^{k-1} \phi^m \leq \sum_{m=0}^{\infty} \phi^m = \frac{1}{1-\phi}, 0 < \phi < 1.$$

We obtain

$$\sum_{j=0}^{k-1} \phi^{k-1-j} \varpi(\|Z(j)\|) \leq \frac{1}{1-\phi} \sup_{0 \leq j \leq k-1} \varpi(\|Z(j)\|).$$

Then, invoking the monotonicity and sub additivity properties of class $\mathcal{K}_\infty$ functions, we obtain

$$\mathbb{E}\{\|\eta(k)\|\} \leq \beta(\mathbb{E}\{(\|\eta(0)\|, k)\} + \gamma\left(\sup_{0 \leq j \leq k-1} \|Z(j)\| \right),$$

where

$$\beta(r,k) = \alpha_1^{-1}(\phi^k \alpha_2(r)), \quad \gamma(s) = \alpha_1^{-1}\left(\alpha_2\left(\alpha_3^{-1}(\varpi(s))\right)\right)$$

for any $r, s \geq 0$ and some fixed constant $\phi \in (0,1)$, where $\alpha_1^{-1}(\cdot)$ and $\alpha_3^{-1}(\cdot)$ denote the inverse functions of the strictly increasing functions $\alpha_1(\cdot)$ and $\alpha_3(\cdot)$, respectively. This concludes the proof. □

Theorem 2. *Given positive integers q and τ, and scalars $\delta_0 > 0$, $\delta_1 \in (0,1)$, $\sigma \in (0,1)$ and $p \in [0,1]$, suppose that there exist matrices $R_1 > 0$, $R_2 > 0$, $P = \mathrm{diag}(P_1, P_2) > 0$, Y, X, and scalars $\mu_1 > 0$, $\mu_2 > 0$, $\mu_3 > 0$, such that the LMIs* (3.1), (3.8), *and*

$$\Omega = \begin{bmatrix} -P + \check{E}P\check{E} - \mu_3 \check{U} & -\mu_3 \widetilde{U}^\top & 0 & \check{A}^\top \\ * & -2\mu_3 I & 0 & P \\ * & * & -P & \check{B}_2^\top \\ * & * & * & -P \end{bmatrix} < 0 \tag{3.25}$$

are satisfied, where

$$\check{A}_2 = \begin{bmatrix} P_1 A + BX & 0 \\ 0 & A - LC \end{bmatrix}, \quad \check{E} = \begin{bmatrix} E & 0 \\ E & 0 \end{bmatrix}, \quad \check{B}_2 = \begin{bmatrix} BY & 0 \\ 0 & 0 \end{bmatrix}.$$

Then, if (3.19) *holds true, 1) the SNS in* (2.1) *is guaranteed to be detectable in the presence of FDI attacks, 2) the ISS of the closed-loop SNS in* (2.11) *is ensured. In this case, the observer–gain and controller–gain can be obtained, respectively by* (3.10) *and the following formula:*

$$K = P_1^{-1} X. \tag{3.26}$$

Proof. 1) Since (3.1), (3.8), and (3.19) hold true, it is inferred from Theorem 1 that the SNS (2.1) is guaranteed to be detectable in the presence of FDI attacks.

2) An ISS-LF is selected as:

$$V_3(\cdot) = \eta(\cdot)^\top P\eta(\cdot).$$

From (2.11),

$$\begin{aligned}\mathbb{E}\{\Delta V_3(k)\} &= \mathbb{E}\{V_3(k+1)\} - \mathbb{E}\{V_3(k)\}\\ &\le \mathbb{E}\{V_3(k+1)\} - \mathbb{E}\{V_3(k)\} - \mu_3 \begin{bmatrix}\eta(k)\\ F(\eta(k))\end{bmatrix}^\top \begin{bmatrix}\check{U} & \widetilde{U}^\top\\ * & 2I\end{bmatrix}\begin{bmatrix}\eta(k)\\ F(\eta(k))\end{bmatrix}\\ &= \Phi(k)^\top \check{\Omega}\Phi(k) + Z(k)^\top PZ(k),\end{aligned} \tag{3.27}$$

where

$$\Phi(k) = \begin{bmatrix}\eta(k)^\top & F(\eta(k))^\top & Z(k)^\top\end{bmatrix}^\top,$$

$$\check{\Omega} = \begin{bmatrix}A_2^\top PA_2 + \check{E}^\top P\check{E} - P - \mu_3\check{U} & A_2^\top P - \mu_3\widetilde{U}^\top & A_2^\top P\check{B}\\ * & P - 2\mu_3 I & \check{B}^\top P\\ * & * & \check{B}^\top P\check{B} - P\end{bmatrix}$$

with

$$A_2 = \begin{bmatrix}A + BK & 0\\ 0 & A - LC\end{bmatrix}, \quad \check{E} = \begin{bmatrix}E & 0\\ E & 0\end{bmatrix}, \quad \check{B} = \begin{bmatrix}BK & 0\\ 0 & 0\end{bmatrix}.$$

One can derive from (3.25) that $\check{\Omega} < 0$ holds. From this and (3.27), we obtain

$$\mathbb{E}\{V_3(k+1)\} - \mathbb{E}\{V_3(k)\} \le -\lambda_{\min}(-\check{\Omega})\|\eta(k)\|^2 + \lambda_{\max}(P)\|Z(k)\|^2.$$

Choosing

$$\begin{aligned}\alpha_1(\mathbb{E}\{\eta(\cdot)\}) &= \lambda_{\min}\{P\}\mathbb{E}\left\{\|\eta(\cdot)\|^2\right\},\\ \alpha_2(\mathbb{E}\{\eta(\cdot)\}) &= \lambda_{\max}\{P\}\mathbb{E}\left\{\|\eta(\cdot)\|^2\right\},\\ \alpha_3(\mathbb{E}\{\|\eta(\cdot)\|\}) &= \lambda_{\min}\{-\check{\Omega}\}\mathbb{E}\left\{\|\eta(\cdot)\|^2\right\},\\ \varpi(\|Z(\cdot)\|) &= \lambda_{\max}\{P\}\|Z(\cdot)\|^2,\end{aligned}$$

we can obtain (3.23) and (3.24). Based on Lemma 4, the ISS of the closed-loop SNS (2.11) is deduced. This concludes the proof. □

4. Numerical example

The effectiveness and robustness of the proposed method are verified in the present section. We consider the SNS (2.1) with the following parameter matrices and function:

$$A = \begin{bmatrix}0.79 & -0.13\\ 0.43 & -1.23\end{bmatrix}, \quad E = \begin{bmatrix}0.2 & 0.1\\ 0.25 & 0.1\end{bmatrix}, \quad B = \begin{bmatrix}2.2 & -0.8\\ 0 & 0.5\end{bmatrix}, \quad C = \begin{bmatrix}0.5 & 0.5\end{bmatrix},$$

$$f(\rho(k)) = \begin{bmatrix}-0.5\rho_1(k) + \tanh(0.65\rho_1(k)) - 0.15\rho_2(k)\\ 1.1\rho_2(k) - \tanh(0.95\rho_2(k))\end{bmatrix},$$

where $f(\cdot)$ meets (2.2) with the following matrices:

$$U_l = \begin{bmatrix} -0.5 & -0.15 \\ 0 & 1.1 \end{bmatrix}, \quad U_r = \begin{bmatrix} 0.15 & -0.15 \\ 0 & 0.25 \end{bmatrix}.$$

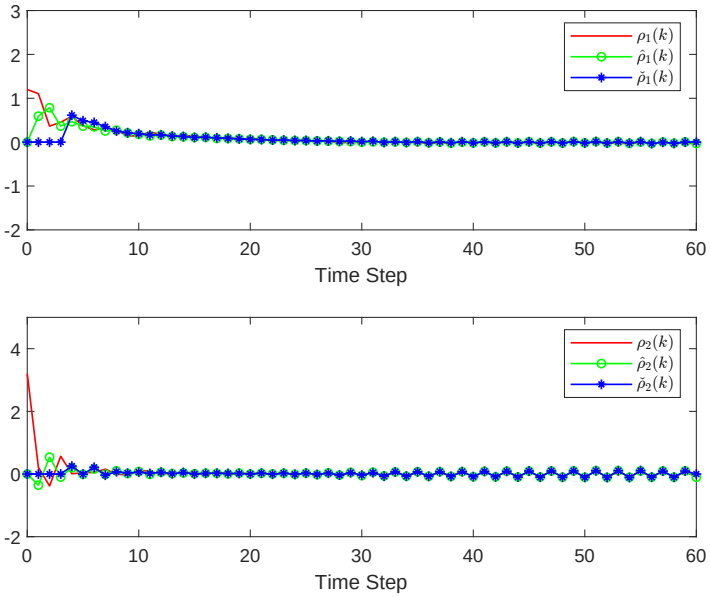

Figure 2. Time responses of the actual state $\rho_i(k)$, observer estimate $\hat{\rho}_i(k)$, and decoder output $\check{\rho}_i(k)$ for $i = 1, 2$ under FDI attacks.

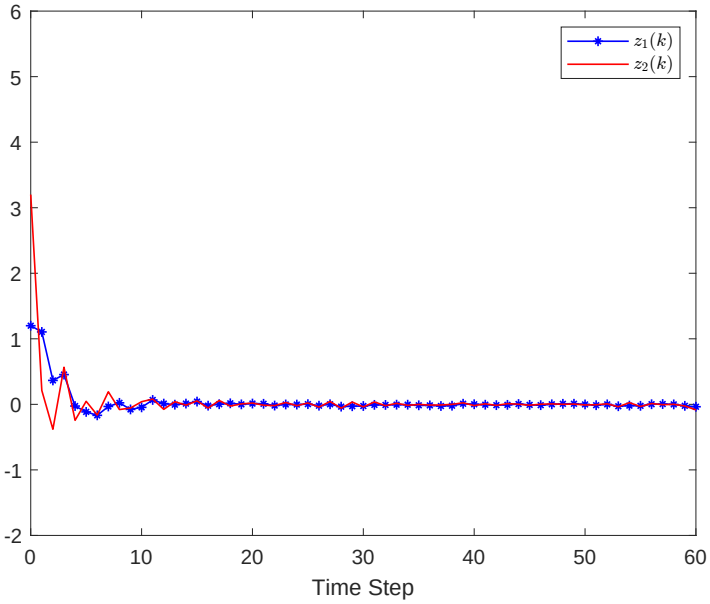

Figure 3. Time responses of decoding errors $z_i(k) = \rho_i(k) - \check{\rho}_i(k)$ for $i = 1, 2$ under FDI attacks.

In the encoding–decoding framework, the SNS (2.1) is subject to FDI attacks triggered by a Bernoulli stochastic process with a probability of $p = 0.75$ at each time step. The injection intensity is set to

Table 1. Comparison of encoding and decoding times of different methods.

Methods	Encoding and decoding times	Coding period
Encoding and decoding methods in [39–42]	60	$\tau = 1$
	30	$\tau = 2$
Encoding and decoding method in this paper	20	$\tau = 3$
	15	$\tau = 4$

$\sigma = 0.3$. To ensure detectability and stability under such attacks, the other design parameters are selected as follows: $\delta_0 = 0.9$, and the matrix inequality (3.1) is solved using the YALMIP toolbox in MATLAB R2023a, with MOSEK as the underlying solver, which results in $c_0 = 1.7577$. Then, $\delta_1 = 0.7$ and the coding period $\tau = 4$ are chosen. According to (3.8) and (3.9), the constant $c_1 = 0.1459$ is obtained. Finally, based on inequality (3.19) in Theorem 1, the quantization level is set to $q = 100$.

As a first step, we investigate the detectability property of the SNS (2.1). By solving the LMI condition (3.8), the resulting observer–gain is given by

$$L = R_0^{-1} Y^T = \begin{bmatrix} 0.2690 & -0.1620 \end{bmatrix}^T.$$

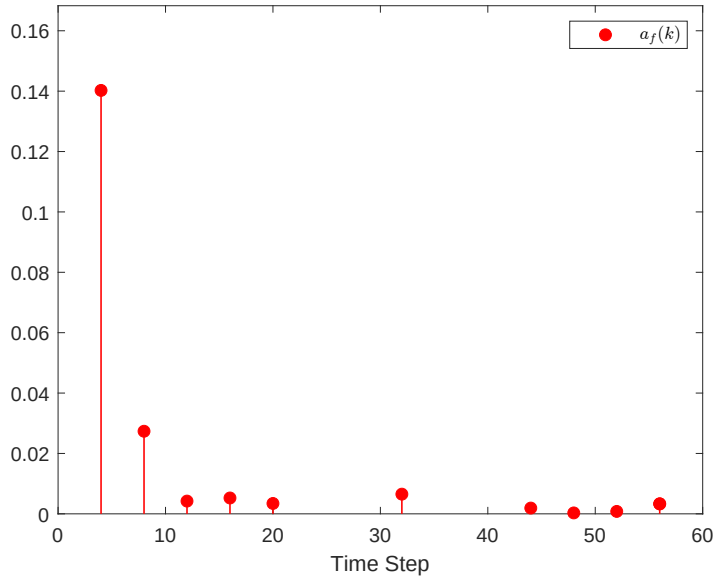

Figure 4. The occurrence time of the FDI attacks and the magnitude of the attack signal a_f.

The simulation outcomes are depicted in Figures 2–4. In particular, Figure 2 demonstrates the trajectories of the actual $\rho_i(k)$, the observer-based estimate $\hat{\rho}_i(k)$, and the decoded state $\check{\rho}_i(k)$ over time steps under FDI attacks. Figure 3 presents the decoding errors $z_1(k)$ and $z_2(k)$ are close to zero. This confirms that the decoder is capable of reconstructing the real system states. Figure 4 illustrates the occurrence time of the FDI attacks and the magnitude of the attack signal a_f.

To better illustrate the trade-off between encoding–decoding frequency and coding period, Table 1 compares the number of encoding and decoding operations required by existing methods [39–42] and the proposed scheme under a fixed time horizon of 60 steps. It can be observed that while traditional methods require one encoding–decoding operation per time step ($\tau = 1$), the proposed method supports longer

coding periods (e.g., $\tau = 3$ or $\tau = 4$), thereby reducing the number of encoding–decoding invocations. This reduction contributes to lowering the average data rate and alleviating the computational burden.

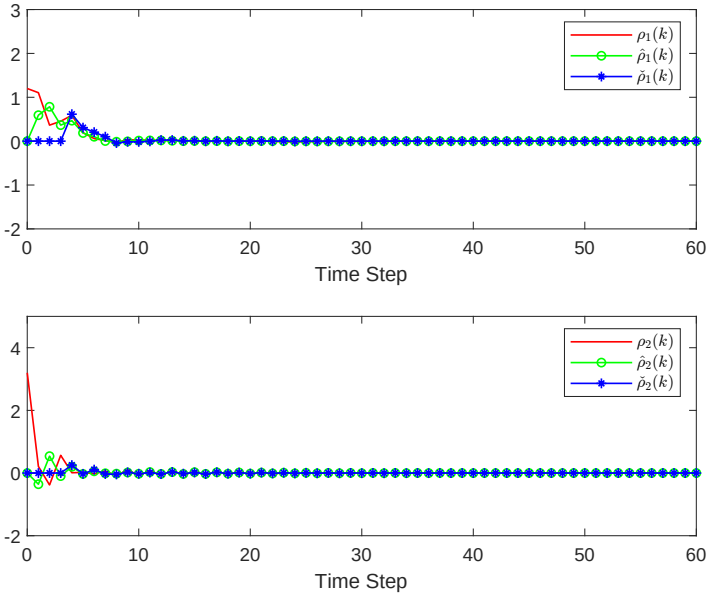

Figure 5. Time responses of the actual state $\rho_i(k)$, observer estimate $\hat{\rho}_i(k)$, and decoder output $\check{\rho}_i(k)$ for $i = 1, 2$ under FDI attacks with the controller–gain K applied.

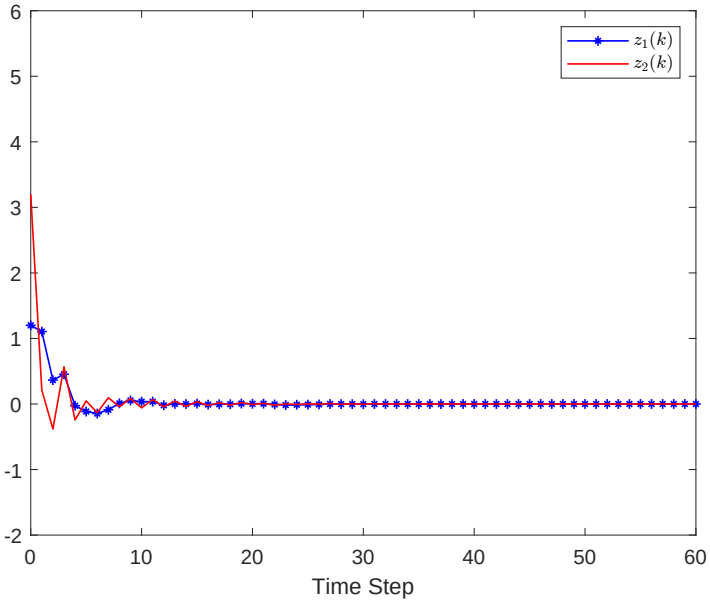

Figure 6. Time responses of decoding errors $z_i(k) = \rho_i(k) - \check{\rho}_i(k)$ for $i = 1, 2$ under FDI attacks with the designed controller–gain K.

In the following, we shall test the ISS of the closed-loop SNS (2.11). By solving the LMI condition (3.25), the gain matrix of the designed controller is provided as

$$K = P_1^{-1}X = \begin{bmatrix} -0.2354 & 0.1900 \\ -0.2859 & 0.5276 \end{bmatrix}.$$

Table 2. RMSE values for different combinations of p and σ.

$p\backslash\sigma$	0.1	0.3	0.5	0.7
0.2	0.083215	0.083402	0.083679	0.084120
0.4	0.083216	0.083389	0.083728	0.084274
0.6	0.083231	0.083358	0.083727	0.084208
0.8	0.083194	0.083384	0.083759	0.084226

As stated in Theorem 2, the given controller above ensures the ISS of the closed-loop SNS (2.11). Figures 5 and 6 present the simulation results. It can be observed from Figure 5 that the trajectories of the actual state $\rho_i(k)$, the observer-based estimate $\hat{\rho}_i(k)$, and the decoder reconstruction $\check{\rho}_i(k)$ (for $i = 1, 2$) all converge to a consistent trajectory under FDI attacks. Figure 6 shows the decoding errors $z_1(k)$ and $z_2(k)$. Therefore, the simulation examples confirm the ISS of the closed-loop SNS and validate the theoretical results established in Theorem 2.

To illustrate the impact of the FDI attack signal intensity σ and the probability p of FDI attacks on system performance, Table 2 summarizes the root mean square error (RMSE) values obtained from experiments with a sample size of 1000, where $p \in \{0.2, 0.4, 0.6, 0.8\}$ and $\sigma \in \{0.1, 0.3, 0.5, 0.7\}$. The results show that: 1) RMSE values lie in a range between 0.08 and 0.09, indicating that the proposed FDI attack-resilient periodic encoding–decoding scheme performs well; 2) when p is held constant, an increase in σ leads to a gradual rise in RMSE, reflecting the negative impact of increased attack signal intensity on control performance.

5. Conclusions

This study has investigated observer-based networked control for SNSs under FDI attacks and constrained communication bandwidth. To counter FDI attacks while reducing communication overhead, we have developed an FDI attack-resilient periodic encoding–decoding scheme utilizing uniform quantization. Under this scheme, we have established a detectability criterion, as presented in Theorem 1, for the considered SNS. Subsequently, we have derived a sufficient condition, given in Theorem 2, which further ensures the ISS of the closed-loop SNS. This condition enables the determination of desired observer and controller gains through LMIs (3.1), (3.8), and (3.25), which can be readily verified using available MATLAB tools, such as YALMIP, CVX, and SeDuMi. Finally, we have demonstrated the effectiveness and robustness of the proposed control design through a case study. Future work will explore more complex attack models and evaluate the proposed approach through practical application cases in networked control systems.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this paper.

Acknowledgments

This work was supported by the Undergraduate Innovation and Entrepreneurship Training Program of Anhui University of Technology.

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. X. Ge, F. Yang, Q. L. Han, Distributed networked control systems: A brief overview, *Inf. Sci.*, **380** (2017), 117–131. https://doi.org/10.1016/j.ins.2015.07.047
2. X. M. Zhang, Q. L. Han, X. Ge, D. Ding, L. Ding, D. Yue, et al., Networked control systems: A survey of trends and techniques, *IEEE/CAA J. Autom. Sin.*, **7** (2019), 1–17. https://doi.org/10.1109/JAS.2019.1911651
3. J. Zhang, B. Zhou, D. Yang, Y. Luo, G. Li, Distributed dynamic event-triggered consensus control of multiagent systems subject to external disturbances, *Inf. Sci.*, **709** (2025), 122072. https://doi.org/10.1016/j.ins.2025.122072
4. J. Zhao, B. Li, S. Wo, X. Han, Hidden Markov model-based finite-time H_∞ control for singular Markovian jump delay systems with input saturation, *Proc. Inst. Mech. Eng., Part I: J. Syst. Control Eng.*, **237** (2023), 1469–1479. https://doi.org/10.1177/09596518231153256
5. Y. Gong, Consensus control of multi-agent systems with delays, *Electron. Res. Arch.*, **32** (2024), 4887–4904. https://doi.org/10.3934/era.2024224
6. X. Yang, A. Li, Q. Zhu, Dynamic periodic event-triggered control of stochastic complex networks with time-varying delays, *Neural Networks*, **190** (2025), 107659. https://doi.org/10.1016/j.neunet.2025.107659
7. N. Gunasekaran, M. S. Ali, S. Arik, H. I. A. Ghaffar, A. A. Z. Diab, Finite-time and sampled-data synchronization of complex dynamical networks subject to average dwell-time switching signal, *Neural Networks*, **149** (2022), 137–145. https://doi.org/10.1016/j.neunet.2022.02.013
8. H. Wei, Q. Li, S. Zhu, D. Fan, Y. Zheng, Event-triggered resilient asynchronous estimation of stochastic Markovian jumping CVNs with missing measurements: A co-design control strategy, *Inf. Sci.*, **712** (2025), 122167. https://doi.org/10.1016/j.ins.2025.122167
9. Y. Zhao, H. Wu, Fixed/Prescribed stability criterions of stochastic system with time-delay, *AIMS Math.*, **9** (2024), 14425–14453. https://doi.org/ 10.3934/math.2024701
10. Q. Li, K. Zhang, H. Wei, F. Sun, J. Wang, Non-fragile asynchronous H∞ estimation for piecewise-homogeneous Markovian jumping neural networks with partly available transition rates: A dynamic event-triggered scheme, *Neurocomputing*, **640** (2025), 130292. https://doi.org/10.1016/j.neucom.2025.130292
11. Y. Yao, J. Tan, J. Wu, X. Zhang, A unified fuzzy control approach for stochastic high-order nonlinear systems with or without state constraints, *IEEE Trans. Fuzzy Syst.*, **30** (2022), 4530–4540. https://doi.org/10.1109/TFUZZ.2022.3155297
12. X. Hou, H. Wu, J. Cao, Practical finite-time synchronization for Lur'e systems with performance constraint and actuator faults: A memory-based quantized dynamic event-triggered control strategy, *Appl. Math. Comput.*, **487** (2025), 129108. https://doi.org/10.1016/j.amc.2024.129108

13. H. Wu, X. Zhao, L. Wang, J. Cao, Observer-based fixed-time topology identification and synchronization for complex networks via quantized pinning control strategy, *Appl. Math. Comput.*, **507** (2025), 129568. https://doi.org/10.1016/j.amc.2025.129568

14. H. Xu, Q. Zhu, W. X. Zheng, Exponential stability of stochastic nonlinear delay systems subject to multiple periodic impulses, *IEEE Trans. Autom. Control*, **69** (2024), 2621–2628. https://doi.org/10.1109/TAC.2023.3335005

15. X. Zhao, H. Wu, J. Cao, L. Wang, Prescribed-time synchronization for complex dynamic networks of piecewise smooth systems: A hybrid event-triggering control approach, *Qual. Theory Dyn. Syst.*, **24** (2025), 11. https://doi.org/10.1007/s12346-024-01166-x

16. Q. Zhu, Event-triggered sampling problem for exponential stability of stochastic nonlinear delay systems driven by Lévy processes, *IEEE Trans. Autom. Control*, **70** (2025), 1176–1183. https://doi.org/10.1109/TAC.2024.3448128

17. H. Sun, H. G. Han, J. F. Qiao, Observer-based control for networked Takagi-Sugeno fuzzy systems with stochastic packet losses, *Inf. Sci.*, **644** (2023), 119275. https://doi.org/10.1016/j.ins.2023.119275

18. X. Li, X. Qin, Z. Wan, W. Tai, Chaos synchronization of stochastic time-delay Lur'e systems: An asynchronous and adaptive event-triggered control approach, *Electron. Res. Arch.*, **31** (2023), 5589–5608. https://doi.org/10.3934/era.2023284

19. G. Zhang, Q. Zhu, Event-triggered optimized control for nonlinear delayed stochastic systems, *IEEE Trans. Circuits Syst. I: Regul. Pap.*, **68** (2021), 3808–3821. https://doi.org/10.1109/TCSI.2021.3095092

20. R. Vadivel, P. Hammachukiattikul, Q. Zhu, N. Gunasekaran, Event-triggered synchronization for stochastic delayed neural networks: Passivity and passification case, *Asian J. Control*, **25** (2023), 2681–2698. https://doi.org/10.1002/asjc.2965

21. F. Xu, X. Ruan, X. Pan, Event-triggered leader-following consensus control of multi-agent systems against DoS attacks, *Int. J. Control Autom. Syst.*, **22** (2024), 3424–3433. https://doi.org/10.1007/s12555-024-0327-0

22. Y. Ni, Z. Wang, Y. Fan, X. Huang, H. Shen, Resilient hybrid event-triggered control for secure synchronization of Lur'e systems against DoS attacks, *IEEE Trans. Network Sci. Eng.*, **12** (2025), 1053–1065. https://doi.org/10.1109/TNSE.2024.3522991

23. J. Zhou, D. Xu, W. Tai, C. K. Ahn, Switched event-triggered $\mathcal{H}_\infty$ security control for networked systems vulnerable to aperiodic DoS attacks, *IEEE Trans. Network Sci. Eng.*, **10** (2023), 2109–2123. https://doi.org/10.1109/TNSE.2023.3243095

24. X. Si, Z. Wang, X. Huang, Y. Fan, H. Shen, Resilient-sampling-based bipartite synchronization of cooperative-antagonistic neural networks with hybrid attacks: Designing interval-dependent functions, *IEEE Trans. Autom. Sci. Eng.*, **22** (2025), 2935–2945. https://doi.org/10.1109/TASE.2024.3386699

25. Y. Zhang, Z. Peng, G. Wen, J. Wang, T. Huang, Optimal stealthy linear man-in-the-middle attacks with resource constraints on remote state estimation, *IEEE Trans. Syst., Man, Cybern.: Syst.*, **54** (2023), 445–456. https://doi.org/10.1109/TSMC.2023.3311853

26. T. Chen, K. Shi, X. Cai, M. Zhu, D. Chen, S. Han, et al., UUB stability of Ncss under asynchronous packet loss and random UDP attacks: LMI method-based controller design technology, *Int. J. Robust Nonlinear Control*, (2025), in press. https://doi.org/10.1002/rnc.70117

27. X. Cai, Y. Sun, K. Shi, X. Xie, Y. C. Soh, C. Qiao, et al., Enhancing networked control system resilience to TCP/IP protocol DoS attacks: Performance analysis and intelligent controller design, *IEEE Trans. Autom. Sci. Eng.*, **22** (2025), 6608–6618. https://doi.org/10.1109/TASE.2024.3449882

28. Y. Yao, Y. Kang, Y. Zhao, P. Li, J. Tan, Prescribed-time output feedback control for cyber–physical systems under output constraints and malicious attacks, *IEEE Trans. Cybern.*, **54** (2024), 6518–6530. https://doi.org/10.1109/TCYB.2024.3418384

29. J. Zhou, J. Dong, S. Xu, C. K. Ahn, Input-to-state stabilization for Markov jump systems with dynamic quantization and multimode injection attacks, *IEEE Trans. Syst., Man, Cybern.: Syst.*, **54** (2024), 2517–2529. https://doi.org/10.1109/TSMC.2023.3344869

30. M. Ahmed, A. S. K. Pathan, False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure, *Complex Adapt. Syst. Model.*, **8** (2020), 1–14. https://doi.org/10.1186/s40294-020-00070-w

31. M. A. Husnoo, A. Anwar, N. Hosseinzadeh, S. N. Islam, A. N. Mahmood, R. Doss, False data injection threats in active distribution systems: A comprehensive survey, *Future Gener. Comput. Syst.*, **140** (2023), 344–364. https://doi.org/10.1016/j.future.2022.10.021

32. H. Guo, Z. Pang, J. Sun, J. Li, Detection of stealthy false data injection attacks against cyber-physical systems: A stochastic coding scheme, *J. Syst. Sci. Complexity*, **35** (2022), 1668–1684. https://doi.org/10.1007/s11424-022-1005-z

33. M. Irfan, A. Sadighian, A. Tanveer, S. J. Al-Naimi, G. Oligeri, A survey on detection and localisation of false data injection attacks in smart grids, *IET Cyber-Phys. Syst.: Theory Appl.*, **9** (2024), 313–333. https://doi.org/10.1049/cps2.12093

34. W. Xu, I. M. Jaimoukha, F. Teng, Robust moving target defence against false data injection attacks in power grids, *IEEE Trans. Inf. Forensics Secur.*, **18** (2023), 29–40. https://doi.org/10.1109/TIFS.2022.3210864

35. Y. Liu, Z. Fang, J. H. Park, F. Fang, Quantized event-triggered synchronization of discrete-time chaotic neural networks with stochastic deception attack, *IEEE Trans. Syst., Man, Cybern.: Syst.*, **53** (2023), 4511–4521. https://doi.org/10.1109/TSMC.2023.3251355

36. M. Joby, M. Sathishkumar, L. S. Ramya, S. Santra, Resilient control strategies for probabilistic nonlinear systems with time delays subject to scaling attacks, *Math. Methods Appl. Sci.*, **48** (2025), 12174–12185. https://doi.org/10.1002/mma.11020

37. P. Tabuada, Event-triggered real-time scheduling of stabilizing control tasks, *IEEE Trans. Autom. Control*, **52** (2007), 1680–1685. https://doi.org/10.1109/TAC.2007.904277

38. M. C. F. Donkers, W. P. M. H. Heemels, Output-based event-triggered control with guaranteed $\mathcal{L}_\infty$-gain and improved and decentralized event-triggering, *IEEE Trans. Autom. Control*, **57** (2012), 1362–1376. https://doi.org/10.1109/TAC.2011.2174696

39. J. Wang, Quantized feedback control of discrete-time MIMO linear systems with input and output quantization over finite data rate channels, *IEEE Trans. Autom. Control*, **68** (2022), 6277–6284. https://doi.org/10.1109/TAC.2022.3232991

40. Y. Liu, W. Yang, C. Y. Su, Y. Luo, X. Wang, Observer-based control of networked periodic piecewise systems with encoding–decoding mechanism, *IEEE Trans. Cybern.*, **55** (2025), 2754–2764. https://doi.org/10.1109/TCYB.2025.3543878

41. S. Singh, A. Sachan, J. K. Goyal, S. Purwar, X. Xiong, Encoder/decoder mismatch for input quantisation with discrete time $[\mathcal{K},\mathcal{KL}]$ sector, *Int. J. Syst. Sci.*, (2025), in press. https://doi.org/10.1080/00207721.2025.2467839

42. S. Zhou, J. Song, H. K. Lam, S. He, Z. Cao, Coding–decoding-based sliding mode control for Markovian jump systems under constrained bit bate: An adaptive quantizer approach, *IEEE Trans. Control Network Syst.*, **11** (2023), 257–270. https://doi.org/10.1109/TCNS.2023.3280458

43. Z. Zhang, X. Huang, Y. Chen, J. Zhou, Input-to-state learning of recurrent neural networks with delay and disturbance, *Int. J. Adapt. Control Signal Process.*, **35** (2021), 1438–1453. https://doi.org/10.1002/acs.3251

44. M. Sathishkumar, M. Joby, Y. K. Ma, S. M. Anthoni, S. Santra, Secure finite-time filtering for switched fuzzy systems with scaling attacks and stochastic sensor faults, *Nonlinear Dyn.*, **113** (2025), 13485–13506. https://doi.org/10.1007/s11071-025-11042-1

45. X. Liu, K. Shi, Y. Tang, L. Tang, Y. Wei, Y. Han, A novel adaptive event-triggered reliable H_∞ control approach for networked control systems with actuator faults, *Electron. Res. Arch.*, **31** (2023), 1840–1862. https://doi.org/10.3934/era.2023095

46. J. Wu, X. Zhang, F. Wang, Fuzzy adaptive output feedback control for a class of stochastic nonlinear systems under input/output quantization, *Nonlinear Dyn.*, **113** (2025), 8555–8570. https://doi.org/10.1007/s11071-024-10576-0

47. Y. X. Li, X. Y. Hu, C. K. Ahn, Z. S. Hou, H. H. Kang, Event-based adaptive neural asymptotic tracking control for networked nonlinear stochastic systems, *IEEE Trans. Network Sci. Eng.*, **9** (2022), 2290–2300. https://doi.org/10.1109/TNSE.2022.3161645

48. L. Fan, Q. Zhu, W. X. Zheng, Stability analysis of switched stochastic nonlinear systems with state-dependent delay, *IEEE Trans. Autom. Control*, **69** (2024), 2567–2574. https://doi.org/10.1109/TAC.2023.3315672

49. M. E. Hesari, A. A. Bagheri, M. Davoudi, N. Pariz, Observer-based controller design for class of nonlinear wireless stochastic networked systems with communication delays and denial of service jamming attacks: Comparison of observer position, *Int. J. Dyn. Control*, **13** (2025), 1–15. https://doi.org/10.1007/s40435-024-01505-5

50. Y. Yao, Y. Kang, Y. Zhao, P. Li, J. Tan, A novel prescribed-time control approach of state-constrained high-order nonlinear systems, *IEEE Trans. Syst., Man, Cybern.: Syst.*, **54** (2024), 2941–2951. https://doi.org/10.1109/TSMC.2024.3352905

51. S. Tong, L. Zhang, Y. Li, Observed-based adaptive fuzzy decentralized tracking control for switched uncertain nonlinear large-scale systems with dead zones, *IEEE Trans. Syst., Man, Cybern.: Syst.*, **46** (2016), 37–47. https://doi.org/10.1109/TSMC.2015.2426131

52. Y. Yao, X. Liang, Y. Kang, Y. Zhao, J. Tan, L. Gu, Dual flexible prescribed performance control of input saturated high-order nonlinear systems, *IEEE Trans. Cybern.*, **55** (2025), 1147–1158. https://doi.org/10.1109/TCYB.2024.3524242

53. H. Yuan, Q. Zhu, The well-posedness and stabilities of mean-field stochastic differential equations driven by G-Brownian motion, *SIAM J. Control Optim.*, **63** (2025), 596–624. https://doi.org/10.1137/23M1593681

54. Q. Li, H. Wei, D. Hua, J. Wang, J. Yang, Stabilization of semi-Markovian jumping uncertain complex-valued networks with time-varying delay: A sliding-mode control approach, *Neural Process. Lett.*, **56** (2024), 111. https://doi.org/10.1007/s11063-024-11585-1

55. J. Zhou, Y. Wang, X. Zheng, Z. Wang, H. Shen, Weighted $\mathcal{H}_\infty$ consensus design for stochastic multi-agent systems subject to external disturbances and ADT switching topologies, *Nonlinear Dyn.*, **96** (2019), 853–868. https://doi.org/10.1007/s11071-019-04826-9

56. D. Xu, X. Li, W. Tai, J. Zhou, Event-triggered stabilization for networked control systems under random occurring deception attacks, *Math. Biosci. Eng.*, **20** (2023), 859–878. https://doi.org/10.3934/mbe.2023039

57. S. Xu, J. Hu, D. Chen, Z. Wu, State estimation for uncertain discrete-time nonlinear systems via the coding-decoding scheme, in *2020 Chinese Control And Decision Conference (CCDC)*, IEEE, (2020), 862–867. https://doi.org/10.1109/CCDC49329.2020.9164587

58. L. Wang, Z. Wang, Q. L. Han, G. Wei, Synchronization control for a class of discrete-time dynamical networks with packet dropouts: A coding–decoding-based approach, *IEEE Trans. Cybern.*, **48** (2017), 2437–2448. https://doi.org/10.1109/TCYB.2017.2740309

59. S. Boyd, L. E. Ghaoui, E. Feron, V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*, SIAM, Philadelphia, 1994. https://doi.org/10.1137/1.9781611970777