Electronic Research Archive

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

ERA, 31(12): 7496–7510.
DOI: 10.3934/era.2023378
Received: 08 September 2023
Revised: 02 November 2023
Accepted: 16 November 2023
Published: 24 November 2023

Research article

Robust memory control design for semi-Markovian jump systems with cyber attacks

Ramalingam Sakthivel[1], Palanisamy Selvaraj[1], Oh-Min Kwon[1,*], Seong-Gon Choi[2,*] and Rathinasamy Sakthivel[3,4]

[1] School of Electrical Engineering, Chungbuk National University, Cheongju 28644, South Korea
[2] School of Information and Communication Engineering, Chungbuk National University, Cheongju 28644, South Korea
[3] Department of Applied Mathematics, Bharathiar University, Coimbatore 641046, India
[4] Department of Mathematics, Sungkyunkwan University, Suwon 440746, South Korea

* **Correspondence:** Email: madwind@chungbuk.ac.kr, sgchoi@cbnu.ac.kr; Tel: +82432612422; Fax: +82432632419.

Abstract: This paper addressed the problem of observer-based memory state feedback control design for semi-Markovian jump systems subject to input delays and external disturbances, where the measurement output was vulnerable to randomly occurring cyber attacks. To facilitate analysis, the cyber attacks were described by a nonlinear function that meets Lipschitz continuity and the possible attack scenarios were represented by a stochastic parameter that follows the Bernoulli distribution. Based on the information from the considered system and state observer, an augmented closed loop system was constructed. Then, by using the Lyapunov stability theory, an extended Wirtinger's integral inequality and stochastic analysis, the required stability criterion was proposed in the form of linear matrix inequalities. As a result, the control and observer gain matrices were efficiently derived, ensuring the stochastic stability of closed-loop systems with H_∞ performance, regardless of cyber attacks. To demonstrate the effectiveness and theoretical value of the proposed robust memory state feedback control design, simulation results were presented.

Keywords: memory control; semi-Markovian jump systems; input delays; cyber attacks

1. Introduction

Past few decades, Markovian jump systems (MJSs) have emerged as a powerful modeling tool for practical systems that undergo random changes due to component failures, repairs, sudden environmental disturbances, and alterations in subsystem interconnections [1–7]. Particularly, in [3], the dynamic-output-feedback control approach to uncertain singular systems has been designed for MJSs with time-varying delays. The delay-dependent stochastic stabilization of MJSs modeled by fractional Brownian motion via a quantized controller has been proposed in [4]. However, MJSs do have limitations in their application, particularly arising from the exponential distribution of jump times in Markov chains. This leads to constant transition rates and conservative results. To overcome these limitations, semi-Markovian jump systems (s-MJSs) have been introduced as a more practical alternative [8]. Unlike MJSs, s-MJSs permit more general probability distributions for sojourn time, without being constrained to exponential distributions. In s-MJSs, the transition rates depend on the jump time, providing a more realistic representation of practical dynamical systems [9]. This fundamental distinction makes s-MJSs less conservative and more applicable to various real-world scenarios. Notably, many results established for MJSs are seen as special cases of s-MJSs, considering that the transition rates in s-MJSs can be time-dependent rather than constant [10].

As control performance requirements continue to increase, the network-based communication mechanism has been widely adopted in real-time system design. Despite offering various benefits, the open and shared nature of these communication networks makes them susceptible to cyber attacks. In existing literature, three primary attack modes are often discussed: Denial-of-service attacks [11], deception attacks [12] and replay attacks [13]. Among these, deception attacks, also known as false-data injection attacks, are particularly concerning due to their secretive and destructive nature, posing a significant threat to network or internet security. These attacks transmit false information to the sensor or actuator by exploiting network transmission vulnerabilities, thereby altering the actual values of the sensor or controller [14–18]. As a result, system performance can be severely deteriorated. Consequently, developing effective control measures for s-MJS in the presence of deception attacks becomes a challenging task, especially as the adversaries often hide their attack strategies. This challenge forms the motivation for this work.

On the other hand, state feedback control synthesis problems for MJSs are typically classified into two types, delay-independent memoryless state feedback controllers and delay-dependent memory state feedback controllers. From the viewpoint of the stochastic nature of Markovian jump systems, memory controllers are natural state feedback controllers and memory controllers [19–21] achieve better performances than memoryless controllers can be expected. This strategy enhances the performance of control systems by enriching the dynamics of the controller. In [19], the robust H_∞ tracking problem for stochastic time-delay systems was investigated using a memory state feedback control strategy. In [20], the authors developed a non-fragile memory H_∞ control design for the discrete-time singular MJS with actuator saturation to explore its finite-time stability. A new aperiodic memory sampled-data control framework for a kind of fuzzy MJS with time-varying delay was proposed in [21]. The memory control strategy integrates memory into the controller's dynamics, offering numerous benefits, including improved control system performance, enhanced robustness, and adaptability to diverse operating conditions. It enables the controller to exhibit adaptive behaviors, refining its actions based on the system's evolution. However, accurate measurement of the system state information for control design can be difficult due to external disturbances and cyber attacks. As a result, recent control research communities have shown interest in the Luenberger state observer-based feedback control design [22, 23]. Despite its practical significance, only a limited number of studies on observer-based memory state feedback control design have been published for s-MJSs in the existing literature, which motivates the present study.

Considering these aspects, this study is aimed at exploring the Luenberger state based memory state feedback control design for s-MJSs subject to external disturbance. The key contributions of this study can be summarized as follows.

1) The memory state feedback control problem of s-MJSs with external disturbances is studied based on the linear matrix inequality (LMI) technique. In order to reflect a more realistic environment, the concept of cyber attacks is considered in state estimation for s-MJSs.
2) A Luenberger-type state observer is designed to estimate unmeasured states. A novel effective control algorithm for selecting the gain matrices for the controllers and observers is developed and also takes the past state information into account.
3) By using Lyapunov function methods and an extended Wirtinger's integral inequality techniques, a new set of LMI-based sufficient conditions are derived to ensure the stochastic stability of the error system. Numerical simulations show that these conditions are computationally effective in the analysis and synthesis of s-MJSs with and without cyber attacks.

The remainder of this paper is structured as follows. Preliminary discussions of the problem are found in Section 2. Section 3 puts forth the primary theoretical findings. Section 4 employs numerical examples to verify the proposed theory. Lastly, conclusions are drawn in Section 5.

2. Problem formulation

Consider the continuous-time s-MJSs with external disturbances:

$$\begin{aligned} \dot{x}(t) &= A(q(t))x(t) + B(q(t))u(t) + C(q(t))\omega(t), \\ y(t) &= D(q(t))x(t), \end{aligned} \tag{2.1}$$

where $x(t) \in \Re^n$, $u(t) \in \Re^m$, and $y(t) \in \Re^w$ represent the state, the control input and the measured output, respectively; $\omega(t)$ is the external disturbance that belongs to $\mathcal{L}_2[0,\infty)$; $A(q(t))$, $B(q(t))$, $C(q(t))$ and $D(q(t))$ are given matrices with appropriate dimensions. The process $\{q(t), t > 0\}$ is a semi-Markov process taking values as $\mathcal{P}\{q(t+\varkappa) = s | q(t) = r\} = \begin{cases} \Pi_{rs}(\varkappa)\varkappa + o(\varkappa), \text{if } r \neq s, \\ 1 + \Pi_{rr}(\varkappa)\varkappa + o(\varkappa), \text{if } r = s, \end{cases}$ where $\varkappa > 0$ is the sojourn time, $\lim\limits_{\varkappa\to 0}(o(\varkappa)/\varkappa) = 0$ and $\Pi_{rs}(\varkappa) \geq 0$ for $r \neq s$ is the transition rate from mode r at time t to mode s at time $t+\varkappa$ and $\Pi_{rr}(\varkappa) = -\sum_{s=1,s\neq r}^{\mathcal{N}} \Pi_{rs}(\varkappa)$.

For the dynamics (2.1), we construct the below state estimator with cyber attacks:

$$\begin{aligned} \dot{\hat{x}}(t) =& A(q(t))\hat{x}(t) + B(q(t))u(t) + L(q(t))(\tilde{y}(t) - \hat{y}(t)), \\ \tilde{y}(t) =& (1-\beta(t))y(t) + \beta(t)D(q(t))g(x(t)), \\ \hat{y}(t) =& D(q(t))\hat{x}(t), \end{aligned} \tag{2.2}$$

where $\hat{x}(t)$ and $\hat{y}(t)$ are the estimates of $x(t)$ and $y(t)$, respectively; $L(q(t))$ are the estimator gain matrices to be determined; $g(x(t))$ denotes the cyber attacks; $\beta(t)$ is the stochastic variable which satisfies the Bernoulli distribution [16].

In this study, we are designing a memory controller of the below form:

$$u(t) = K_1(q(t))\hat{x}(t) + K_2(q(t))\hat{x}(t-\tau), \tag{2.3}$$

where $K_1(q(t))$ and $K_2(q(t))$ are the control gain matrices to be designed; τ denotes the constant time delay. For representation convenience, hereafter we denote the semi-Markov process parameter $q(t)$ by subscript r that is, $A(q(t))$ is denoted by A_r.

By substituting the memory control law (2.3) in (2.2), we have

$$\dot{\hat{x}}(t) =(A_r + B_rK_{1r})\hat{x}(t) + B_rK_{2r}\hat{x}(t-\tau) + (1-\beta(t))L_rD_rx(t) + \beta(t)L_rD_rg(x(t)) - L_rD_r\hat{x}(t). \quad (2.4)$$

Denote $e(t) = x(t) - \hat{x}(t)$ and $z(t) = y(t) - \hat{y}(t)$, then the error dynamics are described as

$$\dot{x}(t) =(A_r + B_rK_{1r})x(t) - B_rK_{1r}e(t) + B_rK_{2r}x(t-\tau) - B_rK_{2r}e(t-\tau) + C_r\omega(t). \quad (2.5)$$
$$\dot{e}(t) =(A_r + L_rD_r)e(t) + C_r\omega(t) - (1-\beta(t))L_rD_rx(t) - \beta(t)L_rD_rg(x(t)) - L_rD_rx(t). \quad (2.6)$$
$$z(t) =D_re(t). \quad (2.7)$$

Further, by defining $\Phi(t) = [x^T(t) \quad e^T(t)]^T$, $g(\Phi(t)) = [g^T(x(t)) \quad g^T(e(t))]^T$, and combining Eqs (2.5) and (2.6), the following augmented s-MJSs can be written as

$$\begin{aligned}\dot{\Phi}(t) &=\tilde{A}_r\Phi(t) + \tilde{B}_r\Phi(t-\tau) + \tilde{C}_rg(\Phi(t)) + \tilde{D}_r\omega(t),\\ \tilde{z}(t) &=\tilde{E}_r\Phi(t),\end{aligned} \quad (2.8)$$

where

$$\tilde{A}_r = \begin{bmatrix} A_r + B_rK_{1r} & -B_rK_{1r} \\ \Gamma_r & A_r + L_rD_r \end{bmatrix},\ \tilde{B}_r = \begin{bmatrix} B_rK_{2r} & -B_rK_{2r} \\ 0 & 0 \end{bmatrix},\ \tilde{C}_r = \begin{bmatrix} 0 & 0 \\ \nu_r & 0 \end{bmatrix},\ \tilde{D}_r = \begin{bmatrix} C_r \\ C_r \end{bmatrix},\ \tilde{E}_r = [0 \quad D_r],$$

$\nu_r = -\bar{\beta}L_rD_r - (\beta(t) - \bar{\beta})L_rD_r$, $\Gamma_r = -(1-\bar{\beta})L_rD_r - (\bar{\beta} - \beta(t))L_rD_r - L_rD_r$ and $g(e(t)) = g(x(t)) - g(\hat{x}(t))$.

In order to derive the main results of this paper, consider the below assumption, lemma and definition.

Assumption 1. *The nonlinear function $g(\cdot)$ satisfies the Lipschitz condition such that $\|g(\Phi(t))\| \leq \|\mathcal{G}\Phi(t)\|$, where $\mathcal{G} > 0$ is a known diagonal matrix.*

Lemma 1. *[24] For any positive matrix $G = G^T$, the below inequality holds*

$$(s-h)\int_h^s \dot{\Phi}^T(q)G\dot{\Phi}(q)dq \geq \Theta_1^TG\Theta_1 + 3\Theta_2^TG\Theta_2 + 5\Theta_3^TG\Theta_3,$$

where $\Theta_1 = \Phi(s) - \Phi(h)$, $\quad \Theta_2 = \Phi(s) + \Phi(h) - \frac{2}{s-h}\int_h^s \Phi(r)dr$, $\quad \Theta_3 = \Phi(s) - \Phi(h) - \frac{6}{s-h}\int_h^s \Phi(r)dr + \frac{12}{(s-h)^2}\int_h^s dq\int_h^q \Phi(r)dr.$

Definition 1. *[21] The augmented s-MJSs* (2.8) *are stochastically stable with an H_∞ performance level $\delta > 0$. If it is stable and the response $\tilde{z}(t)$ under zero initial condition satisfies, then*

$$\mathbb{E}\Big\{\int_0^{t_m} \tilde{z}^T(t)\tilde{z}(t)dt\Big\} \leq \mathbb{E}\Big\{\delta^2\int_0^{t_m} \omega^T(t)\omega(t)dt\Big\}, \quad (2.9)$$

for all $t > 0$ and any nonzero $\omega(t) \in \mathcal{L}_2[0,\infty)$.

3. Main results

The memory control issue of the augmented s-MJSs (2.8) is addressed by employing the Lyapunov functions method.

Theorem 1. *Let Assumption 1 hold. For given scalars $\tau > 0$, $\alpha > 0$, $\sigma,\bar{\beta} \in [0, 1]$, diagonal matrix $\mathcal{G}$, known gain matrices K_{1r}, K_{2r} and L_r, the considered augmented s-MJSs* (2.8) *are stochastically stable with an H_∞ performance index $\delta > 0$, if there exists symmetric matrices $\mathcal{P}_r > 0$, $\mathcal{Q} > 0$, $\mathcal{R} > 0$ and a scalar $\gamma > 0$ such that the following matrix inequality holds:*

$$\begin{bmatrix} \bar{\Gamma}_{rs} & \Theta_r & \bar{\Sigma} \\ * & -\alpha\mathcal{P}_r & 0 \\ * & * & -\bar{\eta} \end{bmatrix} < 0, \tag{3.1}$$

$$\sum_{s=1}^{\mathcal{N}} \pi_{rs}(\varkappa)\alpha\mathcal{P}_s - \alpha\mathcal{R} \leq 0, \tag{3.2}$$

where

$$\bar{\Gamma}_{rs} = [\Omega]_{rs}^{6\times 6},\ [\Omega]_{rs}^{1,1} = \mathcal{P}_r\tilde{A}_r + \tilde{A}_r^T\mathcal{P}_r + \mathcal{Q} + \sum_{r=1}^{\mathcal{N}} \pi_{rr}(\varkappa)\mathcal{P}_r - 9\alpha\mathcal{P}_r + \tilde{E}^T\tilde{E} + \gamma\mathcal{G}^T\mathcal{G},\ [\Omega]_{rs}^{1,2} = \mathcal{P}_r\tilde{B}_r + 3\alpha\mathcal{P}_r,$$
$$[\Omega]_{rs}^{1,3} = 18\alpha\mathcal{P}_r,\ [\Omega]_{rs}^{1,4} = -2\alpha\mathcal{P}_r,\ [\Omega]_{rs}^{1,5} = \mathcal{P}_r\tilde{C}_r,\ [\Omega]_{rs}^{1,6} = \mathcal{P}_r\tilde{D}_r,\ [\Omega]_{rs}^{2,2} = -\mathcal{Q} - 9\alpha\mathcal{P}_r,\ [\Omega]_{rs}^{2,3} = -15\alpha\mathcal{P}_r,$$
$$[\Omega]_{rs}^{2,4} = 5\alpha\mathcal{P}_r,\ [\Omega]_{rs}^{3,3} = -48\alpha\mathcal{P}_r,\ [\Omega]_{rs}^{3,4} = 15\alpha\mathcal{P}_r,\ [\Omega]_{rs}^{4,4} = -5\alpha\mathcal{P}_r,\ [\Omega]_{rs}^{5,5} = -\gamma I,\ [\Omega]_{rs}^{6,6} = -\delta^2 I,$$
$$\Theta_r = [\tau\alpha\mathcal{P}_r\tilde{A}_r \quad \tau\alpha\mathcal{P}_r\tilde{B}_r \quad 0 \quad 0 \quad \tau\alpha\mathcal{P}_r\tilde{C}_r \quad \tau\alpha\mathcal{P}_r\tilde{D}_r]^T,\ \bar{\eta} = \mathrm{diag}\{\mathcal{P}_1, \ldots, \mathcal{P}_{r-1}, \mathcal{P}_{r+1}, \ldots, \mathcal{P}_{\mathcal{N}}\},$$
$$\bar{\Sigma} = [\ \sqrt{\pi_{r1}(\varkappa)}\mathcal{P}_r^T, \ldots,\ \sqrt{\pi_{r(r+1)}(\varkappa)}\mathcal{P}_r^T, \ldots,\ \sqrt{\pi_{r\mathcal{N}}(\varkappa)}\mathcal{P}_r^T],$$

and the remaining parameters of Ω_{rs} are zero.

Proof. Choose a Lyapunov-Krasovskii functional candidate for the augmented s-MJSs (2.8) as follows:

$$\mathcal{M}(r, \Phi(t)) = \Phi^T(t)\mathcal{P}_r\Phi(t) + \int_{t-\tau}^{t} \Phi^T(s)\mathcal{Q}\Phi(s)\mathrm{d}s + \tau\int_{t-\tau}^{t}\int_{\theta}^{t} \dot{\Phi}^T(s)\alpha\mathcal{P}_r\dot{\Phi}(s)\mathrm{d}s\mathrm{d}\theta, \tag{3.3}$$

where $\mathcal{P}_r = \mathrm{diag}\{\mathcal{P}_{1r}, \mathcal{P}_{2r}\}$ and $\mathcal{Q} = \mathrm{diag}\{\mathcal{Q}_1, \mathcal{Q}_2\}$. Further, the infinitesimal operator of the semi-Markovian process is denoted by £. By applying infinitesimal operator on (3.3) and taking mathematical expectation, we get

$$\begin{aligned}\mathbb{E}\{£\mathcal{M}(r, \Phi(t))\} =& \mathbb{E}\{\Phi^T(t)\mathcal{P}_r\dot{\Phi}(t) + \dot{\Phi}^T(t)\mathcal{P}_r\Phi(t) + \Phi^T(t)\sum_{s=1}^{\mathcal{N}} \pi_{rs}(\varkappa)\mathcal{P}_s\Phi(t) + \Phi^T(t)\mathcal{Q}\Phi(\ell) - \Phi^T(\ell-\tau)\mathcal{Q}\Phi(\ell-\tau),\\ &+ \dot{\Phi}^T(t)\tau^2\alpha\mathcal{P}_r\dot{\Phi}(t) - \tau\int_{t-\tau}^{t} \dot{\Phi}^T(s)\alpha\mathcal{P}_r\dot{\Phi}(s)\mathrm{d}s + \tau\int_{t-\tau}^{t}\int_{\theta}^{t} \dot{\Phi}^T(s)\sum_{s=1}^{\mathcal{N}} \pi_{rs}(\varkappa)\alpha\mathcal{P}_s\dot{\Phi}(s)\mathrm{d}s\mathrm{d}\theta\}.\end{aligned} \tag{3.4}$$

Further, by using Lemma 1 to the integral term in Eq (3.4), we can get

$$-\tau\int_{t-\tau}^{t} \dot{\Phi}^T(s)\alpha\mathcal{P}_r\dot{\Phi}(s)\mathrm{d}s \leq \begin{bmatrix} \Phi(t) \\ \Phi(t-\tau) \\ \frac{2}{\tau}\int_{t-\tau}^{t}\Phi(s)\mathrm{d}s \\ \frac{12}{\tau^2}\int_{t-\tau}^{t}\int_{t-\tau}^{\theta}\Phi(s)\mathrm{d}s\mathrm{d}\theta \end{bmatrix}^T \begin{bmatrix} -9\alpha\mathcal{P}_r & 3\alpha\mathcal{P}_r & 18\alpha\mathcal{P}_r & -2\alpha\mathcal{P}_r \\ * & -9\alpha\mathcal{P}_r & -15\alpha\mathcal{P}_r & 5\alpha\mathcal{P}_r \\ * & * & -48\alpha\mathcal{P}_r & 15\alpha\mathcal{P}_r \\ * & * & * & -5\alpha\mathcal{P}_r \end{bmatrix} \begin{bmatrix} \Phi(t) \\ \Phi(t-\tau) \\ \frac{2}{\tau}\int_{t-\tau}^{t}\Phi(s)\mathrm{d}s \\ \frac{12}{\tau^2}\int_{t-\tau}^{t}\int_{t-\tau}^{\theta}\Phi(s)\mathrm{d}s\mathrm{d}\theta \end{bmatrix}. \tag{3.5}$$

From (3.2), it is clear that

$$\tau \int_{t-\tau}^{t} \int_{\theta}^{t} \dot{\Phi}^T(s) \sum_{r=1}^{\mathcal{N}} \pi_{rs}(\varkappa)\alpha\mathcal{P}_r\dot{\Phi}(s)\mathrm{d}s\mathrm{d}\theta \le \tau \int_{t-\tau}^{t} \int_{\theta}^{t} \dot{\Phi}^T(s)\alpha\mathcal{R}\dot{\Phi}(s)\mathrm{d}s\mathrm{d}\theta. \tag{3.6}$$

For any scalar $\gamma > 0$, we can get from Assumption 1 that

$$\gamma\Phi^T(t)\mathcal{G}^T\mathcal{G}\Phi(t) - \gamma g^T(\Phi(t))g(\Phi(t)) \ge 0. \tag{3.7}$$

Now, by adding H_∞ performance attenuation to $\mathcal{M}(r, \Phi(t))$ and associating (3.4)–(3.7), it is easy to obtain that

$$\mathbb{E}\{\pounds\mathcal{M}(r, \Phi(t)) + \tilde{z}^T(t)\tilde{z}(t) - \delta^2\omega^T(t)\omega(t)\} \le \mathbb{E}\{\xi^T(t)\Gamma_{rs}\xi(t)\}, \tag{3.8}$$

where $\xi(t) = [\Phi^T(t) \quad \Phi^T(t-\tau) \quad \frac{2}{\tau}\int_{t-\tau}^{t}\Phi^T(s)\mathrm{d}s \quad \frac{12}{\tau^2}\int_{t-\tau}^{t}\int_{t-\tau}^{\theta}\Phi^T(s)\mathrm{d}s\mathrm{d}\theta \quad g^T(\Phi(t)) \quad \omega^T(t)]^T$ and $\Gamma_{rs} = [\Omega]_{rs}^{6\times 6} + \dot{\Phi}^T(t)\tau^2\alpha\mathcal{P}_r\dot{\Phi}(t) + \nabla^T\nabla + \Phi^T(t)\sum_{s=1}^{\mathcal{N}}\pi_{rs}(\varkappa)\mathcal{P}_s\Phi(t)$. By using the Schur complement, we have Γ_{rs} can be equivalently written as $\bar{\Gamma}_{rs}$ which is defined in the theorem statement. Thus, it can be observed that $\mathbb{E}\{\pounds\mathcal{M}(r, \Phi(t)) + \tilde{z}^T(t)\tilde{z}(t) - \delta^2\omega^T(t)\omega(t)\} < 0$ if the LMI (3.1) holds. Thus, by Definition 1, it is concluded that the augmented s-MJSs (2.8) are stochastically stable with an H_∞ performance index $\delta > 0$. This completes the proof of the theorem.

Control synthesis conditions are established by LMIs on the basis of Theorem 1, which are presented as follows.

Theorem 2. *Let Assumption 1 hold. For given scalars $\tau > 0$, $\alpha > 0$, $\kappa > 0$, $\sigma, \bar{\beta} \in [0, 1]$, and known diagonal matrix $\mathcal{G}$, the considered augmented s-MJSs* (2.8) *are stochastically stable with an H_∞ performance index $\delta > 0$, if there exists symmetric matrices $\mathcal{P}_r > 0$, $\mathcal{Q} > 0$, any matrices $\mathcal{X}_r$, $\mathcal{W}_{1r}$, $\mathcal{W}_{2r}$, $\mathcal{T}_r$, and a scalar $\gamma > 0$ such that LMI* (3.2) *and the below matrix inequality holds:*

$$\begin{bmatrix} \bar{\Gamma}_{rs} & \hat{\Theta}_r & \bar{\Sigma} \\ * & -\alpha\mathcal{P}_r & 0 \\ * & * & -\bar{\eta} \end{bmatrix} < 0, \tag{3.9}$$

$$\begin{bmatrix} -\kappa I & (B_r\mathcal{X}_r - \mathcal{P}_{1r}B_r)^T \\ * & -\kappa I \end{bmatrix} < 0, \tag{3.10}$$

where
$\hat{\Gamma}_{rs} = [\bar{\Omega}]_{rs}^{6\times 6}$, $[\bar{\Omega}]_{rs}^{1,1} = \hat{\mathcal{A}}_r + \hat{\mathcal{A}}_r^T + \mathcal{Q} + \sum_{r=1}^{\mathcal{N}}\pi_{rr}(\varkappa)\mathcal{P}_r - 9\alpha\mathcal{P}_r + \tilde{E}^T\tilde{E} + \gamma\mathcal{G}^T\mathcal{G}$, $[\bar{\Omega}]_{rs}^{1,2} = \hat{\mathcal{B}}_r + 3\alpha\mathcal{P}_r$, $[\bar{\Omega}]_{rs}^{1,5} = \hat{\mathcal{C}}_r$, $[\bar{\Omega}]_{rs}^{1,6} = \hat{\mathcal{D}}_r$, $\hat{\mathcal{A}}_r = \begin{bmatrix} \mathcal{P}_{1r}A_r + B_r\mathcal{W}_{1r} & -B_r\mathcal{W}_{1r} \\ -(1-\bar{\beta})\mathcal{T}_rD_r + \mathcal{T}_rD_r & \mathcal{P}_{2r}A_r - \mathcal{T}_rD_r \end{bmatrix}$, $\hat{\mathcal{B}}_r = \begin{bmatrix} B_r\mathcal{W}_{2r} & -B_r\mathcal{W}_{2r} \\ 0 & 0 \end{bmatrix}$, $\hat{\mathcal{C}}_r = \begin{bmatrix} 0 & 0 \\ -\bar{\beta}\mathcal{T}_rD_r & 0 \end{bmatrix}$, $\hat{\mathcal{D}}_r = \begin{bmatrix} \mathcal{P}_{1r}C_r \\ \mathcal{P}_{2r}C_r \end{bmatrix}$, $\hat{\Theta}_r = [\tau\alpha\hat{\mathcal{A}}_r \quad \tau\alpha\hat{\mathcal{B}}_r \quad 0 \quad 0 \quad \tau\alpha\hat{\mathcal{C}}_r \quad \tau\alpha\hat{\mathcal{D}}_r]^T$ and the other elements of $[\bar{\Omega}]_{rs}$ are defined as $[\Omega]_{rs}$, which are given in the Theorem 1. Further, the gain matrices can be obtained by the below conditions: $K_{1r} = \mathcal{X}_r^{-1}\mathcal{W}_{1r}$, $K_{2r} = \mathcal{X}_r^{-1}\mathcal{W}_{2r}$ and $L_r = \mathcal{P}_{2r}^{-1}\mathcal{T}_r$.

Proof. Let us assume that the linear congruence transformations (LCTs) are as follows: $\mathcal{P}_{1r}B_r = B_r\mathcal{X}_r$, $\mathcal{W}_{1r} = \mathcal{X}_rK_{1r}$, $\mathcal{W}_{2r} = \mathcal{X}_rK_{2r}$ and $\mathcal{T}_r = \mathcal{P}_{2r}L_r$. Then, by utilizing LCTs, the inequality in (3.1) can be the same as (3.9). It is noted that the assumption $\mathcal{P}_{1r}B_r = B_r\mathcal{X}_r$ is equally constraining. So it could not be directly solved via the LMI Toolbox. To deal with this issue, we replace the condition $\mathcal{P}_{1r}B_r = B_r\mathcal{X}_r$ by the constraint *trace* $[(B_r\mathcal{X} - \mathcal{P}_{1r}B_r)^T(B_r\mathcal{X} - \mathcal{P}_{1r}B_r)] < \kappa I$, for known scalar $\kappa > 0$. Now, by using the Schur complement, the inequality constraint can be converted to the LMI in (3.10). This completes the proof of the theorem.

Remark 1. *In recent years, cyber attacks have threatened information security, such as file confidentiality, communication integrity, and data transmission effectiveness. Cyber attacks have gradually become the main issuse hindering the effective communication of MJSs. Very recently, some interesting results on state estimation for MJSs under cyber attacks have been discussed in [16–18]. For example, Zha et al. [16] addressed the analysis and synthesis of state estimation for MJSs subject to cyber attacks by utilizing the finite-time adaptive event-triggered method. In [18], an observer-based sliding control law was designed, which guarantees the MJSs under actuator attacks to be reliable. Moreover, so far in the literature, no work has been reported on memory control problem of s-MJSs with cyber attacks and input delays. Thus, the main contribution of this paper is to fill such a gap through employing an observer-based memory control law for achieving stochastic stabilization in s-MJSs against cyber attacks.*

4. Simulation examples

To illustrate the effectiveness of the designed controller, we consider two simulation studies in this section.

Example 1.

Consider the s-MJSs in the form of (2.1) with two modes and associated matrices are given as follows.

Mode 1:

$$A_1 = \begin{bmatrix} -2.4 & 0 & 1.4 \\ 0.1 & -0.4 & -0.3 \\ 0.7 & 0 & 0.3 \end{bmatrix}, \ B_1 = \begin{bmatrix} 0.12 & 0 \\ 0.13 & 0.4 \\ 0.1 & 0.1 \end{bmatrix}, \ C_1 = \begin{bmatrix} 0.5 \\ 0.05 \\ -0.01 \end{bmatrix}, \text{ and } D_1 = \begin{bmatrix} -0.1 & 0 & 1 \\ 0.15 & -2 & -0.1 \\ 0.1 & 0.2 & 0.1 \end{bmatrix}.$$

Mode 2:

$$A_2 = \begin{bmatrix} -3.6 & 0 & 2.2 \\ 0.3 & -0.4 & -0.7 \\ 0.1 & 0 & -0.4 \end{bmatrix}, \ B_2 = \begin{bmatrix} 0.11 & 0 \\ 0.14 & 0.4 \\ 0.2 & 0.1 \end{bmatrix}, \ C_2 = \begin{bmatrix} 0.4 \\ 0.03 \\ -0.02 \end{bmatrix}, \text{ and } D_2 = \begin{bmatrix} -0.2 & 0 & 1 \\ 0.16 & -1 & -0.1 \\ 0.2 & 0.3 & 0.1 \end{bmatrix}.$$

Further, the external disturbances and cyber attacks function are taken as $\omega(t) = 0.3\sin(5\pi t)$ and $g(x(t)) = [-0.45\tanh(x_1(t)) \quad -0.25\tanh(x_2(t)) \quad -0.15\tanh(x_3(t))]^T$. Moreover, the transition rates $\Pi_{12}(\varkappa)$ and $\Pi_{21}(\varkappa)$ can be represented as $\Pi_{12}(\varkappa) = \sum_{k=1}^{2}\psi_k\Pi_{12,k}$ and $\sum_{k=1}^{2}\psi_k = 1$ with $\Pi_{12}(\varkappa) \in [0.1\ 0.3]$ and $\Pi_{21}(\varkappa) \in [0.2\ 0.4]$. Moreover, the other parameters are chosen as $\tau = 2$, $\alpha = 0.001$, $\sigma = 0.5$, $\bar{\beta} = 0.4$ and $\mathcal{G} = \text{diag}\{0.45, 0.25, 0.15\}$.

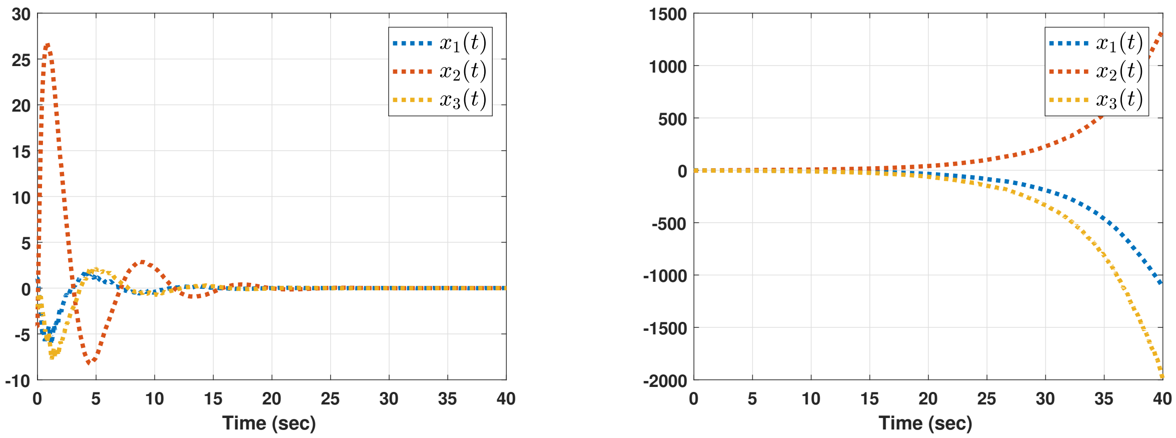
Based on these values, the memory control and observer gain parameter are computed as below:

$$K_{11} = \begin{bmatrix} -93.5834 & 19.1919 & -46.9853 \\ 43.4856 & -67.5993 & 7.9646 \end{bmatrix}, \quad K_{12} = \begin{bmatrix} -26.9227 & -11.1151 & -24.6391 \\ 15.8148 & -8.3630 & 13.1298 \end{bmatrix},$$

$$K_{21} = \begin{bmatrix} 0.0026 & -0.0115 & -0.0030 \\ -0.0012 & 0.0209 & 0.0043 \end{bmatrix}, \quad K_{22} = \begin{bmatrix} 0.0019 & -0.0024 & -0.0012 \\ -0.0021 & 0.0083 & 0.0012 \end{bmatrix},$$

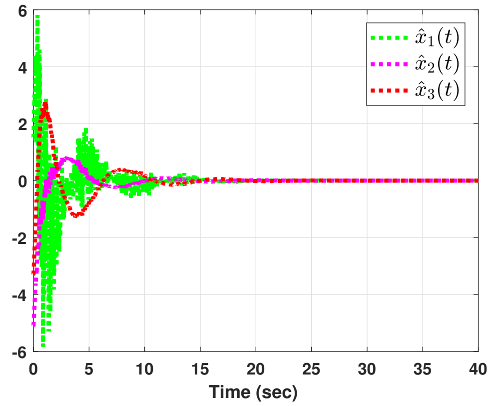
$$L_1 = \begin{bmatrix} -1.5813 & 29.4874 & 333.3484 \\ 0.1677 & 3.1112 & 35.9142 \\ 2.3518 & 1.5364 & 19.9485 \end{bmatrix}, \text{ and } L_2 = \begin{bmatrix} 18.3136 & 27.9459 & 114.7521 \\ 1.8261 & 2.3703 & 10.3630 \\ 1.6228 & 1.1022 & 7.2568 \end{bmatrix}.$$

We apply these gains to the system results of simulation under initial conditions $x(t) = [1.1 \quad -4.2 \quad -2.2]^T$ and $\hat{x}(t) = [1.5 \quad -5.1 \quad -3.3]^T$ as shown in Figures 1–6. The state curves of addressed system (2.1) with and without control are plotted in Figure 1(a,b), respectively. It can be seen that the state curves with control in Figure 1(a) converge to zero, which shows the efficiency of the proposed control strategy. Furthermore, the estimated state curves of s-MJSs (2.2) with and without cyber attacks are given in Figure 2(a,b), and it can be seen that the convergence speed of the estimated state curves in Figure 2(b) are faster than that in Figure 2(a), which indicates that cyber attacks can affect the estimate performance of the system state. Moreover, the corresponding error state curves of s-MJSs (2.7) with and without cyber attacks are displayed in Figure 3(a,b). Lastly, Figures 4–6 show the mode transitions, the occurrence probability of cyber attacks and the function of cyber attacks, respectively. However, these figures are provided to demonstrate the validity and applicability of the proposed control scheme.

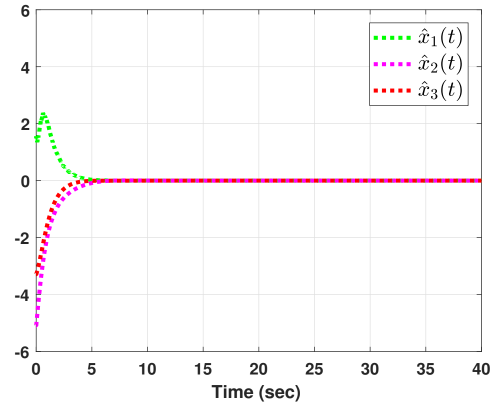


(a) With control (b) Without control

Figure 1. State curves of s-MJSs (2.1) with and without control.

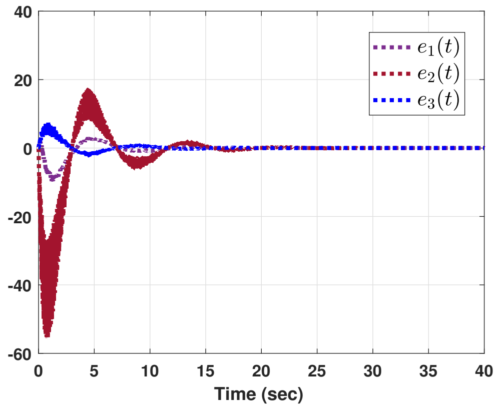


(a) With cyber attacks

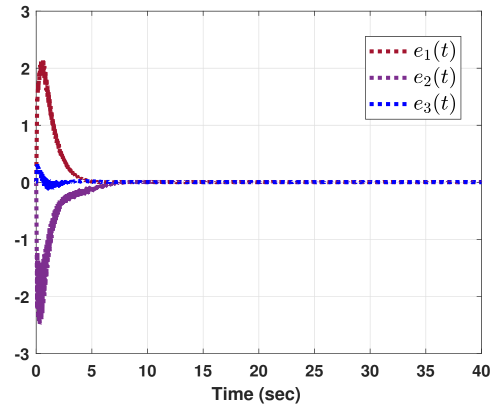


(b) Without cyber attacks

Figure 2. Estimated state curves of s-MJSs (2.2) with and without cyber attacks.



(a) With cyber attacks



(b) Without cyber attacks

Figure 3. Error state curves of s-MJSs (2.7) with and without cyber attacks.

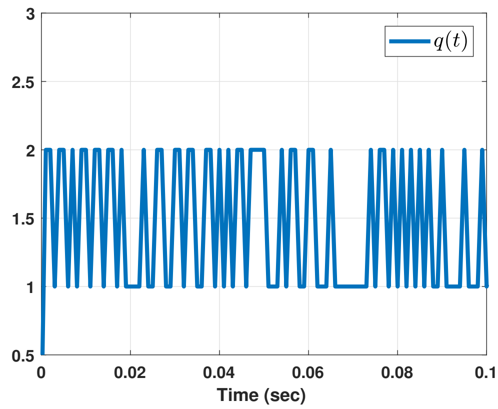


Figure 4. The Mode transitions.

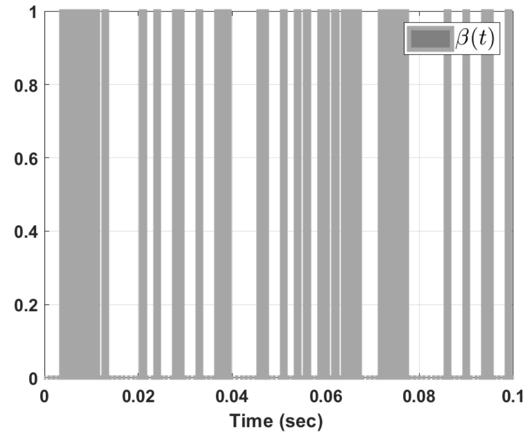


Figure 5. The occurrence probability of cyber attacks.

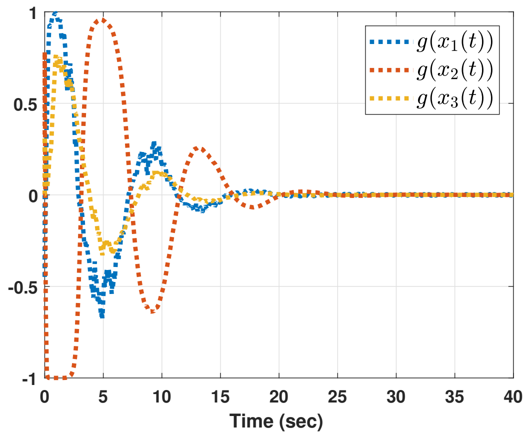


Figure 6. The function of cyber attacks.

Example 2.

An F-404 aircraft engine model is borrowed from [25], which is considered the s-MJSs in the form of (2.1) with two modes. The associated matrices are given as follows:

Mode 1:

$$A_1 = \begin{bmatrix} -1.46 & 0 & 2.428 \\ -0.3357 & -1.4 & -0.3788 \\ 0.3107 & 0 & -2.23 \end{bmatrix}, \; B_1 = \begin{bmatrix} 0.055 & 0.05 \\ 0.1 & -1 \\ 0.075 & -0.05 \end{bmatrix}, \; C_1 = \begin{bmatrix} 0.1 \\ -0.2 \\ -0.5 \end{bmatrix}, \text{ and } D_1 = \begin{bmatrix} -0.1 & 0 & 1 \\ 0.15 & -2 & -0.1 \\ 0.1 & 0.2 & 0.1 \end{bmatrix}.$$

Mode 2:

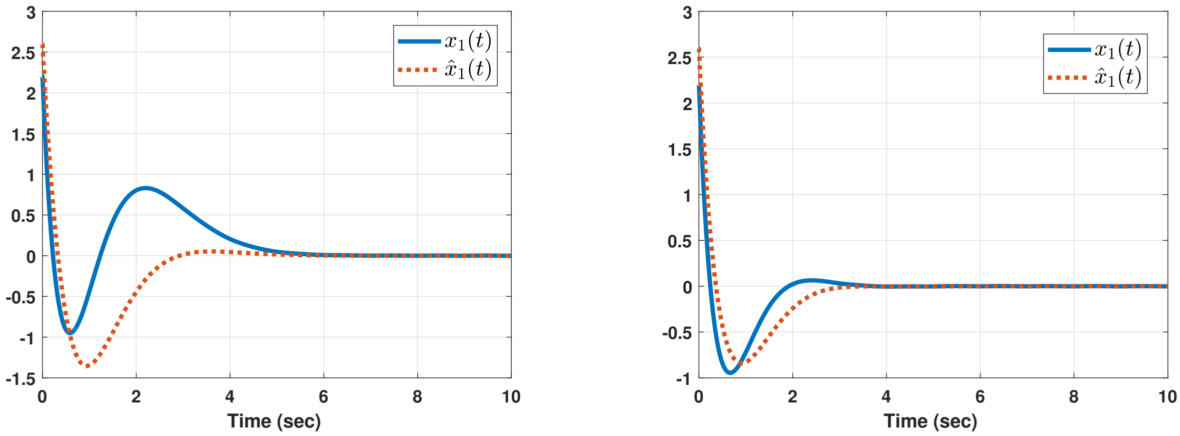
$$A_2 = \begin{bmatrix} -1.46 & 0 & 2.428 \\ -0.8357 & -2.4 & -0.3788 \\ 0.3107 & 0 & -2.23 \end{bmatrix}, \; B_2 = \begin{bmatrix} 0.055 & 0.05 \\ 0.075 & -1 \\ 0.05 & -0.05 \end{bmatrix}, \; C_2 = \begin{bmatrix} 0.4 \\ -0.3 \\ -0.2 \end{bmatrix}, \text{ and } D_2 = \begin{bmatrix} -0.1 & 0 & 1 \\ 0.15 & -2 & -0.1 \\ 0.1 & 0.2 & 0.1 \end{bmatrix}.$$

Moreover, the external disturbances and cyber attacks function are selected as $\omega(t) = 0.5\sin(2\pi t)$ and $g(x(t)) = [-0.65\tanh(x_1(t)) \quad -0.25\tanh(x_2(t)) \quad -0.35\tanh(x_3(t))]^T$. Furthermore, the transition rates $\Pi_{12}(\varkappa)$ and $\Pi_{21}(\varkappa)$ are given in Example 1. Therefore, the remaining parameters are taken as $\tau = 1$, $\alpha = 0.01$, $\sigma = 0.2$, $\bar{\beta} = 0.6$ and $\mathcal{G} = \mathrm{diag}\{0.65, 0.25, 0.35\}$.

Based on the above values, the memory controller and observer gain matrices are computed as follows:

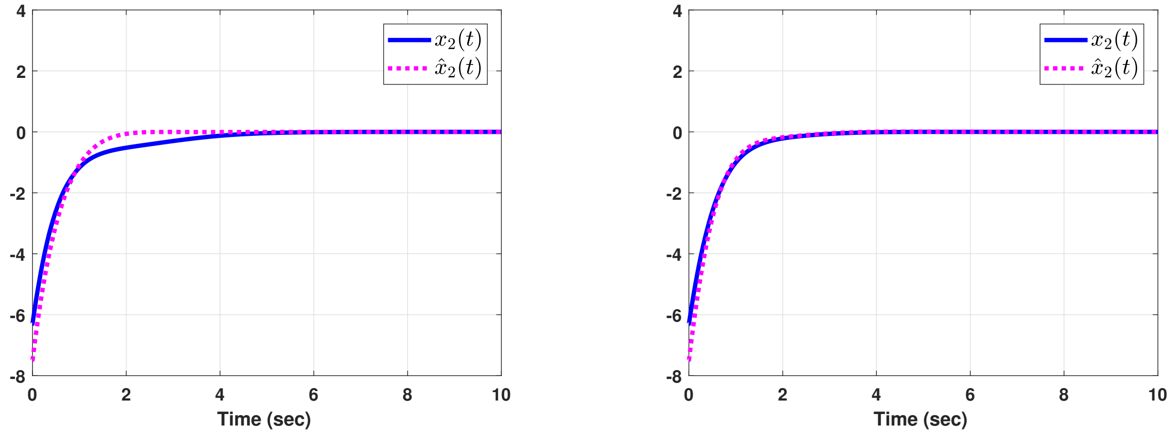
$$K_{11} = \begin{bmatrix} -15.2057 & -0.8366 & 3.3212 \\ -1.7014 & -0.0061 & -0.2313 \end{bmatrix}, \quad K_{12} = \begin{bmatrix} -23.3056 & 1.2995 & -1.2568 \\ -2.4397 & -0.0248 & -0.3595 \end{bmatrix},$$
$$K_{21} = \begin{bmatrix} -0.0237 & -0.0045 & -0.0282 \\ -0.0023 & 0.0051 & -0.0020 \end{bmatrix}, \quad K_{22} = \begin{bmatrix} -0.0489 & -0.0040 & -0.0244 \\ -0.0037 & 0.0073 & -0.0003 \end{bmatrix},$$
$$L_1 = \begin{bmatrix} 2.5444 & -0.5562 & 0.9756 \\ 0.1376 & -0.0787 & 0.1280 \\ -7.1661 & 0.1602 & 0.8970 \end{bmatrix}, \text{ and } L_2 = \begin{bmatrix} 2.7831 & -1.2368 & 3.6411 \\ 0.0473 & -0.3510 & -1.8192 \\ -7.1524 & 0.2981 & 3.1258 \end{bmatrix}.$$

Based on these gains values of simulation results under initial conditions $x(t) = [2.2 \quad -6.3 \quad -3.1]^T$ and $\hat{x}(t) = [2.6 \quad -7.5 \quad -4.2]^T$ as shown in Figures 7–9. Which depict the dynamics of the system states and their estimations, it is clear that the proposed method can estimate states well if the states are immeasurable. The state curves $x(t)$ and its estimates $\hat{x}(t)$ with and without cyber attacks are showed in Figures 7(a,b), 8(a,b) and 9(a,b), respectively. By contrast, it can be seen that the convergence speed of the estimated state curves in Figures 7(b), 8(b) and 9(b) are faster than that in Figures 7(a), 8(a) and 9(a), which indicates that cyber attacks can affect the stability and estimate performance of the system state. Thus, from these simulation results, we can conclude that the proposed controller effectively estimated states of the F-404 aircraft engine system even in the presence of cyber attacks.



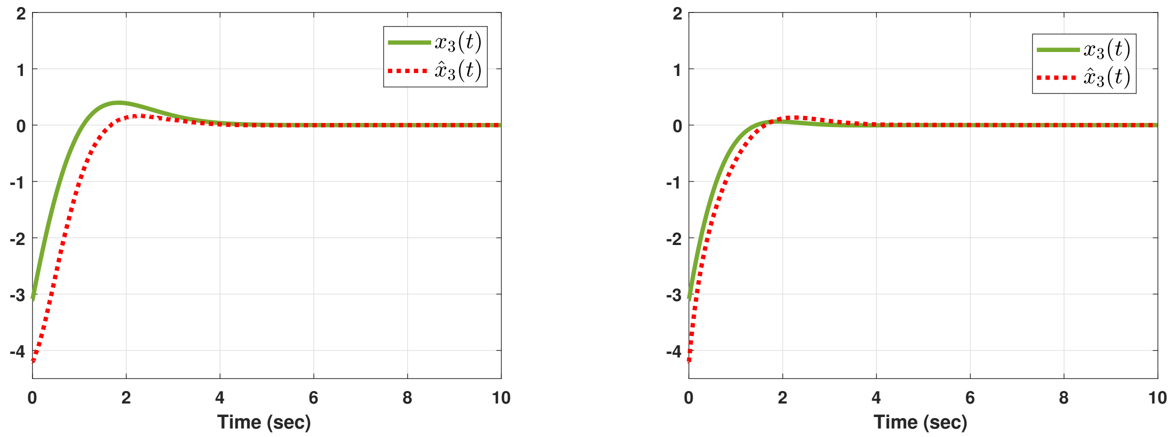
(a) With cyber attacks (b) Without cyber attacks

Figure 7. First state curves $x_1(t)$ and its estimates $\hat{x}_1(t)$ with and without cyber attacks.



(a) With cyber attacks (b) Without cyber attacks

Figure 8. Second state curves $x_2(t)$ and its estimates $\hat{x}_2(t)$ with and without cyber attacks.



(a) With cyber attacks (b) Without cyber attacks

Figure 9. Third state curves $x_3(t)$ and its estimates $\hat{x}_3(t)$ with and without cyber attacks.

5. Conclusions

The observer-based memory state feedback control design problem for S-MJSs subject to external disturbance and randomly occurring cyber attacks has been addressed in this paper. First, the cyber attacks have been represented by the Lipschitz continuous nonlinear function, with the randomness phenomenon denoted by the Bernoulli distributed stochastic parameter. Next, on the basis of measurement output, the state observer was constructed for the addressed system. By using the Lyapunov stability theory and matrix integral inequality, sufficient conditions ensuring the desired stability and observer design of the addressed system have been obtained. To reduce conservatism, an extended Wirtinger's integral inequality has been employed in the proof of stability criterion. Finally, two numerical examples have been provided to illustrate the feasibility and potential value of the proposed observer-based memory state feedback control design approach.

Use of AI tools declaration

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

Acknowledgments

This research was supported by "Regional Innovation Strategy (RIS)" through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (MOE) (2021RIS-001).

Conflict of interest

The authors declare that there is no conflict of interest.

References

1. C. E. de Souza, Robust stability and stabilization of uncertain discrete-time Markovian jump linear systems, *IEEE Trans. Autom. Control*, **51** (2006), 836–841. https://doi.org/10.1109/TAC.2006.875012
2. X. Li, R. Rakkiyappan, N. Sakthivel, Non-fragile synchronization control for Markovian jumping complex dynamical networks with probabilistic time-varying coupling delays, *Asian J. Control*, **17** (2015), 1678–1695. https://doi.org/10.1002/asjc.984
3. W. Chen, F. Gao, S. Xu, Y. Li, Y. Chu, Robust stabilization for uncertain singular Markovian jump systems via dynamic output-feedback control, *Syst. Control Lett.*, **171** (2023), 105433. https://doi.org/10.1016/j.sysconle.2022.105433
4. X. Xu, L. Wang, Z. Du, Y. Kao, Stochastic stabilization of Markovian jump neutral systems with fractional Brownian motion and quantized controller, *J. Franklin Inst.*, **358** (2021), 9449–9466. https://doi.org/10.1016/j.jfranklin.2021.09.005
5. W. Xia, S. Xu, J. Lu, Y. Li, Y. Chu, Z. Zhang, Event-triggered filtering for discrete-time Markovian jump systems with additive time-varying delays, *Appl. Math. Comput.*, **391** (2021), 125630. https://doi.org/10.1016/j.amc.2020.125630
6. J. Wang, H. Zhang, J. Fu, H. Liang, Q. Meng, Dissipativity-based consensus tracking control of nonlinear multiagent systems with generally uncertain Markovian switching topologies and event-triggered strategy, *IEEE Trans. Cybern.*, **53** (2023), 4763–4778. https://doi.org/10.1109/TCYB.2022.3141599
7. B. Jiang, Z. Wu, H. R. Karimi, A traverse algorithm approach to stochastic stability analysis of Markovian jump systems with unknown and uncertain transition rates, *Appl. Math. Comput.*, **422** (2022), 126968. https://doi.org/10.1016/j.amc.2022.126968
8. D. Ding, J. Liu, H. Yang, Robust non-fragile control of positive semi-Markovian jump systems with actuator saturation, *IEEE Access*, **7** (2019), 86758–86768. https://doi.org/10.1109/ACCESS.2019.2922715

9. F. Li, P. Shi, L. Wu, M. V. Basin, C. C. Lim, Quantized control design for cognitive radio networks modeled as nonlinear semi-Markovian jump systems, *IEEE Trans. Ind. Electron.*, **62** (2015), 2330–2340. https://doi.org/10.1109/TIE.2014.2351379

10. Y. Tian, H. Yan, H. Zhang, S. X. Yang, Z. Li, Observed-based finite-time control of nonlinear semi-Markovian jump systems with saturation constraint, *IEEE Trans. Syst. Man Cybern.: Syst.*, **51** (2021), 6639–6649. https://doi.org/10.1109/TSMC.2019.2962318

11. H. Ye, P. Cheng, X. Zhang, S. He, W. Zhang, Event-triggered-based control for Markov jump cyber-physical systems against denial-of-service attacks, *Appl. Math. Comput.*, **451** (2023), 128030. https://doi.org/10.1016/j.amc.2023.128030

12. R. Sakthivel, O. M. Kwon, M. J. Park, S. M. Lee, R. Sakthivel, Disturbance rejection for multi-weighted complex dynamical networks with actuator saturation and deception attacks via hybrid-triggered mechanism, *Neural Networks*, **162** (2023), 225–239. https://doi.org/10.1016/j.neunet.2023.02.031

13. X. Li, X. Xu, L. Chen, H. Zhang, Z. Ju, W. Guo, Longitudinal speed tracking control for an electric connected vehicle with actuator saturation subject to a replay attack, *Nonlinear Dyn.*, **111** (2023), 1369–1383. https://doi.org/10.1007/s11071-022-07898-2

14. H. He, W. Qi, H. Yan, J. Cheng, K. Shi, Adaptive fuzzy resilient control for switched systems with state constraints under deception attacks, *Inf. Sci.*, **621** (2023), 596–610. https://doi.org/10.1016/j.ins.2022.11.074

15. J. Yan, Y. Xia, X. Feng, Y. Zhang, Deception attack detection based on bandwidth allocation for switched systems with quantization, *Automatica*, **154** (2023), 111094. https://doi.org/10.1016/j.automatica.2023.111094

16. L. Zha, R. Liao, J. Liu, X. Xie, J. Cao, L. Xiong, Finite-time adaptive event-triggered asynchronous state estimation for Markov jump systems with cyber-attacks, *Int. J. Robust Nonlinear Control*, **32** (2022), 583–599. https://doi.org/10.1002/rnc.5836

17. X. Gao, F. Deng, H. Zhang, P. Zeng, Adaptive neural state estimation of Markov jump systems under scheduling protocols and probabilistic deception attacks, *IEEE Trans. Cybern.*, **53** (2022), 1830–1842. https://doi.org/10.1109/TCYB.2022.3140415

18. B. Jiang, D. Liu, H. R. Karimi, B. Li, Observer-based event-triggered H_∞ sliding control of Markovian jump system suffer from actuator attacks, *Asian J. Control*, **25** (2023), 2975–2987. https://doi.org/10.1002/asjc.2998

19. J. Xia, J. H. Park, T. H. Lee, B. Zhang, H_∞ tracking of uncertain stochastic time-delay systems: memory state-feedback controller design, *Appl. Math. Comput.*, **249** (2014), 356–370. https://doi.org/10.1016/j.amc.2014.10.029

20. Y. Ma, X. Jia, Q. Zhang, Robust finite-time non-fragile memory H_∞ control for discrete-time singular Markovian jumping systems subject to actuator saturation, *J. Franklin Inst.*, **354** (2017), 8256–8282. https://doi.org/10.1016/j.jfranklin.2017.10.019

21. J. Zhang, D. Liu, Y. Ma, P. Yu, Non-fragile H_∞ memory sampled-data state-feedback control for continuous-time nonlinear Markovian jump fuzzy systems with time-varying delay, *Inf. Sci.*, **577** (2021), 214–233. https://doi.org/10.1016/j.ins.2021.06.081

22. R. Sakthivel, O. M. Kwon, S. G. Choi, R. Sakthivel, Observer-based state estimation for discrete-time semi-Markovian jump neural networks with round-robin protocol against cyber attacks, *Neural Networks*, **165** (2023), 611–624. https://doi.org/10.1016/j.neunet.2023.05.046

23. J. Cai, J. Wang, J. Feng, G. Chen, Y. Zhao, Observer-based consensus for multi-agent systems with semi-Markovian jumping via adaptive event-triggered SMC, *IEEE Trans. Network Sci. Eng.*, **10** (2023), 1736–1751. https://doi.org/10.1109/TNSE.2023.3234168

24. L. Zhang, L. He, Y. Song, New results on stability analysis of delayed systems derived from extended Wirtinger's integral inequality, *Neurocomputing*, **283** (2018), 98–106. https://doi.org/10.1016/j.neucom.2017.12.044

25. H. Li, P. Shi, D. Yao, Adaptive sliding-mode control of Markov jump nonlinear systems with actuator faults, *IEEE Trans. Autom. Control*, **62** (2016), 1933–1939. https://doi.org/10.1109/TAC.2016.2588885