SCIENCE CHINA
Information Sciences

• LETTER •

May 2023, Vol. 66 159204:1–159204:2
https://doi.org/10.1007/s11432-020-3238-x

Observer-based event-triggered asynchronous control of networked Markovian jump systems under deception attacks

Xiaobin GAO, Feiqi DENG*, Hongyang ZHANG & Pengyu ZENG

School of Automation Science and Engineering, South China University of Technology, Guangzhou 510641*, China*

Received 25 November 2020/Revised 13 January 2021/Accepted 26 February 2021/Published online 4 November 2022

Citation Gao X B, Deng F Q, Zhang H Y, et al. Observer-based event-triggered asynchronous control of networked Markovian jump systems under deception attacks. Sci China Inf Sci, 2023, 66(5): 159204, https://doi.org/10.1007/s11432-020-3238-x

Dear editor,

Markovian jump systems (MJSs) have been investigated for decades [1, 2]. Most existing results on MJSs assume that the mode switching of the controller/filter is synchronized with the operational system. However, due to time delays, packet dropouts, etc., controller/filter may work asynchronously [3]. In addition, when MJS control components are connected via communication networks, problems associated with information congestion and cybersecurity cannot be ignored [4–6]. To address information congestion issues, an event-triggered mechanism (ETM) is considered as an effective way to save network bandwidth. However, few studies have addressed MJSs under cyberattacks, particularly deception attacks. How to address event-triggered controller design for networked MJSs with deception attacks and asynchronous modes remains challenging. This study provides a solution to this problem.

The primary contributions of this paper are as follows. (1) With the help of a hidden Markov model (HMM), the designed ETM and observer-based controller can function asynchronously, which is more reasonable in practical applications. (2) A neural network (NN) approach is applied to estimate deception attacks, which makes it possible to design the adaptive neural controller. Consequently, the influence of deception attacks can be mitigated effectively.

Problem description. We consider the following MJS:

$$\begin{cases} x(k+1) = A_{r_k}x(k) + B_{r_k}(u(k) + w(k)), \\ y(k) = C_{r_k}x(k), \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^{n_x}$, $u(k) \in \mathbb{R}^{n_u}$ and $y(k) \in \mathbb{R}^{n_y}$ denote the state, control input, and system output, respectively. $w(k)$ is the external disturbance obeying $\|w(k)\| \leqslant w_{\max}$. A_{r_k}, B_{r_k}, and C_{r_k} are known matrices. $\{r_k, k \geqslant 0\}$ is a Markov chain taking values in $\mathcal{L} = \{1, 2, \ldots, N\}$. The transition probability matrix $\pi = \{\pi_{ij}\}$ is defined as follows: $P(r_{k+1} = j | r_k = i) = \pi_{ij}$ with $\pi_{ij} \geqslant 0$ and $\sum_{j=1}^{N} \pi_{ij} = 1$.

To deal with the system state estimation (1), we devise the asynchronous observer:

$$\begin{cases} \hat{x}(k+1) = A_{\tau_k}\hat{x}(k) + B_{\tau_k}u(k) + L_{\tau_k}(\hat{y}(k) - y(k)), \\ \hat{y}(k) = C_{\tau_k}\hat{x}(k), \end{cases} \tag{2}$$

where $\hat{x}(k) \in \mathbb{R}^{n_x}$ is the estimated state, $\hat{y}(k) \in \mathbb{R}^{n_y}$ denotes the estimated output, and L_{τ_k} is the observer gain to be devised later. The process $\tau_k \in \mathcal{S} = \{1, 2, \ldots, M\}$ denotes the HMM that satisfies the conditional probability matrix $\varpi = \{\varpi_{im}\}$ with $P\{\tau_k = m | r_k = i\} = \varpi_{im}$, $i \in \mathcal{L}, m \in \mathcal{S}$, where $0 \leqslant \varpi_{im} \leqslant 1$ and $\sum_{m=1}^{M} \varpi_{im} = 1$.

An asynchronous ETM is adopted to reduce the transmission of unnecessary data. The event-triggered condition is defined as follows:

$$\begin{aligned} & e_{\rm ET}^{\rm T}(k) M_{\tau_k} e_{\rm ET}(k) \geqslant \rho \hat{x}^{\rm T}(k) N_{\tau_k} \hat{x}(k), \\ & k = k_s, \ldots, k_{s+1} - 1, \quad s \in \mathbb{N}, \end{aligned} \tag{3}$$

where $e_{\rm ET}(k) = \hat{x}(k_s) - \hat{x}(k)$, $M_{\tau_k} > 0$ and $N_{\tau_k} > 0$ represent the weighting matrices, and $\rho \in [0, 1)$ is a given scalar. $\{k_s, s \in \mathbb{Z}_{\geqslant 0}\}$ is a triggering instant sequence with $k_0 = 0$.

It is assumed that the channel between the controller and actuator is subject to deception attacks. Then, the control input transmitted to system (1) can be expressed as

$$u(k) = u_a(k) + \Phi(\hat{x}(k_s)), \tag{4}$$

where $\Phi(\hat{x}(k_s))$ is the malicious unknown nonlinear signal, and $u_a(k)$ is the computed control signal to be designed. To estimate and mitigate the effect of deception attacks, we use the NN approach to approximate the false data $\Phi(\hat{x}(k_s))$ with the following expression:

$$\Phi(\hat{x}(k_s)) = W^{\rm T} S(V^{\rm T} \hat{x}(k_s)) + \varepsilon(\hat{x}(k_s)) \tag{5}$$

for all $\hat{x}(k_s) \in \Omega \subset \mathbb{R}^{n_x}$. Here, Ω is a compact set, $W \in \mathbb{R}^{l \times n_u}$ represents the target weight matrix, $S(\cdot) \in \mathbb{R}^l$ is the basis function with $\|S(\cdot)\| \leqslant S_{\max}$, and $V \in \mathbb{R}^{n_x \times l}$ stands for the randomly assigned input weight matrix. The residual error is denoted as $\varepsilon(\cdot) \in \mathbb{R}^{n_u}$ with $\|\varepsilon(\cdot)\| \leqslant \varepsilon_{\max}$, and l is the number of hidden neurons.

* Corresponding author (email: aufdeng@scut.edu.cn)

We construct the NN estimation of $\Phi(\hat{x}(k_s))$ as follows:

$$\hat{\Phi}(\hat{x}(k_s)) = \hat{W}^{\mathrm{T}}(k)S(V^{\mathrm{T}}\hat{x}(k_s)), \tag{6}$$

where $\hat{W}(k) \in \mathbb{R}^{l\times n_u}$ is the NN weight matrix estimate. In this study, the NN weight update law is chosen as

$$\begin{aligned}\hat{W}(k+1) = {} & \hat{W}(k) - \sigma\hat{W}(k)\\ & - \frac{\eta S(V^{\mathrm{T}}\hat{x}(k_s))z^{\mathrm{T}}(k+1)}{1+\|S(V^{\mathrm{T}}\hat{x}(k_s))\|^2\|z(k+1)\|^2},\end{aligned} \tag{7}$$

where

$$z(k+1) = \begin{cases} \Big[\bar{y}^{\mathrm{T}}(k+1), \underbrace{0,\ldots,0}_{n_u - n_y}\Big]^{\mathrm{T}}, & n_u \geqslant n_y,\\ \Big[\bar{y}_1^{\mathrm{T}}(k+1),\ldots,\bar{y}_{n_u}^{\mathrm{T}}(k+1)\Big]^{\mathrm{T}}, & n_u \leqslant n_y,\end{cases}$$

and $\bar{y}(k) = \hat{y}(k) - y(k)$, $\eta > 0$ is the design parameter, and σ denotes the sigma modification term.

Thus, the signal $u_a(k)$ in (4) can be designed as

$$u_a(k) = K_{\tau_k}\hat{x}(k_s) - \hat{\Phi}(\hat{x}(k_s)). \tag{8}$$

For simplicity, let $r_k = i$, and $\tau_k = m$. Then, the closed-loop system can be obtained as the following compact form:

$$\begin{cases} \bar{x}(k+1) = \bar{A}_{im}\bar{x}(k) + \bar{B}_{im}e_{\mathrm{ET}}(k) + \bar{H}_{im}(\tilde{W}^{\mathrm{T}}(k)\\ \qquad\qquad \times S(V^{\mathrm{T}}\hat{x}(k_s)) - \varepsilon(\hat{x}(k_s)) - w(k)),\\ \bar{y}(k) = C_{im}\bar{x}(k), \end{cases} \tag{9}$$

where

$$\begin{aligned}
&\bar{x}(k) = [x^{\mathrm{T}}(k) \quad e_{OB}^{\mathrm{T}}(k)]^{\mathrm{T}}, \quad \bar{y}(k) = \hat{y}(k) - y(k),\\
&\bar{A}_{im} = \begin{bmatrix}\bar{A}_{im}^{11} & \bar{A}_{im}^{12}\\ \bar{A}_{im}^{21} & \bar{A}_{im}^{22}\end{bmatrix}, \quad \bar{B}_{im} = \begin{bmatrix} B_iK_m\\ (B_m - B_i)K_m\end{bmatrix},\\
&\bar{H}_{im} = \begin{bmatrix} -B_i\\ B_i - B_m\end{bmatrix}, \quad \bar{C}_{im} = \begin{bmatrix} C_m - C_i & C_m\end{bmatrix},\\
&\bar{A}_{im}^{11} = A_i + B_iK_m, \quad \bar{A}_{im}^{12} = B_iK_m,\\
&\bar{A}_{im}^{21} = A_m - A_i + (B_m - B_i)K_m + L_m(C_m - C_i),\\
&\bar{A}_{im}^{22} = A_m + (B_m - B_i)K_m + L_mC_m,
\end{aligned}$$

and $\tilde{W}(k) = \hat{W}(k) - W$ is the weight estimate error.

Some preliminaries are provided in Appendix A.

Our main results are listed as follows.

Lemma 1. Consider the NN weight estimate dynamics (7) with bounded initial weight estimation $\hat{W}(0)$. Then for $\frac{1}{4\gamma} < \sigma < 1$, $\gamma > 1$, and $\eta > 0$, the NN weight estimation error $\tilde{W}(k)$ is bounded in probability.

The proof of Lemma 1 is given in Appendix B.

Theorem 1. Consider the system (9) subject to deception attacks and unmeasured states. Given $0 \leqslant \rho < 1$, if there exist matrices $P_i > 0$, $\bar{P}_i > 0$, and R_{im}, scalars $0 < \kappa < 1$, $\lambda_1 > 0$, and $\mu > 0$, such that $\forall i \in \mathcal{L}$, $m \in \mathcal{S}$,

$$\sum_{m=1}^{M}\varpi_{im}R_{im} < P_i, \tag{10}$$

$$\begin{bmatrix} 2\bar{A}_{im}^{\mathrm{T}}\bar{P}_i\bar{A}_{im} + \rho\bar{N}_{1m} - R_{im} & \rho\bar{N}_{2m}\\ * & 4\bar{B}_{im}^{\mathrm{T}}\bar{P}_i\bar{B}_{im} - M_m\end{bmatrix} < 0, \tag{11}$$

$$12\sup_{i\in\mathcal{L},m\in\mathcal{S}}\Big\{\lambda_{\max}(\bar{H}_{im}^{\mathrm{T}}\bar{P}_i\bar{H}_{im})\Big\}S_{\max}^2 - \mu\kappa < 0 \tag{12}$$

hold, where

$$\bar{N}_{1m} = \begin{bmatrix} N_m & N_m\\ * & N_m\end{bmatrix}, \quad \bar{N}_{2m} = \begin{bmatrix} N_m\\ N_m\end{bmatrix},$$

then, with bounded initial values, the closed-loop system (9) is bounded in probability.

The proof of Theorem 1 is given in Appendix C. Stability analysis of networked MJSs under deception attacks is provided in Theorem 1.

The observer-based controller design problem and simulation results are shown in Appendixes D and E, respectively.

Conclusion. In this study, we have investigated the observer-based event-triggered asynchronous control problem for networked MJSs under deception attacks and external disturbances. Based on the HMM modeling approach, the proposed ETM and observer can run asynchronously. Employing an NN technique reduces the influence of malicious deception attacks and external disturbances. The boundedness in probability of the closed-loop system has been guaranteed by a series of sufficient conditions. Note that the proposed method can be extended to more complex systems, such as nonlinear time-varying stochastic systems [7] and semi-Markov jump systems [8], which is extremely interesting and worthy of further study.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 62073144, 61873099, 61733008), Natural Science Foundation of Guangdong Province (Grant No. 2020A1515010441), and Guangzhou Science and Technology Planning Project (Grant Nos. 202002030389, 202002030158).

Supporting information Appendixes A–E. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Yang D, Zong G D, Su S F. H_∞ tracking control of uncertain Markovian hybrid switching systems: a fuzzy switching dynamic adaptive control approach. IEEE Trans Cybern, 2022, 52: 3111–3122

2 Wang J, Xia J W, Shen H, et al. H_∞ synchronization for fuzzy Markov jump chaotic systems with piecewise-constant transition probabilities subject to PDT switching rule. IEEE Trans Fuzzy Syst, 2021, 29: 3082–3092

3 Wu Z G, Shi P, Shu Z, et al. Passivity-based asynchronous control for markov jump systems. IEEE Trans Automat Contr, 2017, 62: 2020–2025

4 Liu L, Ma L F, Zhang J, et al. Sliding mode control for nonlinear Markovian jump systems under denial-of-service attacks. IEEE/CAA J Autom Sin, 2020, 7: 1638–1648

5 Yang Y, Li Y F, Yue D. Event-trigger-based consensus secure control of linear multi-agent systems under DoS attacks over multiple transmission channels. Sci China Inf Sci, 2020, 63: 150208

6 Zong G D, Ren H L, Karimi H R. Event-triggered communication and annular finite-time H_∞ filtering for networked switched systems. IEEE Trans Cybern, 2021, 51: 309–317

7 Ma L F, Wang Z D, Hu J, et al. Probability-guaranteed envelope-constrained filtering for nonlinear systems subject to measurement outliers. IEEE Trans Automat Contr, 2021, 66: 3274–3281

8 Liu Y A, Xia J W, Meng B, et al. Extended dissipative synchronization for semi-Markov jump complex dynamic networks via memory sampled-data control scheme. J Franklin Inst, 2020, 357: 10900–10920