SCIENCE CHINA
Information Sciences

• LETTER •

September 2023, Vol. 66 190207:1–190207:2
https://doi.org/10.1007/s11432-022-3684-x

Special Topic: Control, Optimization, and Learning for Networked Systems

Iterative learning security control for discrete-time systems subject to deception and DoS attacks

Wenjun XIONG[1], Zijian LUO[1], Guanghui WEN[2*] & Tao YANG[3]

[1]*School of Computing and Artificial Intelligence, Southwestern University of Finance and Economics, Chengdu* 611130*, China;*
[2]*Department of Systems Science, School of Mathematics, Southeast University, Nanjing* 211189*, China;*
[3]*State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang* 110819*, China*

Received 28 July 2022/Revised 4 November 2022/Accepted 4 January 2023/Published online 17 August 2023

Citation Xiong W J, Luo Z J, Wen G H, et al. Iterative learning security control for discrete-time systems subject to deception and DoS attacks. Sci China Inf Sci, 2023, 66(9): 190207, https://doi.org/10.1007/s11432-022-3684-x

Malicious cyber-attacks often occur in cyberspace during the signal transmission process. It might result in data dropout and system failure. This problem then draws attention to secure control, and a number of security control protocols are proposed [1–3].

In reality, the co-existence of multiple cyber-attacks increases the difficulty of the theoretical analysis. Furthermore, some sufficient conditions for achieving security are difficult to check when the dimension of the model is high. As a result, the applicable approaches are needed for analyzing and obtaining some concise conditions.

In contrast to the traditional tracking control methods, iterative learning control (ILC) technology provides an effective approach to achieve system targets. Such a control method has been applied in urban road networks [4] and security analysis [5]. Until now, the research on ILC still attracts the interest of the control science and engineering communities.

When deception and DoS attacks occur alternately, it is difficult to obtain the actual output of the system as the attacks may falsify the observations. To achieve system security, an output estimation formula under the DoS and deception attacks is proposed in this study. Furthermore, the appropriate ILC algorithms are designed based on the output estimation formula.

The following are the main contributions of this study: (1) The system security problem is investigated under the deception and DoS attacks. A novel output estimation formula is proposed to evaluate the unavailable measurement of the real output. (2) System security is achieved by using ILC strategies, and our schemes ensure that the system trajectory is bounded. (3) Compared with the existing literature, the present ILC strategies are simple and can be easily checked in practice.

Notations. $x = [x_1, \ldots, x_n]^{\mathrm{T}}$ and $y = [y_1, \ldots, y_n]^{\mathrm{T}}$ are two real vectors, and symbol T denotes transpose. The partial order relation $\prec$ is defined as $x \prec y$ if and only if $x_i \leqslant y_i$ for all $i \in \{1, \ldots, n\}$. $\|x\|$ represents the norm of vector x. $\|A\|$ denotes the matrix norm of matrix A. The zero matrix is defined as $\boldsymbol{O}$, and the unit matrix is described by I. $\mathbb{E}(\cdot)$ is the mathematical expectation of a stochastic vector. $\mathcal{T} = \{1, \ldots, l\}$ is the time interval, and l is the fixed terminal time.

Problem formulation. A discrete-time system is

$$\begin{cases} x_k(t+1) = Ax_k(t) + Bu_k(t), & t \in \mathcal{T} \setminus \{l\}, \\ y_k(t) = Cx_k(t) + Du_k(t), & t \in \mathcal{T}, \end{cases} \tag{1}$$

where k represents the kth iteration process. $x_k(t)$, $u_k(t)$, $y_k(t)$ are the state vector, input vector, and output vector, respectively. Matrices A, B, C, and D in (1) are with appropriate dimensions. Furthermore, two output modes are considered in this study, i.e., $D = \boldsymbol{O}$ and $D \neq \boldsymbol{O}$.

Inspired by [2], we consider the following impact pattern of random deception and DoS attacks:

$$\hat{y}_k(t) = y_k(t) + \alpha_{k,t}\beta_{k,t}\mu_k(t) + \alpha_{k,t}(1-\beta_{k,t})\nu_k(t), \tag{2}$$

where $\hat{y}_k(t)$ is the received signal by the observer subject to attacks. $\mu_k(t)$ and $\nu_k(t)$ denote the deception attack and the DoS attack, respectively. The deception attack is described as

$$\mu_k(t) = -y_k(t) + \xi_k(t), \tag{3}$$

where $\xi_k(t)$ is a bounded signal, $\|\xi_k(t)\| \leqslant \xi_b$, $\xi_b > 0$. The DoS attack mode is

$$\nu_k(t) = -y_k(t). \tag{4}$$

Bernoulli stochastic variables $\alpha_{k,t}$ and $\beta_{k,t}$ in (2) are mutually uncorrelated and satisfy

$$\mathrm{Prob}\{\alpha_{k,t} = 1\} = \mathbb{E}(\alpha_{k,t}) = \bar{\alpha}, \quad 0 \leqslant \bar{\alpha} < 1,$$
$$\mathrm{Prob}\{\beta_{k,t} = 1\} = \mathbb{E}(\beta_{k,t}) = \bar{\beta}, \quad 0 \leqslant \bar{\beta} < 1,$$

where $\bar{\alpha}$ and $\bar{\beta}$ are two known constants. Moreover, α_{k_1,t_1} and α_{k_2,t_2} are mutually independent for all $k_1 \neq k_2$ and t_1, $t_2 \in \mathcal{T}$, and so is $\beta_{k,t}$. From (2)–(4), one obtains

$$\hat{y}_k(t) = (1-\alpha_{k,t})y_k(t) + \alpha_{k,t}\beta_{k,t}\xi_k(t). \tag{5}$$

* Corresponding author (email: ghwen@seu.edu.cn)

Define the tracking error as $e_k(t) = y_d(t) - y_k(t)$, where $y_d(t)$ is the desired output. However, the real output series $\{y_k(t)\}$ might not be directly obtained due to cyber attacks. Thus, the tracking target is difficult to be achieved. Then, the desired output is applied to compensate for the incorrect output. The estimation output is designed as

$$\check{y}_k(t) = \hat{y}_k(t) + \alpha_{k,t} y_d(t), \tag{6}$$

and the available tracking error is $\check{e}_k(t) = y_d(t) - \check{y}_k(t)$. For system (1), the ILC strategy is constructed as

$$u_{k+1}(t) = u_k(t) + \mathcal{K}_1 \check{e}_k(t) + \mathcal{K}_2 \check{e}_k(t+1), \tag{7}$$

where $\mathcal{K}_1$ and $\mathcal{K}_2$ are learning gains, and the initial input $u_0(t)$ is chosen arbitrarily.

Definition 1. Let the desired security level be specified as $\sigma > 0$. The repetitive discrete-time system (1) is said to have the σ-secure in the meaning sense if the inequality $\lim_{k\to\infty} \mathbb{E}(\|e_k(t)\|) \leqslant \sigma$ holds for $t \in \mathcal{T}$.

Our purpose is to analyze the security of the system in line with Definition 1 and ILC protocol (7). The following assumptions are required.

Assumption 1. Each iteration's initial state is fixed, i.e., $x_k(0) = x_{k+1}(0)$.

Assumption 2. For any desired output $y_d(t)$ and system (1) with $D \neq \boldsymbol{O}$, there exist desired state $x_d(t)$ and bounded desired input $u_d(t)$ such that

$$\begin{cases} x_d(t+1) = Ax_d(t) + Bu_d(t), & t \in \mathcal{T} \setminus \{l\}, \\ y_d(t) = Cx_d(t) + Du_d(t), & t \in \mathcal{T}. \end{cases} \tag{8}$$

Robust convergence and boundedness analysis. The following section studies the robust convergence and boundedness of system trajectories.

Theorem 1. Letting Assumptions 1 and 2 hold, ILC strategy (7) with $\mathcal{K}_2 = \boldsymbol{O}$ is applied to system (1), where $D \neq \boldsymbol{O}$. Then, the σ-secure is achieved if the inequality $\|I - \mathcal{K}_1 D\| < 1$ holds.

Theorem 2. Letting Assumptions 1 and 2 hold, ILC strategy (7) with $\mathcal{K}_2 = \boldsymbol{O}$ is applied to system (1), where $D \neq \boldsymbol{O}$. If the inequality $\|I - \mathcal{K}_1 D\| < 1$ holds, one has $\sup_{k\in Z_+, t\in\mathcal{T}} \mathbb{E}(\|x_k(t)\|) \leqslant \mathcal{B}_x$, $\sup_{k\in Z_+, t\in\mathcal{T}} \mathbb{E}(\|u_k(t)\|) \leqslant \mathcal{B}_u$, $\sup_{k\in Z_+, t\in\mathcal{T}} \mathbb{E}(\|y_k(t)\|) \leqslant \mathcal{B}_y$, $\sup_{k\in Z_+, t\in\mathcal{T}} \mathbb{E}(\|e_k(t)\|) \leqslant \mathcal{B}_e$, where $\mathcal{B}_x \geqslant 0$, $\mathcal{B}_u \geqslant 0$, $\mathcal{B}_y \geqslant 0$, and $\mathcal{B}_e \geqslant 0$ are finite constants.

Theorem 3. Letting Assumption 1 hold, ILC strategy (7) with $\mathcal{K}_1 = \boldsymbol{O}$ is applied to system (1), where $D = \boldsymbol{O}$. Then, the σ-secure is achieved if the inequality $\|I - CB\mathcal{K}_2\| < 1$ holds.

Theorem 4. Letting Assumption 1 hold, ILC strategy (7) with $\mathcal{K}_1 = \boldsymbol{O}$ is applied to system (1), where $D = \boldsymbol{O}$. If the inequality $\|I - \mathcal{K}_2 CB\| < 1$ holds, one has $\sup_{k\in Z_+, t\in\mathcal{T}} \mathbb{E}(\|x_k(t)\|) \leqslant \tilde{\mathcal{B}}_x$, $\sup_{k\in Z_+, t\in\mathcal{T}} \mathbb{E}(\|u_k(t)\|) \leqslant \tilde{\mathcal{B}}_u$, $\sup_{k\in Z_+, t\in\mathcal{T}} \mathbb{E}(\|y_k(t)\|) \leqslant \tilde{\mathcal{B}}_y$, and $\sup_{k\in Z_+, t\in\mathcal{T}} \mathbb{E}(\|e_k(t)\|) \leqslant \tilde{\mathcal{B}}_e$, where $\tilde{\mathcal{B}}_x \geqslant 0$, $\tilde{\mathcal{B}}_u \geqslant 0$, $\tilde{\mathcal{B}}_y \geqslant 0$, and $\tilde{\mathcal{B}}_e \geqslant 0$ are finite constants.

The proofs of theorems are provided in Appendixes A–D. Appendix E contains a simulation example.

Remark 1. Compared with one type of attack in [1, 5], the co-existence of two attacks in this study increases the difficulty of the theoretical analysis. Therefore, it is difficult to obtain the actual output of the system because the two attacks might falsify the observations. As a result, ILC strategies are proposed to address this difficulty.

Acknowledgements This work was jointly supported by National Natural Science Foundation of China (Grant Nos. 61873344, U22B2046, 62073079, 62088101), General Joint Fund of the Equipment Advance Research Program of Ministry of Education (Grant No. 8091B022114), and Fundamental Research Funds for the Central Universities (Grant No. JBK190502).

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 Zhao D, Wang Z, Wei G, et al. A dynamic event-triggered approach to observer-based PID security control subject to deception attacks. Automatica, 2020, 120: 109128
2 Zhao D, Wang Z D, Ho D W C, et al. Observer-based PID security control for discrete time-delay systems under cyber-attacks. IEEE Trans Syst Man Cybern Syst, 2021, 51: 3926–3938
3 Guo L, Cui T T, Yu H, et al. Stability of networked control system subject to denial-of-service. Sci China Inf Sci, 2021, 64: 129203
4 Yan F, Tian F L, Shi Z K. Iterative learning approach for traffic signal control of urban road networks. IET Control Theor Appl, 2017, 11: 466–475
5 Xiong W J, Gong K, Wen G H, et al. Security analysis of discrete nonlinear systems with injection attacks under iterative learning schemes. IEEE Trans Syst Man Cybern Syst, 2022, 52: 927–935