SCIENCE CHINA
Information Sciences

• **Supplementary File** •

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*

Appendix A Proof of Theorem 1

Proof. Let $\delta x_k(t) = x_d(t) - x_k(t)$ and $\delta u_k(t) = u_d(t) - u_k(t)$. From Assumption 2 and system (1), one can obtain $e_k(t) = y_d(t) - y_k(t) = C\delta x_k(t) + D\delta u_k(t)$, $\delta x_k(t+1) = A\delta x_k(t) + B\delta u_k(t)$.

With Assumption 1, one obtains

$$\begin{aligned}\delta x_k(t) &= A\delta x_k(t-1) + B\delta u_k(t-1)\\ &= A^2\delta x_k(t-2) + AB\delta u_k(t-2) + B\delta u_k(t-1)\\ &= \cdots\cdots\\ &= \sum_{i=0}^{t-1} A^i B\delta u_k(t-1-i), \quad t > 1.\end{aligned} \tag{A1}$$

From ILC strategy (7) with $\mathcal{K}_2 = \mathbf{O}$, one has

$$\begin{aligned}\delta u_{k+1}(t) &= u_d(t) - u_k(t) + u_k(t) - u_{k+1}(t)\\ &= \delta u_k(t) - [u_{k+1}(t) - u_k(t)]\\ &= \delta u_k(t) - \mathcal{K}_1[y_d(t) - \breve{y}_k(t)].\end{aligned} \tag{A2}$$

Linking with (6) and (A1), Eq. (A2) becomes

$$\begin{aligned}\delta u_{k+1}(t) &= \delta u_k(t) - \mathcal{K}_1[y_d(t) - (1-\alpha_{k,t})y_k(t) - \alpha_{k,t}\beta_{k,t}\xi_k(t) - \alpha_{k,t}y_d(t)]\\ &= \delta u_k(t) - \mathcal{K}_1[(1-\alpha_{k,t})e_k(t) - \alpha_{k,t}\beta_{k,t}\xi_k(t)]\\ &= \delta u_k(t) - \mathcal{K}_1[(1-\alpha_{k,t})(C\delta x_k(t) + D\delta u_k(t)) - \alpha_{k,t}\beta_{k,t}\xi_k(t)]\\ &= [I - (1-\alpha_{k,t})\mathcal{K}_1 D]\delta u_k(t) - (1-\alpha_{k,t})\mathcal{K}_1 C\delta x_k(t) + \mathcal{K}_1\alpha_{k,t}\beta_{k,t}\xi_k(t)\\ &= [I - (1-\alpha_{k,t})\mathcal{K}_1 D]\delta u_k(t) - (1-\alpha_{k,t})\mathcal{K}_1 C\sum_{i=0}^{t-1} A^i B\delta u_k(t-1-i) + \mathcal{K}_1\alpha_{k,t}\beta_{k,t}\xi_k(t).\end{aligned} \tag{A3}$$

Taking norm on both sides of (A3), one has

$$\begin{aligned}\|\delta u_{k+1}(t)\| \leqslant\ & \|I - (1-\alpha_{k,t})\mathcal{K}_1 D\|\|\delta u_k(t)\| + (1-\alpha_{k,t})\sum_{i=0}^{t-1}\|\mathcal{K}_1 CA^i B\|\|\delta u_k(t-1-i)\|\\ & +\alpha_{k,t}\beta_{k,t}\|\mathcal{K}_1\|\|\xi_k(t)\|.\end{aligned}$$

Further, it is not difficult to get

$$\begin{aligned}\mathbb{E}(\|\delta u_{k+1}(t)\|) \leqslant\ & \mathbb{E}(\|I - (1-\alpha_{k,t})\mathcal{K}_1 D\|)\mathbb{E}(\|\delta u_k(t)\|) + (1-\bar{\alpha})\sum_{i=0}^{t-1}\|\mathcal{K}_1 CA^i B\|\mathbb{E}(\|\delta u_k(t-1-i)\|)\\ & +\bar{\alpha}\bar{\beta}\|\mathcal{K}_1\|\mathbb{E}(\|\xi_k(t)\|).\end{aligned} \tag{A4}$$

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

Since $\alpha_{k,t}$ is Bernoulli stochastic variables, $\|I-(1-\alpha_{k,t})\mathcal{K}_1D\|=1$ if $\alpha_{k,t}=1$, $\|I-(1-\alpha_{k,t})\mathcal{K}_1D\|=\|I-\mathcal{K}_1D\|$ if $\alpha_{k,t}=0$. Thus, $\mathbb{E}(\|I-(1-\alpha_{k,t})\mathcal{K}_1D\|)=\bar{\alpha}\times 1+(1-\bar{\alpha})\times\|I-\mathcal{K}_1D\|$. Note $\|I-\mathcal{K}_1D\|<1$, one knows $\mathbb{E}(\|I-(1-\alpha_{k,t})\mathcal{K}_1D\|):=\psi<1$. Linking with $\|\xi_k(t)\|\leqslant\xi_b$, (A4) becomes

$$\mathbb{E}(\|\delta u_{k+1}(t)\|)\ \leqslant\ \psi\mathbb{E}(\|\delta u_k(t)\|)+(1-\bar{\alpha})\sum_{i=0}^{t-1}\|\mathcal{K}_1CA^iB\|\mathbb{E}(\|\delta u_k(t-1-i)\|)+\bar{\alpha}\bar{\beta}\|\mathcal{K}_1\|\xi_b. \tag{A5}$$

According to (A5), one gets

$$\underbrace{\begin{bmatrix}\mathbb{E}(\|\delta u_{k+1}(0)\|)\\ \mathbb{E}(\|\delta u_{k+1}(1)\|)\\ \vdots\\ \mathbb{E}(\|\delta u_{k+1}(l)\|)\end{bmatrix}}_{E_{k+1}}\prec\ \Psi_1\underbrace{\begin{bmatrix}\mathbb{E}(\|\delta u_k(0)\|)\\ \mathbb{E}(\|\delta u_k(1)\|)\\ \vdots\\ \mathbb{E}(\|\delta u_k(l)\|)\end{bmatrix}}_{E_k}+\underbrace{\begin{bmatrix}\bar{\alpha}\bar{\beta}\|\mathcal{K}_1\|\xi_b\\ \bar{\alpha}\bar{\beta}\|\mathcal{K}_1\|\xi_b\\ \vdots\\ \bar{\alpha}\bar{\beta}\|\mathcal{K}_1\|\xi_b\end{bmatrix}}_{M_\xi}, \tag{A6}$$

where the matrix Ψ_1 is

$$\Psi_1=\begin{bmatrix}\psi & 0 & \cdots & 0\\ (1-\bar{\alpha})\|\mathcal{K}_1CB\| & \psi & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ (1-\bar{\alpha})\|\mathcal{K}_1CA^{l-1}B\| & (1-\bar{\alpha})\|\mathcal{K}_1CA^{l-2}B\| & \cdots & \psi\end{bmatrix}. \tag{A7}$$

From (A6), by using induction, one gets

$$\begin{aligned}E_{k+1}\ &\prec\ \Psi_1E_k+M_\xi\prec\Psi_1^2E_{k-1}+(\Psi_1+I)M_\xi\prec\cdots\\ &\prec\ \Psi_1^{k+1}E_0+\sum_{i=1}^{k}\Psi_1^iM_\xi,\end{aligned} \tag{A8}$$

where $\Psi_1^i=\underbrace{\Psi_1\times\cdots\times\Psi_1}_{i}$. Due to $\psi<1$, one knows $\rho(\Psi_1)<1$. This implies $\lim\limits_{k\to\infty}\Psi_1^{k+1}E_0=\mathbf{0}$, $\mathbf{0}$ represents the zero vector. Meanwhile, the matrix series $\sum_{i=1}^{k}\Psi_1^i$ is absolute convergence according to the matrix theory. It means that $\sum_{i=1}^{\infty}\Psi_1^iM_\xi=\tilde{\Psi}_1M_\xi$. Hence, $\lim\limits_{k\to\infty}E_{k+1}\prec\tilde{\Psi}_1M_\xi$, i.e. $\forall\ t\in\mathcal{T}$, $\lim\limits_{k\to\infty}\mathbb{E}(\|\delta u_k(t)\|)\leqslant\mathcal{M}_{\delta u}$, $\mathcal{M}_{\delta u}$ is the maximum element in vector $\tilde{\Psi}_1M_\xi$. For $t\in\mathcal{T}\setminus\{0\}$, from (A1), one obtains

$$\begin{aligned}\lim_{k\to\infty}\mathbb{E}(\|\delta x_k(t)\|)\ &\leqslant\ \lim_{k\to\infty}\sum_{i=0}^{t-1}\|A^iB\|\mathbb{E}(\|\delta u_k(t-1-i)\|)\\ &\leqslant\ \sum_{i=0}^{t-1}\|A\|^i\|B\|\mathcal{M}_{\delta u}\leqslant\mathcal{M}_A\|B\|\mathcal{M}_{\delta u}\end{aligned}$$

where $\mathcal{M}_A=\frac{1-\|A\|^l}{1-\|A\|}$ as $\|A\|\neq 1$ or $\mathcal{M}_A=l+1$ as $\|A\|=1$. Therefore,

$$\begin{aligned}\lim_{k\to\infty}\mathbb{E}(\|e_k(t)\|)\ &\leqslant\ \|C\|\lim_{k\to\infty}\mathbb{E}(\|\delta x_k(t)\|)+\|D\|\lim_{k\to\infty}\mathbb{E}(\|\delta u_k(t)\|)\\ &\leqslant\ (\mathcal{M}_A\|C\|\|B\|+\|D\|)\mathcal{M}_{\delta u}.\end{aligned} \tag{A9}$$

Let $\sigma=(\mathcal{M}_A\|C\|\|B\|+\|D\|)\mathcal{M}_{\delta u}$, according to Definition 1, the σ-secure is achieved.

Remark 1. Theorem 1 illustrates our ILC strategy can effectively achieve the system security. Compared with the lifting technique in [1], the partial order relation approach is used in the theoretical analysis, which can reduce the conservatism of convergence results. As a result, the convergence condition in Theorem 1 is simpler than that in [1]. Moreover, Theorem 1 is the same as the traditional result when $\alpha_{k,t}=0$. That is, our strategy is an extension of the traditional lifting technique.

Appendix B Proof of Theorem 2

Proof. According to the fourth equality of (A3), one can derive

$$\mathbb{E}(\|\delta u_{k+1}(t)\|)\ \leqslant\ \psi\mathbb{E}(\|\delta u_k(t)\|)+\phi_k(t), \tag{B1}$$

where $\psi:=\mathbb{E}(\|I-(1-\alpha_{k,t})\mathcal{K}_1D\|)<1$ and $\phi_k(t)=(1-\bar{\alpha})\|\mathcal{K}_1C\|\mathbb{E}(\|\delta x_k(t)\|)+\bar{\alpha}\bar{\beta}\|\mathcal{K}_1\|\xi_b$. The induction method of Theorem 1 in [2] is applied in the following.

Step 1. Let $t=0$, we have $\mathbb{E}(\|\delta x_k(t)\|)=0\leqslant b_x(0)$, $b_x(0)\geqslant 0$ from Assumption 1, and $\phi_k(0)=\bar{\alpha}\bar{\beta}\|\mathcal{K}_1\|\xi_b$. According to the Lemma 2 in [2], then $\sup\limits_{k\in Z_+}\mathbb{E}(\|\delta u_k(0)\|)\leqslant b_u(0)$, $b_u(0)\geqslant 0$. The desired input $u_d(t)$ is bounded, then $\mathbb{E}(\|u_k(0)\|)\leqslant\mathbb{E}(\|\delta u_k(0)\|)+\mathbb{E}(\|u_d(0)\|)$ is also bounded. As a result, $\sup\limits_{k\in Z_+}\mathbb{E}(\|u_k(0)\|)\leqslant b_u(0)+\sup\limits_{k\in Z_+}\mathbb{E}(\|u_d(0)\|):=\mathcal{B}_u(0)$. Similarly, it is not difficult to get $\mathbb{E}(\|x_k(0)\|)\leqslant\mathcal{B}_x(0)$.

Step 2. For any $t > 0$, we assume that $\sup_{k\in Z_+} \mathbb{E}(\|\delta x_k(t)\|) \leqslant b_x(t)$ and $\sup_{k\in Z_+} \mathbb{E}(\|\delta u_k(t)\|) \leqslant b_u(t)$ for some bounds $b_x(t) \geqslant 0$ and $b_u(t) \geqslant 0$. Since $\mathbb{E}(\|u_k(t)\|) \leqslant \mathbb{E}(\|\delta u_k(t)\|) + \mathbb{E}(\|u_d(t)\|)$, one obtains $\sup_{k\in Z_+} \mathbb{E}(\|u_k(t)\|) \leqslant b_u(t) + \sup_{k\in Z_+} \mathbb{E}(\|u_d(t)\|) := \mathcal{B}_u(t)$. Further, one can get $\sup_{k\in Z_+} \mathbb{E}(\|x_k(t)\|) \leqslant \mathcal{B}_x(t)$ according to system (1).

Next, we prove $\mathbb{E}(\|x_k(t+1)\|) \leqslant \mathcal{B}_x(t+1)$ and $\sup_{k\in Z_+} \mathbb{E}(\|u_k(t+1)\|) \leqslant \mathcal{B}_u(t+1)$ for some bounds $\mathcal{B}_x(t+1) \geqslant 0$ and $\mathcal{B}_u(t+1) \geqslant 0$. From system (1) and Assumption 2, one derives that

$$\begin{aligned} \mathbb{E}(\|\delta x_k(t+1)\|) &\leqslant \|A\|\mathbb{E}(\|\delta x_k(t)\|) + \|B\|\mathbb{E}(\|\delta u_k(t)\|) \\ &\leqslant \|A\|b_x(t) + \|B\|b_u(t) \\ &:= b_x(t+1), \quad \forall\ k \in Z_+. \end{aligned} \tag{B2}$$

Combing (B1) with (B2), one has

$$\begin{aligned} \mathbb{E}(\|\delta u_{k+1}(t+1)\|) &\leqslant \psi\mathbb{E}(\|\delta u_k(t+1)\|) + (1-\bar{\alpha})\|\mathcal{K}_1 C\|\mathbb{E}(\|\delta x_k(t+1)\|) + \bar{\alpha}\bar{\beta}\|\mathcal{K}_1\|\xi_b \\ &\leqslant \psi\mathbb{E}(\|\delta u_k(t+1)\|) + \phi_k(t+1), \end{aligned} \tag{B3}$$

where $\phi_k(t+1) = (1-\bar{\alpha})\|\mathcal{K}_1 C\|\mathbb{E}(\|\delta x_k(t+1)\|) + \bar{\alpha}\bar{\beta}\|\mathcal{K}_1\|\xi_b$. According to the result of Lemma 2 in [2], one knows $\sup_{k\in Z_+} \mathbb{E}(\|\delta u_k(t+1)\|) \leqslant b_u(t+1)$. Then, one derives $\sup_{k\in Z_+} \mathbb{E}(\|u_k(t+1)\|) \leqslant b_u(t+1) + \sup_{k\in Z_+} \mathbb{E}(\|u_d(t+1)\|) := \mathcal{B}_u(t+1)$, and $\sup_{k\in Z_+} \mathbb{E}(\|x_k(t+1)\|) \leqslant \mathcal{B}_x(t+1)$. By induction, one can conclude $\sup_{k\in Z_+} \mathbb{E}(\|u_k(t)\|) \leqslant \mathcal{B}_u(t)$, $\forall\ t \in \mathcal{T} \setminus \{l\}$ and $\sup_{k\in Z_+} \mathbb{E}(\|x_k(t)\|) \leqslant \mathcal{B}_x(t)$, $\forall\ t \in \mathcal{T}$ for some bounded $\mathcal{B}_u(t) \geqslant 0$ and $\mathcal{B}_x(t) \geqslant 0$. Thus, one can see the result in Theorem 2 holds as $\mathcal{B}_u = \max_{t\in\mathcal{T}^-} \mathcal{B}_u(t)$ and $\mathcal{B}_x = \max_{t\in\mathcal{T}} \mathcal{B}_x(t)$.

Furthermore, according to system (1) and the result in Theorem 2, one has

$$\begin{aligned} \mathbb{E}(\|y_k(t)\|) &\leqslant \|C\|\mathbb{E}(\|x_k(t)\|) + \|D\|\mathbb{E}(\|u_k(t)\|) \\ &\leqslant \|C\|\mathcal{B}_x(t) + \|D\|\mathcal{B}_u(t) \\ &\leqslant \|C\|\mathcal{B}_x + \|D\|\mathcal{B}_u := \mathcal{B}_y, \end{aligned} \tag{B4}$$

which means $\sup_{k\in Z_+, t\in\mathcal{T}} \mathbb{E}(\|y_k(t)\|) \leqslant \mathcal{B}_y$. In addition, according to $e_k(t) = y_d(t) - y_k(t) = C\delta x_k(t) + D\delta u_k(t)$, one can get $\sup_{k\in Z_+, t\in\mathcal{T}} \mathbb{E}(\|e_k(t)\|) \leqslant \mathcal{B}_e$. Thus, Theorem 2 is proved.

Remark 2. Compared with Theorem 1 in [2], Theorem 2 provides the boundedness results under the deception and DoS attacks, which has a wilder application. Also, the convergence condition of Theorem 2 is easier to be satisfied than condition (5) of Theorem 1 in [2].

Appendix C Proof of Theorem 3

Proof. From system (1), one has

$$\begin{aligned} e_{k+1}(t) &= y_d(t) - y_{k+1}(t) \\ &= y_d(t) - y_k(t) - [y_{k+1}(t) - y_k(t)] \\ &= e_k(t) - C[x_{k+1}(t) - x_k(t)]. \end{aligned} \tag{C1}$$

Then, we tackle with $\Delta x_k(t) := x_{k+1}(t) - x_k(t)$.

$$\begin{aligned} \Delta x_k(t) &= A[x_{k+1}(t-1) - x_k(t-1)] + B\mathcal{K}_2[y_d(t) - y_k(t) + y_k(t) - \breve{y}_k(t)] \\ &= A\Delta x_k(t-1) + B\mathcal{K}_2 e_k(t) + B\mathcal{K}_2[y_k(t) - \breve{y}_k(t)]. \end{aligned} \tag{C2}$$

Substituting (C2) into (C1), one has

$$e_{k+1}(t) = [I - CB\mathcal{K}_2]e_k(t) - CA\Delta x_k(t-1) - CB\mathcal{K}_2[y_k(t) - \breve{y}_k(t)]. \tag{C3}$$

From (6), one knows $y_k(t) - \breve{y}_k(t) = -\alpha_{k,t}\beta_{k,t}\xi_k(t) - \alpha_{k,t}e_k(t)$. Then (C3) becomes

$$e_{k+1}(t) = [I - (1-\alpha_{k,t})CB\mathcal{K}_2]e_k(t) - CA\Delta x_k(t-1) + \alpha_{k,t}\beta_{k,t}CB\mathcal{K}_2\xi_k(t). \tag{C4}$$

By using induction analysis, (C4) is rewritten as

$$\begin{aligned} e_{k+1}(t) = {} & [I - (1-\alpha_{k,t})CB\mathcal{K}_2]e_k(t) - \sum_{i=0}^{t-1}(1-\alpha_{k,t-1-i})CA^{i+1}B\mathcal{K}_2 e_k(t-1-i) \\ & + \sum_{i=0}^{t}\alpha_{k,t-i}\beta_{k,t-i}CA^iB\mathcal{K}_2\xi_k(t-i). \end{aligned} \tag{C5}$$

On both sides of (C5), one can get

$$\mathbb{E}(\|e_{k+1}(t)\|) \leqslant \mathbb{E}(\|I - (1-\alpha_{k,t})CB\mathcal{K}_2\|)\mathbb{E}(\|e_k(t)\|)$$

$$+\sum_{i=0}^{t-1}(1-\bar{\alpha})\|CA^{i+1}B\mathcal{K}_2\|\mathbb{E}(\|e_k(t-1-i)\|)+\sum_{i=0}^{t}\bar{\alpha}\bar{\beta}\|CA^{i}B\mathcal{K}_2\|\xi_b. \tag{C6}$$

Similarly, since $\alpha_{k,t}$ is Bernoulli stochastic variables, one has $\mathbb{E}(\|I-(1-\alpha_{k,t})CB\mathcal{K}_2\|):=\phi<1$ if $\|I-CB\mathcal{K}_2\|<1$. From (C6), one can get

$$\underbrace{\begin{bmatrix}\mathbb{E}(\|e_{k+1}(0)\|)\\ \mathbb{E}(\|e_{k+1}(1)\|)\\ \vdots\\ \mathbb{E}(\|e_{k+1}(l)\|)\end{bmatrix}}_{E'_{k+1}} \prec\ \Psi_2 \underbrace{\begin{bmatrix}\mathbb{E}(\|e_{k}(0)\|)\\ \mathbb{E}(\|e_{k}(1)\|)\\ \vdots\\ \mathbb{E}(\|e_{k}(l)\|)\end{bmatrix}}_{E'_{k}} + \underbrace{\begin{bmatrix}\bar{\alpha}\bar{\beta}\|CB\mathcal{K}_2\|\xi_b\\ \bar{\alpha}\bar{\beta}\sum_{i=0}^{1}\|CA^iB\mathcal{K}_2\|\xi_b\\ \vdots\\ \bar{\alpha}\bar{\beta}\sum_{i=0}^{l}\|CA^iB\mathcal{K}_2\|\xi_b\end{bmatrix}}_{M'_{\xi}}, \tag{C7}$$

where the matrix Ψ_2 is

$$\Psi_2=\begin{bmatrix}\phi & 0 & \cdots & 0\\ (1-\bar{\alpha})\|CAB\mathcal{K}_2\| & \phi & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ (1-\bar{\alpha})\|CA^lB\mathcal{K}_2\| & (1-\bar{\alpha})\|CA^{l-1}B\mathcal{K}_2\| & \cdots & \phi\end{bmatrix}. \tag{C8}$$

The remainder of the proof is omitted because it is the same as Theorem 1. Analogously, one knows that the σ-secure can be achieved according to Definition 1.

Appendix D Proof of Theorem 4

Proof. From system (1) and ILC (7) with $\mathcal{K}_1=\mathbf{O}$, one has

$$\begin{aligned}u_{k+1}(t) &= u_k(t)+\mathcal{K}_2[y_d(t+1)-\check{y}_k(t+1)]\\ &= u_k(t)+\mathcal{K}_2[(1-\alpha_{k,t+1})y_d(t+1)-(1-\alpha_{k,t+1})Cx_k(t+1)-\alpha_{k,t+1}\beta_{k,t+1}\xi_k(t+1)]\\ &= u_k(t)+\mathcal{K}_2[(1-\alpha_{k,t+1})y_d(t+1)-\alpha_{k,t+1}\beta_{k,t+1}\xi_k(t+1)]\\ &\quad -(1-\alpha_{k,t+1})\mathcal{K}_2C[Ax_k(t)+Bu_k(t)]\\ &= [I-(1-\alpha_{k,t+1})\mathcal{K}_2CB]u_k(t)+\varphi_k(t),\end{aligned} \tag{D1}$$

where $\varphi_k(t)=\mathcal{K}_2[(1-\alpha_{k,t+1})y_d(t+1)-\alpha_{k,t+1}\beta_{k,t+1}\xi_k(t+1)-(1-\alpha_{k,t+1})CAx_k(t)]$.

According to Eq. (D1), it is easy to get

$$\mathbb{E}(\|u_{k+1}(t)\|)\leqslant\mathbb{E}(\|I-(1-\alpha_{k,t+1})\mathcal{K}_2CB\|)\mathbb{E}(\|u_k(t)\|)+\mathbb{E}(\|\varphi_k(t)\|), \tag{D2}$$

and $\mathbb{E}(\|\varphi_k(t)\|)\leqslant\|\mathcal{K}_2\|[(1-\bar{\alpha})\|y_d(t+1)\|+\bar{\alpha}\bar{\beta}\xi_b+(1-\bar{\alpha})\|CA\|\mathbb{E}(\|x_k(t)\|)]$. One can derive $\mathbb{E}(\|I-(1-\alpha_{k,t+1})\mathcal{K}_2CB\|)<1$ if $\|I-\mathcal{K}_2CB\|<1$. Next, the boundedness in the sense of expectation needs to be clarified. The rest of the proof is omitted here since the results can be obtained by using the similar proof of Theorem 1 in [2].

Remark 3. Compared with [3], our strategies provide a more reasonable method to analyze the system security. And our obtained conditions are simpler and easier to be checked. Compared with [4], the deception and DoS attacks are considered simultaneously, which is more general in the real application.

Appendix E Illustrative example

To illustrate the validity of our results, a numerical example is presented in the following. Consider system (1) with the single-input and single-output, and define $A=\begin{bmatrix}1 & 0.4\\ -0.4 & 0.8\end{bmatrix}$, $B=\begin{bmatrix}-0.5\\ 1\end{bmatrix}$, $C=\begin{bmatrix}0.5 & 0.5\end{bmatrix}$. Let $t\in\mathcal{T}=[0,l]$, $l=10$, $x_{k+1}(0)=x_k(0)=\begin{bmatrix}1\\ -1\end{bmatrix}$. In addition, $\bar{\alpha}=0.5$ and $\bar{\beta}=0.3$ denote respectively the success probabilities of the attacks. And let ξ_b be the boundary of $\xi_k(t)$, i.e., $\|\xi_k(t)\|\leqslant\xi_b=1$. Further, set the desired trajectory of output as $y_d(t)=2\sin(0.2\pi t)$.

Case 1. The deception and DoS attacks occur randomly.

i) System (1) with $D=0.5$. In strategy (7), define $\mathcal{K}_1=0.5$ and $\mathcal{K}_2=0$. Set the initial input $u_0(t)=0$. With a simple calculation, one knows that $\|I-D\mathcal{K}_1\|=0.75<1$, then the conditions of Theorems 1 and 2 hold.

ii) System (1) with $D=0$. In strategy (7), define $\mathcal{K}_1=0$ and $\mathcal{K}_2=0.5$. Set the initial input $u_0(t)=0$. With a simple calculation, one knows the $\|I-CB\mathcal{K}_1\|=\|I-\mathcal{K}_1CB\|=0.875<1$, then the conditions of Theorems 3 and 4 hold.

The tracking trajectories and errors of Case 1 are shown in Figs. E1 and E2. Fig. E1 shows the tracking trajectories at the 100th iteration. Fig. E2 shows the tracking error from the first iteration to the 150th iteration. According to Figs. E1 and E2, one knows the result of our algorithm can be satisfied since the chattering of the tracking error is small. Further, from Fig. E2, one can see that the purple line has the smallest fluctuation. That is, the convergence effect of Theorem 1 in this paper is the best than those in Theorem 3 and Theorem 2 of [1]. The possible reason is that the control term in

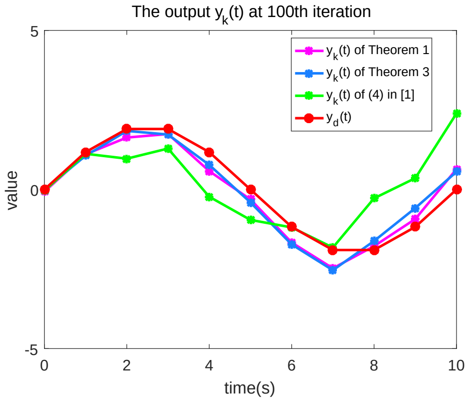

Figure E1 The tracking trajectories under deception and DoS attacks.

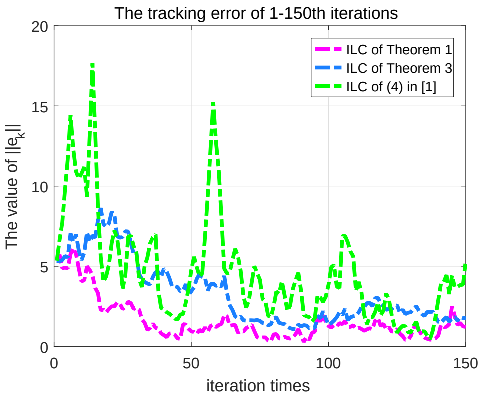

Figure E2 The tracking error under deception and DoS attacks.

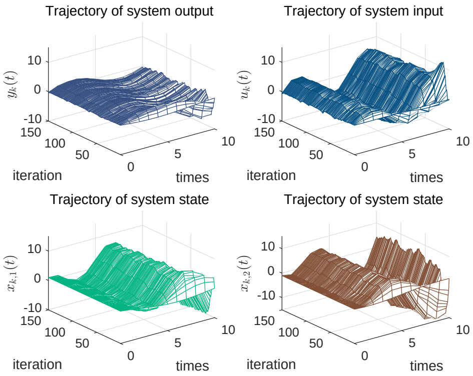

Figure E3 System trajectories of Theorems 1.

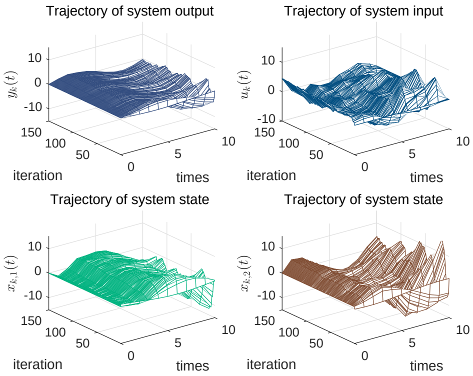

Figure E4 System trajectories of Theorems 3.

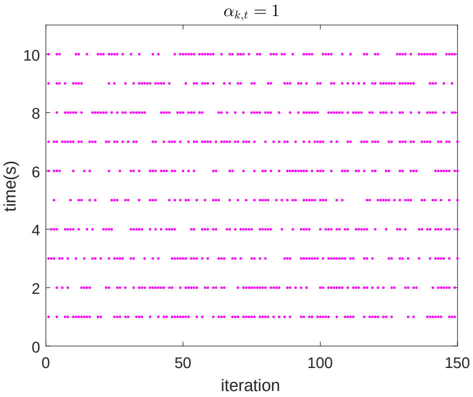

Figure E5 The situation of $\alpha_{k,t} = 1$ in each iteration.

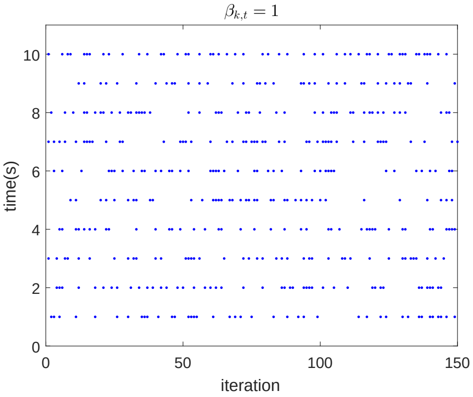

Figure E6 The situation of $\beta_{k,t} = 1$ in each iteration.

the observer is used to reduce the impact of cyber-attacks. From Figs. E3 and E4, one knows all variables' trajectories are bounded. Furthermore, Figs. E5 and E6 show the attack profile of $\alpha_{k,t}$ and $\beta_{k,t}$.

Case 2. The deception or DoS attacks occur individually.

i) Only DoS attack exists, i.e. $\beta_{k,t} \equiv 0$ or $\xi_k(t) \equiv 0$. Figs. E7 and E8 show the tracking trajectories and errors in this situation. One knows that the tracking error e_k can asymptotically tend to zero. Compared with the ILC algorithm (4) of [1], ILC strategy in Theorem 1 has the smaller transient tracking error. Moreover, the ILC algorithm in Theorem 1 has the faster convergence speed than that in Theorem 3. The reason is that those control terms in the observer can help to resist the impact of the DoS attack.

ii) Only deception attack exists, i.e. $\beta_{k,t} \equiv 1$. Figs. E9 and E10 show the tracking trajectories and errors in this situation. According to these figures, one has that the chattering range of the tracking error trajectories is bigger than case 1. It demonstrates that a deception attack has a worse negative impact on the system security. From Fig. E10, one can

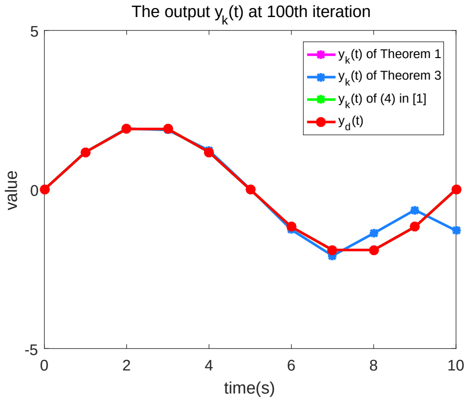

Figure E7 The tracking trajectories under the DoS attack.

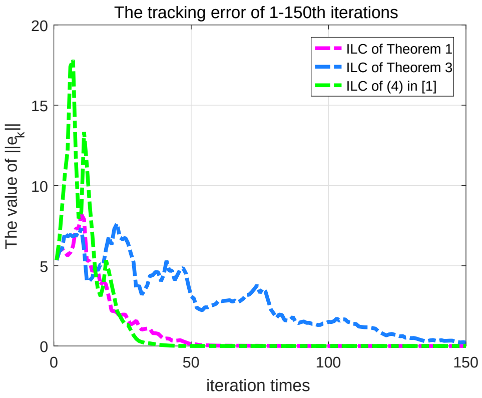

Figure E8 The tracking error under the DoS attack.

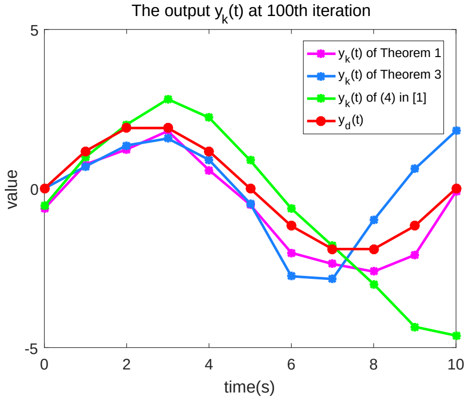

Figure E9 The tracking trajectories under the deception attack.

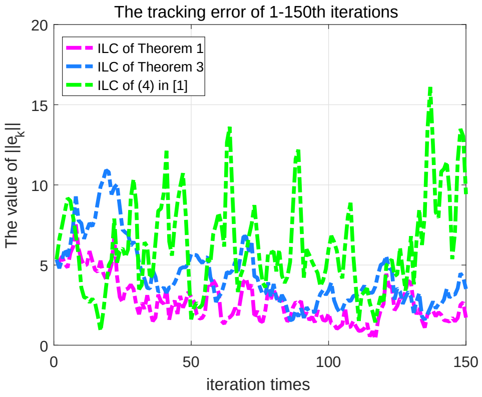

Figure E10 The tracking error under the deception attack.

also see that ILC algorithm in Theorem 1 has a good tracking result.

According to the above analysis, one knows that the ILC strategy in this paper can effectively achieve the σ-security. And our algorithm can guarantee the boundedness of the trajectory of each variable of systems. Malicious attacks, especially deception attacks, can make the tracking error fluctuate greatly. The control term in the observer can help to reduce the impact of cyber-attacks. Additionally, the convergence conditions in this paper are simpler than those in some previous literature. According to the above figures, one can see that the deception attack is the primary factor to affect the system security. As a result, one has to pay attention on deception attacks in the real application.

References

1 Liu J, Ruan X E. Networked iterative learning control design for nonlinear systems with stochastic output packet dropouts. Asian J. Control, 2018, 20: 1077-1087

2 Meng D Y, Moore K L. Robust iterative learning control for nonrepetitive uncertain systems. IEEE Trans Auto Contr, 2017, 62: 907-913

3 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

4 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