Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

False data injection attacks for networked control systems with sensor fault and actuator saturation

Qing Geng * **Fucai Liu** * **Yafeng Li** *

* *Institute of Electrical Engineering, Yanshan University, Qinhuangdao 066004, China. Email: gengqingsjz@163.com;lfc@ysu.edu.cn;y.f.li@foxmail.com*

Abstract: This paper presents the design problem of false data injection (FDI) attacks against the networked predictive control (NPC) strategy, where the sensor fault and actuator saturation are considered. An estimator is designed to estimate system states and sensor fault simultaneously. A predictive controller which can generate a sequence of predictive signals is designed to actively compensate the time-varying delays for the networked control system (NCS). A sufficient condition is derived for stability of the NCS by a switched system theory. Finally, a numerical simulation demonstrates the effectiveness of proposed method for the NCS.

Keywords: Networked control system, FDI attacks, sensor fault, actuator saturation.

1. INTRODUCTION

There are many advantages for NCSs in system scalability, economy, flexible control and maintenance, etc Hu et al. (2017), Yuan et al. (2016), Wang et al. (2016). However, many constraints such as time-varying delays, packet dropouts, bandwidth limitations, malicious cyber attacks seriously affect the performance of NCSs Li et al. (2017), Zhang et al. (2017). Scholars are making a great effort to develop advanced control techniques to improve the stability and reliability of NCSsYang et al. (2018). Due to the openness of communication networks, NCSs prone to be invaded by attacks, which may result in control performance degradation and even system crash Lei et al. (2016). If the measured data and control signals are transmitted through the unprotected network, network attack can lead to destroy the normal operation of the physical or cyber-physical systems, and even endanger human life Feng et al. (2016), Ding et al. (2017). Therefore, it has become an arduous task to ensure network security in NCSs. FDI attack is one of typical cyber-attacks that can modify both measurement data and control signals to affect system performance Guo et al. (2017). In Pang et al. (2012), a secure NCS architecture has been presented to guarantee performance of control systems suffering from deception attacks. For deception attacks, security threat assessment of automated canal systems has been designed with regulatory and supervisory control layer Amin et al. (2013). Typical deception attacks include data replay attacks and FDI attacks. Compared with replay attacks, FDI attacks can modify both measurement data and control signals to cause the huge possible damage with stealthiness Manandhar et al. (2014), Guo et al. (2017). Two-channel FDI attacks that attack both forward and feedback channels can bring greater threats to NCSs than single-channel FDI attacks Pang et al. (2016). Single type of cyber-attacks are vulnerable to targeting and prevention, which only causes limited impacts for NCSs. For the variousness of cyber-attacks in actual environments, a double attack strategy is worth considering in order to bring as much damage to NCSs as possible Pang et al. (2016).

Actuator saturation is a common phenomenon of control systems which are applicable to various aspects of engineering and science virtually, which can affect performance of the control systems and even cause the control system instability if they are not considered in the control design stage Feng G. (2015), Yanumula et al. (2017). Because of sensor aging, zero displacement, electromagnetic interference and network interference, sensor failure and data distortion are unavoidable, which may lead to intolerable system performance Lee et al. (2018), Xu et al. (2018). Therefore, it is necessary and important to tolerate data distortion and sensor failures. Recently, some methods were developed to maintain desired control performance for NCSs with limited communication bandwidth. One effective approach for the performance optimization is the NPC, which has been widely applied to analyze the stability of NCSs Zhang et al. (2013), Li et al. (2014). The NPC strategy has been investigated by some relevant works on model predictive control for complex networks' consensus and flocking control Zhan et al. (2013). From the attackers' perspectives, the NPC is meaningful to considered to design a attack strategy.

In this paper, cyber-attackers are supposed to have ability to intercept and modify measurement data and two types of FDI attacks are designed in the NCS. Both sensor fault and actuator saturation are considered in a NCS. Both time-varying delays in the forward and feedback channels are considered. Sufficient conditions are derived for stability of the NCS by using a switched system theory. Moreover, two forms of sensor fault i.e., constant fault and time-varying bias are considered in a simulation example to illustrate the effectiveness of the proposed method in this paper. For distinguishing existing works on cyber-

attacks, the contributions of this paper are included as follows:
(1) From attackers' perspective, cyber attacks are proposed for both the feedback and forward channels without the detection of an attack detector.
(2) A state and fault estimator is designed to estimate system states and sensor fault simultaneously for a NCS suffering from FDI attacks.
(3) A predictive controller is designed to actively compensate the effect of transmission delays for the NCS with sensor fault and actuator saturation.

2. PROBLEM FORMULATION AND PRELIMINARIES

2.1 System Description

Consider the following discrete linear system

$$x(k+1) = Ax(k) + B\text{sat}(u(k)) + \omega(k), \tag{1}$$
$$z(k) = Cx(k) + \nu(k), \tag{2}$$
$$y(k) = z(k) + Ff(k), \tag{3}$$

where $u(k) \in \mathcal{R}^p$, $x(k) \in \mathcal{R}^n$, $z(k) \in \mathcal{R}^q$ and $y(k) \in \mathcal{R}^q$ are vectors of the control input, the system state, the system output and the output signal of the sensor, respectively. $A \in \mathcal{R}^{n\times n}$, $B \in \mathcal{R}^{n\times p}$ and $C \in \mathcal{R}^{q\times n}$ are constant matrices. $\omega(k)$ and $\nu(k)$ are system noise and output noise, respectively. $F \in \mathcal{R}^{q\times m}$ is a fault distribution matrix and $f(k) \in \mathcal{R}^m$ is a specific external sensor fault. $\omega(k)$ and $\nu(k)$ are uncorrelated Gaussian white noises with $\omega(k) \sim N(0, S)$ and $\nu(k) \sim N(0, R)$, where S and R are covariance matrices. The structure of a NCS with sensor fault, time-varying delays and actuator saturation is shown in Fig. 1.

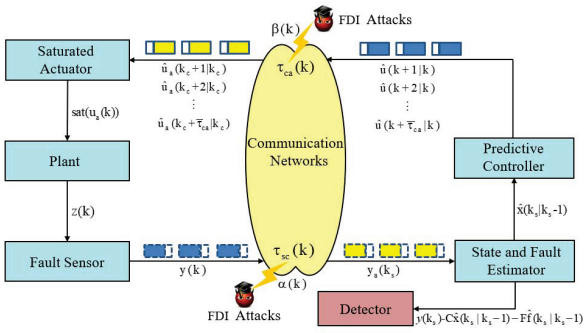

Fig. 1. Schematic diagram of NCS.

As shown in Fig. 1, the NCS consists of a plant, a sensor, a state and fault estimator, a predicted controller and a saturated actuator. Two-channel FDI attacks in the forward and feedback communication channels are considered in the NCS.

Time-varying delays in feedback and forward communication channels are denoted as $\tau_{sc}(k)$ and $\tau_{ca}(k)$, respectively. The upper bounds of $\tau_{sc}(k)$ and $\tau_{ca}(k)$ are $\bar{\tau}_{sc}$ and $\bar{\tau}_{ca}$, respectively. The round-trip time (RTT) delay is given as $\tau(k) = \tau_{sc}(k) + \tau_{ca}(k)$ and the upper bound of RTT delay is $\bar{\tau}$. $\alpha(k)$ and $\beta(k)$ are FDI attacks for the feedback and forward communication channels, respectively. The output signal $y(k)$ is attacked by the FDI attacks $\alpha(k)$. $y_a(k_s)$ is the output signal to be attacked which is transmitted to the state and fault estimator. A control signal sequence $\hat{u}(k+1|k), \hat{u}(k+2|k), \cdots, \hat{u}(k+\bar{\tau}|k)$ is calculated by the predicted controller and transmitted to the actuator through networks. $\hat{u}_a(k+1|k), \hat{u}_a(k+2|k), \cdots, \hat{u}_a(k+\bar{\tau}|k)$ is the control signal sequence which is attacked by forward channel FDI attacks $\beta(k)$. The saturated actuator is given to constraint the system input signals $\hat{u}_a(k)$. The saturation function is given as $\text{sat}(u(t_k))^T = [\text{sat}(u_1(t_k))^T\ \text{sat}(u_2(t_k))^T\ \ldots\ \text{sat}(u_p(t_k))^T]$ with $\text{sat}(u_i(t_k)) = \begin{cases} 1, & \text{if } u_i(t_k) \geq 1 \\ u_i(t_k), & \text{if } -1 < u_i(t_k) < 1 \\ -1, & \text{if } u_i(t_k) \leq -1 \end{cases}$ for each $i \in [1, p]$. In this paper, we assume that the pair (A, C) is detectable, and the pair (A, B) is stabilizable. The actuator and the sensor are time-driven. The controller is event-driven. Packets transmitted through networks are with time stamps.

2.2 Estimator and Detector

We design a state and fault estimator to estimate the system state and the sensor fault simultaneously by considering the sensor fault [Pang et al. (2013)].

$$\hat{x}(k_s+1|k_s) = A\hat{x}(k_s) + B\text{sat}(u(k_s)), \tag{4}$$
$$\hat{x}(k_s+1) = \hat{x}(k_s+1|k_s) + K_1(y_a(k_s+1) - C\hat{x}(k_s+1|k_s) - F\hat{f}(k_s+1)), \tag{5}$$
$$\hat{f}(k_s+1) = M_1C\hat{x}(k_s+1|k_s)) + K_2(y_a(k_s) - C\hat{x}(k_s|k_s-1) - F\hat{f}(k_s)) - M_1y_a(k_s+1), \tag{6}$$

Then the estimated state is transmitted to the predictive controller together with a time stamp.

To detect attacks, the detector is necessary to be introduced. In this paper, a χ^2 anomaly detector is designed using the estimator in equations (4)-(6). The residual $\zeta_a(k)$ is defined as

$$\zeta_a(k_s) = y_a(k_s) - C\hat{x}(k_s|k_s-1) - F\hat{f}(k_s). \tag{7}$$

The residual $\zeta_a(k_s)$ is Gaussian independent identically distributed with zero mean and covariance $\varsigma = CPC^T + FHF^T + R$, i.e., $\zeta(k_s) \sim \mathcal{N}(0, \varsigma)$. At each time instant k, the χ^2 anomaly detector first computes the value $\zeta_a(k_s)$, and then compares $\zeta_a(k_s)$ with a prescribed threshold α. If $\zeta_a(k_s) > \alpha$, then an alarm will be triggered. When the system operates normally (i.e. without attacks), $\zeta_a(k_s)$ satisfies a χ^2 distribution implying low probability of a large $\zeta_a(k_s)$. Moreover, the FDI attacks in the feedback and forward communication channels lead to a value of $\|\zeta_a(k_s)\|$ induce the detector to trigger an alarm.

2.3 Predictive Controller

In this subsection, a NPC strategy is given in the following. The state feedback control law is designed as $\hat{u}(k_s|k_s) = \hat{u}(k_s) = -L\hat{x}(k_s)$, where $L \in \mathcal{R}^{p\times n}$ is the gain matrix to be designed. The transmission delays in the feedback communication channel are actively compensated in the following. From system (1)-(3), the predictions of the system state and control signal up to time $k_s + \bar{\tau}_{sc}$ are obtained as

$$\hat{x}(k_s+i|k_s) = A\hat{x}(k_s+i-1|k_s) + B\text{sat}(\hat{u}(k_s+i-1|k_s))$$
$$\hat{u}(k_s+i|k_s) = -L\hat{x}(k_s+i|k_s)$$

for $i = 1, 2, \cdots, \bar{\tau}_{sc}$. For $k_s = k-\tau_{sc}(k)$, then the predictive controller at time instant k is designed as

$$\hat{u}(k) = \hat{u}(k_s+\tau_{sc}(k)|k_s) = -L\hat{x}(k). \quad (8)$$

The predictions of the system state and control signal up to time $k+\bar{\tau}_{ca}$ are given as

$$\hat{x}(k+i|k) = A\hat{x}(k+i-1|k) + B\text{sat}(\hat{u}(k+i-1|k)), \quad (9)$$
$$\hat{u}(k+i|k) = -L\hat{x}(k+i|k), \quad (10)$$

for $i = 1, 2, \cdots, \bar{\tau}_{ca}$, where $\hat{u}(k|k) = \hat{u}(k)$. In order to avoid the waste of energy in the packet transmission process, it is only needed to transfer the following control prediction sequence to the saturated actuator.

$$U_k = [\hat{u}(k+1|k), \hat{u}(k+2|k), \cdots, \hat{u}(k+\bar{\tau}_{ca}|k)]^T.$$

2.4 The Feedback and Forward Channel Attacks

In NCS (1)-(3), cyber-attackers are supposed to have ability to intercept and modify measurement data Guo et al. (2017); Pang et al. (2016). Note that linear deception attacks are a typical type of FDI attacks.

As shown in Fig. 1, the system output under FDI attacks in the feedback channel is shown as

$$y_a(k_s) = y(k_s) + \alpha(k), \quad (11)$$

with $k_s = k - \tau_{sc}(k)$ and

$$\alpha(k) = -y(k) + C\hat{x}(k|k-1) + F\hat{f}(k) + \xi(k), \quad (12)$$

where $\xi(k)$ is the Gaussian white noise with $\xi(k) \sim \mathcal{N}(0, \rho)$ and ρ is a covariance matrice. It is obvious that the residual $\zeta_a(k)$ is Gauss white noise with covariance matrix. As a result, the FDI attack $\alpha(k)$ cannot be detected by the output residual detector (7). That is, the FDI attack $\alpha(k)$ in this paper is deceptive and stealthy.

As shown in Fig. 1, the control data U_k arriving at the actuator through forward network are falsified by the attacker as $U_k^a = [\hat{u}_a(k_c+1|k_c), \hat{u}_a(k_c+2|k_c), \cdots, \hat{u}_a(k_c+\bar{\tau}_{ca}|k_c)]^T$ with

$$\hat{u}_a(k_c+i|k_c) = \hat{u}(k_c+i|k_c) + \beta(k_c+i), \quad (13)$$

where $k_c = k-\tau_{ca}(k)$, $\hat{u}_a(k_c+i|k_c)$ is the attacked control prediction and $\beta(k+i)$ are the forward channel attacks for $i = 1, 2, \cdots, \bar{\tau}_{ca}$. The attacks in forward channel can be given as

$$\beta(k+1) = \Gamma\beta(k), \quad (14)$$

where $\Gamma \in \mathcal{R}^{p\times p}$ is an attack matrix. Then we have $\beta(k+i) = \Gamma^i\beta(k)$. At time instant k, for $k_c = k-\tau_{ca}(k)$, the real control input is

$$u_a(k) = \hat{u}_a(k_c+\tau_{ca}(k)|k_c), \quad (15)$$

which is selected in the control prediction sequence U_k^a to control the plant. Under the FDI attacks in equations (11) and (13), the NCS (1)-(3) is expressed as

$$x(k+1) = Ax(k) + B\text{sat}(u_a(k)) + \omega(k), \quad (16)$$
$$y_a(k) = Cx(k) + Ff(k) + \nu(k) + \alpha(k). \quad (17)$$

Before ending this section, a lemma is given to drive our main results in this paper.

Lemma 1. Feng G. (2015) Denote $\eta(u(k)) = u(k) - \text{sat}(u(k))$, then there exists a real number $\varepsilon \in (0,1)$ such that

$$\eta^T(u(k))M\eta(u(k)) \le \varepsilon u^T(k)Mu(k).$$

where $\eta = [\eta_1, \eta_2, \cdots, \eta_p]^T \in \mathcal{R}^m$ with η_i is the dead-zone nonlinearity function, $i = 1, 2, \cdots, p$. M is a arbitrary symmetric positive definite matrix.

3. MAIN RESULTS

In this section, the effectiveness of the state and fault estimator is proved and stabilization of the NCS with two FDI attacks is analyzed. Define the estimation errors of system state and sensor fault as follows

$$e_x(k_s) = x(k_s) - \hat{x}(k_s), \quad (18)$$
$$e_f(k_s) = f(k_s) - \hat{f}(k_s). \quad (19)$$

Theorem 1. If there exist matrixes Q, K_1 and K_2, such that the following inequality

$$\Phi^T Q\Phi - Q < 0, \quad (20)$$

where $\Phi = \begin{bmatrix} A-K_1C & -K_1F \\ M_1CA-K_2C & -K_2F \end{bmatrix}$ hold, then the following equations are guaranteed $\lim_{k_s\to\infty}\mathbf{E}(e_x(k_s)) = 0$ and $\lim_{k_s\to\infty}\mathbf{E}(e_f(k_s)) = 0$.

Proof. From equations (4)-(6) and (16)-(19), the estimation errors of system state and sensor fault are given as $e_x(k_s+1) = (A-K_1C)e_x(k_s) - K_1Fe_f(k_s) + \omega(k_s) - K_1\nu(k_s) - K_1\alpha(k_s)$, and $e_f(k_s+1) = M_1CAe_x(k_s) - K_2Ce_x(k_s) - K_2Fe_f(k_s) + K_2\alpha(k) + M_1C\omega(k_s) + M_1\nu(k_s+1) + M_1\alpha(k_s+1)$. Then, we have $\mathbf{E}(\bar{e}(k_s+1)) = \Phi\mathbf{E}(\bar{e}(k_s))$, where $\bar{e}(k_s) = [e_x^T(k_s)\ e_f^T(k_s)]^T$. Give a Lyapunov function

$$V(\bar{e}(k_s)) = \mathbf{E}(\bar{e}^T(k_s))Q\mathbf{E}(\bar{e}(k_s)).$$

We have $\Delta V(\bar{e}(k_s)) = \mathbf{E}(\bar{e}^T(k_s))(\Phi^TQ\Phi - Q)\mathbf{E}(\bar{e}(k_s))$. If $\Phi^TQ\Phi - Q < 0$, then it is shown that $\Delta V(\bar{e}(k_s)) < 0$. As a result, we have $\lim_{k_s\to\infty}\mathbf{E}(e_x(k_s)) = 0$ and $\lim_{k_s\to\infty}\mathbf{E}(e_f(k_s)) = 0$. The proof is completed.

Theorem 2. Under two-channel FDI attacks, the NCS (16)-(17) is stable with $\lim_{k\to\infty}\mathbf{E}(x(k)) = 0$ if there exist $\bar{\tau}$ positive definite matrices P_i and P_j such that the following inequalities hold for all $\{i, j\} \in \{0, 1, 2, \cdots, \bar{\tau}\}$

$$2\Lambda_i^TP_j\Lambda_i - P_i + 4(1+\varepsilon)\Pi^T\Omega_i^T\Xi^TP_j\Xi\Omega_i\Pi < 0 \quad (21)$$

where $\Xi^T = [I_n, 0^T_{(\bar{\tau}+2)n\times n}]^T$, $\Omega_i = -BL(A-BL)^i$, $\Pi^T = [0^T_{n\times(i-1)n}, I_n, 0^T_{n\times(\bar{\tau}-i)n}]$ and

$$\Lambda_i = \begin{bmatrix} A & 0_{n\times\bar{\tau}n} & K_1C & K_1F \\ \mathbf{I}_{\bar{\tau}n} & \mathbf{0}_{\bar{\tau}n\times n} & \mathbf{0}_{\bar{\tau}n\times n} & \mathbf{0}_{\bar{\tau}n\times n} \\ & & A-K_1C & -K_1F \\ & \mathbf{0}_{2n\times(\bar{\tau}+1)n} & & \\ & & M_1C-K_2C & -K_2F \end{bmatrix}$$

Proof. It is obtained from (4), (5), (18) and (19) that

$$\hat{x}(k+1|k) = A\hat{x}(k|k-1) + K_1Ce_x(k) + K_1Fe_f(k) + B\text{sat}(u(k)+\beta(k)) + K_1\nu(k) + K_1\alpha(k).$$

Then we have $\mathbf{E}(\hat{X}(k+1)) = \Lambda_i\mathbf{E}(\hat{X}(k)) + \Xi B\text{sat}(u(k)+\beta(k))$, where $\hat{X}^T(k) = [\hat{x}^T(k|k-1), \hat{x}^T(k-1|k-2), \cdots, \hat{x}^T(k-\bar{\tau}|k-\bar{\tau}-1), e_x^T(k), e_f^T(k)]^T$. From equations (8)-(10), it is noted that $u(k) = -L\hat{x}(k) = -L(A-BL)^{\tau(k)}\hat{x}(k-\tau(k)|k-\tau(k)-1)$. Give a switched Lyapunov function as $V(\hat{X}(k)) = \mathbf{E}(\hat{X}^T(k))P_i\mathbf{E}(\hat{X}(k))$. It is shown that

$$\Delta V(\hat{X}(k)) \le \mathbf{E}(\hat{X}^T(k))(2\Lambda_i^T P_j\Lambda_i - P_i)\mathbf{E}(\hat{X}(k)) + 2\text{sat}(u^T(k)+\beta^T(k))B^T\Xi^T P_j\Xi B\text{sat}(u(k)+\beta(k)).$$

According to Lemma 1, it is noted that

$$\text{sat}(u^T(k)+\beta^T(k))B^T\Xi^T P_j\Xi B\text{sat}(u(k)+\beta(k)) \le 2(1+\varepsilon)u^T(k)B^T\Xi^T P_j\Xi Bu(k)$$

Then, we have

$$\Delta V(\hat{X}(k)) \le \mathbf{E}(\hat{X}^T(k))(2\Lambda_i^T P_j\Lambda_i - P_i + 4(1+\varepsilon)\Pi^T\Omega_i^T\Xi^T P_j\Xi\Omega_i\Pi)\mathbf{E}(\hat{X}(k)),$$

If there exist P_i, P_j such that $2\Lambda_i^T P_j\Lambda_i - P_i + 4(1+\varepsilon)\Pi^T\Omega_i^T\Xi^T P_j\Xi\Omega_i\Pi < 0$, then it is shown that $\Delta V(\hat{X}(k)) < 0$. As a result, it is obtained that the NCS (16)-(17) is asymptotically stable with $\lim_{k\to\infty}\mathbf{E}(x(k)) = 0$.

Remark 1. In this paper, cyber-attackers are supposed to own abilities that intercept and modify measurement data Guo et al. (2017). Note that linear deception attacks are a typical type of FDI attacks Pang et al. (2016). Two-channel FDI attacks are considered for the NCS subject to sensor fault and actuator saturation in this paper. In this paper we assume that the attacker is able to read the data transmitted through the feedback and forward communication channels and modify them arbitrarily, i.e., the attacker knows the system parameters. Meanwhile, the system is also assumed to know the attacking signal exactly, i.e., the NCS knows $\alpha(k)$ and $\beta(k)$.

4. NUMERICAL SIMULATION

An numerical example of an inverted pendulum system in Fig. 2 is provided in this section to demonstrate the effectiveness of the proposed methods in this paper.

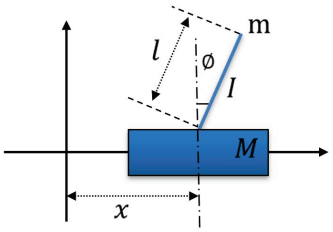

Fig. 2 The physical structure of inverted pendulum model.

The constant parameters of the inverted pendulum model are given in Table 1.

Linearize the nonlinear dynamics equations Pang et al. (2013). Considering sensor fault in the inverted-pendulum model and taking the sample period as $\mathtt{T} = 0.01s$, a discretized linear system is obtained as

$$x(k+1) = \begin{bmatrix} 1.0000 & 0.0100 & 0 & 0 \\ 0 & 1.0000 & 0 & 0 \\ 0 & 0 & 1.0015 & 0.0100 \\ 0 & 0 & 0.2941 & 1.0015 \end{bmatrix} x(k) \quad (22)$$

$$+ \begin{bmatrix} -0.0001 \\ -0.0100 \\ 0.0002 \\ 0.0300 \end{bmatrix} \text{sat}(u(k)) + \omega(k) \quad (23)$$

$$y(k) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} x(k) + \begin{bmatrix} 1 \\ 1 \end{bmatrix} f(k) + \nu(k) \quad (24)$$

where $\omega(k)$ and $\nu(k)$ are zero-mean Gaussian noises uncorrelated Gaussian white noises with covariances $S = diag\{10^{-4}, 0, 10^{-4}, 0\}$ and $R = diag\{10^{-4}, 10^{-4}\}$, respectively.

To verify the proposed theory in this paper, let system (23)-(24) access networks which is transformed to be the NCS (16)-(17). The time-varying delay for feedback communication channel $\tau_{sc}(k)$, the time-varying delay in forward communication channel $\tau_{ca}(k)$ and the RTT delay $\tau(k)$ are given as Fig. 3.

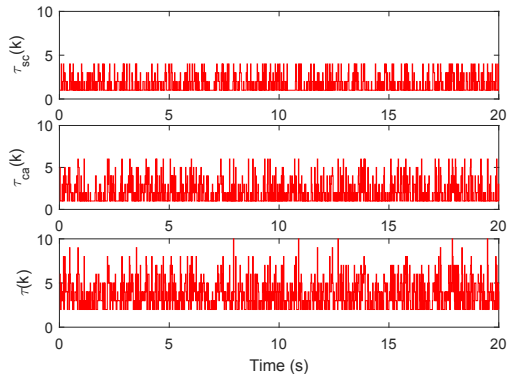

Fig. 3 The time-varying delay $\tau_{sc}(k)$, $\tau_{ca}(k)$ and $\tau(k)$.

In the NCS (16)-(17), the upper bound of the time-varying delays for feedback and forward communication channels are given as $\bar{\tau}_{sc}(k) = 4$ and $\bar{\tau}_{ca}(k) = 6$, respectively. FDI attacks are considered to strick both the feedback and forward communication channels. $\alpha(k)$ and $\beta(k)$ are the FDI attacks for feedback and forward communication channels, respectively. Let $M_1 = [-0.5 - 0.5]$ and $\Gamma = 0.6$. The observer gain matrices K_1 and K_2 in the observer (4)-(6) is designed as

Table 1. The parameters in the inverted pendulum model

Symbol	Value	Meaning
M	$1.096\ Kg$	Mass of the cart
m	$0.109\ Kg$	Mass of the pendulum rod
l	$0.25\ m$	Length from axis to centroid
b	$0.1\ N/m/sec$	The friction coefficient of cart
I	$0.0034kg*m*m$	Inertia of the rod
g	$9.81m/s^2$	Gravitational constant

$$K_1 = \begin{bmatrix} -0.0709 & 0.3399 \\ -0.1075 & 0.2254 \\ -1.1770 & 1.4521 \\ -4.5493 & 6.1744 \end{bmatrix} \text{ and } K_2 = [\,0.6340 \;\; -0.9033\,].$$

By solving equalities in (21) of Theorem 2, the state feedback gain matrix L is designed as

$$L = [\,28.7118 \;\; 18.4434 \;\; 67.8519 \;\; 12.2877\,]^T.$$

The sensor fault is in many forms, such as constant fault, time-varying bias and so on. In this paper, sinusoidal signal fault and constant fault are given in Fig. 4 and Fig. 5, respectively. The dashed lines in Fig. 4 and Fig. 5 represent estimates of the two types of sensor faults.

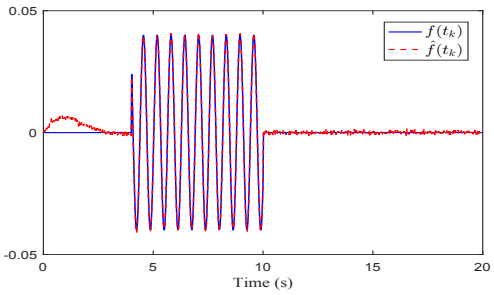

Fig. 4 State curves of $f(t_k)$ and $\hat{f}(t_k)$ with sinusoidal signal fault.

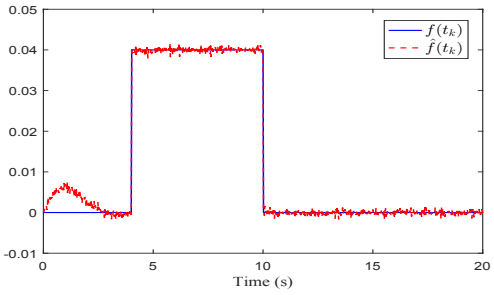

Fig. 5 State curves of $f(t_k)$ and $\hat{f}(t_k)$ with constant fault.

The initial states of the NCS (16)-(17) and observer (4)-(6) are given as $x_0 = [0.1\ 0\ 0\ 0]^T$ and $\hat{x}_0 = [0.1\ 0\ 0\ 0]^T$, respectively. The trajectories of the state response $x_1(t_k)$, $x_2(t_k)$, $x_3(t_k)$ and $x_4(t_k)$ are plotted in Fig. 6 and Fig. 7 for the NCS (16)-(17) with the two types of sensor faults. The trajectories of the observer state response $\hat{x}_1(t_k)$, $\hat{x}_2(t_k)$, $\hat{x}_3(t_k)$ and $\hat{x}_4(t_k)$ are plotted in Fig. 6 and Fig. 7 for observer (4)-(6) with the two types of sensor faults.

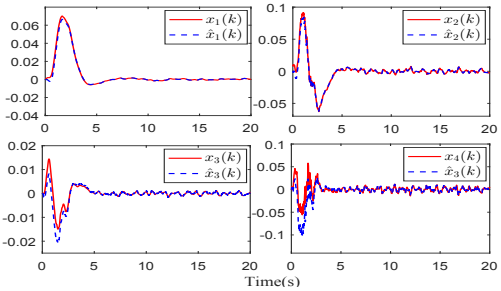

Fig. 6 System states and observer states curves with sinusoidal signal fault.

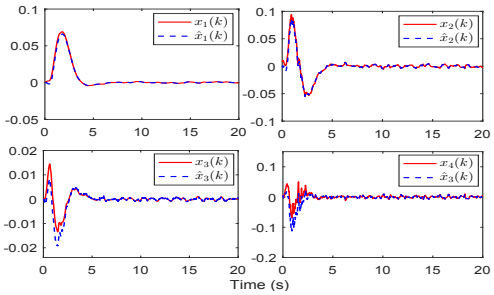

Fig. 7 System states and observer states curves with constant fault.

In Fig. 6 and Fig. 7, it is seen clearly that the four observer states $\hat{x}_1(t_k)$, $\hat{x}_2(t_k)$, $\hat{x}_3(t_k)$ and $\hat{x}_4(t_k)$ asymptotically approaching state curves of $x_1(t_k)$, $x_2(t_k)$, $x_3(t_k)$ and $x_4(t_k)$ which shows the effectiveness of the observer (4)-(6). The four observer states and state curves of the NCS (16)-(17) converge to zero point, then it is indicates that the state feedback control law stabilizes the NCS (23)-(24). The output signals $y(t_k)$ with sinusoidal signal fault and constant fault are plotted in Fig. 8 and Fig. 9, respectively.

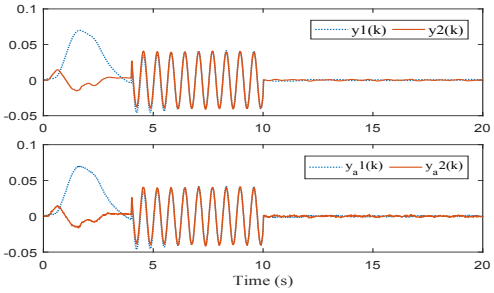

Fig. 8 Output curves of $y(t_k)$ with sinusoidal signal fault.

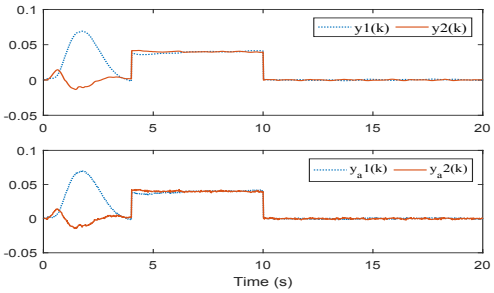

Fig. 9 Output curves of $y(t_k)$ with constant fault.

The control signals $u(t_k)$ with sinusoidal signal fault and constant fault are plotted in Fig. 10 and Fig. 11, respectively.

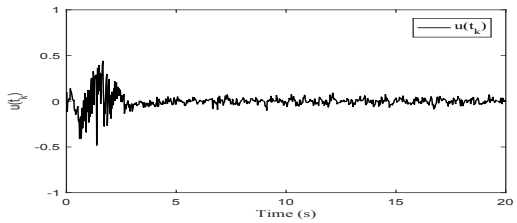

Fig. 10 Input curves of $u(t_k)$ with sinusoidal signal fault.

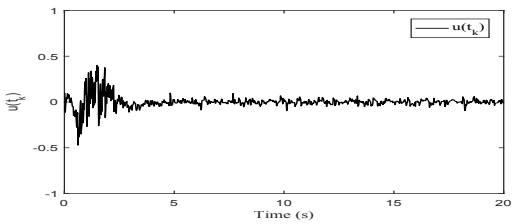

Fig. 11 Input curves of $u(t_k)$ with constant fault.

The simulation results verify the effectiveness of the designed method.

5. CONCLUSION

In this paper, two-channel FDI attacks have been designed via a NPC strategy for the NCS with sensor fault and actuator saturation. A state and fault estimator has been designed to estimate system states and sensor fault simultaneously. A predictive controller which can generate a sequence of predictive control signals has been designed to actively compensate the time-varying delays. A sufficient condition has been derived for stability of the NCS by using the switched system theory. A numerical example has been given to illustrate the effectiveness and potential for the developed techniques.

REFERENCES

Hu et al.(2017) Robust H_∞ control for networked systems with transmission delays and successive packet dropouts under stochastic sampling. *International Journal of Robust & Nonlinear Control*, 27(1), 84-107.

Yuan et al.(2016) Resilient control of networked control system under DoS attacks: A unified game approach. *IEEE Transactions on Industrial Informatics*, 12(5), 1786-1794.

Wang et al.(2016) Event-triggered fault detection filter design for a continuous-time networked control system. *IEEE Transactions on Cybernetics*, 46(12), 3414-3426.

Li et al.(2017) Robust tracking control of networked control systems with communication constraints and external disturbance. *IEEE Transactions on Industrial Electronics*, 64(5), 4037-4047.

Zhang et al.(2017) Analysis and synthesis of networked control systems: A survey of recent advances and challenges. *ISA Transactions*, 66, 376-392.

Yang et al.(2018) Nonuniform sampling Kalman filter for networked systems with Markovian packets dropout *Journal of the Franklin Institute*, 335(10), 4218-4240.

Lei et al.(2016) False data injection attack on consensus-based distributed estimation. *International Journal of Robust and Nonlinear Control*, 27(9), 3595-3610.

Feng et al.(2016) Distributed consensus tracking for multi-agent systems under two types of attacks. *International Journal of Robust and Nonlinear Control*, 26(5), 896-918.

Ding et al.(2017) Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. *Automatica*, 78, 231-240.

Pang et al.(2012) Design and implementation of secure networked predictive control systems under deception attacks. *IEEE Transactions on Control Systems Technology*, 20(5), 1334-1342.

Amin et al.(2013) Cyber security of water SCADA systems-part i: Analysis and experimentation of stealthy deception attacks. *IEEE Transactions on Control Systems Technology*, 21(5), 1963-1970.

Manandhar et al.(2014) Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Transactions on Control of Network Systems*, 1(4), 370-379.

Guo et al.(2017) Optimal linear cyber-attack on remote state estimation. *IEEE Transactions on Control of Network Systems*, 4(1), 4-13.

Pang et al.(2016) Two-channel false data injection attacks against output tracking control of networked systems. *IEEE Transactions on Industrial Electronics*, 63(5), 3242-3251.

Feng G.(2015) Control design for a class of affine nonlinear descriptor systems with actuator saturation. *IEEE Transactions on Automatic Control*, 60(8), 2195-2200.

Yanumula et al.(2017) Consensus of second-order multi-agents with actuator saturation and asynchronous time-delays. *IET Control Theory & Applications*, 11(17), 3201-3210.

Lee et al.(2018) Observer-based H_∞ fault-tolerant control for linear systems with sensor and actuator faults. *IEEE Systems Journal*, 13(2), pp. 1981-1990.

Xu et al.(2018) Generalized correntropy filter-based fault diagnosis and tolerant control for non-gaussian stochastic systems subject to sensor faults. *IEEE Access*, 6, 12598-12607.

Zhang et al.(2013) Fuzzy delay compensation control for T-S fuzzy systems over network. *IEEE Transactions on Cybernetics*, 43(1), 259-268.

Li et al.(2014) Network-based predictive control for constrained nonlinear systems with two-channel packet dropouts. *IEEE Transactions on Industrial Electronics*, 61(3), 1574-1582.

Zhan et al.(2013) Consensus of sampled-data multi-agent networking systems via model predictive control. *Automatica*, 49(8), 2502-2507.

Pang et al.(2013) Active fault tolerant control of networked systems with sensor fault. *Chinese Control And Decision Conference*, 6468-6473.

Geng et al.(2018) Self-triggered sampling control for networked control systems with delays and packets dropout. *International Journal of Systems Science*, 47(15), 1464-5319.