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; ffc@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 NCSs Yang 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

\[ x(k+1) = Ax(k) + Bsat(u(k)) + \omega(k), \]

\[ z(k) = Cx(k) + \nu(k), \]

\[ y(k) = z(k) + Ff(k), \]

where \( u(k) \in \mathbb{R}^p, x(k) \in \mathbb{R}^n, z(k) \in \mathbb{R}^q \) and \( y(k) \in \mathbb{R}^q \) are vectors of the control input, the system state, the system output and the output signal of the sensor, respectively. \( A, B \in \mathbb{R}^{n \times n}, C \in \mathbb{R}^{q \times n} \) are constant matrices. \( \omega(k) \) and \( \nu(k) \) are system noise and output noise, respectively. \( F \in \mathbb{R}^{q \times m} \) is a fault distribution matrix and \( f(k) \in \mathbb{R}^m \) 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.](image)

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 \( \tau_{ac}(k) \) and \( \tau_{ca}(k) \), respectively. The upper bounds of \( \tau_{ac}(k) \) and \( \tau_{ca}(k) \) are \( \tau_{ac} \) and \( \tau_{ca} \), respectively. The round-trip time (RTT) delay is given as \( \tau(k) = \tau_{ac}(k) + \tau_{ca}(k) \) 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 \( \alpha(k) \). \( y_a(k) \) is the output signal to be attacked which is transmitted to the state and fault estimator. A control signal sequence \( \bar{u}(k+1), \bar{u}(k+2), \ldots, \bar{u}(k+\bar{\tau}(k)) \) is calculated by the predicted controller and transmitted to the actuator through networks. \( \bar{u}_a(k+1), \bar{u}_a(k+2), \ldots, \bar{u}_a(k+\bar{\tau}(k)) \) 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 \( \bar{u}_a(k) \). The saturation function is given as

\[ sat(u(t_k)) = \begin{cases} 1, & \text{if } u(t_k) \geq 1 \\ -1, & \text{if } u(t_k) \leq -1 \\ u(t_k), & \text{if } 0 < u(t_k) < 1 \end{cases} \]

with \( sat(u_i(t_k)) = \begin{cases} 0, & \text{if } u_i(t_k) \geq 1 \\ -1, & \text{if } u_i(t_k) \leq -1 \\ u_i(t_k), & \text{if } 0 < u_i(t_k) < 1 \end{cases} \)

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)].

\[ \hat{x}(k_s+1|k_s) = A\hat{x}(k_s) + Bsat(u(k_s)), \]

\[ \hat{x}(k_s + 1) = \hat{x}(k_s + 1|k_s) + K_1y_a(k_s + 1) - C\hat{x}(k_s + 1|k_s) - F\hat{f}(k_s + 1), \]

\[ \hat{f}(k_s + 1) = M_1C\hat{x}(k_s + 1|k_s) + K_2y_a(k_s) - C\hat{x}(k_s|k_s - 1) - F\hat{f}(k_s) - M_1y_a(k_s + 1). \]

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 \( \chi^2 \) anomaly detector is designed using the estimator in equations (4)-(6). The residual \( \zeta(k) \) is defined as

\[ \zeta(k_s) = y_a(k_s) - C\hat{x}(k_s|k_s - 1) - F\hat{f}(k_s). \]

The residual \( \zeta(k_s) \) is Gaussian independent identically distributed with zero mean and covariance \( \zeta \sim N(0, \zeta) \). At each time instant, the \( \chi^2 \) anomaly detector first computes the value of \( \zeta(k_s) \), and then compares \( \zeta(k_s) \) with a prescribed threshold \( \zeta \). If \( \zeta(k_s) > \zeta \), then an alarm will be triggered. When the system operates normally (i.e., without attacks), \( \zeta(k_s) \) satisfies a \( \chi^2 \) distribution implying low probability of a large \( \zeta(k_s) \). Moreover, the FDI attacks in the feedback and forward communication channels lead to a value of \( ||\zeta(k_s)|| \) 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 \( L \in \mathbb{R}^{p \times n} \) 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 \( k_s + \tau_{ac} \) are obtained as
\(\hat{x}(k + i|k) = A\hat{x}(k + i - 1|k) + B\text{sat}(\hat{u}(k + i - 1|k))\)
\[\hat{u}(k + i|k) = -L\hat{x}(k + i|k)\]
for \(i = 1, 2, \ldots, \tau_{ca}\). For \(k = k - \tau_{ca}(k)\), then the predictive controller at time instant \(k\) is designed as
\[\hat{u}(k) = \hat{u}(k + \tau_{ca}(k)|k) = -L\hat{x}(k)\] \hspace{1cm} (8)

The predictions of the system state and control signal up to time \(k + \tau_{ca}\) are given as
\[\hat{x}(k + i|k) = A\hat{x}(k + i - 1|k) + B\text{sat}(\hat{u}(k + i - 1|k)),\] \hspace{1cm} (9)
\[\hat{u}(k + i|k) = -L\hat{x}(k + i|k),\] \hspace{1cm} (10)
for \(i = 1, 2, \ldots, \tau_{ca}\), 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.

\[U_k = [\hat{u}(k + 1|k), \hat{u}(k + 2|k), \ldots, \hat{u}(k + \tau_{ca}|k)]^T.\] \hspace{1cm} (11)

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
\[y_k = y(k) + \alpha(k),\] \hspace{1cm} (12)
with \(k_s = k - \tau_{ca}(k)\) and
\[\alpha(k) = -y(k) + C\hat{x}(k|k - 1) + F\hat{f}(k) + \xi(k),\] \hspace{1cm} (13)
where \(\xi(k)\) is the Gaussian white noise with \(\xi(k) \sim N(0, \rho)\) and \(\rho\) is a covariance matrix. It is obvious that the residual \(\zeta(k)\) is Gaussian 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 \(U_k^a = [\hat{u}_a(k_c + 1|k_c), \hat{u}_a(k_c + 2|k_c), \ldots, \hat{u}_a(k_c + \tau_{ca}|k_c)]^T\) with
\[\hat{u}_a(k + i|k) = \hat{u}_a(k + i|k_c) + \beta(k + i),\] \hspace{1cm} (14)
for \(k_c = k - \tau_{ca}(k), \hat{u}_a(k + i|k)\) is the attacked control prediction and \(\beta(k + i)\) are the forward channel attacks for \(i = 1, 2, \ldots, \tau_{ca}\). The attacks in forward channel can be given as
\[\beta(k + 1) = \Gamma\beta(k),\] \hspace{1cm} (15)
where \(\Gamma \in \mathbb{R}^{p \times p}\) 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
\[u_a(k) = \hat{u}_a(k_c + \tau_{ca}(k)|k_c),\] \hspace{1cm} (16)
which is selected in the control prediction sequence \(U_k\) to control the plant. Under the FDI attacks in equations (11) and (13), the NCS (1)-(3) is expressed as
\[x(k + 1) = Ax(k) + B\text{sat}(u_a(k + 1)) + \omega_k,\] \hspace{1cm} (17)
\[y_a(k) = Cx(k) + Fu(k + \nu(k) + \alpha(k).\] \hspace{1cm} (18)

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
\[\eta^T(u(k))M\eta(u(k)) \leq \varepsilon u^T(k)M u(k),\] \hspace{1cm} (19)
where \(\eta = [\eta_1, \eta_2, \ldots, \eta_p]^T \in \mathbb{R}^p\) with \(\eta_i\) is the dead-zone nonlinearity function, \(i = 1, 2, \ldots, p\). \(M\) 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
\[e_x(k) = x(k) - \hat{x}(k),\] \hspace{1cm} (20)
\[e_f(k) = f(k) - \hat{f}(k).\] \hspace{1cm} (21)

Theorem 1. If there exist matrices \(Q, K_1\) and \(K_2\) such that the following inequality holds
\[\Phi^TQ\Phi - Q < 0,\] \hspace{1cm} (22)
where \(\Phi = \begin{bmatrix} A - K_1C & -K_1F \\ M_1CA - K_2C - K_2F \end{bmatrix}\) hold, then the following equations are guaranteed limit \(\lim_{k_s \to \infty} E(e_x) = 0\) and \(\lim_{k_s \to \infty} E(e_f(k)) = 0\).

Proof. From equations (4)-(6) and (16)-(19), the estimation errors of system state and sensor fault are given as \(e_x(k + 1) = (A - K_1C)e_x(k) - K_1Fe_f(k) + \omega_k - K_1\nu_k - K_1\alpha(k)\) and \(e_f(k + 1) = M_1CAe_x(k) - K_2Ce_f(k) + K_2\alpha(k) + M_1\nu_k + M_1\alpha(k + 1)\). Then, we have \(E(e_x(k + 1)) = \Phi E(e_x(k))\), \(where e_x(k) = [e_x^T(k) e_f(k)]^T\). Give a Lyapunov function
\[V(e_x) = E(e_x^T(k))Q E(e_x(k)).\] \hspace{1cm} (23)
We have \(\Delta V(e_x) = E(e_x^T(k))Q^T \Phi E(e_x(k)) < 0\) if \(\Phi^TQ\Phi - Q < 0\). As a result, we have \(\lim_{k_s \to \infty} E(e_x) = 0\) and \(\lim_{k_s \to \infty} E(e_f(k)) = 0\). The proof is completed.

Theorem 2. Under two-channel FDI attacks, the NCS (16)-(17) is stable with \(\lim_{k_s \to \infty} E(x(k)) = 0\) if there exist \(\varepsilon > 0\) positive definite matrices \(P_1\) and \(P_2\) such that the following inequalities hold for all \(i, j \in \{0, 1, 2, \ldots, \tau\}\)
\[2\varepsilon^T P_2 \Gamma \Omega_i - P_1 + 4(1 + \varepsilon)\Pi^T \Omega_i \Pi < 0\] \hspace{1cm} (24)
where \(\Xi = [I_{n}, 0_{n \times (\tau + 2)n\times n}, T, \Omega_i = -BL(A - BL)^i, i = 0, 1, 2, \ldots, n\times T \in [0_{n \times (\tau + 1)n}, I_{n}, 0_{n \times (\tau + 1)n}^T] and \Lambda_i = \begin{bmatrix} A & 0_{n \times n} & K_1C & K_1F \\ I_{n} & 0_{n \times n} & 0_{n \times n} & 0_{n \times n} \\ 0_{2n \times (\tau + 1)n} & 0_{n \times n} & -K_1C & -K_1F \end{bmatrix} M_1C - K_2C - K_2F \end{bmatrix}\] \hspace{1cm} (25)
Proof. It is obtained from (4), (5), (18) and (19) that
\[
\hat{x}(k + 1|k) = A\hat{x}(k|k − 1) + K_1C_{ex}(k) + K_1F_{ef}(k) + B\text{sat}(u(k) + \ldots)
\]

From equations (8)-(10), it is noted that \( u(k) = -\dot{L}\dot{x}(k) = -L(A - BL)^T\hat{x}(\tau(k))\). Give a switched Lyapunov function as \( V(X(k)) = E(\hat{X}(T(k)))P_1E(X(k)) \). It is shown that
\[
\Delta V(\hat{X}(k)) \leq E(\hat{X}(T(k)))(2\Lambda_i^T P_j \Lambda_i - P_i)E(\hat{X}(k)) + 2\text{sat}(u^T(k) + \beta^T(k))B^T\Sigma T P_j \Sigma Bu(k)
\]

Then, we have
\[
\Delta V(\hat{X}(k)) \leq E(\hat{X}(T(k)))(2\Lambda_i^T P_j \Lambda_i - P_i) + 4(1 + \varepsilon)\Pi^T \Omega^T \Sigma T P_j \Sigma \Xi \Sigma \hat{X}(k),
\]

If there exist \( P_i, P_j \) such that \( 2\Lambda_i^T P_j \Lambda_i - P_i + 4(1 + \varepsilon)\Pi^T \Omega^T \Sigma T P_j \Sigma \Xi \Xi \Omega \Pi \leq 0 \), 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 \( \lim_{k \to \infty} E(x(k)) = 0 \).

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.](image)

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

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>( M )</td>
<td>1.096 Kg</td>
<td>Mass of the cart</td>
</tr>
<tr>
<td>( m )</td>
<td>0.109 Kg</td>
<td>Mass of the pendulum rod</td>
</tr>
<tr>
<td>( I )</td>
<td>0.25 m</td>
<td>Length from axis to centroid</td>
</tr>
<tr>
<td>( b )</td>
<td>0.1 N/m/sec</td>
<td>The friction coefficient of cart</td>
</tr>
<tr>
<td>( g )</td>
<td>9.81 m/s^2</td>
<td>Gravitational constant</td>
</tr>
</tbody>
</table>

Table 1. The parameters in the inverted pendulum model

In the NCS (16)-(17), the upper bound of the time-varying delays for feedback and forward communication channels are given as \( \tau_{sc}(k) = 4 \) and \( \tau_{ca}(k) = 6 \), respectively. FDI attacks are considered to stick 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

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

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.

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

![Fig. 7 System states and observer states curves with constant fault.](image)

![Fig. 8 Output curves of $y(t_k)$ with sinusoidal signal fault.](image)

![Fig. 9 Output curves of $y(t_k)$ with constant fault.](image)

![Fig. 10 Input curves of $u(t_k)$ with sinusoidal signal fault.](image)
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


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


