Two-Channel False Data Injection Attacks against Output Tracking Control of Networked Systems

Zhong-Hua Pang, *Member, IEEE,* Guo-Ping Liu, *Fellow, IEEE,*
Donghua Zhou, *Senior Member, IEEE,* Fangyuan Hou, and Dehui Sun

***Abstract*—This paper addresses the design problem of false data injection (FDI) attacks against the output tracking control of networked systems, where the network-induced delays in the feedback and forward channels are considered. The main contributions of this paper are as follows: (i) To actively compensate for the two-channel network-induced delays, a Kalman filter-based networked predictive control scheme is designed for stochastic linear discrete-time systems; (ii) From an attacker's perspective, stealthy FDI attacks are proposed for both the feedback and forward channels so as to disrupt the stability of the resulting closed-loop system while avoiding the detection of a Kalman filter-based attack detector; (iii) Both numerical simulations and practical experiments are carried out to show the effectiveness of the proposed method.**

***Index Terms*—False data injection attacks, networked control systems (NCSs), network-induced delay, output tracking control, predictive control, stability analysis.**

I. Introduction

NETWORKED control systems (NCSs) are control systems in which the controller and the plant are connected via communication networks, which have many merits such as simple installation and maintenance, reduced weight and power requirement, as well as high flexibility and reliability. However, the introduction of networks into the control loop inevitably causes some adverse effects such as network-induced delay and packet dropout, which may deteriorate the system performance or even destabilize the closed-loop system. Therefore, NCSs have become an active research topic in the past decade [1]-[5].

Nowadays, NCSs have found numerous applications in various fields such as process control, intelligent transportation, as well as the measurement and control of critical infrastructures (e.g., electricity, water, and gas distribution). In these systems, measurement data and control commands travel through the open and unprotected network, which are susceptible to be corrupted by attackers [6]-[9]. For example, the typical malwares such as Stuxnet and Duqu have been reported to disrupt the control systems of critical infrastructures [10]. Such attacks may significantly hamper the economy and environment, and even endanger human lives. Therefore, the security of NCSs is of paramount importance for various applications.

A. Related Work

Network attacks can be classified into two kinds: denial of service (DoS) attacks and deception attacks [11]-[13]. The DoS attacks aim to obstruct the transmission of data. To handle them, some secure control schemes have been proposed in [14]-[16]. Deception attacks are to compromise the integrity of data, which are usually more subtle and stealthy than DoS attacks. Typical deception attacks include data replay attacks and false data injection (FDI) attacks. In [17] and [18], Mo et al. analyzed the performance of the control system under replay attacks, and provided model-based countermeasures to improve the probability of attack detection.

The FDI attacks against the measurement data and control commands are to a certain degree similar to sensor faults and actuator faults, respectively. However, the faults are usually assumed to be random and independent events with a fixed failure rate probability. On the contrary, the FDI attacks can be carefully designed by smart attackers so as to cause the greatest possible damage without being detected, which thus may result in more serious consequences. In this case, such smart attacks would be difficult to detect by existing fault detection techniques [19]-[21].

During the past five years, the FDI attacks have been paid increasing attention. Mo et al. [22] proposed a simple FDI attack model to compromise the sensors of a linear control system. Manandhar et al. [23] showed that the FDI attack in [22] could be detected by the proposed Euclidean-based detector. Niu and Huie [24] analyzed the impact of the sensor

Manuscript received August 21, 2015; revised December 08, 2015; accepted January 09, 2016.

This work was supported in part by the National Natural Science Foundation of China under Grant 61203230, Grant 61273104, Grant 61333003, Grant 61210012, Grant 61490701, Grant 61174116, and Grant 61573024, in part by the Beijing Natural Science Foundation under Grant 4152014, in part by the Outstanding Young Scientist Award Foundation of Shandong Province of China under Grant BS2013DX015, in part by the Scientific Research Foundation of North China University of Technology (NCUT), in part by the Excellent Youth Scholar Nurturing Program of NCUT, in part by the Fund of Key Laboratory of Wireless Sensor Network and Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, in part by the Fund of Key Laboratory of Embedded System and Service Computing, Ministry of Education, Tongji University, China, and in part by the Research Fund for the Taishan Scholar Project of Shandong Province of China.

Z. H. Pang and D. Sun are with Key Laboratory of Fieldbus Technology and Automation of Beijing, North China University of Technology, Beijing 100144, China (e-mail: zhonghua.pang@ia.ac.cn, sundehui@ncut.edu.cn).

G. P. Liu is with the School of Engineering, University of South Wales, Pontypridd CF37 1DL, UK and is also with the CTGT Center, Harbin Institute of Technology, Harbin 150001, China (e-mail: guoping.liu@southwales.ac.uk).

D. Zhou is with the College of Electrical Engineering and Automation, Shandong University of Science and Technology, Qingdao 266590, China and is also with the Department of Automation, Tsinghua University, Beijing 100084, China (e-mail: zdh@mail.tsinghua.edu.cn).

F. Hou is with the School of Automation, Beijing Institute of Technology, Beijing 100081, China (e-mail: fang_and_yuan@126.com).

FDI attack on the performance of the Kalman filter for linear dynamic systems. Teixeira et al. [25] studied the cyber security of state estimators in supervisory control and data acquisition systems, and showed that undetectable FDI attacks could be designed even when an attacker had limited resources. Kwon et al. [26] gave the conditions under which the FDI attacks on the sensors or/and actuators could fail the state estimators while successfully bypassing the monitoring system.

As can be seen from the above, the studies on stealthy FDI attacks are only in their embryonic stage. Furthermore, in the aforementioned works [22]-[26], there exist some common drawbacks: (i) All of them are not concerned with the network-induced constraints although they are inevitable in practical NCSs. (ii) In [22]-[25], only the FDI attacks on the measurement data are considered, and in [26], although the FDI attacks on both sensors and actuators are considered, only the case of open-loop control is investigated. (iii) The theoretical results in [22]-[26] are just tested by numerical simulation. The foregoing three facts motivate the present study.

B. Contributions and Outline

The goal of this paper is to design the FDI attacks on the measurement data in the feedback channel and the control commads in the forward channel so as to destroy the output tracking performance of NCSs without being detected. The network-induced delays in the feedback and forward channels are considered, and the predictive control scheme in [27] is extended to solve the networked output tracking problem for a stochastic linear system. It is assumed that the NCS is equipped with a Kalman filter-based attack detector in the controller. Then, we propose stealthy FDI attack models for the two channels of the NCS to destabilize the closed-loop system while successfully bypassing the attack detector.

Compared with the existing works on the FDI attacks [22]-[26], the main advantages of this paper include the following three aspects: (i) The two-channel network-induced delays are considered, and then to compensate for them, a Kalman filter-based networked predictive output tracking control (NPOTC) scheme is designed; (ii) For the resulting closed-loop NCSs, the stealthy FDI attacks are proposed for both the feedback and forward channels, and thus the results derived in this paper are more general than those in [22]-[26]; (iii) Beyond the simulation verification, a Internet-based servo motor system is constructed to show the effectiveness of the proposed method.

This paper is organized as follows. In Section II, a Kalman filter-based NPOTC scheme is proposed. Two-channel FDI attacks and their effect on the resulting NPOTC system are introduced in Section III. In Section IV, two-channel stealthy FDI attack models are designed and the main results for them are presented. Simulation and experimental results for different attack scenarios are presented in Section V and VI, respectively. Section VII concludes this paper.

Notation: The notations used here are fairly standard. $\Delta x(k)$ is defined as $\Delta x(k) = x(k)-x(k-1)$. $x(k+i|k)$ refers to the ith-step-ahead predictive value of $x(k)$ based on the data up to time k. $\mathbf{E}(\cdot)$ denotes the mathematical expectation operation.

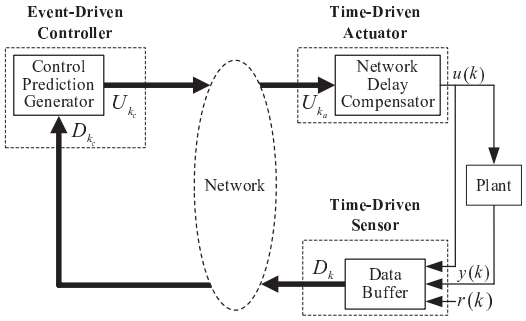


Fig. 1. NPOTC systems.

II. Kalman Filter-Based NPOTC Systems

An NPOTC system is designed, as depicted in Fig. 1, which consists of five parts: a physical plant, a data buffer in the sensor, a communication network, a control prediction generator in the controller, and a network delay compensator in the actuator. Each part will be described in the following subsections. It is assumed that the sensor and actuator are time-driven and synchronous, while the controller is event-driven.

A. Physical Plant

Suppose that the physical plant in Fig. 1 is described by the following linear system:

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) + \omega(k) \\ y(k) &= Cx(k) + \upsilon(k) \end{aligned} \tag{1}$$

where $x(k) \in \mathbb{R}^n$ is the system state, $u(k) \in \mathbb{R}^m$ is the control input, $y(k) \in \mathbb{R}^q$ is the measurement output, $\omega(k) \in \mathbb{R}^n$ is the system noise, and $\upsilon(k) \in \mathbb{R}^q$ is the measurement noise. A, B, and C are system matrices with appropriate dimensions. $\omega(k)$ and $\upsilon(k)$ are the uncorrelated Gaussian white noises with

$$\omega(k) \sim \mathcal{N}(0, Q) \text{ and } \upsilon(k) \sim \mathcal{N}(0, R)$$

where Q and R are the covariance matrices. It is assumed that (A, C) is observable, (A, B) is controllable, and the matrix $\begin{bmatrix} A - I_n & B \\ C & 0_{q\times m} \end{bmatrix}$ has full row rank.

The incremental form of (1) is

$$\begin{aligned} \Delta x(k+1) &= A\Delta x(k) + B\Delta u(k) + \Delta\omega(k) \\ \Delta y(k) &= C\Delta x(k) + \Delta\upsilon(k). \end{aligned} \tag{2}$$

Define the output tracking error

$$e(k) = r(k) - y(k) \tag{3}$$

where $r(k) \in \mathbb{R}^q$ is the reference input. It is obtained from (2) and (3) that

$$\begin{aligned} e(k+1) =& e(k) - CA\Delta x(k) - CB\Delta u(k) + \Delta r(k+1) \\ & - C\Delta\omega(k) - \Delta\upsilon(k+1). \end{aligned} \tag{4}$$

From (2) and (4), we obtain the following augmented system:

$$\begin{aligned} x_e(k+1) &= A_e x_e(k) + B_e\Delta u(k) + E_e\Delta r(k+1) \\ &\quad + W_e\Delta\omega(k) + V_e\Delta\upsilon(k+1) \\ \Delta y(k) &= C_e x_e(k) + \Delta\upsilon(k) \end{aligned} \tag{5}$$

where

$$x_e(k)=\begin{bmatrix}\Delta x(k)\\ e(k)\end{bmatrix}\in\mathbb{R}^{\bar{n}},\ A_e=\begin{bmatrix}A & 0_{n\times q}\\ -CA & I_q\end{bmatrix},$$
$$B_e=\begin{bmatrix}B\\ -CB\end{bmatrix},\ E_e=\begin{bmatrix}0_{n\times q}\\ I_q\end{bmatrix},\ W_e=\begin{bmatrix}I_n\\ -C\end{bmatrix},$$
$$V_e=\begin{bmatrix}0_{n\times q}\\ -I_q\end{bmatrix},\ C_e=\begin{bmatrix}C & 0_{q\times q}\end{bmatrix},\ \bar{n}=n+q.$$

Thus, the output tracking problem of system (1) can be solved by the feedback control of the augmented state $x_e(k)$.

B. Data Buffer

In general, the full state of the plant is not directly measurable. To obtain the estimation of the state $x(k)$ in the controller, at each sampling instant k, the following data

$$D_k=\left[y(k)^T\ u(k-1)^T\ R(k)^T\right]^T \tag{6}$$

are transmitted to the controller together with the timestamp k, where $R(k)=[r(k)^T\ r(k+1)^T\cdots r(k+\bar{\tau})^T]^T$.

C. Communication Network

The Ethernet-like network is considered in this paper. The packets travel through the network from the sensor to the controller and then from the controller to the actuator. As a result, network-induced delays are inevitable during the packet transmission, which are generally random with unknown distribution. In this paper, it is assumed that the round-trip time (RTT) delay τ_k is bounded by $\bar{\tau}$.

D. Control Prediction Generator

To obtain the state estimation $\hat{x}(k_c)$, the following Kalman filter is usually used [18]:

$$\begin{cases}P_{k_c|k_c-1}=AP_{k_c-1}A^T+Q\\ K_{k_c}=P_{k_c|k_c-1}C^T(CP_{k_c|k_c-1}C^T+R)^{-1}\\ P_{k_c}=(I-K_{k_c}C)P_{k_c|k_c-1}\\ \hat{x}(k_c|k_c-1)=A\hat{x}(k_c-1)+Bu(k_c-1)\\ \hat{x}(k_c)=\hat{x}(k_c|k_c-1)+K_{k_c}\big(y(k_c)-C\hat{x}(k_c|k_c-1)\big)\end{cases} \tag{7}$$

with the initial conditions

$$\hat{x}(0)=\mathbf{E}\big(x(0)\big),\quad P_0=\mathbf{E}\Big(\big(x(0)-\hat{x}(0)\big)\big(x(0)-\hat{x}(0)\big)^T\Big)$$

where $k_c\le k$ is the timestamp of the following feedback data available in the controller:

$$D_{k_c}=\left[y(k_c)^T\ u(k_c-1)^T\ R(k_c)^T\right]^T. \tag{8}$$

Although the filter gain K_{k_c} in (7) is time-varying, it usually converges in a few steps [18]. Hence, K can be defined as

$$K\triangleq PC^T(CPC^T+R)^{-1} \tag{9}$$

where $P\triangleq\lim_{k_c\to\infty}P_{k_c|k_c-1}$, and thus the Kalman filter in (7) is reduced to the following estimator with a fixed gain:

$$\begin{cases}\hat{x}(k_c|k_c-1)=A\hat{x}(k_c-1)+Bu(k_c-1)\\ \hat{x}(k_c)=\hat{x}(k_c|k_c-1)+K\big(y(k_c)-C\hat{x}(k_c|k_c-1)\big).\end{cases} \tag{10}$$

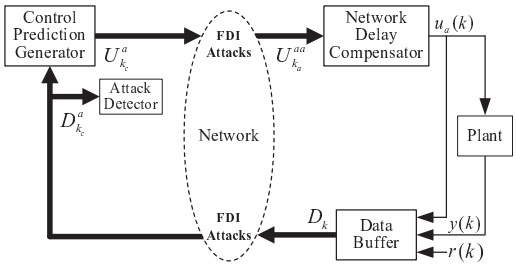


Fig. 2. NPOTC systems under two-channel FDI attacks.

The following state feedback control law is designed:

$$\Delta\hat{u}(k_c|k_c)=-L\hat{x}_e(k_c) \tag{11}$$

where $\hat{x}_e(k_c)=[\Delta\hat{x}(k_c)^T\ e(k_c)^T]^T$, and $L\in\mathbb{R}^{m\times\bar{n}}$ is the gain matrix. Then the predicted augmented states and control increments from k_c+1 to $k_c+\bar{\tau}$ are obtained as follows:

$$\begin{aligned}\hat{x}_e(k_c+i|k_c)=&A_e\hat{x}_e(k_c+i-1|k_c)+B_e\Delta\hat{u}(k_c+i-1|k_c)\\ &+E_e\Delta r(k_c+i)\end{aligned} \tag{12}$$

$$\Delta\hat{u}(k_c+i|k_c)=-L\hat{x}_e(k_c+i|k_c) \tag{13}$$

for $i=1,2,\cdots,\bar{\tau}$, where $\hat{x}_e(k_c+i|k_c)=[\Delta\hat{x}(k_c+i|k_c)^T\ e(k_c+i|k_c)^T]^T$, and $\hat{x}_e(k_c|k_c)=\hat{x}_e(k_c)$. Thus, we obtain the following i-step control predictions:

$$\hat{u}(k_c+i|k_c)=\hat{u}(k_c+i-1|k_c)+\Delta\hat{u}(k_c+i|k_c) \tag{14}$$

for $i=0,1,2,\cdots,\bar{\tau}$, where $\hat{u}(k_c-1|k_c)=u(k_c-1)$. Clearly, Equation (14) yields the control prediction sequence

$$U_{k_c}=[\hat{u}(k_c|k_c)^T\ \hat{u}(k_c+1|k_c)^T\cdots\hat{u}(k_c+\bar{\tau}|k_c)^T]^T \tag{15}$$

which is sent to the actuator together with the timestamp k_c.

E. Network Delay Compensator

In the actuator, the network delay compensator is designed to store the latest control prediction sequence and then use it to control the plant. Without loss of generality, the latest control prediction sequence at time k is expressed as

$$U_{k_a}=[\hat{u}(k_a|k_a)^T\ \hat{u}(k_a+1|k_a)^T\cdots\hat{u}(k_a+\bar{\tau}|k_a)^T]^T \tag{16}$$

where $k_a\le k_c$ is the timestamp of U_{k_a}. Its RTT delay is

$$\tau_k=k-k_a. \tag{17}$$

To compensate for the RTT delay, the following control signal is chosen to control the plant at time k:

$$u(k)=\hat{u}(k_a+\tau_k|k_a)=\hat{u}(k|k-\tau_k). \tag{18}$$

III. FDI ATTACKS AGAINST NPOTC SYSTEMS

It is assumed that the attacker is able to (i) read the data transmitted through the feedback and forward channels and modify them arbitrarily, and (ii) know the system parameters, i.e., A, B, C, Q, and R. The objective of this paper is to design stealthy FDI attacks on the feedback data and the control data (see Fig. 2), i.e., D_{k_c} in (8) and U_{k_a} in (16), such that the

resulting NPOTC system becomes unstable while the two-channel FDI attacks fail to be detected.

As shown in Fig. 2, under FDI attacks, the feedback data arriving at the controller are assumed to be modified as

$$D_{k_c}^a = \left[y_a(k_c)^T \ u(k_c-1)^T \ R(k_c)^T\right]^T \tag{19}$$

with

$$y_a(k_c) = y(k_c) + \alpha(k_c) \tag{20}$$

where $y_a(k_c)$ is the attacked output, and $\alpha(k_c)$ is the feedback channel attack. Similarly, the control data arriving at the actuator are falsified by the attacker as

$$U_{k_a}^{aa} = [\hat{u}_a(k_a|k_a)^T \ \hat{u}_a(k_a+1|k_a)^T \cdots \hat{u}_a(k_a+\bar{\tau}|k_a)^T]^T \tag{21}$$

with

$$\hat{u}_a(k_a+i|k_a) = \hat{u}(k_a+i|k_a) + \beta(k_a+i) \tag{22}$$

for $i = 0, 1, 2, \cdots, \bar{\tau}$, where $\hat{u}_a(k_a+i|k_a)$ is the attacked control prediction, and $\beta(k_a+i)$ is the forward channel attack.

Remark 1: It is noted that the FDI attacks in (20) and (22) are respectively related to the timestamps of the packets transmitted through the feedback and forward channels, i.e., k_c and k_a. In the NPOTC system, the packet transmitted through networks is with a timestamp. As a consequence, although the measurement data and control data are randomly delayed in their transmission due to the presence of random network-induced delays, with the help of the timestamps, the FDI attacks in (20) and (22) can still be easily designed.

To detect these FDI attacks, a general strategy is to deploy a detector in the controller, as shown in Fig. 2. Here, an attack detector is designed using the Kalman filter in (10) as well as the feedback data $D_{k_c}^a$ in (19). Due to the presence of FDI attacks, the Kalman filter in (10) becomes

$$\begin{cases} \hat{x}_a(k_c|k_c-1) = A\hat{x}_a(k_c-1) + Bu(k_c-1) \\ \hat{x}_a(k_c) = \hat{x}_a(k_c|k_c-1) + K\big(y_a(k_c) - C\hat{x}_a(k_c|k_c-1)\big) \end{cases} \tag{23}$$

where $\hat{x}_a(k_c)$ is the state estimation under attacks. Then, the residual $z_a(k_c)$ is defined as

$$\begin{aligned} z_a(k_c) &= y_a(k_c) - \hat{y}_a(k_c) \\ &= y_a(k_c) - C\big(A\hat{x}_a(k_c-1) + Bu(k_c-1)\big) \end{aligned} \tag{24}$$

where $\hat{y}_a(k_c)$ is the output estimation under attacks. If some rough FDI attacks are performed in the feedback and forward channels, they usually leads to a large value of $\|z_a(k_c)\|$, which thus induces the detector to trigger an alarm.

If no attacks are injected into the NPOTC system, the residual is

$$\begin{aligned} z(k_c) &= y(k_c) - \hat{y}(k_c) \\ &= y(k_c) - C\big(A\hat{x}(k_c-1) + Bu(k_c-1)\big). \end{aligned} \tag{25}$$

Lemma 1 [18]: The residual $z(k_c)$ in (25) is Gaussian independent identically distributed (i.i.d.) with zero mean and covariance $S = CPC^T + R$, i.e.,

$$z(k_c) \sim \mathcal{N}(0, S). \tag{26}$$

Under the FDI attacks in (20) and (22), the physical plant is expressed as

$$\begin{aligned} x_a(k+1) &= Ax_a(k) + B\big(u(k) + \beta(k)\big) + \omega(k) \\ y(k) &= Cx_a(k) + \upsilon(k) \end{aligned} \tag{27}$$

where $x_a(k) \in \mathbb{R}^n$ is the system state under attacks. Equations (11), (12), and (13) also become

$$\Delta\hat{u}(k_c|k_c) = -L\hat{x}_{ea}(k_c) \tag{28}$$

$$\begin{aligned} \hat{x}_{ea}(k_c+i|k_c) =& A_e\hat{x}_{ea}(k_c+i-1|k_c) \\ &+ B_e\Delta\hat{u}(k_c+i-1|k_c) + E_e\Delta r(k_c+i) \end{aligned} \tag{29}$$

$$\Delta\hat{u}(k_c+i|k_c) = -L\hat{x}_{ea}(k_c+i|k_c) \tag{30}$$

for $i = 1, 2, \cdots, \bar{\tau}$, where $\hat{x}_{ea}(k_c+i|k_c) = [\Delta\hat{x}_a(k_c+i|k_c)^T \ e_a(k_c+i|k_c)^T]^T$, and $\hat{x}_{ea}(k_c|k_c) = \hat{x}_{ea}(k_c) = [\Delta\hat{x}_a(k_c)^T \ e_a(k_c)^T]^T$ with

$$e_a(k_c) = r(k_c) - y_a(k_c). \tag{31}$$

IV. Main Results

In this section, we investigate the design of stealthy FDI attacks in the feedback and forward channels for the NPOTC system. The following definition is first given.

Definition 1: The NPOTC system is successfully attacked, if the residual $z_a(k)$ follows the same distribution as $z(k)$, i.e.,

$$z_a(k) \sim \mathcal{N}(0, S) \tag{32}$$

and for the constant reference input,

$$\lim_{k\to\infty} \mathbf{E}\big(e_a(k)\big) = 0 \tag{33}$$

$$\lim_{k\to\infty} \mathbf{E}\big(e(k)\big) = \infty. \tag{34}$$

In this paper, the feedback channel attack is designed as

$$\alpha(k) = -y(k) + CA\hat{x}_a(k-1) + CBu(k-1) + \xi(k) \tag{35}$$

where $\xi(k) \sim \mathcal{N}(0, S)$ is the Gaussian white noise. It is clear form (24)-(26) that the feedback channel attack in (35) always satisfies the condition in (32), i.e.,

$$z_a(k) = \xi(k) \sim \mathcal{N}(0, S). \tag{36}$$

Next, the attacked output tracking error $e_a(k)$ in (33) is analyzed.

Theorem 1: Under the feedback channel FDI attack in (35), $\lim_{k\to\infty} \mathbf{E}\big(e_a(k)\big) = 0$ for the constant reference input if and only if the eigenvalues of matrix $A_e - B_eL$ are within the unit circle.

Proof: According to the network delay compensation strategy in (18), it is obtained from (28) and (30) that

$$\Delta u(k) = \Delta\hat{u}(k|k-\tau_k) = -L\hat{x}_{ea}(k|k-\tau_k) \tag{37}$$

where

$$\hat{x}_{ea}(k|k-\tau_k) = A_e\hat{x}_{ea}(k-1|k-\tau_k) + B_e\Delta\hat{u}(k-1|k-\tau_k). \tag{38}$$

Under the feedback channel attack in (35), from (20) we have

$$y_a(k) = CA\hat{x}_a(k-1) + CBu(k-1) + \xi(k) \tag{39}$$

and then from (23) and (31), we obtain

$$\Delta\hat{x}_a(k+1) = A\Delta\hat{x}_a(k) + B\Delta u(k) + K\Delta\xi(k+1) \quad (40)$$

$$\begin{aligned} e_a(k+1) &= e_a(k) - \Delta y_a(k+1) \\ &= e_a(k) - CA\Delta\hat{x}_a(k) - CB\Delta u(k) - \Delta\xi(k+1). \end{aligned} \quad (41)$$

The combination of (40) and (41) yields

$$\mathbf{E}\big(\hat{x}_{ea}(k+1)\big) = A_e\mathbf{E}\big(\hat{x}_{ea}(k)\big) + B_e\Delta u(k) \quad (42)$$

where $\hat{x}_{ea}(k) = [\Delta\hat{x}_a(k)^T \ e_a(k)^T]^T$. With (37), subtracting (29) from (42) leads to the following equation:

$$\begin{aligned} &\mathbf{E}\big(\hat{x}_{ea}(k+1)\big) - \hat{x}_{ea}(k+1|k-\tau_k) \\ =&A_e\Big(\mathbf{E}\big(\hat{x}_{ea}(k)\big) - \hat{x}_{ea}(k|k-\tau_k)\Big) \\ =&A_e^{\tau_k+1}\Big(\mathbf{E}\big(\hat{x}_{ea}(k-\tau_k)\big) - \hat{x}_{ea}(k-\tau_k|k-\tau_k)\Big) \\ =&0 \end{aligned} \quad (43)$$

since $\hat{x}_{ea}(k-\tau_k|k-\tau_k) = \hat{x}_{ea}(k-\tau_k)$. That is,

$$\hat{x}_{ea}(k|k-\tau_k) = \mathbf{E}\big(\hat{x}_{ea}(k)\big). \quad (44)$$

Then (37) can be rewritten as

$$\Delta u(k) = -L\mathbf{E}\big(\hat{x}_{ea}(k)\big). \quad (45)$$

Thus, substituting (45) into (42) gives rise to

$$\mathbf{E}\big(\hat{x}_{ea}(k+1)\big) = (A_e - B_eL)\mathbf{E}\big(\hat{x}_{ea}(k)\big). \quad (46)$$

It is obvious from (46) that $\lim_{k\to\infty}\mathbf{E}\big(e_a(k)\big) = 0$ if and only if the eigenvalues of $A_e - B_eL$ are within the unit circle. ■

Finally, we analyze the real output tracking error $e(k)$ in (34) for the constant reference input. Under the feedback channel attack in (35), it is obtained from (23) that

$$\hat{x}_a(k+1) = A\hat{x}_a(k) + Bu(k) + K\xi(k+1) \quad (47)$$

Then from (27) and (47), we have

$$\begin{aligned} \tilde{x}_a(k+1) &= x_a(k+1) - \hat{x}_a(k+1) \\ &= A\tilde{x}_a(k) + B\beta(k) + \omega(k) - K\xi(k+1). \end{aligned} \quad (48)$$

In this paper, the forward channel attack is designed as

$$\beta(k+1) = F\beta(k) \quad (49)$$

where $F \in \mathbb{R}^{m\times m}$ is the attack matrix. Combining (48) and (49) yields

$$X_\beta(k+1) = \Lambda X_\beta(k) \quad (50)$$

where

$$X_\beta(k) = \begin{bmatrix} \mathbf{E}\big(\tilde{x}_a(k)\big) \\ \beta(k) \end{bmatrix}, \ \Lambda = \begin{bmatrix} A & B \\ 0 & F \end{bmatrix}.$$

Then from (3), (27), (31), (39), and (47), we have

$$\mathbf{E}\big(e(k)\big) - \mathbf{E}\big(e_a(k)\big) = -C\mathbf{E}\big(\tilde{x}_a(k)\big). \quad (51)$$

Thus, we obtain

$$\lim_{k\to\infty}\mathbf{E}\big(e(k)\big) = -C\lim_{k\to\infty}\mathbf{E}\big(\tilde{x}_a(k)\big) \quad (52)$$

since $\lim_{k\to\infty}\mathbf{E}\big(e_a(k)\big) = 0$ if the matrix $A_e - B_eL$ is stable.

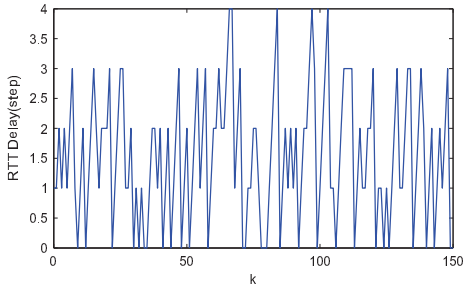


Fig. 3. RTT delays.

Obviously, the matrix Λ in (50) is a block upper triangular matrix. It is well known that a block upper triangular linear system is stable if and only if each block diagonal subsystem is stable. Thus, it can be concluded from (50) and (52) that, with the stable matrix $A_e - B_eL$, if A is stable and F is unstable, or if A is unstable, we will have $\lim_{k\to\infty}\mathbf{E}\big(e(k)\big) = \infty$. Therefore, we can obtain the following main results:

Theorem 2: Under the feedback channel attack in (35) and the forward channel attack in (49), the closed-loop NPOTC system is stable and further $\mathbf{E}\big(\mathrm{e}(\infty)\big) = 0$ if and only if the matrices $A_e - B_eL$, A, and F are stable.

Theorem 3: If the system matrix A is stable, the NPOTC system can be attacked successfully without being detected by injecting the feedback channel attack in (35) and the forward channel attack in (49) with an unstable matrix F.

Theorem 4: If the system matrix A is unstable, the NPOTC system can be attacked successfully without being detected by injecting the feedback channel attack in (35) and any arbitrary attack in the forward channel.

Remark 2: It is easy to observe from Theorems 3 and 4 that, no matter whether the system matrix A is unstable or stable, the control system can be attacked successfully without being detected. While in [22] and [26], it is required that the matrix A is unstable, where only the FDI attack on the sensor data are considered. Therefore, in this paper, by performing two-channel FDI attacks simultaneously, the derived results are more general.

V. Simulation Results

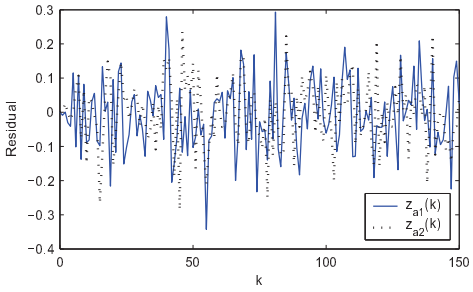
In this section, numerical simulations are carried out for three cases: (i) A and F are stable; (ii) A is stable and F is unstable; and (iii) A is unstable and F is stable. The network-induced delays in two channels are considered, which lead to 0∼4 steps RTT delays shown in Fig. 3.

A. Case 1: A and F are Stable

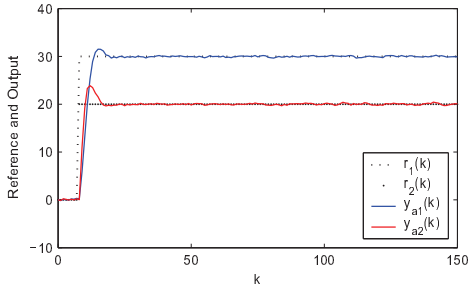
Consider a stable system with matrices

$$A = \begin{bmatrix} 0.2071 & 0.3705 & 0.0439 \\ 0.6072 & 0.5751 & 0.0272 \\ 0.6299 & 0.4514 & 0.3127 \end{bmatrix}, \ B = \begin{bmatrix} 0.1730 & 0.2523 \\ 0.9797 & 0.8757 \\ 0.2714 & 0.7373 \end{bmatrix},$$

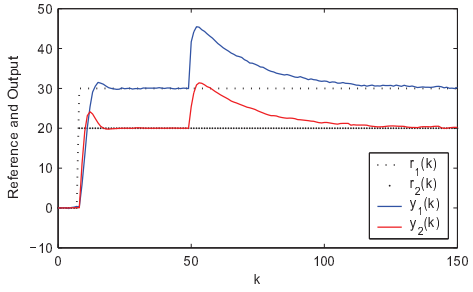
$$C = \begin{bmatrix} 0.1365 & 0.8939 & 0.2987 \\ 0.0118 & 0.1991 & 0.6614 \end{bmatrix}. \quad (53)$$



(a) Residual $z_a(k)$



(b) Attacked output response



(c) Real output response

Fig. 4. Simulation results of Case 1.

With Q= 0.0001 and R= 0.01, by using the Kalman filter in (7), we obtain the filter gain

$$K = \begin{bmatrix} 0.0241 & 0.0171 \\ 0.0495 & 0.0323 \\ 0.0514 & 0.0434 \end{bmatrix}. \tag{54}$$

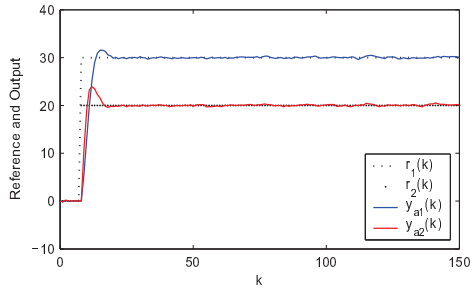
By using the assignment of the closed-loop poles $[0.6 \pm 0.3j \ 0.2 \ 0.1]$, the controller gain L is designed to be

$$L = \begin{bmatrix} 0.0244 & -0.7056 & -0.4480 & -0.0840 & 1.5769 \\ 0.7696 & 1.1064 & 0.4683 & -0.2284 & -1.3080 \end{bmatrix}. \tag{55}$$

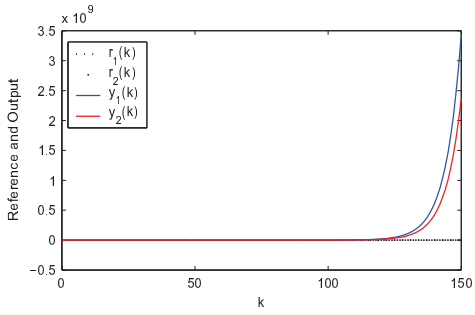
The feedback channel attack in (35) as well as the forward channel attack in (49) with $\beta(50) = [10 \ 10]^T$ and the stable matrix

$$F = \begin{bmatrix} 0.0579 & 0.8132 \\ 0.3529 & 0.0099 \end{bmatrix} \tag{56}$$

are injected into the NPOTC system at time $k = 50$. The simulation result is shown in Fig. 4. It can be seen that the attacked output $y_a(k)$ track well the reference signal $r(k)$, and the real output $y(k)$ also ultimately converges to $r(k)$ with the diminishment of the forward channel attack $\beta(k)$, which



(a) Attacked output response



(b) Real output response

Fig. 5. Simulation results of Case 2.

coincides with the result of Theorem 2. Furthermore, the two-channel attacks cannot be detected by using the residual $z_a(k)$ in Fig. 4(a).

B. Case 2: A is Stable and F is Unstable

Consider the same stable system as Case 1 with the same K and L. The feedback channel attack in (35) as well as the forward channel attack in (49) with $\beta(50) = [10 \ 10]^T$ and the unstable matrix

$$F = \begin{bmatrix} 0.9501 & 0.6068 \\ 0.2311 & 0.4860 \end{bmatrix} \tag{57}$$

are injected into the NPOTC system at time $k = 50$. The simulation result is shown in Fig. 5. It can be seen that the attacked output $y_a(k)$ still track well the reference signal $r(k)$, but the real output $y(k)$ ultimately diverges from $r(k)$, which coincides with the result of Theorem 3.

C. Case 3: A is Unstable and F is Stable

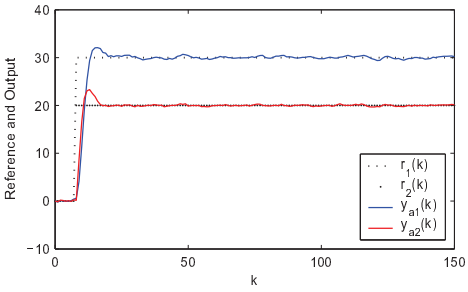
Consider an unstable system with matrix

$$A = \begin{bmatrix} 0.2312 & 0.6724 & 0.5630 \\ 0.4161 & 0.9383 & 0.1189 \\ 0.2988 & 0.3431 & 0.1690 \end{bmatrix} \tag{58}$$

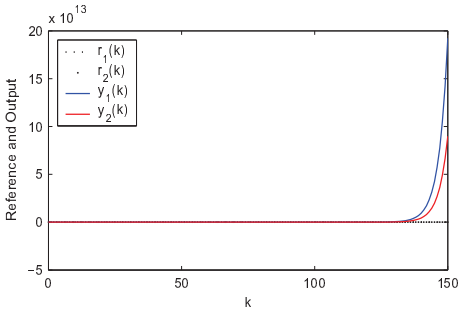
and matrices B and C in (53). Using the same design procedure as Case 1, the matrices K and L are obtained as

$$K = \begin{bmatrix} 0.2740 & 0.1274 \\ 0.3267 & 0.1502 \\ 0.1627 & 0.0813 \end{bmatrix} \tag{59}$$

$$L = \begin{bmatrix} 0.0506 & 0.8601 & 0.3087 & -0.5182 & 2.0070 \\ 0.4128 & 0.0181 & -0.2153 & 0.1520 & -1.5753 \end{bmatrix}. \tag{60}$$



(a) Attacked output response



(b) Real output response

Fig. 6. Simulation results of Case 3.

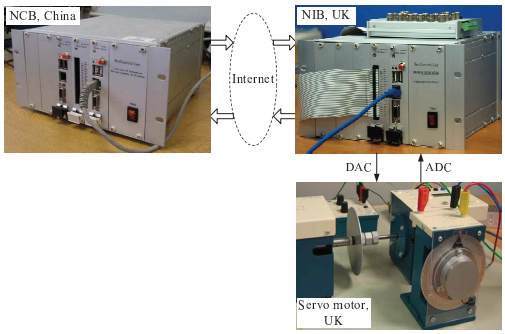
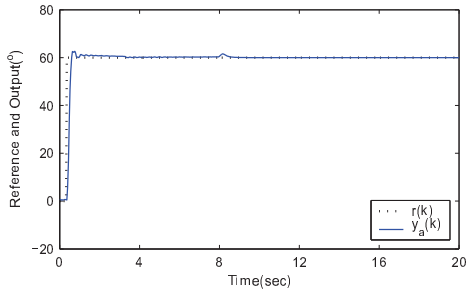


Fig. 7. Internet-based servo motor system.

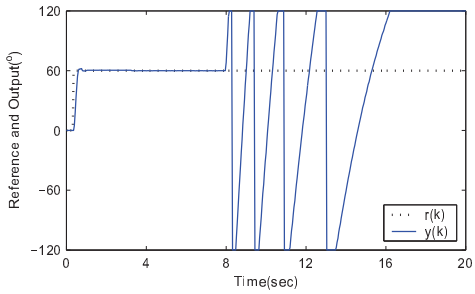
The feedback channel attack in (35) as well as the forward channel attack in (49) with $\beta(50) = [10\ 10]^T$ and the stable matrix in (56) are injected into the NPOTC system at time $k = 50$. The simulation result is shown in Fig. 6. It can be seen that the attacked output $y_a(k)$ still track well the reference signal $r(k)$. Although the injected forward channel attack $\beta(k)$ is convergent, the closed-loop system still becomes unstable, which coincides with the result of Theorem 4.

VI. Experimental Results

To further test the proposed method, an Internet-based servo motor system test rig has been constructed, as shown in Fig. 7. It consists mainly of a servo motor system, a networked controller, a local control board, as well as the Internet from the Tsinghua University, Beijing, China to the University of South Wales, Pontypridd, UK. The RTT delays of the Internet vary randomly from 3 to 8 steps. For the details of the experimental setup, refer to [27].



(a) Attacked output response



(b) Real output response

Fig. 8. Experimental results of Case 1.

Our objective is to control the position of the servo motor system. With the sampling period 0.04s, the model of the servo motor system is identified as

$$A = \begin{bmatrix} 1.2998 & -0.4341 & 0.1343 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},\ B = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix},$$

$$C = \begin{bmatrix} 3.5629 & 2.7739 & 1.0121 \end{bmatrix}. \tag{61}$$

whose input and output are the control voltage (-10V to 10V) and the angle position (-120°∼120°), respectively. The filter gain K and the controller gain L are chosen as

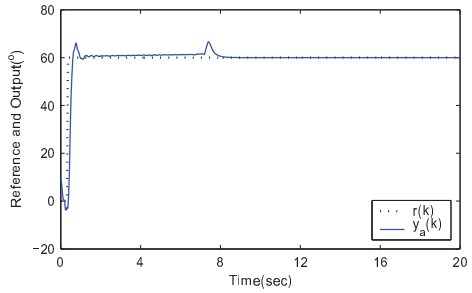
$$K = \begin{bmatrix} 0.1070 & 0.0877 & 0.0178 \end{bmatrix}^T \tag{62}$$

$$L = \begin{bmatrix} 0.7125 & -0.2593 & 0.1253 & -0.0245 \end{bmatrix}. \tag{63}$$

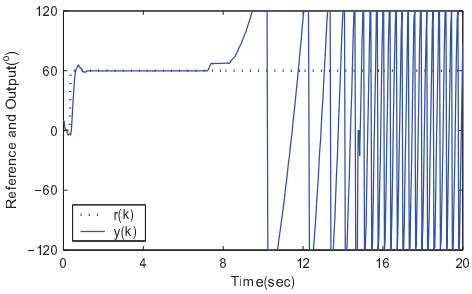
From (61), we know that the servo motor system is open-loop critically stable. In the following, practical experiments are performed for two cases: (i) F is stable and (ii) F is unstable.

A. Case 1: F is Stable

The feedback channel attack in (35) as well as the forward channel attack in (49) with the initial value $\beta(199) = 2$ and the stable matrix $F = 0.99$ are injected into the NPOTC system at time $t = 7.96$s. The experimental result is shown in Fig. 8, which indicates that the attacked output $y_a(k)$ track well the reference signal $r(k)$, but the real position of the servo motor deviates from the reference signal $r(k)$. With the disappearance of the forward channel attack $\beta(k)$, the servo motor finally stops at a certain position rather than the reference signal $r(k)$.



(a) Attacked output response



(b) Real output response

Fig. 9. Experimental results of Case 2.

B. Case 2: F is Unstable

The feedback channel attack in (35) as well as the forward channel attack in (49) with the initial value $\beta(180) = 0.1$ and the unstable matrix $F = 1.02$ are injected into the NPOTC system at time $t = 7.20$s. The experimental result is shown in Fig. 9. It is clear that the two-channel attacks lead to the instability of the closed-loop control system.

It should be pointed out that in Fig. 8(a) and Fig. 9(a), when the two-channel attacks are added, slight fluctuations occur on the attacked output $y_a(k)$, which do not appear in the aforementioned numerical simulations. This phenomenon results from the mismatch between the model in (61) and the practical servo motor system.

VII. Conclusion

This paper has investigated the design problem of FDI attacks against the output tracking control of networked systems. To compensate for two-channel network-induced delays, a Kalman filter-based NPOTC method has been proposed for stochastic linear systems. Then from an attacker's viewpoint, the stealthy FDI attacks have been designed for the measurement data in the feedback channel and the control data in the forward channel, which can avoid being detected by a Kalman filter-based detector. Both simulation and experimental results have illustrated the effectiveness of the proposed method.

It is worth mentioning that, in general, the research on FDI attacks includes three aspects: attack design, attack detection, and secure control design. This paper mainly focuses on the first aspect, i.e., the design of stealthy FDI attacks. The rest two aspects are more important and interesting, which thus deserve further investigation in our future research.

References

[1] R. A. Gupta and M.-Y. Chow, "Networked control system: Overview and research trends," *IEEE Trans. Ind. Electron.*, vol. 57, no. 7, pp. 2527–2535, Jul. 2010.

[2] L. Zhang, H. Gao, and O. Kaynak, "Network-induced constraints in networked control systems–A survey," *IEEE Trans. Ind. Inf.*, vol. 9, no. 1, pp. 403–416, Feb. 2013.

[3] S. Yin, X. Li, H. Gao, and O. Kaynak, "Data-based techniques focused on modern industry: An overview," *IEEE Trans. Ind. Electron.*, vol. 62, no. 1, pp. 657–667, Jan. 2015.

[4] Z. H. Pang, G. P. Liu, D. H. Zhou, and D. H. Sun, "Data-based predictive control for networked nonlinear systems with network-induced delay and packet dropout," *IEEE Trans. Ind. Electron.*, vol. 63, no. 2, pp. 1249–1257, Feb. 2016.

[5] J. Qiu, H. Gao, and S. X. Ding, "Recent advances on fuzzy-model-based nonlinear networked control systems: A survey," *IEEE Trans. Ind. Electron.*, vol. 63, no. 2, pp. 1207–1217, Feb. 2016.

[6] D. Dzung, M. Naedele, T. P. Von Hoff, et al, "Security for industrial communication systems," *Proc. IEEE*, vol. 93, no. 6, pp. 1152–1177, 2005.

[7] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems-Part I: Analysis and experimentation of stealthy deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1963-1970, Sep. 2013.

[8] W. Zeng and M. Y. Chow, "A reputation-based secure distributed control methodology in D-NCS," *IEEE Trans. Ind. Electron.*, vol. 61, no. 11, pp. 6294–6303, Nov. 2014.

[9] S. Huang, C. J. Zhou, S. H. Yang, and Y. Q. Qin, "Cyber-physical system security for networked industrial processes," *Int. J. Autom. Comput.*, vol. 12, no. 6, pp. 567–578, Dec. 2015.

[10] A. Ghosh and G. McGraw, "Lost decade or golden era: Computer security since 911," *IEEE Secur. Privacy*, vol. 10. no. 1, pp. 6–10, 2012.

[11] A. A. Cárdenas, S. Amin, and S. S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshop*, 2008, pp. 495-500.

[12] Z. H. Pang and G. P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 5, pp. 1334–1342, Sep. 2012.

[13] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.

[14] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proc. 12th Int. Conf. Hybrid Syst. Comput. Control*, 2009, pp. 31–45.

[15] Z. H. Pang, G. P. Liu, and Z. Dong, "Secure networked control systems under denial of service attacks," in *Proc. 18th IFAC World Congr.*, 2011, pp. 8908-8913.

[16] Y. Yuan, F. Sun, and Q. Zhu, "Resilient control in the presence of DoS attack: Switched system approach," *Int. J. Control Autom. Syst.*, vol. 13, no. 6, pp. 1423–1435, Dec. 2015.

[17] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun. Control Comput.*, 2009, pp. 911–918.

[18] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*,vol. 22, no. 4, pp. 1396–1407, 2014.

[19] Z. Gao, C. Cecati, and S. X. Ding, "A survey of fault diagnosis and fault-tolerant techniques–Part I: Fault diagnosis with model-based and signal-based approaches," *IEEE Trans. Ind. Electron.*, vol. 62, no. 6, pp. 3757–3767, Jun. 2015.

[20] S. Yin, G. Wang, and H. Gao, "Data-driven process monitoring based on modified orthogonal projections to latent structures," *IEEE Trans. Control Syst. Technol.*, DOI: 10.1109/TCST.2015.2481318, 2015.

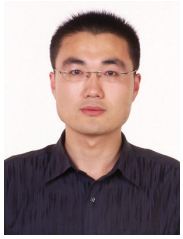
[21] G. Wang and S. Yin, "Quality-related fault detection approach based on orthogonal signal correction and modified PLS," *IEEE Trans. Ind. Inf.*, vol. 11, no. 2, pp. 398-405, Apr. 2015.

[22] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Proc. 1st workshop Secure Control Syst.*, 2010, pp. 1-6.

[23] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attacks in smart grid using kalman filter," *IEEE Trans. Control Network Syst.*, vol. 1, no. 4, pp. 370-379, Dec. 2014.

[24] R. Niu and L. Huie, "System state estimation in the presence of false information injection," *IEEE Stat. Signal Process. Workshop*, 2012, pp. 385-388.

[25] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. 49th IEEE Conf. Decis. Control*, 2010, pp. 5991-5998.
[26] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *Proc. Am. Control Conf.*, 2013, pp. 3344–3349.
[27] Z. H. Pang, G. P. Liu, D. H. Zhou, and M. Y. Chen, "Output tracking control for networked systems: A model-based prediction approach," *IEEE Trans. Ind. Electron.*, vol. 61, no. 9, pp. 4867–4877, Sep. 2014.



Zhong-Hua Pang (M'11) received the B.Eng. degree in automation and the M.Eng. degree in control theory & control engineering from the Qingdao University of Science and Technology in 2002 and 2005, respectively, and the Ph.D. degree in control theory & control engineering from the Institute of Automation, Chinese Academy of Sciences in 2011.

He was a postdoctoral fellow with the Department of Automation, Tsinghua University, China from 2011 to 2014. He is currently an associate professor in the School of Electrical and Control Engineering, North China University of Technology, China. His research interests include networked control systems, security of cyber-physical systems, and advanced control in environmental protection industry.

Guo-Ping Liu (F'11) is the chair of control engineering in the University of South Wales. He received his B.Eng. and M.Eng. degrees in automation from the Central South University of Technology (now Central South University) in 1982 and 1985, respectively, and his Ph.D. degree in control engineering from UMIST (now University of Manchester) in 1992.

He has been a professor in the University of South Wales (formerly University of Glamorgan) since 2004, a Hundred-Talent Program visiting professor of the Chinese Academy of Sciences since 2001, and a Changjiang Scholar visiting professor of Harbin Institute of Technology since 2008. He is the editor-in-chief of the International Journal of Automation and Computing and IET fellow. He has authored more than 400 publications on control systems and authored/co-authored 8 books. His main research areas include networked control systems, nonlinear system identification and control, advanced control of industrial systems, and multiobjective optimization and control.

Donghua Zhou (SM'99) received the B.Eng., M.Sci., and Ph.D. degrees in electrical engineering from the Shanghai Jiaotong University in 1985, 1988, and 1990, respectively.

He was an Alexander von Humboldt research fellow (1995-1996) in the University of Duisburg and a visiting scholar in the Yale University (Jul. 2001-Jan. 2002). He joined the Tsinghua University in 1997, and was a professor and the head of the Department of Automation, Tsinghua University, during 2008 and 2015. He is now the vice president of the Shandong University of Science and Technology. He has authored and coauthored over 130 peer-reviewed international journal papers and 6 monographs in the areas of fault diagnosis, fault-tolerant control, reliability prediction, and predictive maintenance. He is a member of the IFAC Technical Committee on Fault Diagnosis and Safety of Technical Processes, an associate editor of the Journal of Process Control, the associate Chairman of Chinese Association of Automation (CAA).

Fangyuan Hou received the B.Eng. degree in automation and the M.Eng. degree in control theory & control engineering from the Qingdao Technological University in 2013 and 2015, respectively. She is currently pursuing the Ph.D. degree in control science & engineering from the School of Automation, Beijing Institute of Technology, China.

Her research interest lies in the security of cyber-physical systems, especially in networked control systems.

Dehui Sun received the B.Eng. degree in automation from the Northeastern University in 1983, and the Ph.D. degree in control theory & control engineering from the University of Science and Technology Beijing in 2005.

Since 2002, he has been working as a professor in the Department of Automation, North China University of Technology, China. He is currently the director of the Key Laboratory of Fieldbus Technology and Automation of Beijing, North China University of Technology, a member of the Fault Diagnosis and Fault Tolerant Control Technical Committee of Chinese Association of Automation, and a member of the Information Management and Control Technical Committee of Chinese Association of Artificial Intelligence. His research interests include field bus technology and networked control systems, fault diagnosis and fault tolerant control, and advanced control in environmental protection industry.