Adv. Manuf. (2017) 5:243–250
DOI 10.1007/s40436-017-0189-2

A brief overview on secure control of networked systems

Hong-Tao Sun[1] · Chen Peng[1] · Peng Zhou[1] · Zhi-Wen Wang[2]

Received: 10 November 2016 / Accepted: 26 July 2017 / Published online: 8 September 2017

Abstract This paper focuses on the issues of the security of networked control systems by summarizing recent progress in secure control of this research and application area. We mainly discuss existing results, especially in modeling issues, of three aspects: (1) attack mechanisms and their impacts on control systems, (2) the identification and design of attacks, and (3) secure estimation and control strategies. A conclusion is drawn at the end of this paper. In addition, several promising research tendencies of the development for secure control in networked control system are presented.

Keywords Networked control system · Security · Attack · Estimation and control

1 Introduction

Networked control systems (NCSs), which include physical processes, computational resources and communication capability, have permeated in many areas of our daily lives including smart transportation, electricity network, and industrial automation systems [1, 2]. NCS, as an abstract of cyber-physical system (CPS), is expected to have more efficiency, reliability, and adaptability than traditional control systems because of the seamless integration with physical world, cyberspace and coordinate control. However, due to the increased opening of networks, NCSs have significant potential security threats and are more vulnerable to various attacks. Once the security of NCSs is destroyed, there will be serious consequences in industrial manufacturing with the loss of control functionality. With the emergence of events such as Maroochy water breach [3], SQL Slammer worm attack on the Davis-Besse nuclear plant [4] and the Stuxnet computer worm [5], the security of control systems in the network environment appears on the public horizon. Today, the secure control of the coupling between a vulnerable cyberspace and a complex physical system imposes fundamentally new challenges for NCSs [6].

The security of NCSs is different from traditional IT security [7, 8]. The security of a system is not a new topic in traditional IT, but a few works involve the security of control systems. Traditional network security pays more attention to the confidentiality, integrity, and availability (CIA) of data [9]. Defending against attacks is the primary mission for traditional IT security. A few examples include the data encryption technique, firewall technique and intrusion detection technique. However, the natural differences from a traditional control system that lie in the communication among sensors, controllers, and actuators can affect the manufacturing or industrial dynamics. To some extent, certain kinds of IT security measures do not apply to control systems. For instance, encryption methods may introduce an additional time-delay while it can effectively protect data authenticity. Hence, the traditional security measures are only partial solutions for the security of NCSs because these measures are invalid when attacks are a fait accompli. In view of a control system, the CIA of data is often satisfied

✉ Chen Peng
c.peng@shu.edu.cn

Hong-Tao Sun
sht371322@163.com

[1] Department of Automation, School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200240, People's Republic of China

[2] College of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou 730050, Gansu, People's Republic of China

naturally during the design of the classical control system while the security of data in NCSs is rarely considered [10]. Therefore, the separation of control and network is not helpful for the performance improvement of NCSs, especially in the condition that NCSs are vulnerable to remote access over a communication network.

The security of NCSs is also different from traditional fault tolerance [11]. There are substantial differences between secure control and fault tolerant control in terms of either concept or technique. On one hand, the purpose of fault tolerance control theory is to handle the uncertainties and disturbances as well as the fault diagnosis and mitigation. When faults in physical components (e.g., sensors and actuators) are detected, the fault tolerant technique can be used to sustain the system operations. That is to say, the "faults" in fault tolerant control mainly refer to the failures of system components rather than network attacks. Although the network attacks can also affect the dynamics of physical systems and cause degradation of the performance of NCSs just like "faults" in a control system, the concept of an "attack" in the security of NCSs mainly refers to the failure or false injection of data in the process of signal transmission [12]. On the other hand, "faults" in fault tolerant control are often considered as the "normal" events which can affect the behaviors of physical systems, and these events are deemed to be aimless. Otherwise, an "attack" on the security of NCSs is mainly manifested on its stronger purpose of implementing an attack over certain significant nodes in a coordinated fashion [13]. As an example, the actual sensor or control data can be replaced by a false data injection attack and can be prevented by a denial of service (DoS) attack, so the correctness and real-time of physical data, which is the premise of control implementation, are no longer tenable under the circumstance of a network attack. Thus, the security of NCSs is of importance in monitoring, detection, and control.

The current research on IT security is necessary for securing control systems but not sufficient [14, 15]. In order to distinguish from traditional IT security and fault tolerant control, in this paper we attempt to review recent works on the security of NCSs from the perspective of a control framework. The remainder of this paper is organized as follows. Section 2 analyzes attack mechanisms and their impacts on a control system. Section 3 summarizes detection methods with attack design. Section 4 presents some recent works on secure control strategies. Section 5 concludes this paper with beneficial discussions.

2 Attacks and their effects on NCSs

In this section, a few common categories of attacks, and their effects on control systems are presented with the example of linear dynamics [16]. To achieve greater generality, the following discrete-time state-space model is shown as

$$\begin{cases} \boldsymbol{x}(k+1) = \boldsymbol{A}\boldsymbol{x}(k) + \boldsymbol{B}\hat{\boldsymbol{u}}(k) + \boldsymbol{w}(k), \\ \boldsymbol{y}(k) = \boldsymbol{C}\boldsymbol{x}(k) + \boldsymbol{v}(k), \end{cases} \tag{1}$$

where $\boldsymbol{x}(k) \in \mathbf{R}^n$, $\boldsymbol{u}(k) \in \mathbf{R}^p$ and $\boldsymbol{y}(k) \in \mathbf{R}^m$ are the system state, control input and output, respectively. $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{C}$ are constant matrices with appropriate dimensions. $\boldsymbol{w}(k) \in \mathbf{R}^q$ and $\boldsymbol{v}(k) \in \mathbf{R}^l$ are independent Gaussian noise sequences with $\boldsymbol{w}(k) \sim \mathbf{N}(0, \mathbf{Q})$ and $\boldsymbol{v}(k) \sim \mathbf{N}(0, \mathbf{R})$.

In the controller side, sensor input is denoted as $\hat{\boldsymbol{y}}(k)$ and output as $\boldsymbol{u}(k)$; whereas, in the plant side, the actual output of a sensor is $\boldsymbol{y}(k)$ and the actual input of an actuator is $\hat{\boldsymbol{u}}(k)$. Under perfect conditions, the following equations are satisfied

$$\boldsymbol{u}(k) = \hat{\boldsymbol{u}}(k), \tag{2}$$

$$\boldsymbol{y}(k) = \hat{\boldsymbol{y}}(k). \tag{3}$$

However, various attacks may lead to the case in which Eq. (2) or (3) does not hold indicating whether the system is normal or not. Generally, these cases can be mainly divided into three categories: physical attacks, false data injection attacks and DoS attacks. Any one of them can cause Eq. (2) or (3) to be no longer true. Although the response of the system under these attacks is described in Refs. [11, 14, 16].

The first scenario is physical attacks. These attacks often invalidate physical components, just like the faults of a control system. However, network security can hardly defend against these types of attacks because these attacks can implement their destruction locally (e.g., for a local temperature sensor, an attacker can cause deliberate heating or cooling to change its measures). The partial solutions of these problems can be learned from fault tolerant control theory. The general form of system dynamics under physical attacks is given by

$$\begin{cases} \boldsymbol{x}(k+1) = \boldsymbol{A}\boldsymbol{x}(k) + \boldsymbol{B}\hat{\boldsymbol{u}}(k) + \boldsymbol{w}(k) + \boldsymbol{F}\boldsymbol{\beta}(k), \\ \boldsymbol{y}(k) = \boldsymbol{C}\boldsymbol{x}(k) + \boldsymbol{v}(k), \end{cases} \tag{4}$$

where $\boldsymbol{F}$ is the fault matrix and $\boldsymbol{\beta}(k)$ is unknown or is the signal for an attack.

From this system structure, we can learn the effects of the attack on the NCSs by analyzing $\boldsymbol{\beta}(k)$ [17, 18]. In another case, the attacks may tailor their attack strategies carefully without being detected. The object of these attacks is to disrupt the infrastructure of NCSs such as the physical systems [19], sensors [20], and actuators [21]. To some extent, these attacks can be included in the following scenarios although they aim to attack the components of systems.

The following scenario is false data injection attack. These kinds of attacks tamper the actual values of sensor measures through network intrusion and tricking of the controller such that it changes the operation state. In the course of the attack implementation, attackers can tamper or replace the control packets or output packets by the following form

$$\begin{cases} \hat{\boldsymbol{u}}(k) = \boldsymbol{u}(k) + \boldsymbol{\Gamma}^{\boldsymbol{u}}\boldsymbol{a}_k^{\boldsymbol{u}}, \\ \hat{\boldsymbol{y}}(k) = \boldsymbol{y}(k) + \boldsymbol{\Gamma}^{\boldsymbol{y}}\boldsymbol{a}_k^{\boldsymbol{y}}, \end{cases} \tag{5}$$

where $\boldsymbol{a}_k^{\boldsymbol{u}}$ and $\boldsymbol{a}_k^{\boldsymbol{y}}$ are the attack sequences for input of controllers and output of sensors, respectively. $\boldsymbol{\Gamma}^{\boldsymbol{u}}$ and $\boldsymbol{\Gamma}^{\boldsymbol{y}}$ are corresponding attack matrices for $\boldsymbol{a}_k^{\boldsymbol{u}}$ and $\boldsymbol{a}_k^{\boldsymbol{y}}$.

For false data injection attacks, concealment is the major characteristic. The influence on NCSs caused by false data injection mainly includes three aspects: data integrity, causing the controller to make wrong decisions by false data and consuming more network resources [22, 23].

The last scenario, which is also the commonest type of attack, is DoS attack. A DoS attack usually prevents information exchange with a large volume of invalid data designed to deliberately consume the network resources. DoS has the direct manifestation that the controller cannot receive the sensor data $\boldsymbol{y}(k)$ or that the actuator cannot receive the control data $\boldsymbol{u}(k)$. It is mainly embodied as time-delay and the dropout of packets. Similar to false data injection in Eq. (5), the mathematical model can be given as

$$\begin{cases} \boldsymbol{a}_k^{\boldsymbol{u}} = -\boldsymbol{S}_k^{\boldsymbol{u}}\boldsymbol{\Gamma}^{\boldsymbol{u}}\boldsymbol{u}(k), \\ \boldsymbol{a}_k^{\boldsymbol{y}} = -\boldsymbol{S}_k^{\boldsymbol{u}}\boldsymbol{\Gamma}^{\boldsymbol{y}}\boldsymbol{y}(k), \end{cases} \tag{6}$$

where $\boldsymbol{S}_k^{\boldsymbol{u}}$ and $\boldsymbol{S}_k^{\boldsymbol{y}}$ are diagonal matrices that take values from $\{0, 1\}$. $\boldsymbol{S}_k^{\boldsymbol{u}(\boldsymbol{y})} = 1$ represents an attack, and $\boldsymbol{S}_k^{\boldsymbol{u}(\boldsymbol{y})} = 0$ represents no attack.

In general, the data loss due to the DoS attacks may cause the degradation of control performance and even the instability of a control system. However, some proposed methods can be used to solve these new problems. For example, Schenato [24] replaced the absent data with the last received data to deal with the loss of packets in their controller design.

Beyond that, there are many other forms of attacks such as replay attack, zero dynamics attack, and bias injection attack. These can be reflected in a priori knowledge, disclosure resources, and disruption resources of an attacker. The details are shown in Refs. [11, 16].

3 Identification and design of attacks

The goal of an attacker is often characterized by compromising a measurement or controlling data while an effective attack strategy should be designed carefully. In other words, these cunning attacks can damage a healthy system without being detected. Because of the disturbances and errors in a control system, the attack strategies should hide themselves in this normal margin of error and not trigger a false alarm. Rather, a valid detection strategy would devote itself to distinguish this attack behavior from normal disturbances and errors intelligently.

The physical model-based attack detection method, complementary to intrusion detection methods, needs to detect attacks in real time. Mo et al. [25] considered the scenario of false data injection attacks carried over a sensor network for the discrete-time LTI Gaussian system. The critical goal of the design of the attack was to hijack the measurement of a subset of sensors without being detected by the χ^2 failure detector. Commonly, the χ^2 failure detector computes the following condition

$$g_k = \boldsymbol{z}_k^{\mathrm{T}}\boldsymbol{P}^{-1}\boldsymbol{z}_k, \tag{7}$$

where $\boldsymbol{P}$ is the covariance matrix of the residue $\boldsymbol{z}_k$. When $g_k > \delta$ ($\delta > 0$ is a given threshold), the detector would trigger an alarm. Therefore, g_k should be ingeniously designed. Similar to Ref. [24], Kwon et al. [26] also discussed the condition in which the deception attacks fail the estimators while successfully by passing the monitoring system with compound scalar testing [27]. Based on Eq. (7), the following condition is used for the χ^2 detector

$$\begin{cases} H_0, \text{ if } g_k \leqslant \delta, \\ H_1, \text{ if } g_k > \delta. \end{cases} \tag{8}$$

An adversary who wants to be undetectable should avoid a large increase in the power of residuals. These detection methods can be used in a smart-grid [23, 28].

Besides, with the aim of fully utilizing the acquired data in a flexible way, a sequential detection theory [29] is considered in Ref. [14]. The goal of sequential detection is to minimize the number of observations that are required to decide with a given probability of a false alarm and a given probability of detection. Suppose the observation z_k on the condition of H_j is generated with a probability distribution $\boldsymbol{p}_j$. The sequential probability ratio test (SPRT) algorithm in Ref. [30] is described by

$$\begin{cases} S(k+1) = \lg\dfrac{p_1(z_k)}{p_0(z_k)} + S(k), \\ N = \inf\limits_n\{n : S(n) \notin [L, U]\}, \end{cases} \tag{9}$$

where $L \approx \ln\frac{b}{1-a}$, $U \approx \ln\frac{1-b}{a}$, a is the desired probability of a false alarm and b is the desired probability of a missed detection, starting with $S(0) = 0$. The decision rule d_N can be defined as

$$d_N = \begin{cases} H_0, \text{ if } S(N) \geqslant U, \\ H_1, \text{ if } S(N) \leqslant L. \end{cases} \tag{10}$$

Pang et al. [31] investigated the problems with false data injection attacks for output tracking a control system. The output tracking error is regarded as an additional state. The incremental state observer is based on the Kalman filter, and the controller is LQG-based. However, the aim of false data injection attacks should hide itself in the following Euclidean-based detector

$$||z(\boldsymbol{y},\hat{\boldsymbol{y}})|| = \sqrt{(\boldsymbol{y}_1-\hat{\boldsymbol{y}}_1)^2+(\boldsymbol{y}_2-\hat{\boldsymbol{y}}_2)^2+\cdots+(\boldsymbol{y}_n-\hat{\boldsymbol{y}}_n)^2}. \tag{11}$$

In addition, another method is called cosine similarity detection that measures their similarity with the cosine of the angle [32]. The detection model is given as

$$sim(\boldsymbol{X},\boldsymbol{Y}) = \cos\theta = \frac{\sum_{i=1}^{N}(\boldsymbol{x}_i\cdot\boldsymbol{y}_i)}{\sqrt{\sum_{i=1}^{N}\boldsymbol{x}_i^2\cdot\sum_{i=1}^{N}\boldsymbol{y}_i^2}}. \tag{12}$$

Still, Pasqualetti et al. [33] developed the mathematical framework for attacks and monitoring the distributed system. Consider the following LTI descriptor system

$$\begin{cases} \boldsymbol{E}\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}\boldsymbol{u}(t), \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t)+\boldsymbol{D}\boldsymbol{u}(t), \end{cases} \tag{13}$$

where $\boldsymbol{E}$ is possibly singular. A monitor is a mapping

$$\boldsymbol{\Phi}:\ \boldsymbol{\Lambda}\rightarrow\boldsymbol{\Psi}, \tag{14}$$

where $\boldsymbol{\Lambda}=\{\boldsymbol{E},\boldsymbol{A},\boldsymbol{C},\forall t>0\}$, $\boldsymbol{\Psi}=\{\psi_1,\psi_2\}$ with $\psi_1\in\{\text{True},\text{False}\}$ and $\psi_2\subseteq\{1,2,\cdots,n+p\}$. Suppose the attacked signal u_γ is the subset of the attack γ, then the attack $(\boldsymbol{B}_\gamma\boldsymbol{u}_\gamma,\boldsymbol{D}_\gamma\boldsymbol{u}_\gamma)$ is detected by $\boldsymbol{\Phi}$ if $\psi_1=\text{True}$, and the attack $(\boldsymbol{B}_\gamma\boldsymbol{u}_\gamma,\boldsymbol{D}_\gamma\boldsymbol{u}_\gamma)$ is identified by $\boldsymbol{\Phi}$ if $\psi_2=\gamma$. The limitation of the monitor is also discussed in view of a system-theoretic and a graph-theoretic.

In view of adversaries, the goal is to maximize their attack effects with the intent of shaping the policies of the attack. Zhang et al. [34], as a representative to the work on DoS attack design, considered the following LTI dynamics

$$\boldsymbol{x}(k+1) = \boldsymbol{A}\boldsymbol{x}(k)+\boldsymbol{B}\boldsymbol{u}(k)+\boldsymbol{w}(k). \tag{15}$$

They defined a finite time sequence $\boldsymbol{I}_k=\{\theta_1\boldsymbol{x}_1,\theta_2\boldsymbol{x}_2,\cdots,\theta_k\boldsymbol{x}_k,\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_k\}$ that indicates whether the packet $\boldsymbol{x}(k)$ can be received or not. Then they designed the attack section $\theta(\gamma_m,t)$ as

$$\theta(\gamma_m,t) = \begin{cases} 1, & 1-\alpha, \\ 0, & \alpha, \end{cases} \tag{16}$$

where $\theta(\gamma_m,t)=0$ represents that the probability of data can be received by a controller with α but not vice versa.

They formulated an optimal attack schedule to maximize the LQG control cost function with energy constraints as follows

$$\begin{aligned} &\max_{\gamma\in\Theta}\ \mathrm{E}[J(\gamma)] \\ &\text{s.t.}\quad \sum_{t=1}^{T}\gamma_{m,t}\leqslant n, \end{aligned} \tag{17}$$

where $\forall m\in\mathbf{N}$ and $t\in\{1,2,\cdots,T\}$ is the attack schedule space; $\mathrm{E}[\bullet]$ is a symbol of expectation.

In the side of a sensor, Zhang et al. [35] also considered the scenario that an energy-constrained attacker may jam the wireless channel at each sampling time between the sensor and remote estimator. An optimal attack schedule is constructed to maximize the average excepted estimation of the error covariance matrix

$$\begin{aligned} &\max_{\gamma\in\{0,1\}}\ \mathrm{Tr}\left[\frac{1}{T}\sum_{k=1}^{T}\mathrm{E}[\boldsymbol{P}_k(\gamma_k)]\right] \\ &\text{s.t.}\ \ \|\gamma\|_0 = n, \end{aligned} \tag{18}$$

where $\boldsymbol{P}_k(\gamma_k)$ is the covariance matrix under attacks and n represents the energy-constraint. Their related works can be also shown in Refs. [36, 37].

Gupta et al. [38] considered a dynamic zero-sum game problem between the discrete-time LTI plant and a jammer from the controller to the actuator. In finite steps, the state under adversarial jamming evolves

$$\boldsymbol{x}(k+1) = \boldsymbol{A}\boldsymbol{x}(k)+\alpha_k\hat{\boldsymbol{u}}(k)+\boldsymbol{w}(k), \tag{19}$$

where $k=1,2,\cdots,N-1$ and $\alpha_k\in\{0,1\}$. The following equation

$$J = \mathrm{E}\left[\sum_{k=0}^{N-1}(\boldsymbol{x}(k)^2+\alpha_k\boldsymbol{u}^2(k)+\boldsymbol{x}^2(N)\right], \tag{20}$$

is the cost function which needs the controller to minimize and the jammer to maximize. They introduced

$$\begin{cases} \boldsymbol{I}_0\triangleq\{x_0\}, \\ \boldsymbol{I}_k\triangleq\{x_{[0,k]},\alpha_{[0,k-1]}\}, \end{cases} \tag{21}$$

as the information available to both the controller and jammer at time k. By mapping their action to $\{\gamma_k\}$ and $\{\boldsymbol{u}(k)\}$, they let $\boldsymbol{u}(k)=\gamma_k(\boldsymbol{I}_k)$ and $\alpha_k=\boldsymbol{u}_k(\boldsymbol{I}_k)$ which is a standard zero-sum problem. Then, a saddle point equilibrium control and jamming strategy are determined. Similar to the zero-sum game, Zhu and Martinez [39] investigated the Stackelberg game problem on the correlation of attacks to a feedback loop.

After all, the attack should design itself carefully based on a given detector to hide itself and harm the system to the hilt. On the contrary, a detector will commit itself to monitor most anomalies for securing the system. Hence, the design of detection methods and attack strategies are relative and inseparable from each other.

4 Secure estimation and control

Many works focus on data security, but only few involve the security of estimation and control [40]. In terms of a control system, the security of NCSs boils down to the actuation security of the control side and feedback security of the sensor side. The design of estimation algorithms against faults or failures is not a new problem, but they might not be applicable under attacks. In the following, several secure estimation and control strategies are presented from a different perspective.

Fawzi et al. [21] considered the system dynamics in the following form

$$\begin{cases} \boldsymbol{x}(t+1) = \boldsymbol{A}\boldsymbol{x}(t), \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) + \boldsymbol{\gamma}(t). \end{cases} \tag{22}$$

They wanted to reconstruct the initial state $\boldsymbol{x}(0)$with the first M measurements by $\boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{x}(0) + \boldsymbol{\gamma}(t)$. Thus,$q$ measurements are estimated with M steps by the decoder $D: (\mathbf{R}^p)^M \to \mathbf{R}^n$. If for any $\boldsymbol{x}(0) \in \mathbf{R}^n$ with $|\Sigma| \leqslant q$ and any sequence $\gamma(0), \gamma(1), \cdots, \gamma(M-1)$ such that $\mathrm{Sup}\{\gamma(t) \subset \Sigma\}$, then $D(\gamma(0), \gamma(1), \cdots, \gamma(M-1)) = x(0)$, where Σ is a set of attacked sensors. The results show that the maximized number of attacks, if less than half, can be detected and corrected from the function of the pair $(\boldsymbol{A}, \boldsymbol{C})$. More practically, Lee et al. [41] designed an individual Luenberger observer for each sensor to estimate the state correctly by sensing redundancy under sensor attacks. In addition, measurement noise and disturbance are considered in their studies.

Shoukry and Tabuada [42] described the problems of state reconstruction from sensor measurements with spare attacks. The dynamics and attack model are given by

$$\begin{cases} \boldsymbol{x}(t+1) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t), \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) + \boldsymbol{a}(t), \end{cases} \tag{23}$$

where $\boldsymbol{y}(t)$ is the observed measurement and $\boldsymbol{a}(t)$ is an S-spare vector for the model of attacks. By constructing a delayed version for state $\boldsymbol{x}(t-\tau+1)$, an attack vector $\boldsymbol{a}(t-\tau+1), \boldsymbol{a}(t-\tau+2), \cdots, \boldsymbol{a}(t)$ and measurements $\boldsymbol{y}(t-\tau+1), \boldsymbol{y}(t-\tau+2), \cdots, \boldsymbol{y}(t)$, a novel state observer model with S-sparse attack is proposed by

$$\boldsymbol{Y}(t) = \boldsymbol{O}\boldsymbol{x}(t-\tau+1) + \boldsymbol{E}(t), \tag{24}$$

where $\boldsymbol{E}(t)$ is a vector that is reshaped from the attack matrix $\tilde{\boldsymbol{E}}(t)$, $\boldsymbol{O}$ the observation matrix with the appropriate transformation in the data delay structure. Then, the event-triggered technique is used to improve the computational efficiency of the proposed algorithms.

Foroush and Martínez [43] investigated the problem of periodic DoS attacks for a single-input controllable linear system. For continuous-time closed-loop dynamics, they proposed

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t), \tag{25}$$

$$\boldsymbol{u}(t) = \boldsymbol{K}\boldsymbol{x}(t_k), \quad \forall t, t \in [t_k, t_{k+1}], \tag{26}$$

where $\boldsymbol{x}(t) \in \mathbf{R}^n$ and $\boldsymbol{u}(t) \in \mathbf{R}^p$ are the state vector and control input, respectively. They considered a jammer with energy-constraints and periodic features as follows

$$\hat{\boldsymbol{u}}(t) = \begin{cases} \boldsymbol{K}\boldsymbol{x}(t_k), & (n-1)T \leqslant t \leqslant (n-1)T + T_{\mathrm{off}}, \\ 0, & (n-1)T + T_{\mathrm{off}} \leqslant t \leqslant nT, \end{cases} \tag{27}$$

where $\widehat{\boldsymbol{u}}(t)$ depicts the attack action with period T so that communication is possible during $[0, T_{\mathrm{off}}]$ and not possible during $[T_{\mathrm{on}}, T]$. Based on the Lyapunov stability condition, they designed the following trigger law

$$\|\boldsymbol{e}(t_k)\|^2 = \alpha \frac{\|\boldsymbol{Q}\| - 1}{\|\boldsymbol{P}\boldsymbol{B}\boldsymbol{K}\|^2} |\boldsymbol{x}(t_k)|^2, \quad k > 1, \tag{28}$$

where $\alpha \in [0, 1]$. $\boldsymbol{P}$ is the positive definite matrix in Lyapunov function, $\boldsymbol{B}$ the control matrix, $\boldsymbol{K}$ the designed control matrix. The stability under this specific trigger strategy is proven by Jordan decomposition and the proper pole placing method with dimensions of 4 or less.

More generally, Persis and Tesi [44] characterized the input stability of a closed-loop system under a certain frequency and duration of a DoS attack rather than the periodic case. The differences between Ref. [43] and Ref. [44] lie in: (i) only the control signal can be comprised in Ref. [43] while Ref. [44] assumes that the data can be neither sent nor received for the sensor and control signal, (ii) the frequency and duration of attacks are more flexible in Ref. [44] with

$$H_n \triangleq \{h_n\} \cup \{h_n, h_n + \tau_n\} \tag{29}$$

representing the nth attack interval with length τ_n, where $\{h_n\}$ is a pulse at time h_n. The following communication forms are allowed

$$\begin{cases} \Xi(\tau, t) \triangleq \underset{n \in N_0}{\cup} H_n \cap [\tau, t], & \text{denied}, \\ \Theta(\tau, t) \triangleq [\tau, t] \backslash \Xi(\tau, t), & \text{allowed}, \end{cases} \tag{30}$$

and the input-to-state stabilizing in Ref. [44] provides a broader sense of stability analysis. Namely, for the control signal $\hat{\boldsymbol{u}}(t) = \boldsymbol{K}\boldsymbol{x}(t_{k(t)})$ under the above assumptions, the Eq. (14) is globally asymptotically stable when $w \equiv 0$ and

$$\|\boldsymbol{x}(t)\| \leqslant \alpha(\|\boldsymbol{x}(0)\|, t) + \beta(\|\boldsymbol{w}_t\|_\infty). \tag{31}$$

Moreover, resilient control logic that contains periodic and event-based sampling logic are discussed with a trade-

off in the control performance and communication resources.

Amin et al. [45] considered a model for a class of DoS attacks. If control or measurement packets are jammed or compromised by a malicious adversary with safety and power constraints

$$\begin{cases} \widehat{\boldsymbol{u}}(k) = v_k \boldsymbol{u}(k), \\ \widehat{\boldsymbol{x}}(k) = \gamma_k \boldsymbol{x}(k), \end{cases} \tag{32}$$

where v_k and γ_k are the attack sequence according to $\boldsymbol{u}(\boldsymbol{k})$ and $\boldsymbol{x}(\boldsymbol{k})$ with a Bernoulli distribution. The goal is to construct a causal feedback controller that can minimize the following objective function during a finite horizon

$$J_N = \mathrm{E}\left[\boldsymbol{x}_N^{\mathrm{T}} \boldsymbol{Q}_1 \boldsymbol{x}_N + \sum_{k=0}^{N-1} \begin{pmatrix} \boldsymbol{x}(k) \\ \boldsymbol{u}(k) \end{pmatrix} \begin{pmatrix} \boldsymbol{I}_N & 0 \\ 0 & v_k \boldsymbol{I}_m \end{pmatrix} \boldsymbol{Q}_2 \begin{pmatrix} \boldsymbol{x}(k) \\ \boldsymbol{u}(k) \end{pmatrix}\right], \tag{33}$$

where $\boldsymbol{Q}_1 > 0$ and $\boldsymbol{Q}_2 \geqslant 0$ with appropriate dimensions. Subsequently, more details about the attack model and controller parameterizations problem are further discussed.

Feng et al. [46] focused on a distributed coordinated secure control problem for a class of linear multi-agent systems with Lyapunov stochastic stability theory. Consider the following stochastic linear multi-agent system with a group of n agents

$$\mathrm{d}\boldsymbol{x}_i(t) = (\boldsymbol{A}\boldsymbol{x}_i + \boldsymbol{B}\boldsymbol{u}_i(t))\mathrm{d}t + f(\boldsymbol{x}_i(t), t)\mathrm{d}\boldsymbol{w}(t), \tag{34}$$

where $\boldsymbol{x}_i(t)$ and $\boldsymbol{u}_i(t)$ are the state and control input for the ith agent, and $\boldsymbol{w}(t)$ is a one-dimensional Brownian motion satisfying $\mathrm{E}(\mathrm{d}\boldsymbol{w}(t)) = 0$ and $\mathrm{E}(\mathrm{d}\boldsymbol{w}^2(t)) = \mathrm{d}t$. The mean-square stability protocol of a multi-agent system under two types of attacks (connectivity-maintained attacks and connectivity-broken attacks) are studied and subjected to the following control objective

$$\mathrm{E}\left[\|\boldsymbol{x}_i(t) - \boldsymbol{x}_0(t)\|^2\right] \leqslant \alpha \mathrm{e}^{-\lambda(t-t_0)} \mathrm{E}\left[\|\boldsymbol{x}_i(t_0) - \boldsymbol{x}_0(t_0)\|^2\right], \tag{35}$$

where the scalars $\alpha > 0$ and $\lambda > 0$ for $\forall t \geqslant t_0$.

Yuan et al. [47] interpreted the "Resilience" as the ability to be robust with external disturbances and when defending against DoS attacks. The delta operator is used to discretize the continuous-time system, and then, switching system theory is employed to achieve resilient control. However, the switching signal θ_n implies the uncertainty and DoS attacks are modeled as a Markov process, and it lies in the following forms

$$\begin{cases} \widehat{\boldsymbol{y}}(k) = (1 - \gamma_{1,\theta_n})\boldsymbol{y}(k) + \gamma_{1,\theta_n}\boldsymbol{y}(k-1), \\ \widehat{\boldsymbol{u}}(k) = (1 - \gamma_{2,\theta_n})\boldsymbol{u}(k) + \gamma_{2,\theta_n}\boldsymbol{u}(k-1), \end{cases} \tag{36}$$

where γ_{1,θ_n} and γ_{2,θ_n} are both stochastic variables according to the Bernouli distribution and depend on IDS and DoS attacker, respectively.

Befekadu et al. [48] considered that the attacker is modulated by a hidden Markov process, which can jam the control packets stochastically. The following attack model is considered

$$\begin{cases} \boldsymbol{x}(k+1) = \boldsymbol{A}\boldsymbol{x}(k) + \boldsymbol{\gamma}(Z_{k+1})\boldsymbol{B}\boldsymbol{u}(k) + \boldsymbol{w}(k+1), \\ \boldsymbol{y}(k+1) = \boldsymbol{C}\boldsymbol{x}(k) + \boldsymbol{v}(k+1). \end{cases} \tag{37}$$

They then studied the risk-sensitive control problem following an exponential running cost with the quadratic function

$$J(\boldsymbol{u}) = \frac{1}{\theta} E\left[\exp\left(\frac{\theta}{2}\left(\sum_{k=0}^{N-1}(\boldsymbol{x}^{\mathrm{T}}(k)\boldsymbol{Q}\boldsymbol{x}(k)) + \gamma(\boldsymbol{Z}_{k+1})\boldsymbol{u}^{\mathrm{T}}(k)\boldsymbol{R}\boldsymbol{u}(k) + \boldsymbol{x}^{\mathrm{T}}(N)\boldsymbol{P}\boldsymbol{x}(N)\right)\right)\right], \tag{38}$$

where $\theta > 0$ is a risk-sensitive parameter and $\boldsymbol{Z}_{k+1}$ is related to the internal state of attacker. They solved the above optimal control problem of finite-dimensional dynamics through a chain of measurement transformation techniques.

In addition, Pang and Liu [49] considered both the defending and secure control problems in NCSs. Encryption algorithms such as DES and MD5 are used to secure the data transmission on both the control and plant side. Then the recursive networked predictive control (RNPC) method is used to guarantee the control performance under deception attacks.

An adversary is always trying to drive the state to the unsafe region while bypassing a detector. Corresponding to the goal of adversaries, the intent of a secure controller is to minimize the effect of the adversary with safety constraints. Hence, a secure control would make an effort to restore system operation from various attacks.

5 Conclusions

NCSs have been implemented successfully for more than 20 years. However, the security of NCSs, as a fresh research area, derives some rigorous studies of the comprehensive effects, such as detection, identifiability, and remedy schemes for attacks [50]. By reviewing some recent works on these interesting aspects, we attempt to discuss some meaningful issues that have promising directions in this area.

(i) Unified modeling under attacks and uncertainties. The introduction of a network adds more

complexity including security and uncertainties for NCSs [51]. Currently, network attacks and external disturbances are considered separately during the controller design, which is impractical. Therefore, the external uncertainties and internal security should be considered at the same time to improve the overall performance of NCSs.

(ii) Resilient control under attacks. NCSs suffer from the intersection between physical systems and cyberspace and the intersection between external disturbance and adversary attacks. Robust control methods may be effective for external disturbance but inadequate against network attacks. The existing works consider the network attacks that are mostly addressed to a specific attack type but hardly for different attack types. Resilient control, as a next-generation research design that pays more attention to both the external disturbance and vulnerability of a network, may provide a solution to many uncertainties containing various attack types [52, 53].

(iii) Risk assessment. Risk assessment has been studied in-depth for the security of traditional IT. However, more uncertainties and risks should be considered in NCSs. In terms of the "resilience" for operation, we often allowed a faster response or degradation operation to minimize the impacts of those uncertainties and risks. A question is how does one evaluate these impacts on a system. The quantitative risk management approach may be a guide to the safe and stable operation of NCSs [10].

In this paper, we characterize some security problems of NCSs partially from system-theoretic and control-theoretic aspects. Sensing security, network security and control security are discussed. However, as a challenging topic for the security of NCSs, there are still more efforts to be made in different areas.

Acknowledgements This work was supported in part by the National Natural Science Foundation of China (Grant Nos. 61673255, 61263003 and 61273114); the International Corporation Project of Shanghai Science and Technology Commission (Grant No. 14510722500); the Program for Professor of Special Appointment (Eastern Scholar) at Shanghai Institutions of Higher Learning; the Key Project of Science and Technology Commission of Shanghai Municipality (Grant No. 10JC1405000); A Project of Shandong Province Higher Educational Science and Technology Program (Grant No. J17KA084).

References

1. Konstantinou C, Maniatakos M, Saqib F et al (2015) Cyber-physical systems: a security perspective. IEEE Eur Test Symp 1–8
2. Peng C, Zhang J (2016) Delay-distribution-dependent load frequency control of power systems with probabilistic interval delays. IEEE Trans Power Syst 31(4):3309–3317
3. Slay J, Miller M (2007) Lessons learned from the maroochy water breach. In: International conference critical infrastructure protection, Springer, US 73–82
4. Kuvshinkova S (2003) SQL slammer worm lessons learned for consideration by the electricity sector. North Am Electr Reliab Counc 1(2):5
5. Farwell JP, Rohozinski R (2011) Stuxnet and the future of cyber war. Survival 53(1):23–40
6. Wu G, Sun J, Chen J (2016) A survey on the security of cyber-physical systems. Control Theory Technol 14(1):2–10
7. Dong P, Han Y, Guo X et al (2015) A systematic review of studies on cyber physical system security. Int J Secur Appl 9 (1):155–164
8. Amin S, Sastry S (2008) Research challenges for the security of control systems. In: USENIX association conference hot topics in security 1–6
9. O'Connell K (2008) Cia report: cyber extortionists attacked foreign power grid, disrupting delivery. Internet Business Law Services. http://www.ibls.com/internetlawnewsportalview.aspx
10. Sandberg H, Amin S, Johansson K (2015) Cyberphysical security in networked control systems: an introduction to the issue. IEEE Trans Control Syst 35(1):20–23
11. Teixeira A, Shames I, Sandberg H et al (2015) A secure control framework for resource-limited adversaries. Automatica 51:135–148
12. Smith RS (2011) A decoupled feedback structure for covertly appropriating networked control systems. IFAC Proc 44(1):91–95
13. Teixeira A, Dán G, Sandberg H et al (2010) A cyber security study of a scada energy management system: stealthy deception attacks on the state estimator. IFAC Proc 44(1):11271–11277
14. Cárdenas AA, Amin S, Lin ZS et al (2011) Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of ACM symposium information, computer communication security 355–366
15. Mo Y, Kim TH, Brancik K et al (2012) Cyber-physical security of a smart grid infrastructure. Proc IEEE 100(1):195–209
16. Teixeira A, Pérez D, Sandberg H et al (2012) Attack models and scenarios for networked control systems. In: Proceedings of High Confidence Networked System 55–64
17. Sauter D, Li S, Aubrun C (2009) Robust fault diagnosis of networked control systems. Int J Adapt Control Signal Process 23 (8):722–736
18. Ding S (2008) Model-based fault diagnosis techniques: design schemes, algorithms, and tools, vol 49. Springer, Berlin, pp 50–56
19. Amin S, Litrico X, Sastry SS et al (2010) Stealthy deception attacks on water SCADA systems. In: Proceedings of ACM conference hybrid system: computation and control, pp 161–170
20. Mo Y, Sinopoli B(2009) Secure control against replay attacks. In: Annual allerton conference communication, Control Computing, pp 911–918
21. Fawzi H, Tabuada P, Diggavi S (2014) Secure estimation and control for cyber-physical systems under adversarial attacks. IEEE Trans Autom Control 59(6):1454–1467
22. Kosut O, Jia L, Thomas RJ et al (2010) Malicious data attacks on smart grid state estimation: attack strategies and

countermeasures. In: IEEE conference smart grid communications, pp 220–225
23. Liu Y, Ning P, Reiter MK (2011) False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur 14(1):1–16
24. Schenato L (2009) To zero or to hold control inputs with lossy links. IEEE Trans Autom Control 54(5):1093–1099
25. Mo Y, Garone E, Casavola A et al (2010) False data injection attacks against state estimation in wireless sensor networks. In: IEEE Conference Decision Control, pp 5967–5972
26. Kwon C, Liu W, Hwang I (2013) Security analysis for cyber-physical systems against stealthy deception attacks. In: American Control Conference, pp 3344–3349
27. Gertler JJ (1988) Survey of model-based failure detection and isolation in complex plants. Cont Syst Mag 8(6):3–11
28. Manandhar K, Cao X, Hu F et al (2014) Detection of faults and attacks including false data injection attack in smart grid using kalman filter. IEEE Trans Control Netw Syst 1(4):370–379
29. Kailath T, Poor HV (1998) Detection of stochastic processes. IEEE Trans Inf Theory 44(6):2230–2231
30. Wald A (1973) Sequential analysis. Courier Corporation, North Chelmsford
31. Pang ZH, Hou FY, Zhou YG et al (2015) False data injection attacks for output tracking control systems. In: Chinese Control Conference, pp 6747–6752
32. Xu Z, Ji Y, Zhou D (2009) A new real-time reliability prediction method for dynamic systems based on online fault prediction. IEEE Trans Reliab 58(3):523–538
33. Pasqualetti F, Dorfler F, Bullo F (2012) Cyber-physical security via geometric control: distributed monitoring and malicious attacks. In: Annual conference decision and control, pp 3418–3425
34. Zhang H, Cheng P, Shi L et al (2016) Optimal dos attack scheduling in wireless networked control system. IEEE Trans Control Syst Technol 24(3):843–852
35. Zhang H, Cheng P, Shi L et al (2015) Optimal denial-of-service attack scheduling with energy constraint. IEEE Trans Autom Control 60(11):3023–3028
36. Zhang H, Cheng P, Shi L et al (2013) Optimal DoS attack policy against remote state estimation. In: IEEE annual conference decision and control, pp 5444–5449
37. Zhang H, Cheng P, Shi L et al (2014) Optimal denial-of-service attack scheduling against linear quadratic gaussian control. In: American control conference, pp 3996–4001
38. Gupta A, Langbort C, Basar T (2010) Optimal control in the presence of an intelligent jammer with limited actions. In: Annual conference decision and control, pp 1096–1101
39. Zhu M, Martinez S (2011) Stackelberg-game analysis of correlated attacks in cyber-physical systems. In: American control conference, pp 4063–4068
40. Wang EK, Ye Y, Xu X et al (2010) Security issues and challenges for cyber physical system. In: Proc IEEE/ACM conference green computing communication & conference cyber, physical society computing, pp 733–738
41. Lee C, Shim H, Eun Y (2015) Secure and robust state estimation under sensor attacks, measurement noises, and process disturbances: observer-based combinatorial approach. In: European control conference, pp 1872–1877
42. Shoukry Y, Tabuada P (2016) Event-triggered state observers for sparse sensor noise/attacks. IEEE Trans Autom Control 61 (8):2079–2091
43. Foroush H S, Martínez S(2012) On single-input controllable linear systems under periodic dos jamming attacks. arXiv preprint arXiv:1209.4101
44. Persis CD, Tesi P (2015) Input-to-state stabilizing control under denial-of-service. IEEE Trans Autom Control 60(11):2930–2944
45. Amin S, Cárdenas AA, Sastry SS (2009) Safe and secure networked control systems under denial-of service attacks. In: Hybrid systems: computation and control, Springer, pp 31–45
46. Feng Z, Hu G, Wen G (2016) Distributed consensus tracking for multi-agent systems under two types of attacks. Int J Robust Nonlinear Control 26(5):896–918
47. Yuan Y, Sun F, Zhu Q (2015) Resilient control in the presence of dos attack: switched system approach. Int J Control Autom Syst 13(6):1423–1435
48. Befekadu GK, Gupta V, Antsaklis PJ (2015) Risksensitive control under markov modulated denial-of service (DoS) attack strategies. IEEE Trans Autom Control 60(12):3299–3304
49. Pang ZH, Liu GP (2012) Design and implementation of secure networked predictive control systems under deception attacks. IEEE Trans Control Syst Technol 20(55):1334–1342
50. Pasqualetti F, Dorfler F, Bullo F (2015) Controltheoretic methods for cyberphysical security: geometric principles for optimal cross-layer resilient control systems. IEEE Trans Control Syst 35(1):110–127
51. Peng C, Ma SD, Xie XP (2017) Observer-based non-PDC control for networked T-S fuzzy systems with an event-triggered communication. IEEE Transactions on Cybernetics (99):1–9
52. Rieger CG, Gertman DI, McQueen MA (2009) Resilient control systems: next generation design research. In: HIS conference human system interaction, pp 632–636
53. Peng C, Li JC, Fei MR (2016) Resilient event-triggered H_∞ load frequency control for networked power systems with energy-limited DoS attacks. IEEE Trans Power Syst 99:1