Stochastic Communication Protocol-Based Security Control for Discrete-Time Networked Systems Using State Observer

Jian Liu, *Member, IEEE*, Jiachen Ke, Jinliang Liu, *Member, IEEE*, Xiangpeng Xie, *Senior Member, IEEE*, and Engang Tian, *Member, IEEE*

***Abstract*—This article addresses a security control issue for discrete-time networked control systems (DTNCSs) with uncertainty under stochastic communication protocol (SCP) characterizing a class of networked systems, such as autonomous dynamics. Specially, in order to properly take account of the constructed system in practical application, the time-varying uncertainty with norm-bounded parameter is adopted in DTNCSs. To avoid data conflict in the communication network with limited bandwidth, SCP modeled by discrete-time Markov chain is introduced to schedule the transmitted signals, which are subjected to deception attacks described by a random process. In addition, the mode-dependent observer and controller are utilized in line with the scheduling situations led by SCP. Moreover, the stochastic stability of the augmented dynamics is ensured by the presented sufficient condition. Meanwhile, the corresponding gain parameters of the observer and controller can be computed. Ultimately, two simulation experiments are utilized to validate the availability of the proposed security control strategy.**

***Index Terms*—Deception attacks, norm-bounded uncertainty, security control, state observer, stochastic communication protocol (SCP).**

I. Introduction

ALONG with the rapid advances of networked communication, networked control systems (NCSs) are extensively concerned by a gigantic quantity of researchers nowadays [1], [2], [3], [4]. Under its advantages, including easy manipulation, high reliability and affordable cost, NCSs were employed in engineering practice. Nevertheless, due to the unmanageable uncertainty and flexibility originated from the real-world circumstances, the practical implementation of NCSs has enormously increased analysis complexity to a considerable extent. Considering a great variety of mutable factors in industrial production, the uncertain dynamics has been frequently employed to improve the robustness in the analysis of NCSs [5], [6], [7]. So far, abundant research results about uncertain systems were vigorously published in various fields. For example, Wang et al. [8] designed a formation control scheme for autonomous underwater vehicles (AUVs) with external disturbances and uncertainties. In [9], a distributed tracking control problem for AUVs with heterogeneous uncertainty was investigated based on a learning control approach. Thus, from the realistic perspective of implementation, it is worthy of further discussion on NCSs with the uncertain parameters.

In practical engineering, since state information in NCSs is usually hard to measure, the controller design in the presence of state observer has become an extremely important problem. Furthermore, the control strategy using state observer has achieved some interests in academic community and plentifully effective theoretical methods have been applied in linear systems [10] and nonlinear systems [11], [12], [13]. In [14], the state observer-based fuzzy control scheme utilized in nonlinear systems was investigated by proposing a novel linear matrix inequality (LMI) technique. Under event-triggered communication mechanism, the results on an observer-based tracking problem were presented for distributed nonlinear multiagent systems in [15]. In [16], an innovative strategy was designed to address the control issue for semi-Markovian jump systems on the basis of observer. From the existing results above, the research on NCSs with the time-varying uncertainty via state observer would be of abundant practical significance.

On another frontier of research, network security is also a prominent topic of discussion for NCSs, as the shared communication channel is vulnerable to a wide range of malicious attacks. It should be noted that significant financial and private issues may arise [17], [18], [19] when hostile actions are targeted for the networked systems. Thus, the attention on network security in NCSs is enormously concentrated to improve the security control effects. Generally, a variety of malignant attacks can be considered, such as denial-of-service

Manuscript received 1 August 2023; accepted 25 May 2024. Date of publication 17 June 2024; date of current version 20 August 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62001210, Grant 62373252, Grant 61973152, and Grant 62373196; in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20211290; in part by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant KYCX23_1887; and in part by the Startup Foundation for Introducing Talent of NUIST under Grant 2024r063. This article was recommended by Associate Editor N. B. Mehta. *(Corresponding author: Jinliang Liu.)*

Jian Liu and Jiachen Ke are with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: by.liujian@gmail.com; 2212602143@qq.com).

Jinliang Liu is with the School of Computer Science, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: liujinliang@vip.163.com).

Xiangpeng Xie is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: xiexiangpeng1953@163.com).

Engang Tian is with the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China (e-mail: tianengang@163.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSMC.2024.3406563.

Digital Object Identifier 10.1109/TSMC.2024.3406563

(DoS) attacks [20], injection attacks [21], and deception attacks [22], which can be regarded as extremely malicious attacks for the communication network due to the fact that false signal sent by attackers can lead to the networked system controlled mistakenly. In recent decades, the security topic for autonomous dynamics has appealed to ever-increasing interest from domestic and foreign scholars [23], [24]. For instance, the secure tracking control problem under deception attacks for autonomous ground vehicles (AGVs) was investigated by adopting event-triggered mechanism in [25]. Focusing on the content above, it can be witnessed apparently that the security control scheme has received an increasing prevalence of attention under the negative effects of malicious attacks, which is part of inspiring our research.

In engineering applications, all signals could be granted the privilege to transmit via the same communication medium, which may lead to the unexpected data conflict. In an effort to overcome this obstacle, communication protocols are exploited to schedule these signals on the ground of specific rules. The communication protocols mainly include try-once-discard protocol (TODP) [26], stochastic communication protocol (SCP) [27], round-robin protocol (RRP) [28] and FlexRay protocol [29]. Owing to different operating mechanism, there are almost no existing articles comparing SCP with other communication protocols. To be specific, the SCP determines the signal transmission order at each communication step in the form of random probability, which can be reasonably predefined according to the importance of different tasks. Moreover, RRP can schedule nodes in a periodic manner such that it emphasizes the transmitted fairness [30]. The selection principle of TODP is presented by quadratic functions [26] and the scheduled signals can be adjusted at each update moment. As a hybrid mechanism, FlexRay protocol can work under the combination of time-triggered and event-triggered transmissions [29]. At present, a series of research on NCSs adopted communication protocol has been reported to analyse the system performances [31], [32]. For instance, the fuzzy control issue for nonlinear systems under SCP and dynamic quantization was investigated based on LMI technique in [33]. By applying SCP, the sliding mode controller design for uncertain dynamics under unmatched disturbances was conveniently investigated in [34]. As a class of carrier-sense multiple access with collision avoidance protocol, SCP can prevent data conflict before it occurs different from the carrier sense multiple access/collision detect protocol [35]. It should be mentioned that SCP has been commonly applied in theory research and industrial reality, such as local area networks [36]. Hence, it is rational for adopting SCP to avoid data conflict in NCSs. However, the comprehensive consideration of the SCP scheduling behaviors and cyber attacks have received less attention in NCSs, which prompts our further exploration in this work.

Enlighted by the aforementioned investigation, we focus on security controller design for discrete-time NCSs (DTNCSs) with uncertainty under SCP and deception attacks. The significant features of this article can be listed as:

1) This article establishes a security control scheme for uncertain DTNCSs against deception attacks. In comparison with the polytopic uncertainty in [37], the proposed theoretical results can save the computational resources by considering norm-bounded uncertainty. Meanwhile, to lessen the network pressure, SCP are utilized to select the transmitted signals through a shared channel. Different from the static periodic scheduling of RRP [28], the applied SCP places more emphasis on the randomness and dynamicity of scheduling.
2) The secure issues in [25] and [38] have been addressed for realistic systems, however, the state information is regarded as available. Unfortunately, the system states are hard to directly obtain in actual environment. By applying a state observer in this article, the unavailable state can be appropriately estimated so as to conquer the aforementioned problem.
3) A novel augmented model is presented by simultaneously taking account of time-varying uncertainty, SCP described by Markov chain, state observer and random deception attacks. In addition, considering the scheduling behaviors of SCP, the mode-dependent Lyapunov function and observer-based controller are constructed to attain less conservative results compared with [39]. Furthermore, in an effort to assure the stochastic stability of the augmented dynamics, some solvable sufficient design criteria are proposed.

The remaining article is arranged as below. In Section II, the uncertain DTNCSs with SCP scheduling and deception attacks are elaborated. Section III describes the major results of this article. In Section IV, two simulation examples are conducted to validate the availability of the proposed control scheme. Eventually, this article is concluded in Section V. To simplify the next analysis, some adopted mathematical symbols are demonstrated in Table I.

TABLE I
MATHEMATICAL SYMBOLS

Symbol	Connotation
$\mathbb{R}^t$	t-dimensional Euclidean space
$\mathbb{R}^{t\times s}$	$t \times s$ real matrices
Z^{-1}	inverse of Z
Z^T	transpose of Z
I	the identity matrix
$*$	a symmetric term in matrices
$\|\cdot\|$	Euclidean vector norm
$E\{X\}$	the mathematics expectation of X
$\mathcal{H}e\{Y\}$	the sum of matrix Y and Y^T
$l_2[0,\infty)$	the square-summable vector space
Prob$\{Z\}$	the occurrence probability of Z
diag$\{\cdots\}$	a block-diagonal matrix

II. PROBLEM FORMULATION

The DTNCSs under SCP and randomly activated deception attacks are presented in Fig. 1. In this section, the uncertain DTNCSs will be introduced in the first place. Then, we will demonstrate the scheduling behaviors of SCP and the effects of deception attacks in detail. The rest of this section is organized to model the state observer and controller.

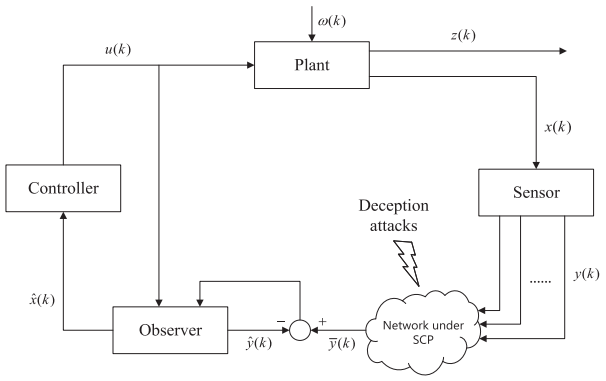


Fig. 1. Structure of the DTNCSs with SCP and deception attacks.

A. System Description

Consider the following uncertain DTNCSs to characterize a class of networked systems, such as autonomous dynamics:

$$\begin{cases} x(k+1) = (A + \Delta A_k)x(k) + Bu(k) + E\omega(k) \\ z(k) = C_1 x(k) + Du(k) + F\omega(k) \\ y(k) = C_2 x(k) \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^{n_x}$ is the system state, $u(k) \in \mathbb{R}^{n_u}$ represents the controlled input, $y(k) \in \mathbb{R}^{n_y}$ denotes measured output, $z(k) \in \mathbb{R}^{n_z}$ is the controlled output, $\omega(k) \in \mathbb{R}^{n_\omega}$ stands for the external disturbance which belongs to $l_2[0, \infty)$. A, B, C_1, C_2, D, E and F indicate given coefficient matrices. The parameter ΔA_k with norm-bounded uncertainty satisfies

$$\Delta A_k = S\Delta_k Q \tag{2}$$

in which S and Q are given real matrices and Δ_k is the time-varying parameters with $\Delta_k^T \Delta_k \le I$.

Remark 1: According to the temporal properties, the uncertainties of NCSs can be divided into two forms: the time-varying uncertainty and the time-invariant uncertainty. In light of [33], the time-varying norm-bounded uncertainty is mainly considered in this system. It should be noted that ΔA_k shown in (2) can easily change as time goes by, which is more coincident with the actual situations in engineering practice. Therefore, the considered DTNCSs (1) in this article is more robust and flexible in comparison with the system containing the time-invariant uncertainty. On the other hand, polytopic approaches [37] have also been investigated to model uncertain parameters. Under this strategy, more precise descriptions of uncertain systems will be obtained. In such sense, the theoretical results adopted the norm-bounded strategy are comparatively more conservative. Nevertheless, it can be noted that the expensive computational cost may occur by applying general polytopic methods with the large number of vertices [40]. From the perspective of limited resources, the norm-bounded uncertainty is more effective for NCSs with constrained communication.

B. SCP and Deception Attacks

As depicted in Fig. 1, the measurement $y(k)$ can be transmitted to observer via a networked communication with restricted bandwidth. It is obvious from Fig. 1 that all sensor signals have an opportunity to be transferred at each time instant. However, since the situation of simultaneous multiple access can tremendously induce the communication burden, the phenomenon of data conflict is more likely to occur in the presence of the confined network resources. Thus, to obviate the aforesaid obstacles, SCP will be adopted to regulate the transmitted sequences of all sensor signals at the k-step.

Let $\varphi_k \in \mathbb{M} \triangleq \{1, 2, \ldots, n_y\}$ represent the scheduled signal acquiring access to a communication channel. Meanwhile, consider the rule of discrete-time Markov chain (DTMC) with the transition probability matrix (TPM) $\mathcal{Q} = [p_{ts}]_{n_y \times n_y}$. In view of [34], the transition probability p_{ts} of $\varphi_{k+1} = s$ condition on $\varphi_k = t$ can be defined as

$$p_{ts} \triangleq \text{Prob}\{\varphi_{k+1} = s | \varphi_k = t\}, \ t, s \in \mathbb{M} \tag{3}$$

where $0 \le p_{ts} \le 1$ and $\sum_{s=1}^{n_y} p_{ts} = 1$.

Remark 2: The scheduling behaviors of SCP can be typically characterized by two different modeling forms: the DTMC [34], and the mutually independent and identically-distributed (i.i.d.) sequence [41]. To be specific, the transition probability (3) can be rewritten as $p_i = \text{Prob}\{\varphi_k = i\}$ with $p_i > 0$ and $\sum_{i=0}^{n_y} p_i = 1$ ($i \in \mathbb{M}$) when the SCP is formulated by the i.i.d. sequence in this article. It is worth mentioning that the former is considered more in NCSs even though the transition probability of the letter is easier and more uniform for all sensor signals via a communication channel at any step. Thus, we take DTMC into account to model the SCP behaviors in this article.

As shown in [42], a Bernoulli variable $\alpha(k)$ can be exploited to represent the stochastic process of deception attacks with the following conditions:

$$\begin{aligned} \text{Prob}\{\alpha(k) = 1\} &= E\{\alpha(k)\} = \bar{\alpha} \\ \text{Prob}\{\alpha(k) = 0\} &= 1 - \bar{\alpha} \end{aligned} \tag{4}$$

where $\alpha(k) \in \{0, 1\}$, $\bar{\alpha} \in [0, 1]$ is a given constant.

Let $y(k) = [y_1^T(k), y_2^T(k), \ldots, y_{n_y}^T(k)]^T$ and $\bar{y}(k) = [\bar{y}_1^T(k), \bar{y}_2^T(k), \ldots, \bar{y}_{n_y}^T(k)]^T$ denote the measured output before and after transmission, respectively. In an effort to characterize the effect of SCP and deception attacks in detail, the comprehensive updating law of $\bar{y}_i(k)$ ($i \in \mathbb{M}$) is formulated as

$$\bar{y}_i(k) = \begin{cases} y_i(k) + \alpha(k)h(k), & \text{if } i = \varphi_k \\ \bar{y}_i(k-1), & \text{otherwise} \end{cases} \tag{5}$$

where $h(k) = -y_i(k) + v(k)$ denotes the false data affecting network transmission, and $v(k)$ denotes the malicious energy satisfying

$$v^T(k)v(k) \le x^T(k)G^T Gx(k) \tag{6}$$

in which G stands for a given parameter to describe the energy restriction.

From (3) and (5), $\bar{y}(k)$ can be easily derived as

$$\bar{y}(k) = (1 - \alpha(k))\phi_{\varphi_k} y(k) + \bar{\phi}_{\varphi_k}\bar{y}(k-1) + \alpha(k)\tilde{\phi}_{\varphi_k} v(k) \tag{7}$$

where $\phi_{\varphi_k} \triangleq \text{diag}\{\delta(\varphi_k - 1), \delta(\varphi_k - 2), \ldots, \delta(\varphi_k - n_y)\}$, $\bar{\phi}_{\varphi_k} = I - \phi_{\varphi_k}$, $\tilde{\phi}_{\varphi_k} = \phi_{\varphi_k} F_y$, $F_y = [I \cdots I]^T$. $\delta(\varphi_k - i) \in \{0, 1\} (i \in \mathbb{M})$ is the Kronecker delta function.

Remark 3: Under the SCP, the unselected sensor signals will be compensated by zero-order holder (ZOH) scheme, which stores the transmitted data at the last updating moment. While only one signal can be selected to transmit at each instant, $\alpha(k) = 0$ indicates an expected transmission process through network arrived at observer, $\alpha(k) = 1$ represents the transmission suffering deception attacks. In addition, by using the zero-input (ZI) strategy [32], the sensor data not obtaining the privilege of communication channel can be replaced by zero and the measured output after network transmission can be derived that $\bar{y}(k) = (1-\alpha(k))\phi_{\varphi_k} y(k) + \alpha(k)\tilde{\phi}_{\varphi_k} v(k)$. On account of the analysis hereinbefore, the ZOH strategy is relatively more reasonable and reliable compared with the ZI method.

Remark 4: In realistic scenarios, the attack-related information, which include peak, probability and so on, can be obtained by the defender due to the abnormal conditions posed by malicious attackers [43]. Therefore, the probability $\bar{\alpha}$ in (4) can be acquired by monitoring the network online. Under the actual implementation, the adversary may unexpectedly launch attack data in a communication network such that the Bernoulli process is applied to characterize this effect motivated by [13] and [44]. In (6), the energy bounded signal $v(k)$ has been utilized to consider the concealment of the adversary, which is more practical in comparison with [45]. Based on the elaboration above, the adopted model has realistic merits and significance. However, the scheme of attack detection is not designed and this is a limitation of this article. In future research, we will endeavor to investigate this problem.

C. Observer and Controller Design

In light of the SCP, the state observer and controller with dependent mode will be designed in this section. Inspired by [13], the dynamics of observer can be modeled as

$$\begin{cases} \hat{x}(k+1) = A\hat{x}(k) + Bu(k) + L_{\varphi_k}\big(\bar{y}(k) - \hat{y}(k)\big) \\ \hat{y}(k) = C_2\hat{x}(k) \end{cases} \tag{8}$$

where $\hat{x}(k) \in \mathbb{R}^{n_x}$ is observer state, $\hat{y}(k) \in \mathbb{R}^{n_y}$ is the estimation of $y(k)$, and L_{φ_k} stands for the observer gain with proper dimensions.

In this article, the estimated state $\hat{x}(k)$ can be transferred to the controller. Then, the rule of the controller is set to be

$$u(k) = K_{\varphi_k}\hat{x}(k) \tag{9}$$

in which K_{φ_k} denotes the gain matrix to be determined.

For convenient description, we abbreviate φ_k and φ_{k+1} as t and s, respectively. Meanwhile, define $e(k) \triangleq x(k) - \hat{x}(k)$ as the estimation error. By combining (1) and (9), it can be derived that

$$\begin{aligned} x(k+1) &= (A + \Delta A_k)x(k) + Bu(k) + E\omega(k) \\ &= (A + \Delta A_k + BK_t)\hat{x}(k) + (A + \Delta A_k)e(k) \\ &\quad + E\omega(k) \end{aligned} \tag{10}$$

$$\begin{aligned} z(k) &= C_1 x(k) + Du(k) + F\omega(k) \\ &= (C_1 + DK_t)\hat{x}(k) + C_1 e(k) + F\omega(k). \end{aligned} \tag{11}$$

From the conditions (7)-(9), we can derive that

$$\begin{aligned} \hat{x}(k+1) &= A\hat{x}(k) + Bu(k) + L_t\big(\bar{y}(k) - \hat{y}(k)\big) \\ &= (A + BK_t - L_tC_2 + (1-\alpha(k))L_t\phi_tC_2)\hat{x}(k) \\ &\quad + (1-\alpha(k))L_t\phi_tC_2e(k) + L_t\bar{\phi}_t\bar{y}(k-1) \\ &\quad + \alpha(k)L_t\tilde{\phi}_t v(k). \end{aligned} \tag{12}$$

According to (10) and (12), one has

$$\begin{aligned} e(k+1) &= (\Delta A_k + L_tC_2 - (1-\alpha(k))L_t\phi_tC_2)\hat{x}(k) \\ &\quad + (A + \Delta A_k - (1-\alpha(k))L_t\phi_tC_2)e(k) \\ &\quad - L_t\bar{\phi}_t\bar{y}(k-1) + E\omega(k) - \alpha(k)L_t\tilde{\phi}_t v(k). \end{aligned} \tag{13}$$

By denoting $\xi(k) \triangleq [\hat{x}^T(k) \;\; e^T(k) \;\; \bar{y}^T(k-1)]^T$, we obtain the augmented dynamics, which is of the formulation as

$$\begin{cases} \xi(k+1) = (M_1 + M_2)\xi(k) + (M_3 + M_4)v(k) + \bar{E}\omega(k) \\ z(k) = \bar{C}\xi(k) + F\omega(k) \end{cases} \tag{14}$$

where

$$\begin{aligned} M_1 &= \begin{bmatrix} \Pi_{11} & \vec{\alpha}L_t\phi_tC_2 & L_t\bar{\phi}_t \\ \Pi_{21} & \Pi_{22} & -L_t\bar{\phi}_t \\ \Pi_{31} & \Pi_{32} & \bar{\phi}_t \end{bmatrix}, \; \bar{E} = \begin{bmatrix} 0 \\ E \\ 0 \end{bmatrix} \\ M_2 &= \begin{bmatrix} -\alpha^*(k)L_t\phi_tC_2 & -\alpha^*(k)L_t\phi_tC_2 & 0 \\ \alpha^*(k)L_t\phi_tC_2 & \alpha^*(k)L_t\phi_tC_2 & 0 \\ -\alpha^*(k)\phi_tC_2 & -\alpha^*(k)\phi_tC_2 & 0 \end{bmatrix} \\ M_3 &= \begin{bmatrix} \bar{\alpha}L_t\tilde{\phi}_t \\ -\bar{\alpha}L_t\tilde{\phi}_t \\ \bar{\alpha}\tilde{\phi}_t \end{bmatrix}, \; M_4 = \begin{bmatrix} \alpha^*(k)L_t\tilde{\phi}_t \\ -\alpha^*(k)L_t\tilde{\phi}_t \\ \alpha^*(k)\tilde{\phi}_t \end{bmatrix} \\ \Pi_{11} &= A + BK_t - L_tC_2 + \vec{\alpha}L_t\phi_tC_2, \; \vec{\alpha} = 1 - \bar{\alpha} \\ \Pi_{21} &= \Delta A_k + L_tC_2 - \vec{\alpha}L_t\phi_tC_2, \; \alpha^*(k) = \alpha(k) - \bar{\alpha} \\ \Pi_{22} &= A + \Delta A_k - \vec{\alpha}L_t\phi_tC_2, \; \Pi_{31} = \Pi_{32} = \vec{\alpha}\phi_tC_2 \\ \bar{C} &= \begin{bmatrix} C_1 + DK_t & C_1 & 0 \end{bmatrix}. \end{aligned}$$

Obviously, $E\{\alpha^*(k)\} = 0$ and $E\{\alpha^*(k)\alpha^*(k)\} = \bar{\alpha}\vec{\alpha}$ can be simply obtained.

In this work, we endeavor to design a security controller for DTNCSs (1) guaranteeing the stochastic stability in the sense of H_∞. Therefore, in order to design the relevant parameters of the applied control scheme, the following requirements and lemmas are applied by giving sufficient condition.

Definition 1 [33]: When $\omega(k) = 0$ with initial condition $\xi(0)$ and φ_0, the augmented dynamics (14) is stochastically stable if the following condition holds:

$$E\left\{\sum_{k=0}^{\infty}\|\xi(k)\|^2\right\} < \infty. \tag{15}$$

Definition 2 [34]: For positive parameter γ, the H_∞ performance of the augmented system (14) with uncertainty can be obtained if

$$E\left\{\sum_{k=0}^{\infty}\|z(k)\|^2\right\} \le \gamma^2\sum_{k=0}^{\infty}\|\omega(k)\|^2. \tag{16}$$

Lemma 1 [46]: Given the matrices $\Omega = \Omega^T$, X, Y and Δ satisfying $\Delta\Delta^T < I$ with suitable dimensions, $\Omega +$

$\mathcal{H}e\{X\Delta Y\} < 0$ holds if given a constant $\tau > 0$, the following inequality can be obtained:

$$\Omega + \tau^{-1}XX^T + \tau Y^T Y < 0. \tag{17}$$

Lemma 2 [47], [48]: The singular value decomposition (SVD) for matrix $\mathcal{F} \in \mathbb{R}^{n_x \times n_u}$ with $\text{rank}(\mathcal{F}) = n_u$ can be expressed as $\mathcal{F} = M\begin{bmatrix} S & 0 \end{bmatrix}N^T$, where $M^TM = I$ and $N^TN = I$. Denote matrices $Z > 0$, $U \in \mathbb{R}^{n_x \times n_x}$ and $V \in \mathbb{R}^{(n_u - n_x)\times(n_u - n_x)}$. There exists matrix $\bar{Z}$ such that $\bar{Z}\mathcal{F} = \mathcal{F}Z$ holds if

$$Z = N\begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix}N^T. \tag{18}$$

III. Main Results

In this position, the stochastic stability of the augmented dynamics (14) will be satisfied by sufficient design condition in Theorem 1. Additionally, the uncertainty ΔA_k can be properly handle in Theorem 2 and then, the desired gains parameters of observer-based controller are obtained in Theorem 3 by solving LMI.

Theorem 1: Given scalars $\gamma > 0$, the probability $\bar{\alpha} \in (0, 1)$, transition probability p_{ts}, and the observer-based controller gains L_t, K_t, the augmented dynamics (14) is stochastically stable if there exist positive-definite symmetric matrix $P_t > 0$ such that

$$\vec{\Omega}_t < 0, \quad t \in \mathbb{M} \tag{19}$$

where

$$\vec{\Omega}_t = \begin{bmatrix} -\bar{P}_t^{-1} & * & * & * & * & * \\ 0 & -\bar{P}_t^{-1} & * & * & * & * \\ 0 & 0 & -I & * & * & * \\ M_1^T & \bar{M}_2^T & \bar{C}^T & -P_t + \bar{G} & * & * \\ M_3^T & \bar{M}_4^T & 0 & 0 & -I & * \\ \bar{E}^T & 0 & F^T & 0 & 0 & -\gamma^2 I \end{bmatrix}$$

$$\bar{M}_2 = \begin{bmatrix} -\mu L_t\phi_t C_2 & -\mu L_t\phi_t C_2 & 0 \\ \mu L_t\phi_t C_2 & \mu L_t\phi_t C_2 & 0 \\ -\mu\phi_t C_2 & -\mu\phi_t C_2 & 0 \end{bmatrix}, \ \bar{M}_4 = \begin{bmatrix} \mu L_t\tilde{\phi}_t \\ -\mu L_t\tilde{\phi}_t \\ \mu\tilde{\phi}_t \end{bmatrix}$$

$$\bar{G} = \begin{bmatrix} G^TG & * & * \\ G^TG & G^TG & * \\ 0 & 0 & 0 \end{bmatrix}, \ \bar{P}_t = \sum_{s=1}^{n_y} p_{ts}P_s, \ \mu = \sqrt{\bar{\alpha}\vec{\alpha}}.$$

Proof: Construct a Lyapunov function with dependent mode as follows:

$$V(k) = \xi^T(k)P_t\xi(k). \tag{20}$$

Define $\Delta V(k) = V(k+1) - V(k)$ representing the forward difference of $V(k)$. Then, taking SCP and deception attacks (6) into account, one derives

$$\begin{aligned} E\{\Delta V(k)\} &\le E\left\{\xi^T(k+1)P_s\xi(k+1) - \xi^T(k)P_t\xi(k)\right\} \\ &\quad + x^T(k)G^TGx(k) - v^T(k)v(k) \\ &= E\{\xi^T(k+1)\sum_{s=1}^{n_y} p_{ts}P_s\xi(k+1) \\ &\quad - \xi^T(k)P_t\xi(k)\} + \xi^T(k)\bar{G}\xi(k) - v^T(k)v(k) \\ &= E\{[(M_1+M_2)\xi(k) + (M_3+M_4)v(k) \\ &\quad + \bar{E}\omega(k)]^T\bar{P}_t[(M_1+M_2)\xi(k) \\ &\quad + (M_3+M_4)v(k) + \bar{E}\omega(k)]\} \\ &\quad + \xi^T(k)\left(-P_t + \bar{G}\right)\xi(k) - v^T(k)v(k) \\ &= \eta^T(k)\Omega_t\eta(k) \end{aligned} \tag{21}$$

where

$$\eta^T(k) = \begin{bmatrix} \xi^T(k) & v^T(k) & \omega^T(k) \end{bmatrix}$$

$$\Omega_t = \begin{bmatrix} \Xi_{11} & * & * \\ \Xi_{21} & \Xi_{22} & * \\ \bar{E}^T\bar{P}_tM_1 & \bar{E}^T\bar{P}_tM_3 & \bar{E}^T\bar{P}_t\bar{E} \end{bmatrix}$$

$$\Xi_{11} = M_1^T\bar{P}_tM_1 + \bar{M}_2^T\bar{P}_t\bar{M}_2 - P_t + \bar{G}$$

$$\Xi_{21} = M_3^T\bar{P}_tM_1 + \bar{M}_4^T\bar{P}_t\bar{M}_2$$

$$\Xi_{22} = M_3^T\bar{P}_tM_3 + \bar{M}_4^T\bar{P}_t\bar{M}_4 - I.$$

According to (19) and (21), under condition $\omega(k) = 0$ and the initial value $\xi(0)$, φ_0, we have

$$\bar{\Omega}_t = \begin{bmatrix} \Xi_{11} & * \\ \Xi_{21} & \Xi_{22} \end{bmatrix} < 0. \tag{22}$$

On basis of the aforementioned analysis, denoting $\bar{\eta}^T(k) = [\xi^T(k) \ \ v^T(k)]$, one has

$$E\{\Delta V(k)\} \le -\lambda_{\min}\left(-\bar{\Omega}_t\right)\bar{\eta}^T(k)\bar{\eta}(k) < 0. \tag{23}$$

Then, summing up both sides of (23) from 0 to ∞, it is simple to derive that

$$E\left\{\sum_{k=0}^{\infty}\|\bar{\eta}(k)\|^2\right\} \le \lambda_{\min}^{-1}\left(-\bar{\Omega}_t\right)V(0) < \infty. \tag{24}$$

We can apparently conclude that $E\{\sum_{k=0}^{\infty}\|\xi(k)\|^2\} \le E\{\sum_{k=0}^{\infty}\|\bar{\eta}(k)\|^2\} < \infty$. Therefore, in line with Definition 1, the stochastic stability of the augmented dynamics (14) can be guaranteed if (24) holds. Then, under the external exogenous disturbance, the H_∞ performance of the considered system will be analyzed.

In light of (14), (19) and (21), we can get

$$E\{\Delta V(k)\} + E\left\{z^T(k)z(k)\right\} - \gamma^2\omega^T(k)\omega(k) \le \eta^T(k)\tilde{\Omega}_t\eta(k) \tag{25}$$

where

$$\tilde{\Omega}_t = \Omega_t + \Gamma, \quad \Gamma = \begin{bmatrix} \bar{C}^T\bar{C} & * & * \\ 0 & 0 & * \\ F^TC & 0 & F^TF - \gamma^2 I \end{bmatrix}.$$

By applying Schur complement, the condition (25) can be converted as

$$E\{\Delta V(k)\} + E\left\{z^T(k)z(k)\right\} - \gamma^2\omega^T(k)\omega(k) \le \eta^T(k)\vec{\Omega}_t\eta(k). \tag{26}$$

Noticing (19) and (26), one can obtain

$$E\{\Delta V(k)\} + E\left\{z^T(k)z(k)\right\} - \gamma^2\omega^T(k)\omega(k) \le 0. \tag{27}$$

With the zero initialization $V(0) = 0$, we sum up (27) on both sides from 0 to ∞ and the condition is elicited as

$$E\left\{\sum_{k=0}^{\infty}\|z(k)\|^2\right\} - \gamma^2\sum_{k=0}^{\infty}\|\omega(k)\|^2 \le 0 \tag{28}$$

which means H_∞ performance (16) is met. The proof is completed. ■

It should be witnessed that the stochastic stability for the constructed augmented dynamics (14) can be guaranteed via Theorem 1. However, the gain matrices of observer-based controller cannot be immediately solved due to the uncertainty and other nonlinear terms in (19). Aiming at this problem, the subsequent analysis will be carried out.

Theorem 2: For some scalars $\gamma > 0$, $\rho > 0$, the probability $\bar{\alpha} \in (0,1)$, transition probability p_{ts}, and the observer-based controller gains L_t, K_t, the augmented dynamics (14) can be obtained under the SCP (3) subject to deception attacks (6) if there exist positive-definite symmetric matrix $P_t > 0$ with proper dimensions such that

$$\Psi_t = \begin{bmatrix} \Lambda_{11} & * & * \\ \Lambda_{21} & -\rho I & * \\ \Lambda_{31} & 0 & -\rho I \end{bmatrix} < 0, \quad t \in \mathbb{M} \tag{29}$$

where

$$\Lambda_{11} = \begin{bmatrix} -\bar{P}_t^{-1} & * & * & * & * & * \\ 0 & -\bar{P}_t^{-1} & * & * & * & * \\ 0 & 0 & -I & * & * & * \\ \Psi_{41}^T & \bar{M}_2^T & \bar{C}^T & -P_t + \bar{G} & * & * \\ M_3^T & \bar{M}_4^T & 0 & 0 & -I & * \\ \bar{E}^T & 0 & F^T & 0 & 0 & -\gamma^2 I \end{bmatrix}$$

$$\Lambda_{21} = \begin{bmatrix} 0 & 0 & 0 & \Psi_{74} & 0 & 0 \end{bmatrix}, \ P_t = \mathrm{diag}\{P_{1,t}, P_{2,t}, P_{3,t}\}$$

$$\Lambda_{31} = \begin{bmatrix} \Psi_{81} & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \ \bar{P}_t = \mathrm{diag}\{\bar{P}_{1,t}, \bar{P}_{2,t}, \bar{P}_{3,t}\}$$

$$\Psi_{41} = \begin{bmatrix} \Upsilon_{11} & \vec{\alpha} L_t \phi_t C_2 & L_t \bar{\phi}_t \\ \Upsilon_{21} & \Upsilon_{22} & -L_t \bar{\phi}_t \\ \vec{\alpha} \phi_t C_2 & \vec{\alpha} \phi_t C_2 & \bar{\phi}_t \end{bmatrix}, \ \Psi_{74} = \begin{bmatrix} Q & Q & 0 \end{bmatrix}$$

$$\Psi_{81} = \begin{bmatrix} 0 & \rho S^T & 0 \end{bmatrix}, \ \Upsilon_{11} = A + BK_t - L_t C_2 + \vec{\alpha} L_t \phi_t C_2$$

$$\Upsilon_{21} = L_t C_2 - \vec{\alpha} L_t \phi_t C_2, \ \Upsilon_{22} = A - \vec{\alpha} L_t \phi_t C_2.$$

Proof: It is noted that the uncertainty ΔA_k in (14) and (19) should be separated first, since it is relatively tough to solve the desired gain parameters according to the sufficient condition in Theorem 1.

According to (2), the matrix inequalities (19) can be rewritten as

$$\vec{\Omega}_t = \hat{\Omega}_t + \mathcal{H}e\{R \Delta_k^T N\} < 0 \tag{30}$$

where

$$R = \begin{bmatrix} 0 & 0 & 0 & \Psi_{74} & 0 & 0 \end{bmatrix}^T$$

$$N = \begin{bmatrix} \rho^{-1} \Psi_{81} & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\hat{\Omega}_t = \begin{bmatrix} -\bar{P}_t^{-1} & * & * & * & * & * \\ 0 & -\bar{P}_t^{-1} & * & * & * & * \\ 0 & 0 & -I & * & * & * \\ \Psi_{41}^T & \bar{M}_2^T & \bar{C}^T & -P_t + \bar{G} & * & * \\ M_3^T & \bar{M}_4^T & 0 & 0 & -I & * \\ \bar{E}^T & 0 & F^T & 0 & 0 & -\gamma^2 I \end{bmatrix}.$$

Then, in light of Lemma 1, we can derive that

$$\hat{\Omega}_t + \rho^{-1} R R^T + \rho N^T N < 0. \tag{31}$$

On the ground of Schur complement, we can readily obtain that (31) will hold if (29) holds. Therefore, under the condition (29), the stochastic stability can be satisfied for the augmented dynamics (14). This completes the proof of Theorem 2. ■

Remark 5: Considering the transition probability p_{ts} (3) of the SCP scheduling behaviors modeled by DTMC, one can have $\bar{P}_t = \sum_{s=1}^{n_y} p_{ts} P_s$. Specially, for the convenience of analysis, positive definite symmetric matrix P_t is described as $\mathrm{diag}\{P_{1,t}, P_{2,t}, P_{3,t}\}$, from which it can be observed that $P_{i,t} > 0$ ($i \in \{1,2,3\}$). Similarly, $\bar{P}_t$ can also be formulated as $\mathrm{diag}\{\bar{P}_{1,t}, \bar{P}_{2,t}, \bar{P}_{3,t}\}$ with $\bar{P}_{i,t} > 0$.

Theorem 3: Given parameters $\bar{\alpha} \in (0,1)$, $\rho > 0$, $\gamma > 0$ and transition probability p_{ts}, the augmented system in the form of (14) is considered to be stochastically stable if there exist the matrices $P_t > 0$, $Y_t > 0$ and U_t with proper dimensions such that

$$\bar{\Psi}_t = \begin{bmatrix} \bar{\Lambda}_{11} & * & * \\ \bar{\Lambda}_{21} & -\rho I & * \\ \bar{\Lambda}_{31} & 0 & -\rho I \end{bmatrix} < 0, \quad t \in \mathbb{M} \tag{32}$$

with

$$L_t^T = U_t \left(Y_t^T\right)^{-1} \tag{33}$$

where

$$\bar{\Lambda}_{11} = \begin{bmatrix} \bar{\Psi}_{11} & * & * & * & * & * \\ 0 & \bar{\Psi}_{22} & * & * & * & * \\ 0 & 0 & -I & * & * & * \\ \bar{\Psi}_{41} & \bar{\Psi}_{42} & \bar{C}^T & -P_t + \bar{G} & * & * \\ \bar{\Psi}_{51} & \bar{\Psi}_{52} & 0 & 0 & -I & * \\ \bar{\Psi}_{61} & 0 & F^T & 0 & 0 & -\gamma^2 I \end{bmatrix}$$

$$\bar{\Lambda}_{21} = \begin{bmatrix} 0 & 0 & 0 & \Psi_{74} & 0 & 0 \end{bmatrix}$$

$$\bar{\Lambda}_{31} = \begin{bmatrix} \bar{\Psi}_{81} & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\bar{\Psi}_{51} = \begin{bmatrix} \bar{\alpha} \tilde{\phi}_t^T U_t & -\bar{\alpha} \tilde{\phi}_t^T U_t & \bar{\alpha} \tilde{\phi}_t^T Y_t^T \end{bmatrix}$$

$$\bar{\Psi}_{52} = \begin{bmatrix} \mu \tilde{\phi}_t^T U_t & -\mu \tilde{\phi}_t^T U_t & \mu \tilde{\phi}_t^T Y_t^T \end{bmatrix}$$

$$\bar{\Psi}_{41} = \begin{bmatrix} \bar{\Upsilon}_{11} & \bar{\Upsilon}_{12} & \vec{\alpha} C_2^T \phi_t^T Y_t^T \\ \vec{\alpha} C_2^T \phi_t^T U_t & \bar{\Upsilon}_{22} & \vec{\alpha} C_2^T \phi_t^T Y_t^T \\ \phi_t^T U_t & -\bar{\phi}_t^T U_t & \phi_t^T Y_t^T \end{bmatrix}$$

$$\bar{\Psi}_{61} = \begin{bmatrix} 0, & E^T Y_t^T, & 0 \end{bmatrix}, \ \bar{\Psi}_{81} = \begin{bmatrix} 0, & \rho S^T Y_t^T, & 0 \end{bmatrix}$$

$$\bar{\Psi}_{42} = \begin{bmatrix} -\mu C_2^T \phi_t^T U_t & \mu C_2^T \phi_t^T U_t & -\mu C_2^T \phi_t^T Y_t^T \\ -\mu C_2^T \phi_t^T U_t & \mu C_2^T \phi_t^T U_t & -\mu C_2^T \phi_t^T Y_t^T \\ 0 & 0 & 0 \end{bmatrix}$$

$$\bar{\Upsilon}_{11} = A^T Y_t^T + V_t B^T - C_2^T U_t + \vec{\alpha} C_2^T \phi_t^T U_t$$

$$\bar{\Upsilon}_{12} = C_2^T U_t - \vec{\alpha} C_2^T \phi_t^T U_t, \ \bar{\Upsilon}_{22} = A^T Y_t^T - \vec{\alpha} C_2^T \phi_t^T U_t$$

$$\bar{\Psi}_{11} = \mathrm{diag}\left\{\bar{P}_{1,t} - \mathcal{H}e\{Y_t\}, \bar{P}_{2,t} - \mathcal{H}e\{Y_t\}, \bar{P}_{3,t} - \mathcal{H}e\{Y_t\}\right\}$$

$$\bar{\Psi}_{22} = \bar{\Psi}_{11}, \ V_t = K_t^T \bar{Y}_t^T, \ \bar{Y}_t^T B^T = B^T Y_t^T.$$

Proof: Define $\mathcal{W} \triangleq \mathrm{diag}\{Y_t, Y_t, I, I, I, I, I, I\}$. With condition (33), premultiplying and postmultiplying both sides of (29) by $\mathcal{W}$ and $\mathcal{W}^T$, one has

$$\tilde{\Psi}_t = \begin{bmatrix} \tilde{\Lambda}_{11} & * & * \\ \tilde{\Lambda}_{21} & -\rho I & * \\ \tilde{\Lambda}_{31} & 0 & -\rho I \end{bmatrix} < 0 \tag{34}$$

where

$$\tilde{\Lambda}_{11}=\begin{bmatrix}\tilde{\Psi}_{11} & * & * & * & * & *\\ 0 & \tilde{\Psi}_{22} & * & * & * & *\\ 0 & 0 & -I & * & * & *\\ \bar{\Psi}_{41} & \bar{\Psi}_{42} & \bar{C}^T & -P_t+\bar{G} & * & *\\ \bar{\Psi}_{51} & \bar{\Psi}_{52} & 0 & 0 & -I & *\\ \bar{\Psi}_{61} & 0 & F^T & 0 & 0 & -\gamma^2 I\end{bmatrix}$$

$$\tilde{\Psi}_{41}=\begin{bmatrix}\vec{\Upsilon}_{11} & \bar{\Upsilon}_{12} & \vec{\alpha}C_2^T\phi_t^T Y_t^T\\ \vec{\alpha}C_2^T\phi_t^T U_t & \bar{\Upsilon}_{22} & \vec{\alpha}C_2^T\phi_t^T Y_t^T\\ \bar{\phi}_t^T U_t & -\bar{\phi}_t^T U_t & \bar{\phi}_t^T Y_t^T\end{bmatrix}$$

$$\vec{\Upsilon}_{11}=A^T Y_t^T+K_t^T B^T Y_t^T-C_2^T U_t+\vec{\alpha}C_2^T\phi_t^T U_t$$

$$\tilde{\Psi}_{11}=\tilde{\Psi}_{22}=\begin{bmatrix}-Y_t\bar{P}_{1,t}^{-1}Y_t^T & * & *\\ 0 & -Y_t\bar{P}_{2,t}^{-1}Y_t^T & *\\ 0 & 0 & -Y_t\bar{P}_{3,t}^{-1}Y_t^T\end{bmatrix}.$$

In order to transform nonlinear matrix inequalities into LMI, we should deal with the nonlinear terms in (34). Therefore, Lemma 2 is provided to solve this problem. It can be noted that $B^T\in\mathbb{R}^{n_u\times n_x}$ with $B^T=M[S\ 0]N^T$, where $M^TM=I$ and $N^TN=I$. Therefore, for $Y_t^T=N\begin{bmatrix}U & 0\\ 0 & V\end{bmatrix}N^T$, we can derive that $\bar{Y}_t^TB^T=B^TY_t^T$ with $\bar{Y}_t^T=MS^{-1}USM^T$. According to the analysis above, the following condition is elicited as:

$$\bar{\Upsilon}_{11}=A^TY_t^T+V_tB^T-C_2^TU_t+\vec{\alpha}C_2^T\phi_t^TU_t. \tag{35}$$

Obviously, $\bar{P}_{i,t}>0$ for positive define matrix $\bar{P}_t$ can be derived. With nonsigular matrix Y_t, the following inequation can be get:

$$\left(\bar{P}_{i,t}-Y_t\right)\bar{P}_{i,t}^{-1}\left(\bar{P}_{i,t}-Y_t\right)^T\geq 0,\quad i\in\{1,2,3\} \tag{36}$$

that is

$$-Y_t\bar{P}_{i,t}^{-1}Y_t^T\leq\bar{P}_{i,t}-\mathcal{H}e\{Y_t\}. \tag{37}$$

Replacing $-Y_t\bar{P}_{i,t}^{-1}Y_t^T$ by $\bar{P}_{i,t}-\mathcal{H}e\{Y_t\}$ in (34), then (32) can be obtained. On basis of the analysis above, the proof of Theorem 3 is completed. ■

Remark 6: In this article, Lyapunov functional approach with LMI technique is utilized to analyze stability results on the augmented dynamics (14) under SCP suffering deception attacks. On the one hand, different from [39], the Lyapunov function with token-mode t proposed in Theorem 1 can reduce the conservation. On the other hand, Riccati difference equation (RDE) method was adopted in [49], but we can also accomplish our analysis target by utilizing LMI.

Remark 7: In order to achieve less conservation of the proposed results, the following strategies have been employed. According to the adopted ZOH method, the unscheduled signals can be compensated by precious data such that the system performance can be partly ensured in comparison with ZI method. Besides, the mode-dependent Lyapunov function has been constructed to reflect different transmission scenarios, which make the LMI condition (32) more accurate in line with the scheduling feature of SCP. Correspondingly, the conservation in this article mainly concentrates on the model of uncertainty in (1) and the completely known TPM in SCP. In subsequent research, the more accurate results will be investigated by adopting polytopic uncertainty and partly unknown transition probability.

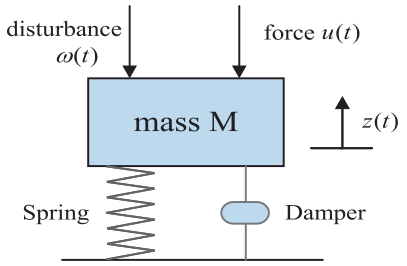


Fig. 2. Structure of the MSDS [36].

TABLE II
PARAMETERS OF MSDS

M	the mass
$u(t)$	the force
$z(t)$	the position
$\omega(t)$	the external disturbance
$w(\dot{z}(t))$	the function in the force
$f(z(t))$	the function in the spring
$g(z(t),\dot{z}(t))$	the function in the damper

IV. NUMERICAL EXAMPLES

To demonstrate the validity of the designed control strategy and SCP scheduling behaviors, two numerical examples will be carried out. In the first place, a mass-spring-damper system (MSDS) will be presented in Example 1. Then, for better testifying the practicability of the proposed theory, we will provide three sets of sensor signals through a communication channel at each time instant in Example 2.

Example 1: In this example, a nonlinear MSDS borrowed from [33] and [36] is shown in Fig. 2, from which the specific dynamics is modeled as

$$M\ddot{z}(t)+g(z(t),\dot{z}(t))+f(z(t))=w(\dot{z}(t))u(t)+\omega(t) \tag{38}$$

where the parameters of MSDS are presented in Table II.

In this article, we choose that $M=1$, $g(z(t),\dot{z}(t))=a_1\dot{z}(t)$, $f(z(t))=a_2(t)z(t)$ and $w(\dot{z}(t))=1+a_3\dot{z}^3(t)$, in which $a_1=1$, $a_2(t)\in[0.5,1.81]$ and $a_3=0.13$. Then, the system state $x(t)=[\dot{z}^T(t)\quad z^T(t)]^T$ is denoted. Inspired by [33], under the sampling period $h=0.2s$, the DTNCSs (1) can be characterized with the parameters as follows: s

$$A=\begin{bmatrix}0.7986 & -0.2078\\ 0.1799 & 0.9784\end{bmatrix},\ B=\begin{bmatrix}0.1217\\ 0.0023\end{bmatrix},\ E=\begin{bmatrix}0.01\\ 0.05\end{bmatrix}$$

$$C_1=\begin{bmatrix}0 & 1\end{bmatrix},\ C_2=\begin{bmatrix}0.2 & 0\\ 0 & 0.2\end{bmatrix},\ D=-1.7899$$

$$S=\begin{bmatrix}0.08 & 0.07\end{bmatrix}^T,\ Q=\begin{bmatrix}0.2 & 0.1\end{bmatrix},\ F=-0.0233.$$

The exogenous disturbance $\omega(k)$ is selected as $3e^{-3k}$ and the uncertainty Δ_k is set to be $0.2\sin(2k)$. In addition, it is obvious that only one signal from sensor is permitted to transfer at the kth step. With the selected signal $\varphi_k\in\mathbb{M}=\{1,2\}$, we can easily obtain $\phi_{\varphi_k}=\text{diag}\{1,0\}$ if $\varphi_k=1$. Under the SCP scheduling, the TPM has been chosen as

$$\mathcal{Q}=\begin{bmatrix}0.45 & 0.55\\ 0.55 & 0.45\end{bmatrix}.$$

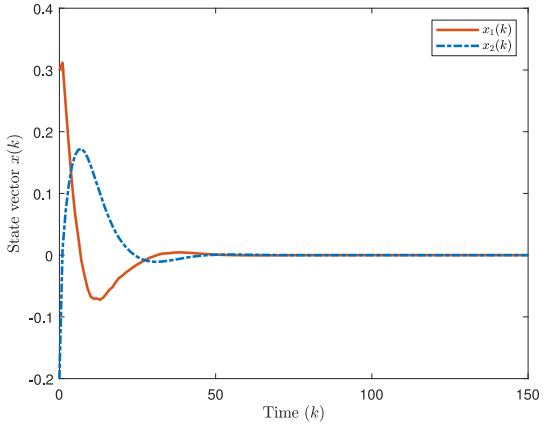


Fig. 3. $x_1(k)$ and $x_2(k)$ of the system with controller in Example 1.

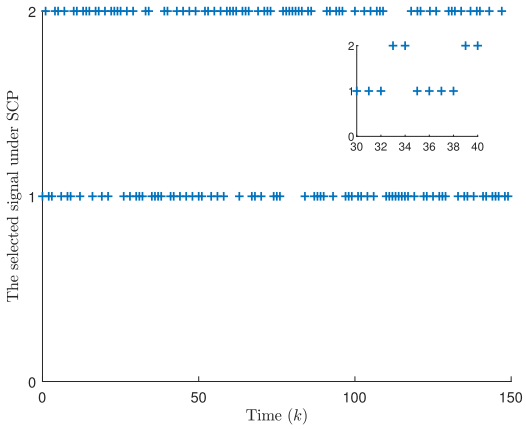


Fig. 4. Distribution of the selected signal under SCP in Example 1.

The malicious signal of deception attacks is given as $v(k) = 0.1\sin(k)x_i(k)$ $(i = 1, 2)$ with $G = \text{diag}\{0.15, 0.15\}$, and its occurrence probability is $\bar{\alpha} = 0.15$. Based on LMI technique, the condition (32) in Theorem 3 with H_∞ performance index $\gamma = 0.45$ and $\rho = 0.1$ can be solved. Subsequently, the desired gain parameters are computed as

$$K_1 = \begin{bmatrix} -0.0254 & 0.5971 \end{bmatrix}, \; K_2 = \begin{bmatrix} 0.2499 & 1.1228 \end{bmatrix}$$
$$L_1 = \begin{bmatrix} 2.1964 & 0.0145 \\ -0.9819 & -0.0019 \end{bmatrix}, \; L_2 = \begin{bmatrix} -0.0155 & -0.7446 \\ 0.0176 & 1.3661 \end{bmatrix}.$$

By initializing $x(0) = \begin{bmatrix} 0.3 & -0.2 \end{bmatrix}^T$, the responses of the system states are presented in Fig. 3, which illustrate a phenomenon that the system is effectively stabilized by the proposed control scheme with the aforementioned parameters. Based on the scheduling of SCP, Fig. 4 plots the distribution of selected signal through a networked communication medium. It is apparent that only one signal is transmitted via the shared communication at any time instant. Hence, the data collision can be obviated under the consideration of SCP. Moreover, the system states and their estimations under the initialization $\hat{x}(0) = \begin{bmatrix} 0 & 0 \end{bmatrix}^T$ are emerged in Figs. 5 and 6, from which we can simply draw a conclusion that the estimated values generated by applying state observer gradually close to the system state and incline to zero. In accordance with the above

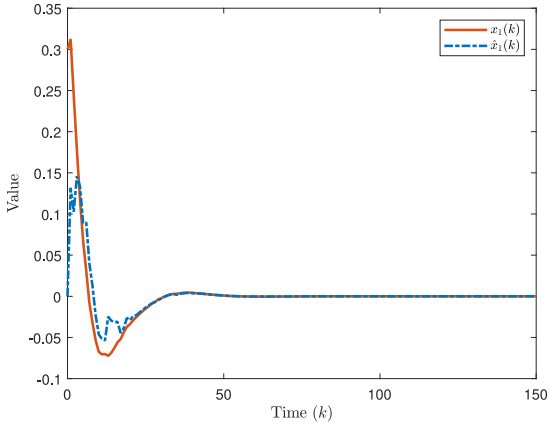


Fig. 5. $x_1(k)$ and its estimation in Example 1.

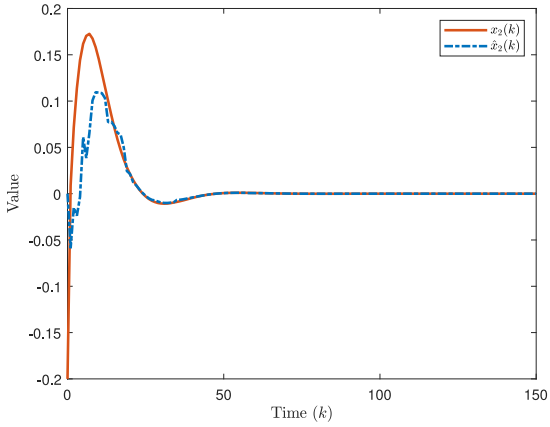


Fig. 6. $x_2(k)$ and its estimation in Example 1.

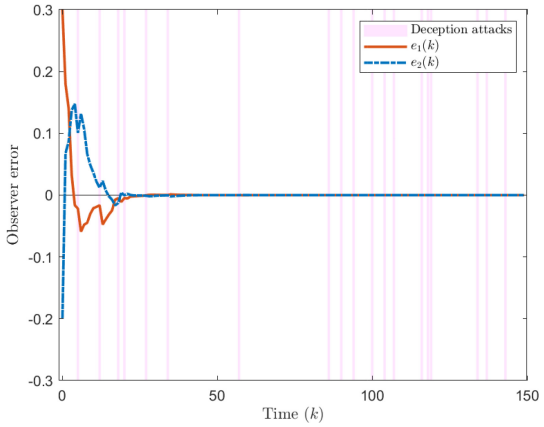


Fig. 7. Observer error under deception attacks in Example 1.

figures, we can obtain that the control strategy based on state observer has an excellent performance.

Fig. 7 displays the stochastic occurrence of deception attacks and the estimation error between the system states and the observer estimations. It is not tough to find that $e(k)$ change rapidly at the beginning of the simulation, but it gradually stabilizes over simulation time under the presented controller. Particularly, the stochastic stability of the considered system suffering intermittent deception attacks can be

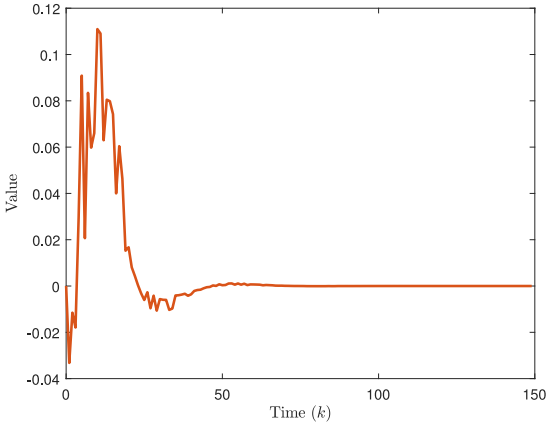


Fig. 8. Response of control input $u(k)$ in Example 1.

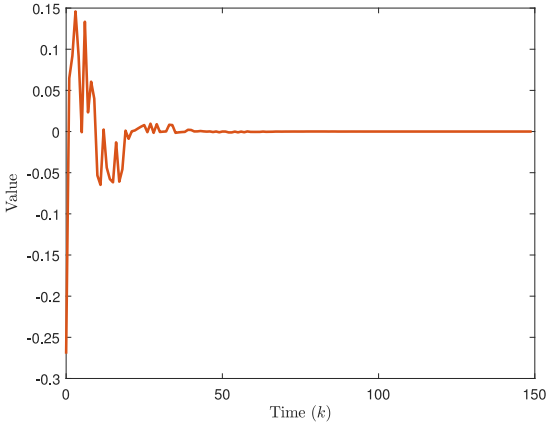


Fig. 9. Response of control output $z(k)$ in Example 1.

further illustrated from Fig. 7. What is more, the trajectories of $u(k)$ and $z(k)$ are presented in Figs. 8 and 9. In the simulation process, the convergence time instant of $u(k)$ and $z(k)$ appears in about 61 and 57 time instant, respectively. This reflects a fact that the MSDS (38) can be effectively stabilized by the security control scheme.

Example 2: In this example, the parameters of the DTNCSs (1) with three sets of sensor signals are given by

$$A=\begin{bmatrix}0.7012 & 0.3121 & 0.4357\\ 0.4133 & 0.3466 & 0.3112\\ 0.0713 & 0.1031 & 0.3130\end{bmatrix},\ B=\begin{bmatrix}1.2817\\ 1.7154\\ 0.7514\end{bmatrix}$$

$$C_1=\begin{bmatrix}-0.8701 & 0.7610 & 0.9179\end{bmatrix},\ E=\begin{bmatrix}0.0003\\ 0.0147\\ 0.0082\end{bmatrix}$$

$$C_2=\begin{bmatrix}-0.31 & 0.01 & 0.03\\ 0.12 & -0.22 & 0\\ -0.23 & 0 & -0.31\end{bmatrix},\ F=-0.0236$$

$$S=\begin{bmatrix}0.05\\ 0.11\\ 0.02\end{bmatrix},\ Q=\begin{bmatrix}0.11 & 0.24 & 0.09\end{bmatrix},\ D=-1.8225$$

with the initial condition $x(0)=\begin{bmatrix}0.3 & 0.1 & -0.1\end{bmatrix}^T$ and $\hat{x}(0)=\begin{bmatrix}0 & 0 & 0\end{bmatrix}^T$.

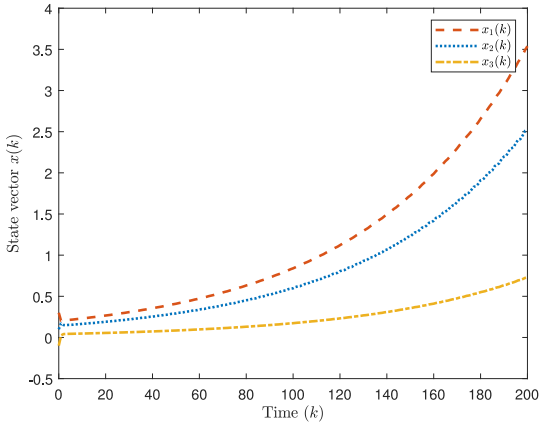


Fig. 10. Responses of state vector $x(k)$ without controller in Example 2.

The uncertainty Δ_k and exogenous disturbance $\omega(k)$ are the same as Example 1. Then, with occurence probability $\tilde{\alpha}=0.25$, the signal of deception attacks $v(k)$ has been selected as $0.1\sin(0.5k)x_i(k)$, where $G=\text{diag}\{0.1,0.1,0.1\}$. Different from Example 1, three sets of sensor signals via a communication channel are considered. Denoting $\varphi_k\in\{1,2,3\}$, $\phi_{\varphi_k}=\text{diag}\{1,0,0\}$ can be ordinarily acquired when $\varphi_k=1$ and the TPM are predefined as

$$\mathcal{Q}=\begin{bmatrix}0.25 & 0.35 & 0.4\\ 0.4 & 0.25 & 0.35\\ 0.35 & 0.4 & 0.25\end{bmatrix}.$$

With the H_∞ performance index $\gamma=0.35$ and $\rho=0.3$, the following gain parameters are outlined based on the condition (32) in Theorem 3:

$$K_1=\begin{bmatrix}-0.4025 & 0.4739 & 0.5222\end{bmatrix}$$
$$K_2=\begin{bmatrix}-0.4993 & 0.5021 & 0.5182\end{bmatrix}$$
$$K_3=\begin{bmatrix}-0.4608 & 0.4420 & 0.5238\end{bmatrix}$$
$$L_1=\begin{bmatrix}-1.5933 & 0.0226 & -0.0274\\ -1.2581 & 0.0069 & -0.0095\\ -0.4542 & -0.0047 & 0.0047\end{bmatrix}$$
$$L_2=\begin{bmatrix}0.0010 & -1.2163 & -0.0013\\ 0.0031 & -1.1004 & -0.0050\\ 0.0036 & -0.8100 & -0.004\end{bmatrix}$$
$$L_3=\begin{bmatrix}0.0018 & -0.0176 & -1.4855\\ 0.0023 & -0.0101 & -1.1300\\ 0.0014 & -0.0098 & -0.3889\end{bmatrix}.$$

The state results on the system ignored controller and applied controller are depicted in Figs. 10 and 11, respectively. Evidently, the open-loop system states cannot tend to zero without applying the designed control scheme. On the contrary, the system is stable as anticipated in spite of large fluctuations before about 48 times if the control gain matrices solved above are utilized. Focusing on the comparison aforementioned, we can conclude that the security control strategy in virtue of state observer is of avail and correct.

As presented in Fig. 12, the selected nodes can be obtained under the adopted SCP at each transmission step. Meanwhile, the phenomenon of data conflict has been commendably

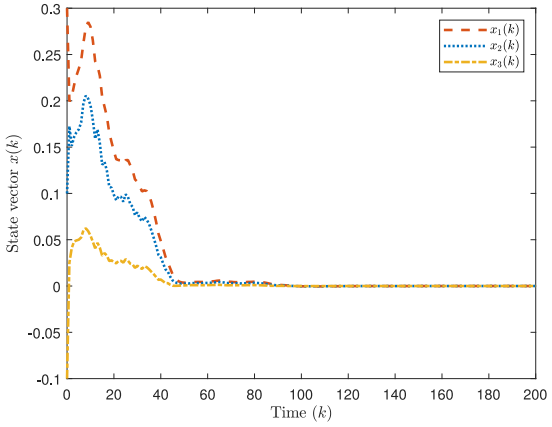


Fig. 11. Responses of state vector $x(k)$ with controller in Example 2.

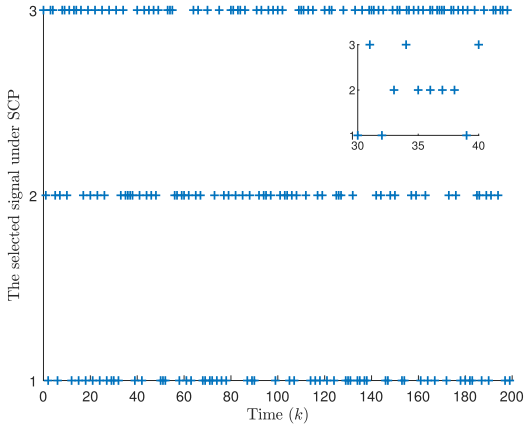


Fig. 12. Distribution of the selected signal under SCP in Example 2.

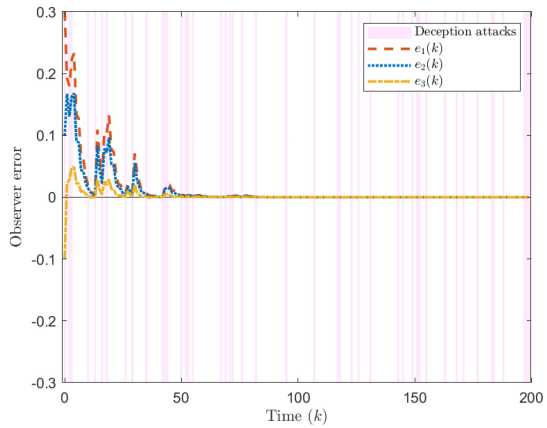


Fig. 13. Observer error under deception attacks in Example 2.

avoided owing to the SCP scheduling, which is accord with actual requirement in practical application. Under the behaviors of SCP, each sensor signal has an opportunity to be transmitted via a networked communication medium. Besides, it can be seen in light of Fig. 13 that the observer error suffering stochastically occurring deception attacks can also tend to zero eventually, which shows a fine performance of the control scheme against attacks.

TABLE III
DIFFERENT CASES OF DECEPTION ATTACKS

The matrix G	Maximum of $v(k)$	Convergence of $x(k)$
$\text{diag}\{0.1, 0.1, 0.1\}$	$0.1sin(0.5k)x_i(k)$	87 times
$\text{diag}\{0.22, 0.22, 0.22\}$	$0.22sin(0.5k)x_i(k)$	82 times
$\text{diag}\{0.34, 0.34, 0.34\}$	$0.34sin(0.5k)x_i(k)$	95 times
$\text{diag}\{0.42, 0.42, 0.42\}$	$0.42sin(0.5k)x_i(k)$	112 times

To further elaborate the validity of the presented security control strategy, the different cases of deception attacks and the convergence of system state $x(k)$ are presented in Table III. With increasing the energy restriction-related matrix G, the maximum tolerable deception attacks are explored according to (6). It can be noted that the amplitude of attack signal $v(k)$ is considered in investigating the control performance. Meanwhile, $G = \text{diag}\{0.42, 0.42, 0.42\}$ is the upper bound such that a feasible solution can be obtained via the LMI condition (32). From Table III, it is readily observed that the system state is stabilized within finite time instant even though the amplitude of deception attacks increases. Thus, the fine security control effects can be obtained in view of the above-mentioned analysis.

V. CONCLUSION

This article investigates a security control approach for uncertain DTNCSs by applying state observer. According to the features of the time-varying uncertainty with the norm-bounded parameter, an augmented closed-loop uncertain system has been constructed. Additionally, to alleviate the network load and avoid data collisions in a communication channel at each step, the SCP scheduling behaviors modeled by DTMC and ZOH strategy are considered. Based on mode-dependent Lyapunov function, the stochastic stability of the augmented system can be guaranteed, and the relevant sufficient condition has been presented. Moreover, the gains of the state observer-based controller can be obtained according to solvable LMI. Ultimately, two examples have been carried out to illustrate the validity of the exhibited control strategy, which aim to provide assistance for other related researches in autonomous systems. Further research directions will include the security optimal control strategy under network attacks with other communication protocols, such as TODP and FlexRay protocol. In addition, in order to make the established model characterizing autonomous dynamics closer to reality, the nonlinear terms and the observer with saturation restriction in polytopic uncertain dynamics will be further considered.

REFERENCES

[1] M. Bahreini, J. Zarei, R. Razavi-Far, and M. Saif, "Robust and reliable output feedback control for uncertain networked control systems against actuator faults," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 4, pp. 2555–2564, Apr. 2022.

[2] M. Klügel et al., "Joint cross-layer optimization in real-time networked control systems," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 4, pp. 1903–1915, Dec. 2020.

[3] H. Yan, J. Wang, H. Zhang, H. Shen, and X. Zhan, "Event-based security control for stochastic networked systems subject to attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 11, pp. 4643–4654, Nov. 2020.

[4] M. Xue, H. Yan, H. Zhang, M. Wang, and D. Zhang, "Dissipative output feedback tracking control of Markov jump systems under compensation scheme," *Automatica*, vol. 146, Dec. 2022, Art. no. 110535.

[5] C. Tan, H. Zhang, W. S. Wong, and Z. Zhang, "Feedback stabilization of uncertain networked control systems over delayed and fading channels," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 260–268, Mar. 2021.

[6] Y. Liu, A. Arumugam, S. Rathinasamy, and F. E. Alsaadi, "Event-triggerednon-fragile finite-time guaranteed cost control for uncertain switched nonlinear networked systems," *Nonlin. Anal. Hybrid Syst.*, vol. 36, May 2020, Art. no. 100884.

[7] B. Sinafar, H. Kharrati, M. A. Badamchizadeh, and M. Baradarannia, "Distributed adaptive switching control of uncertain switched affine multi-agent systems," *Nonlin. Anal. Hybrid Syst.*, vol. 38, Nov. 2020, Art. no. 100941.

[8] J. Wang, C. Wang, Y. Wei, and C. Zhang, "Neuro adaptive sliding mode formation control of autonomous underwater vehicles with uncertain dynamics," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3325–3333, Sep. 2020.

[9] C. Yuan, S. Licht, and H. He, "Formation learning control of multiple autonomous underwater vehicles with heterogeneous nonlinear uncertain dynamics," *IEEE Trans. Cybern.*, vol. 48, no. 10, pp. 2920–2934, Oct. 2018.

[10] H. Yoo and Z. Gajic, "New designs of linear observers and observer-based controllers for singularly perturbed linear systems," *IEEE Trans. Automat. Control*, vol. 63, no. 11, pp. 3904–3911, Nov. 2018.

[11] M. Chen and S. S. Ge, "Adaptive neural output feedback control of uncertain nonlinear systems with unknown hysteresis using disturbance observer," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7706–7716, Dec. 2015.

[12] B. Xiao, S. Yin, and H. Gao, "Reconfigurable tolerant control of uncertain mechanical systems with actuator faults: A sliding mode observer-based approach," *IEEE Trans. Control Syst. Technol.*, vol. 26, no. 4, pp. 1249–1258, Jul. 2018.

[13] J. Liu, E. Gong, L. Zha, E. Tian, and X. Xie, "Observer-based security fuzzy control for nonlinear networked systems under weighted try-once-discard protocol," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 11, pp. 3853–3865, Nov. 2023.

[14] J. Zhang, P. Shi, J. Qiu, and S. K. Nguang, "A novel observer-based output feedback controller design for discrete-time fuzzy systems," *IEEE Trans. Fuzzy Syst.*, vol. 23, no. 1, pp. 223–229, Feb. 2015.

[15] C. Deng, C. Wen, J. Huang, X.-M. Zhang, and Y. Zou, "Distributed observer-based cooperative control approach for uncertain nonlinear mass under event-triggered communication," *IEEE Trans. Automat. Control*, vol. 67, no. 5, pp. 2669–2676, May 2022.

[16] Y. Tan, Q. Liu, J. Liu, X. Xie, and S. Fei, "Observer-based security control for interconnected semi-Markovian jump systems with unknown transition probabilities," *IEEE Trans. Cybern.*, vol. 52, no. 9, pp. 9013–9025, Sep. 2022.

[17] H. Shen, Y.-A. Liu, K. Shi, J. H. Park, and J. Wang, "Event-based distributed secondary control for AC islanded microgrid with semi-Markov switched topology under cyber-attacks," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2927–2938, Jun. 2023.

[18] E. Mousavinejad, X. Ge, Q.-L. Han, F. Yang, and L. Vlacic, "Resilient tracking control of networked control systems under cyber attacks," *IEEE Trans. Cybernet.*, vol. 51, no. 4, pp. 2107–2119, Apr. 2021.

[19] W. Zhang, S. Mao, J. Huang, L. Kocarev, and Y. Tang, "Data-driven resilient control for linear discrete-time multi-agent networks under unconfined cyber-attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 2, pp. 776–785, Feb. 2021.

[20] S. Hu, D. Yue, Z. Cheng, E. Tian, X. Xie, and X. Chen, "Co-design of dynamic event-triggered communication scheme and resilient observer-based control under aperiodic DoS attacks," *IEEE Trans. Cybern.*, vol. 51, no. 9, pp. 4591–4601, Sep. 2021.

[21] W. Xu, Z. Wang, L. Hu, and J. Kurths, "State estimation under joint false data injection attacks: Dealing with constraints and insecurity," *IEEE Trans. Automat. Control*, vol. 67, no. 12, pp. 6745–6753, Dec. 2022.

[22] Y. Sun, J. Yu, X. Yu, and H. Gao, "Decentralized adaptive event-triggered control for a class of uncertain systems with deception attacks and its application to electronic circuits," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 12, pp. 5405–5416, Dec. 2020.

[23] Y. Deng, T. Zhang, G. Lou, X. Zheng, J. Jin, and Q.-L. Han, "Deep learning-based autonomous driving systems: A survey of attacks and defenses," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 7897–7912, Dec. 2021.

[24] X. Xu, J. Zhang, Y. Li, Y. Wang, Y. Yang, and H. T. Shen, "Adversarial attack against urban scene segmentation for autonomous vehicles," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4117–4126, Jun. 2021.

[25] Z. Gu, T. Yin, and Z. Ding, "Path tracking control of autonomous vehicles subject to deception attacks via a learning-based event-triggered mechanism," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 12, pp. 5644–5653, Dec. 2021.

[26] L. Zou, Z. Wang, Q.-L. Han, and D. Zhou, "Ultimate boundedness control for networked systems with try-once-discard protocol and uniform quantization effects," *IEEE Trans. Autom. Control*, vol. 62, no. 12, pp. 6582–6588, Dec. 2017.

[27] X. Wan, Z. Wang, Q.-L. Han, and M. Wu, "A recursive approach to quantized H_∞ state estimation for genetic regulatory networks under stochastic communication protocols," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 9, pp. 2840–2852, Sep. 2019.

[28] Y. Luo, Z. Wang, G. Wei, and F. E. Alsaadi, "H_∞ fuzzy fault detection for uncertain 2-D systems under round-robin scheduling protocol," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 8, pp. 2172–2184, Aug. 2017.

[29] S. Liu, Z. Wang, L. Wang, and G. Wei, "Recursive set-membership state estimation over a FlexRay network," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 6, pp. 3591–3601, Jun. 2022.

[30] Y. Li, L. Wei, J. Liu, X. Xie, and E. Tian, "Secure state estimation for complex networks with multi-channel oriented round robin protocol," *Nonlin. Anal., Hybrid Syst.*, vol. 49, Aug. 2023, Art. no. 101371.

[31] X. Wang, D. Ding, H. Dong, and X.-M. Zhang, "Neural-network-based control for discrete-time nonlinear systems with input saturation under stochastic communication protocol," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 4, pp. 766–778, Apr. 2021.

[32] L. Zou, Z. Wang, Q.-L. Han, and D. Zhou, "Moving horizon estimation of networked nonlinear systems with random access protocol," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 5, pp. 2937–2948, May 2021.

[33] B. Wu, X.-H. Chang, and X. Zhao, "Fuzzy H_∞ output feedback control for nonlinear NCSs with quantization and stochastic communication protocol," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 9, pp. 2623–2634, Sep. 2021.

[34] J. Song, Z. Wang, and Y. Niu, "On H_∞ sliding mode control under stochastic communication protocol," *IEEE Trans. Automat. Control*, vol. 64, no. 5, pp. 2174–2181, May 2019.

[35] J. Li, Z. Wang, H. Dong, and W. Fei, "Delay-distribution-dependent state estimation for neural networks under stochastic communication protocol with uncertain transition probabilities," *Neural Netw.*, vol. 130, pp. 143–151, Oct. 2020.

[36] W. Chen, J. Hu, X. Yu, D. Chen, and Z. Wu, "Robust fault detection for uncertain delayed systems with measurement outliers under stochastic communication protocol," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 8, pp. 684–701, Jul. 2022.

[37] J. Wang, Y. Song, and G. Wei, "Security-based resilient robust model predictive control for polytopic uncertain systems subject to deception attacks and RR protocol," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 8, pp. 4772–4783, Aug. 2022.

[38] E. Tian, H. Chen, C. Wang, and L. Wang, "Security-ensured state of charge estimation of lithium-ion batteries subject to malicious attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2250–2261, May 2023.

[39] Y. Wang, Z. Wang, L. Zou, and H. Dong, "H_∞ PID control fordiscrete-time fuzzy systems with infinite-distributed delays under round-robin communication protocol," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 6, pp. 1875–1888, Jun. 2022.

[40] D. dos Santos and M. Todorov, "On the robustness of Markov jump linear systems with norm-bounded uncertainty on transition rates," *J. Frankl. Inst.*, vol. 359, no. 13, pp. 6986–7003, 2022.

[41] M. Tabbara and D. Nesic, "Input–output stability of networked control systems with stochastic protocols and channels," *IEEE Trans. Automat. Control*, vol. 53, no. 5, pp. 1160–1175, Jun. 2008.

[42] J. Liu, L. Wei, X. Xie, E. Tian, and S. Fei, "Quantized stabilization for T–S fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks," *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 6, pp. 3820–3834, Dec. 2018.

[43] L. Li, H. Yang, Y. Xia, and C. Zhu, "Attack detection and distributed filtering for state-saturated systems under deception attack," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 4, pp. 1918–1929, Dec. 2021.

[44] X. Li, G. Wei, D. Ding, and S. Liu, "Recursive filtering for time-varying discrete sequential systems subject to deception attacks: Weighted try-once-discard protocol," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 6, pp. 3704–3713, Jun. 2022.

[45] W. Yang, Y. Zhang, G. Chen, C. Yang, and L. Shi, "Distributed filtering under false data injection attacks," *Automatica*, vol. 102, pp. 34–44, Apr. 2019.

[46] Z. Wang, F. Yang, D. W. C. Ho, and X. Liu, "Robust H_∞ control for networked systems with random packet losses," *IEEE Trans. Syst., Man, Cybern., Part-B (Cybernet.)*, vol. 37, no. 4, pp. 916–924, Aug. 2007.
[47] L. Zha, R. Liao, J. Liu, X. Xie, E. Tian, and J. Cao, "Dynamic event-triggered output feedback control for networked systems subject to multiple cyber attacks," *IEEE Trans. Cybern.*, vol. 52, no. 12, pp. 13800–13808, Dec. 2022.
[48] Y. Tan, Y. Yuan, X. Xie, E. Tian, and J. Liu, "Observer-based event-triggered control for interval type-2 fuzzy networked system with network attacks," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 8, pp. 2788–2798, Aug. 2023.
[49] L. Zou, Z. Wang, and H. Gao, "Observer-based H_∞ control of networked systems with stochastic communication protocol: The finite-horizon case," *Automatica*, vol. 63, pp. 366–373, Jan. 2016.

Jian Liu (Member, IEEE) received the Ph.D. degree in signal and information processing from the College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China, in 2018.

He is currently an Associate Professor with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing. He has published more than 40 papers in refereed international journals. His research interests include cyber–physical systems, networked control systems, complex dynamical networks, intelligent optimization algorithms, and network security.

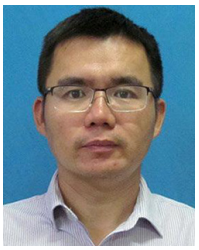
Dr. Liu received the Reward of Outstanding Reviewer for many international journals, such as *Computer Networks* and *Journal of Computational Science*. He has been serving as the Guest Editor for the special issue *Fuzzy Modeling and Fuzzy Control Systems* in Mathematics since August 2022.

Jiachen Ke received the B.Ed. degree in science education from the School of Science, Huzhou University, Huzhou, China, in 2022. He is currently pursuing the M.S. degree in computer science and technology with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, China.

His research interests include fuzzy control, learning-based optimal control methods, and networked control systems.

Jinliang Liu (Member, IEEE) received the Ph.D. degree in control theory and control engineering from the School of Information Science and Technology, Donghua University, Shanghai, China, in 2011.

He was a Postdoctoral Research Associate with the School of Automation, Southeast University, Nanjing, China, from 2013 to 2016. He was a Visiting Researcher/Scholar with the Department of Mechanical Engineering, University of Hong Kong, Hong Kong, from 2016 to 2017. He was a Visiting Scholar with the Department of Electrical Engineering, Yeungnam University, Gyeongsan, South Korea, from 2017 to 2018. He is currently a Professor with the School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, Jiangsu. His research interests include networked control systems, complex dynamical networks, and time-delay systems.



Xiangpeng Xie (Senior Member, IEEE) received the B.S. and Ph.D. degrees in engineering from Northeastern University, Shenyang, China, in 2004 and 2010, respectively.

From 2010 to 2014, he was a Senior Engineer with the Metallurgical Corporation of China Ltd., Beijing, China. He is currently a Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include fuzzy modeling and control synthesis, state estimations, optimization in process industries, and intelligent optimization algorithms.

Prof. Xie serves as an Associate Editor for IEEE TRANSACTIONS ON FUZZY SYSTEMS, IEEE TRANSACTIONS ON CYBERNETICS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *International Journal of Fuzzy Systems*, and *International Journal of Control, Automation, and Systems*.

Engang Tian (Member, IEEE) received the B.S. degree in mathematics from Shandong Normal University, Jinan, China, in 2002, the M.Sc. degree in operations research and cybernetics from Nanjing Normal University, Nanjing, China, in 2005, and the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2008.

From 2011 to 2012, he was a Postdoctoral Research Fellow with the Hong Kong Polytechnic University, Hong Kong. From 2015 to 2016, he was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, Uxbridge, U.K. From 2008 to 2018, he was an Associate Professor and then a Professor with the School of Electrical and Automation Engineering, Nanjing Normal University. In 2018, he was appointed as an Eastern Scholar by the Municipal Commission of Education, Shanghai, and joined the University of Shanghai for Science and Technology, Shanghai, where he is currently a Professor with the School of Optical-Electrical and Computer Engineering. He has published more than 100 papers in refereed international journals. His research interests include networked control systems, cyber attack, as well as nonlinear stochastic control and filtering.