Received: 8 September 2023 | Revised: 10 March 2024 | Accepted: 11 April 2024

DOI: 10.1049/cth2.12676

IET Control Theory & Applications

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

A general matrix decomposition approach with application to stabilization of networked systems with stochastic sampling and two-channel deception attacks

Yizhen Li[1] | Zhipei Hu[1] | Feiqi Deng[2] | Yongkang Su[3] | Guangjie Li[4]

[1]School of Electrical and Information Engineering, Shantou University, Shantou, China

[2]College of Automation Science and Engineering, South China University of Technology, Guangzhou, China

[3]Department of Automatic Control & Systems Engineering, University of Sheffield, Sheffield, UK

[4]School of Mathematics and Statistics, Guangdong University of Foreign Studies, Guangzhou, China

Correspondence
Guangjie Li, School of Mathematics and Statistics, Guangdong University of Foreign Studies, Guangzhou 510006, China.
Email: scutliguangjie@163.com

Funding information
Basic and Applied Basic Research Foundation of Guangdong Province, Grant/Award Numbers: 2023A1515011025, 2023A1515012781; Basic and Applied Basic Research of Guangzhou Basic Research Program, Grant/Award Number: 202201010250; National Natural Science Foundation of China, Grant/Award Number: 62333006

Abstract

This study is concerned with the stabilization analysis and controller design for networked systems with stochastic sampling and two-channel deception attacks. First, we give a general matrix decomposition approach which is applicable to scenarios where the system matrix A contains complex-value eigenvalues. Then, a discrete stochastic framework is established for a class of networked systems which considers the joint effects of sampling errors and two-channel deception attacks. Utilizing the matrix decomposition approach introduced in this study, it becomes feasible to decouple the expectation operations for specific coupling matrices characterized by substantial nonlinearity and randomness. Based on this, a stabilization controller is constructed that ensures the exponential mean-square stability of the resulting discrete stochastic system. Finally, three simulation examples are provided to validate the effectiveness of the proposed approach.

1 | INTRODUCTION

In recent years, great interest has been aroused to the analysis and synthesis problems of networked control systems (NCSs). In NCSs, components (sensors, actuators and controllers) are connected in a closed control loop and exchange data through a communication network. The introduction of cyberspace allows for the avoidance of unnecessary point-to-point wiring in classical systems, simplifying the physical structure of NCSs and facilitating maintenance and updates. Accordingly, NCSs have been widely employed in various engineering domains, ranging from aerospace to industrial automation [1–4]. On the flip side, considering the openness of network, NCSs stands a higher chance of being exposed to malicious attacks [5–8]. Specifically, deception attack is a kind of network attack that intends to compromise the integrity and trustworthiness of transmitted data by inserting some falsified data information into the original data packet while remaining undetected by detectors [9–11]. Since the unexpected data can induce systems of worse stability, great significance has been placed on stabilization analysis and controller design for NCSs with deception attacks [12–17]. For example, a sliding-mode control problem was addressed in [13] for a class of Markovian jump cyber-physical systems under the situation of randomly occurring injection attack. In [14], a Bernoulli binary distributed is used to characterize random occurring deception attacks, and an innovative dynamic-output-feedback robust model predictive control approach is proposed to ensure system security under such conditions. In [15], with the aid of a dynamic event-triggered mechanism, an observer-based PID controller was designed for systems with deception

Abbreviation: NCSs, networked control systems.

attacks. Considering that in control loops sensors and actuators are important components among which the data is transmitted through public network, it should be pointed out that both sensor-to-controller channel and controller-to-actuator channel are susceptible to intruders that launch deceptive attacks in NCSs. Some results about NCSs' security under the situation of two-channel attacks have been derived [18–20]. For example, a distributed H_∞ estimation was derived against two-channel attacks in [19]. A security control problem was studied for fuzzy NCSs with deception attacks at both ends in [20].

Moreover, time-triggered sampling is a widely used approach for transforming the continuous signal to the discrete one when signal is transmitted in networks [21–24]. For time-triggered sampled-data system, the sampling intervals are usually assumed to be an invariable constant. However, in real-world scenarios, some unexpected physical constraints, for example, limited bandwidth of communication channel, failure of the sampler, and clock error drift, can bring deviation to ideal intervals [25, 26]. Under these conditions, the practical sampling intervals are subject to noisy fluctuations, leading to deviations from the normal sampling period. Recently, some scholars have investigated the control problems of NCSs subjected to random sampling intervals [27–33]. For example, a confluent Vandermonde matrix approach was proposed to investigate quantized/saturated control problems in sampled-data systems with random sampling intervals in [27]. For a class of Ito stochastic NCSs subject to time-varying sampling and packet dropouts, [28] discusses the modeling and control problem, in which robustly exponentially mean-square stability of the system with an $\mathcal{H}_\infty$ performance is guaranteed. In [29], an event-triggered communication control scheme, which requires less communication bandwidth, was applied for stability analysis in systems with aperiodically sampled data. A probability-distribution-dependent controller was designed for complex dynamical networks with random sampling intervals and successive packet losses where the categorical distribution is used to characterize the sampling errors of random sampling intervals in [30]. It needs to emphasis that a few results have analysed the stabilization problem for NCSs under two-channel deception attacks while taking random sampling intervals into consideration at the same time. Thus, in this paper we discuss the stabilization analysis and controller design for a class of NCSs which are subject to random sampling intervals and two-channel deception attacks.

Motivated by the previous discussion, this study advanced a general matrix decomposition approach which can be applied to address the stabilization challenges encountered by NCSs subject to random sampling intervals and two-channel deception attacks. The main contributions of this research can be summarized as follows: (1) A mathematical model for NCSs comprising the situations of sampling errors and two-channel deception attacks is established by discrete-time method. Based on this model, a new stabilization problem is investigated. (2) A general matrix decomposition approach is presented, which can deal with the situation that the system matrix A contains complex-value eigenvalues. Finally, two mathematical simulation examples and a practical example are provided to verify the effectiveness of the proposed method, where (i) all the eigenvalues of system matrix A are real-values, and (ii) some eigenvalues of matrix A are complex-values.

2 | THE GENERAL MATRIX DECOMPOSITION APPROACH

In this section, two lemmas are presented in this part to introduce the general matrix decomposition approach.

Lemma 1 [32]. *Denote $\lambda_1, \lambda_2, \dots, \lambda_h$ as the eigenvalues of the matrix $G \in \mathbb{R}^{m_g \times m_g}$. Let l_j be the multiplicity of λ_j as a root of the minimal polynomial for G and $l_1 + l_2 + \cdots + l_h = \bar{m}_g$, where $\bar{m}_g$ is the degree of the minimal polynomial of the matrix G. Then, for matrix $G \in \mathbb{R}^{m_g \times m_g}$ and a scalar δ, one has*

$$e^{G\delta} = \left(\left(\pi(\delta) V_G^{-1}\right) \otimes I\right) \bar{G}, \tag{1}$$

where $\pi(\delta) = \begin{bmatrix} \pi_1(\delta) & \pi_2(\delta) & \cdots & \pi_h(\delta) \end{bmatrix}$ *with* $\pi_j(\delta) = \begin{bmatrix} e^{\lambda_j \delta} & \delta e^{\lambda_j \delta} & \cdots & \delta^{l_j - 1} e^{\lambda_j \delta} \end{bmatrix}$, $V_G = \begin{bmatrix} \Lambda_1 & \Lambda_2 & \cdots & \Lambda_h \end{bmatrix}$ *is the reduced-order confluent Vandermonde matrix of G with*

$$\Lambda_j = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ \lambda_j & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ \lambda_j^{\bar{m}_g - 1} & (\bar{m}_g - 1)\lambda_j^{\bar{m}_g - 2} & \cdots & \frac{(\bar{m}_g - 1)!}{(\bar{m}_g - l_j)!} \lambda_j^{\bar{m}_g - l_j} \end{bmatrix},$$

and $\bar{G} = \begin{bmatrix} I & G^T & \cdots & G^{(\bar{m}_g - 1)^T} \end{bmatrix}^T$.

Lemma 2. *Denoting the probability function of the random variable δ as $f(\delta)$, for $\pi(\delta)$ defined in Lemma 1, one has a matrix U_g such that*

$$\mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\} = U_g^H U_g. \tag{2}$$

Proof. 1) When eigenvalues of matrix G are exclusively of real-value, the $\pi(\delta)$ in (1) is a real matrix. Therefore, for the matrix $\mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\}$, there exists a real matrix U_g which satisfies $\mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\} = \mathbb{E}\left\{\pi^T(\delta)\pi(\delta)\right\} = U_g^T U_g = U_g^H U_g$, that is, $\mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\} = U_g^H U_g$; 2) When matrix G contains complex-value eigenvalues, the $\pi(\delta)$ is a complex matrix. In this case, we let $U = \pi^H(\delta)\pi(\delta)$, then the Hermitian complex matrix U is positive semi-definite. Therefore, for any nonzero complex vector v, one has $v^H \pi^H(\delta)\pi(\delta) v \geq 0$. With $f(\delta) \geq 0$, we further have that $v^H \mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\} v = \int_{-\infty}^{+\infty} v^H \pi^H(\delta)\pi(\delta) v f(\delta) d\delta \geq 0$. Considering that $\mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\}$ is a Hermitian matrix, thus $\mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\}$ is a positive semi-definite matrix. So we have a matrix U_g so that (2) holds. Therefore, no matter if all the eigenvalues of matrix G are real-value or matrix G has complex-value eigenvalues, there exists a matrix U_g so that $\mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\} = U_g^H U_g$. The proof is complete. □

Remark 2.1. In this study, we first transform the matrix exponential $e^{G\delta}$ into a comprehensive matrix formulation as expressed in (1). Subsequently, the operation of expectation concerning $\pi(\delta)$ can be independently addressed in (2). These computational operations set the groundwork for the subsequent design of the controller. Comparable operations are also conducted in some existing literature, for example, [34]. Nevertheless, there is no real matrix that fulfills the equation (8) within Lemma 3 of [34], in the case that the matrix $G = \begin{bmatrix} A & B \\ 0 & 0 \end{bmatrix}$ encompasses complex-value eigenvalues. In contrast to [34], the matrix decomposition approach presented in Lemma 2 is general and can be extended to scenarios that encompass matrix G with complex-value eigenvalues. Note that the complex-value eigenvalues of matrix A remain consistent with those of G in cases where $G = \begin{bmatrix} A & B \\ 0 & 0 \end{bmatrix}$, that is, in contrast to the matrix decomposition approach in [34], the matrix decomposition approach presented in this study is amenable to situations in which the system matrix A in equation (3) contains complex-value eigenvalues.

3 | APPLICATION TO STABILITY ANALYSIS AND SYNTHESIS FOR NCSS WITH STOCHASTIC SAMPLING AND TWO-CHANNEL DECEPTION ATTACKS

In this section, the exponentially mean-square stabilization problem is considered for NCSs under stochastic sampling and two-channel deception attacks with the general matrix decomposition approach.

Consider a continuous-time linear system subject to stochastic sampling and two-channel deception attacks:

$$\dot{x}(t) = Ax(t) + B\hat{u}(t), \tag{3}$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $\hat{u}(t) \in \mathbb{R}^m$ is the control input. A is the system matrix and B is the input matrix.

Normally, the system's state is periodically sampled with a fixed interval which is denoted as T. This paper focuses on the scenario where actual sampling interval is influenced by noisy perturbation. Suppose that the actual sampling period α_k composed of a constant T and a random variable ρ_k, that is, $\alpha_k = T + \rho_k > 0$. T is the ideal sampling interval and ρ_k stands for the sampling error. The probability function of ρ_k is denoted as $f(\rho)$.

We consider that the deception attacks happen in both sensor-to-controller channel and controller-to-actuator channel. Two stochastic variables which obey Bernoulli distribution are used to characterize the occurrence of two-channel deception attacks. In sensor-to-controller channel, we describe the data $\hat{x}(t_k)$ received by the controller as

$$\hat{x}(t_k) = x(t_k) + \varrho(t_k)(-x(t_k) + \varphi(t_k)),$$

where $\varrho(t_k)$ satisfies $\mathcal{P}\{\varrho(t_k) = 1\} = \varsigma$ and $\mathcal{P}\{\varrho(t_k) = 0\} = 1 - \varsigma$. $\varphi(t_k)$ stands for the signal injected by attackers. Then, the controller output $u(t_k)$ is expressed as $u(t_k) = K\hat{x}(t_k) = K(x(t_k) + \varrho(t_k)(-x(t_k) + \varphi(t_k)))$, where K is a gain matrix to be designed.

In controller-to-actuator channel, the control input $\hat{u}(t)$ with a zero-order hold can be represented as follows

$$\begin{aligned}\hat{u}(t) = \hat{u}(t_k) &= u(t_k) + \varpi(t_k)(-u(t_k) + \psi(t_k)) \\ &= (1 - \varpi(t_k))K((1 - \varrho(t_k))x(t_k) + \varrho(t_k)\varphi(t_k)) \\ &\quad + \varpi(t_k)\psi(t_k), t_k \le t < t_{k+1},\end{aligned}$$

where $\varpi(t_k)$ is used to characterize the deception attack occurring in controller-to-actuator channel with $\mathcal{P}\{\varpi(t_k) = 1\} = \theta$ and $\mathcal{P}\{\varpi(t_k) = 0\} = 1 - \theta$, $\psi(t_k)$ stands for the injected signal by the attacker in controller-to-actuator channel.

Besides, due to the energy limit, $\varphi(t_k)$ and $\psi(t_k)$ are assumed to satisfy

$$\|\varphi(t_k)\| \le \|F_1 x(t_k)\|, \|\psi(t_k)\| \le \|F_2 x(t_k)\|, \tag{4}$$

where F_1 and F_2 are constant matrices with appropriate dimensions.

Remark 3.1. From the aspect of defenders, the attacks happen in a random way. Considering that defense mechanisms are widely used to protect systems from deception attacks (e.g. residue detector, detection filters, voting schemes, hypothesis testing etc.), some injected information could be identified. Unavoidable constrains in NCSs also influence the deception attacks. For example, a multi-path routing protocol mentioned in [35] could result in the attacks occurring randomly. Besides, from the aspect of adversaries, considering factors, for example, the detectability of deception attacks, limitations in access and resources and so on prompt attackers to make stochastic decisions to launch an attack or to sleep in order to save energy or elude defenses [36, 37]. For these reasons, the attack phenomenon can be described as a random event. Referring to [38], it makes sense to define resources available to the defender based on the information obtained from the interaction with attackers in order to calculate the outcome for the control loop in a variety of possible scenarios. Bernoulli distribution is used in this paper to describe such a statistic phenomenon of deception attacks [39].

Remark 3.2. In this paper, the injected signals $\varphi(t_k)$ and $\psi(t_k)$ are characterized as bonded signals with prior known matrices F_1 and F_2. In practice, the attacks are limited to some restrains to avoid triggering the monitor's alarm. For example, bad measurement detection is mentioned in [40] by which the deception attacks are easy to be detected if the difference between the vector of injected signals and the vector of original signals is of a large amplitude. Besides, considering constrains of physical devices such as network congestion and limited bandwidth of communication channel, unbonded signal is hard to be injected into the data packet successfully. Hence the malicious data is

assumed as a bonded signal in this paper. The matrices F_1 and F_2 are assumed to be a priori based on known knowledge of the system model which ensures that attacks are of higher possibility to happen [39].

Submitting (4) into (3), we can have by (3) that

$$\begin{aligned}\dot{x}(t) =& Ax(t) + (1-\varpi(t_k))(1-\varrho(t_k))BKx(t_k)\\ &+ (1-\varpi(t_k))\varrho(t_k)BK\varphi(t_k) + \varpi(t_k)B\psi(t_k),\\ &t_k \le t < t_{k+1}\end{aligned} \tag{5}$$

Denote $x(t_k), \varpi(t_k), \varrho(t_k), \varphi(t_k), \psi(t_k)$ as $x_k, \varpi_k, \varrho_k, \varphi_k, \psi_k$ for convenience. Integrating (5) from t_k to t_{k+1}, we have the following discrete-time system by noting that $\alpha_k = t_{k+1} - t_k$:

$$\begin{aligned}x_{k+1} =& \left(e^{A\alpha_k} + (1-\varpi_k)(1-\varrho_k)\int_0^{\alpha_k} e^{As}dsBK\right)x_k\\ &+ (1-\varpi_k)\varrho_k\int_0^{\alpha_k} e^{As}dsBK\varphi_k + \varpi_k\int_0^{\alpha_k} e^{As}dsB\psi_k\end{aligned} \tag{6}$$

Define a square matrix $G = \begin{bmatrix} A & B \\ 0 & 0 \end{bmatrix}$, one has

$$e^{G\alpha_k} = \sum_{j=0}^{\infty}\frac{G^j\alpha_k^j}{j!} = \begin{bmatrix} e^{A\alpha_k} & \int_0^{\alpha_k} e^{As}dsB \\ 0 & I \end{bmatrix}.$$

We further get

$$\begin{aligned}H_1 &\triangleq e^{A\alpha_k} = \begin{bmatrix} I & 0 \end{bmatrix} e^{G\alpha_k} \begin{bmatrix} I & 0 \end{bmatrix}^T,\\ H_2 &\triangleq \int_0^{\alpha_k} e^{As}dsBK = \begin{bmatrix} I & 0 \end{bmatrix} e^{G\alpha_k} \begin{bmatrix} 0 & K^T \end{bmatrix}^T,\\ H_3 &\triangleq \int_0^{\alpha_k} e^{As}dsB = \begin{bmatrix} I & 0 \end{bmatrix} e^{G\alpha_k} \begin{bmatrix} 0 & I \end{bmatrix}^T.\end{aligned}$$

Then, (6) can be equivalently expressed as:

$$\begin{aligned}x_{k+1} =& (H_1 + (1-\varpi_k)(1-\varrho_k)H_2)x_k + (1-\varpi_k)\varrho_k H_2\varphi_k\\ &+ \varpi_k H_3\psi_k.\end{aligned} \tag{7}$$

Our goal is to design a controller which can ensure that the stochastic system (7) is of exponential mean-square stability. The detailed definition is as follows:

Definition 1. The system (7) is exponentially mean-square stable if there exist $\omega > 0$ and $\mu \in (0,1)$ such that

$$\mathbb{E}\left\{\|x_k\|^2\right\} \le \omega\mu^j\mathbb{E}\left\{\|x_0\|^2\right\},$$

holds for all $x_0 \in \mathbb{R}^n$ and $j > \kappa$, where κ is a sufficiently large positive integer.

Theorem 1. *Given the positive parameters θ, ς, and matrices F_1, F_2, the stochastic system (7) is exponentially mean-square stable if there exist $Q > 0$ and R which satisfy the following inequality:*

$$\begin{bmatrix} -Q & 0 & 0 & \hat{\Xi}_1 & \hat{\Xi}_2 & \hat{\Xi}_3 & QF_1^T & QF_2^T \\ * & I-2Q & 0 & 0 & \hat{\Xi}_4 & 0 & 0 & 0 \\ * & * & -I & 0 & 0 & \hat{\Xi}_5 & 0 & 0 \\ * & * & * & -I\otimes Q & 0 & 0 & 0 & 0 \\ * & * & * & * & -I\otimes Q & 0 & 0 & 0 \\ * & * & * & * & * & -I\otimes Q & 0 & 0 \\ * & * & * & * & * & * & -I & 0 \\ * & * & * & * & * & * & * & -I \end{bmatrix} < 0, \tag{8}$$

where

$$\hat{\Xi}_1 = \sqrt{(1-\theta)(1-\zeta)}(\hat{\Pi}_1 + \hat{\Pi}_2)^T, \hat{\Xi}_2 = \sqrt{(1-\theta)\zeta}\hat{\Pi}_1^T,$$
$$\hat{\Xi}_3 = \sqrt{\theta}\hat{\Pi}_1^T, \hat{\Xi}_4 = \sqrt{(1-\theta)\zeta}\hat{\Pi}_2^T, \hat{\Xi}_5 = \sqrt{\theta}\Pi_3^T$$

with

$$\begin{aligned}\hat{\Pi}_1 &= (U_g V_G^{-1}\otimes\begin{bmatrix} I & 0 \end{bmatrix})\overline{G}e^{GT}\begin{bmatrix} Q & 0 \end{bmatrix}^T,\\ \hat{\Pi}_2 &= (U_g V_G^{-1}\otimes\begin{bmatrix} I & 0 \end{bmatrix})\overline{G}e^{GT}\begin{bmatrix} 0 & R^T \end{bmatrix}^T,\\ \Pi_3 &= ((U_g V_G^{-1})\otimes\begin{bmatrix} I & 0 \end{bmatrix})\overline{G}e^{GT}\begin{bmatrix} 0 & I \end{bmatrix}^T.\end{aligned}$$

In addition, if (8) is feasible, we can obtain the desired controller gain matrix by $K = RQ^{-1}$.

Proof of Theorem 1. Consider the following Lyapunov function:

$$V(x_k) = x_k^T P x_k, \tag{9}$$

where $P > 0$ and define the difference of (9) as $\Delta V(x_k) = \mathbb{E}\{V(x_{k+1})|x_k\} - V(x_k)$. With the application of the general matrix decomposition approach presented in this paper, the expectation operation of the matrix $e^{G^T\alpha_k}\left(\begin{bmatrix} I \\ 0 \end{bmatrix} P \begin{bmatrix} I & 0 \end{bmatrix}\right)e^{G\alpha_k}$ can be calculated as follows:

$$\mathbb{E}\{e^{G^T\alpha_k}\left(\begin{bmatrix}I\\0\end{bmatrix}P\begin{bmatrix}I & 0\end{bmatrix}\right)e^{G\alpha_k}\}$$

$$= e^{G^TT}\mathbb{E}\Big\{\overline{G}^T((\pi(\rho_k)V_G^{-1})\otimes I)^T$$

$$\times\left(\begin{bmatrix}I\\0\end{bmatrix}P\begin{bmatrix}I & 0\end{bmatrix}\right)((\pi(\rho_k)V_G^{-1})\otimes I)\overline{G}\Big\}e^{GT}$$

$$= e^{G^TT}\overline{G}^T\mathbb{E}\Big\{(V_G{}^{-H}\pi^H(\rho_k)\pi(\rho_k)V_G{}^{-1})$$

$$\otimes\left(\begin{bmatrix}I\\0\end{bmatrix}P\begin{bmatrix}I & 0\end{bmatrix}\right)\Big\}\overline{G}e^{GT}$$

$$= e^{G^TT}\overline{G}^T\mathbb{E}\Big\{(V_G{}^{-H}U_g^HU_gV_G{}^{-1})\otimes\left(\begin{bmatrix}I\\0\end{bmatrix}P\begin{bmatrix}I & 0\end{bmatrix}\right)\Big\}\overline{G}e^{GT}$$

$$= e^{G^TT}\overline{G}^T\left((U_gV_G^{-1})^T\otimes\begin{bmatrix}I\\0\end{bmatrix}\right)(I\otimes P)((U_gV_G^{-1})\otimes\begin{bmatrix}I & 0\end{bmatrix})\overline{G}e^{GT}$$

$$= \Pi^T(I\otimes P)\Pi, \tag{10}$$

where $\Pi = ((U_gV_G^{-1})\otimes\begin{bmatrix}I & 0\end{bmatrix})\overline{G}e^{GT}$ and U_g is specific in Lemma 2.

Remark 3.3. Note that $\pi(\delta)V_G^{-1}$ in (1) is a real matrix regardless of whether the matrix G contains complex-value eigenvalues or not. Accordingly, $U_gV_G^{-1}$ is a real matrix. In this case, one has $V_G^{-H}U_g^H = V_G^{-T}U_g^T$ in (10).

Accordingly, we can also calculate the following mathematical expectation:

$$\mathbb{E}\{H_1{}^TPH_1\}$$

$$= \begin{bmatrix}I & 0\end{bmatrix}\mathbb{E}\{e^{G^T\alpha_k}\left(\begin{bmatrix}I\\0\end{bmatrix}P\begin{bmatrix}I & 0\end{bmatrix}\right)e^{G\alpha_k}\}\begin{bmatrix}I\\0\end{bmatrix}$$

$$= \begin{bmatrix}I & 0\end{bmatrix}\Pi^T(I\otimes P)\Pi\begin{bmatrix}I\\0\end{bmatrix}$$

$$= \Pi_1^T(I\otimes P)\Pi_1, \tag{11}$$

where $\Pi_1 = \Pi\begin{bmatrix}I & 0\end{bmatrix}^T = ((U_gV_G^{-1})\otimes\begin{bmatrix}I & 0\end{bmatrix})\overline{G}e^{GT}\begin{bmatrix}I & 0\end{bmatrix}^T$. Similarly, we have

$$\mathbb{E}\{H_2^TPH_2\} = \Pi_2^T(I\otimes P)\Pi_2, \mathbb{E}\{H_3^TPH_3\} = \Pi_3^T(I\otimes P)\Pi_3,$$

$$\mathbb{E}\{H_1^TPH_2\} = \Pi_1{}^T(I\otimes P)\Pi_2, \mathbb{E}\{H_1^TPH_3\} = \Pi_1^T(I\otimes P)\Pi_3,$$

$$\mathbb{E}\{(H_1+H_2)^TP(H_1+H_2)\} = (\Pi_1+\Pi_2)^T(I\otimes P)(\Pi_1+\Pi_2)$$

with $\Pi_2 = \Pi\begin{bmatrix}0 & K^T\end{bmatrix}^T$ and $\Pi_3 = \Pi\begin{bmatrix}0 & I\end{bmatrix}^T$.

Then, by (7) and (11), one has

$$\mathbb{E}\{\Delta V(x_k)\}$$

$$= \mathbb{E}\{x_{k+1}^TPx_{k+1} - x_k^TPx_k\}$$

$$= \mathbb{E}\{x_k^T((1-\theta)(1-\varsigma)(\Pi_1+\Pi_2)^T(I\otimes P)(\Pi_1+\Pi_2)$$
$$+ (1-(1-\theta)(1-\varsigma))\Pi_1^T(I\otimes P)\Pi_1 - P)x_k$$
$$+ 2(1-\theta)\varsigma x_k^T\Pi_1^T(I\otimes P)\times\Pi_2\varphi_k + 2\theta x_k^T\Pi_1^T(I\otimes P)\Pi_3\psi_k$$
$$+ (1-\theta)\varsigma\varphi_k^T\Pi_2^T(I\otimes P)\Pi_2\varphi_k + \theta\psi_k^T\Pi_3^T(I\otimes P)\Pi_3\psi_k\}$$

$$\le \mathbb{E}\Delta V(x_k) + \|F_1x_k\|^2 + \|F_2x_k\|^2 - \|\varphi_k\|^2 - \|\psi_k\|^2$$

$$= \mathbb{E}\{x_k^T((1-\theta)(1-\varsigma)(\Pi_1+\Pi_2)^T(I\otimes P)(\Pi_1+\Pi_2)$$
$$+ (1-(1-\theta)(1-\varsigma))\Pi_1^T(I\otimes P)\Pi_1 + F_1^TF_1$$
$$+ F_2^TF_2 - P)x_k + 2(1-\theta)\times\varsigma x_k^T\Pi_1^T(I\otimes P)\Pi_2\varphi_k$$
$$+ 2\theta x_k^T\Pi_1^T(I\otimes P)\Pi_3\psi_k + \varphi_k^T((1-\theta)\varsigma\Pi_2^T(I\otimes P)\Pi_2 - I)\varphi_k$$
$$+ \psi_k^T(\theta\Pi_3^T(I\otimes P)\Pi_3 - I)\psi_k\}$$

$$= \mathbb{E}\{\varepsilon_k^TM\varepsilon_k\},$$

where $\epsilon_k = \begin{bmatrix}x_k\\\varphi_k\\\psi_k\end{bmatrix}$ and $M = \begin{bmatrix}M_{11} & M_{12} & M_{13}\\ * & M_{22} & M_{23}\\ * & * & M_{33}\end{bmatrix}$ with

$$M_{11} = (1-\theta)(1-\varsigma)(\Pi_1+\Pi_2)^T(I\otimes P)(\Pi_1+\Pi_2)$$
$$+ (1-(1-\theta)(1-\varsigma))\Pi_1^T(I\otimes P)\Pi_1 + F_1^TF_1$$
$$+ F_2^TF_2 - P, M_{12} = (1-\theta)\varsigma\Pi_1^T(I\otimes P)\Pi_2,$$

$$M_{13} = \theta\Pi_1^T(I\otimes P)\Pi_3, M_{22} = (1-\theta)\varsigma\Pi_2^T(I\otimes P)\Pi_2 - I,$$

$$M_{23} = 0, M_{33} = \theta\Pi_3^T(I\otimes P)\Pi_3 - I.$$

If $M < 0$, we can conclude that

$$\mathbb{E}\{\Delta V(x_k)\} \le \mathbb{E}\{\epsilon_k^TM\epsilon_k\} \le -\lambda_{min}(-M)\mathbb{E}\{x_k^Tx_k\} < -\sigma\mathbb{E}\{\|x_k\|^2\}, \tag{12}$$

with $0 < \sigma < min\{\lambda_{min}(-M), \lambda_{max}(P)\}$. Then, we can get that $\mathbb{E}\{\Delta V(x_k)\} < -\sigma\mathbb{E}\{\|x_k\|^2\} \le -\frac{\sigma}{\lambda_{max}(P)}\mathbb{E}\{V(x_k)\}$. Considering the Lyapunov function in (9), the following inequality is satisfied.

$$\lambda_{min}(P)\|x_k\|^2 \le V(x_k) \le \lambda_{max}(P)\|x_k\|^2. \tag{13}$$

Referring to the lemma 1 in [41], by (12) and (13) we have that

$$\mathbb{E}\left\{\|x_k\|^2\right\} \le \omega\mu^j\mathbb{E}\left\{\|x_0\|^2\right\},$$

where $\omega = \frac{\lambda_{max}(P)}{\lambda_{min}(P)}$ and $\mu = 1 - \frac{\sigma}{\lambda_{max}(P)} \in (0,1)$. Therefore, the closed-loop system is of exponentially mean-square stable.

To design the stability controller, $M < 0$ can be rewritten as follows by Schur complement.

$$\begin{bmatrix} -P & 0 & 0 & \Xi_1 & \Xi_2 & \Xi_3 & F_1^T & F_2^T \\ * & -I & 0 & 0 & \Xi_4 & 0 & 0 & 0 \\ * & * & -I & 0 & 0 & \hat{\Xi}_5 & 0 & 0 \\ * & * & * & -I \otimes P^{-1} & 0 & 0 & 0 & 0 \\ * & * & * & * & -I \otimes P^{-1} & 0 & 0 & 0 \\ * & * & * & * & * & -I \otimes P^{-1} & 0 & 0 \\ * & * & * & * & * & * & -I & 0 \\ * & * & * & * & * & * & * & -I \end{bmatrix} < 0, \tag{14}$$

where

$$\Xi_1 = \sqrt{(1-\theta)(1-\zeta)}(\Pi_1 + \Pi_2)^T, \Xi_2 = \sqrt{(1-\theta)\zeta}\Pi_1^T,$$

$$\Xi_3 = \sqrt{\theta}\Pi_1^T, \Xi_4 = \sqrt{(1-\theta)\zeta}\Pi_2^T, \hat{\Xi}_5 = \sqrt{\theta}\Pi_3^T.$$

Apply a congruence transformation to (8) with diag $\{\mathcal{Q}^{-1}, \mathcal{Q}^{-1}, I, I, I, I, I, I\}$. Let $P = \mathcal{Q}^{-1}$, $K = RP$. We can get the inequality (14) with $-I \le P^2 - 2P$. Then, the exponentially mean-square stability of system (3) is guaranteed. We complete the proof. □

4 | SIMULATION EXAMPLES

In order to verify the effectiveness of the controller design algorithm, two cases are considered in this section, one is that all the eigenvalues of matrix G are real-value, another is that some eigenvalues of matrix G are complex-value.

Case 1. All the eigenvalues of matrix G are real-value.

i) In this case, the geometric multiplicity of G is equal to the algebraic multiplicity of G. Consider a system described by the following parameter matrices:

$$\mathcal{A} = \begin{bmatrix} -2.1 & 1.2 & 0.4 \\ 0 & -2.1 & 0.63 \\ 0 & 0 & 0.06 \end{bmatrix}, B = \begin{bmatrix} 0.2 \\ 0.1 \\ -0.3 \end{bmatrix}.$$

Then, the roots of the minimal polynomial of G are $\lambda_1 = -2.1$, $\lambda_2 = 0.06$, and $\lambda_3 = 0$, with multiplicities $l_1 = 2$, $l_2 = 1$ and $l_3 = 1$. By (1), the corresponding confluent Vandermonde matrix V_G is obtained as

$$V_G = \begin{bmatrix} 1.0000 & 1.000 & 0.0000 & 1.0000 \\ 0.0600 & -2.1000 & 1.0000 & 0.0000 \\ 0.0036 & 4.4100 & -4.2000 & 0.0000 \\ 0.0002 & -9.2610 & 13.2300 & 0.0000 \end{bmatrix}.$$

The initial system state is assumed as $x_0 = \begin{bmatrix} -1 & 0.5 & -0.3 \end{bmatrix}^T$. Suppose that the ideal time interval $T = 0.8$ and the sampling error follows uniform distribution $\rho_k \sim U(-0.4, 0.4)$. Considering that $\mathbb{E}\{\pi^H(\delta)\pi(\delta)\} = \int_{-\infty}^{+\infty} \pi^H(\delta)\pi(\delta)f(\delta)d\delta$, U_g can be calculated by (2) as follows

$$U_g = \begin{bmatrix} -1.0000 & -0.0001 & -0.0257 & 0.0009 \\ 0.0000 & 0.2309 & 0.0004 & 0.0040 \\ 0.0006 & 0.0000 & -0.0226 & 0.0012 \\ 0.0000 & 0.0000 & 0.0001 & 0.0019 \end{bmatrix}.$$

We assume that the deception attacks rates of S-C channel and C-A channel are $\varsigma = 0.3$, $\theta = 0.3$, respectively. Figures 1 and 2 depict the sampling intervals and the moments when deception attacks happen. The attacks satisfy $\|\varphi(t_k)\| \le \|F_1 x(t_k)\|$ and $\|\psi(t_k)\| \le \|F_2 x(t_k)\|$, where F_1 and F_2 are given as

$$F_1 = \begin{bmatrix} -0.5 & 1 & 0 \\ 0 & 0.2 & -0.6 \\ 0.8 & 0 & -0.3 \end{bmatrix}, F_2 = \begin{bmatrix} 0 & -0.3 & 0.21 \end{bmatrix}.$$

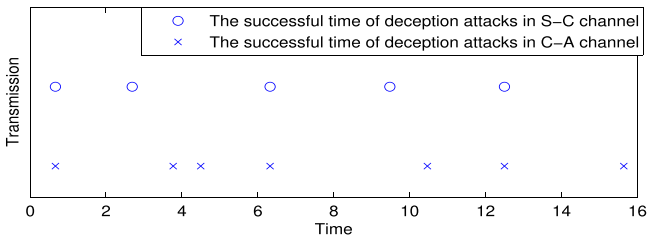

FIGURE 1 Moments of deception attack.

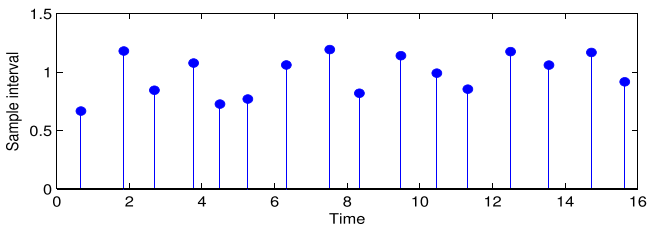

FIGURE 2 Noisy sampling intervals with $\rho_k \sim U(-0.4, 0.4)$.

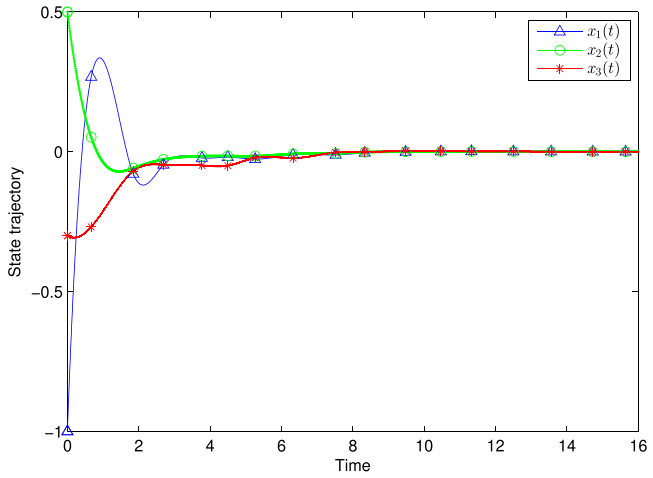

FIGURE 3 State trajectories of systems with control input.

Then, we can obtain Q, R and designed controller K as follows

$$Q = \begin{bmatrix} 1.4382 & 0.6409 & 0.3466 \\ 0.6409 & 1.0988 & 0.2712 \\ 0.3466 & 0.2712 & 0.7617 \end{bmatrix},$$

$$R = \begin{bmatrix} 1.2906 & 1.0692 & 2.0113 \end{bmatrix},$$

$$K = \begin{bmatrix} 0.1904 & 0.2538 & 2.4636 \end{bmatrix}.$$

Figure 3 shows the state trajectories of systems with control input in which the effectiveness of the proposed approach is verified.

ii) In this case, the geometric multiplicity of G is less than the algebraic multiplicity of G. Consider a system described by the following parameter matrices.

$$A = \begin{bmatrix} -1 & 0.1 & 0.2 \\ 0 & -1 & 0.5 \\ 0 & 0 & 0.2 \end{bmatrix}, B = \begin{bmatrix} 0.13 & 0.00 \\ -0.60 & 0.20 \\ 0.30 & 0.55 \end{bmatrix}.$$

The roots of the minimal polynomial of G are $\lambda_1 = -1$, $\lambda_2 = 0$, and $\lambda_3 = 0.2$ with multiplicities $l_1 = 2$, $l_2 = 1$ and $l_3 = 1$. $m_g = 5 > \bar{m}_g = 4$. By (1), the reduced-order confluent Vandermonde matrix V_G is obtained as

$$V_G = \begin{bmatrix} 1.0000 & 1.0000 & 0.0000 & 1.0000 \\ 0.2000 & -1.0000 & 1.0000 & 0.0000 \\ 0.0400 & 1.0000 & -2.0000 & 0.0000 \\ 0.0080 & -1.0000 & 3.0000 & 0.0000 \end{bmatrix}.$$

The initial system state is assumed as $x(0) = \begin{bmatrix} 1 & 0.5 & -0.3 \end{bmatrix}^T$. Suppose that the ideal time interval $T = 0.8$ and the sampling error ρ_k obeys uniform distribution between -0.4 and 0.4. Considering that $\mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\} = \int_{-\infty}^{+\infty} \pi^H(\delta)\pi(\delta) f(\delta) d\delta$, U_g can be calculated by (2) as follows

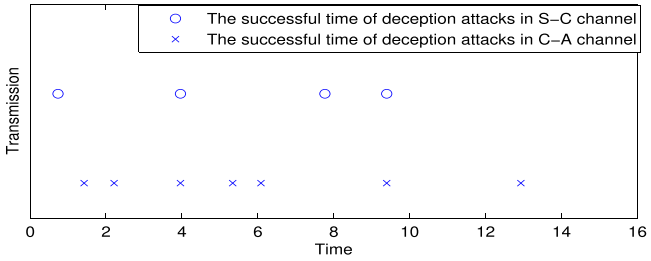

FIGURE 4 Moments of deception attack.

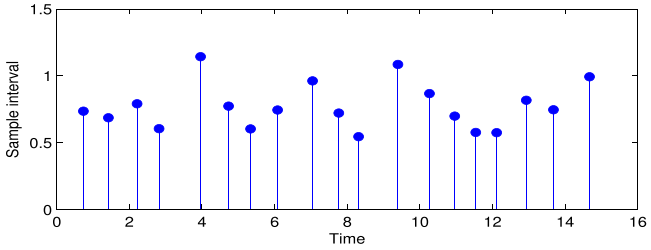

FIGURE 5 Noisy sampling intervals with $\rho_k \sim U(-0.4, 0.4)$.

$$U_g = \begin{bmatrix} -1.0000 & 0.0000 & -0.0266 & 0.0004 \\ 0.0000 & 0.2309 & 0.0000 & 0.0038 \\ 0.0006 & 0.0000 & -0.0237 & 0.0005 \\ 0.0000 & 0.0000 & 0.0000 & 0.0017 \end{bmatrix}.$$

We assume that the deception attacks rates of S-C channel and C-A channel are $\varsigma = 0.3$, $\theta = 0.3$, respectively. F_1 and F_2 are given as

$$F_1 = \begin{bmatrix} -0.1200 & 0.1600 & 0.0000 \\ 0.0000 & 0.0180 & -0.0020 \\ 0.0800 & -0.0300 & 0.0000 \end{bmatrix},$$

$$F_2 = \begin{bmatrix} 0.0000 & -0.3000 & 0.2100 \\ -0.1200 & 0.1600 & 0.0180 \end{bmatrix}.$$

Figures 4 and 5 depict the sampling intervals and the moments when deception attack happens.

We can obtain Q, R and the designed controller K as follows

$$Q = \begin{bmatrix} 1.0290 & 0.0106 & 0.0170 \\ 0.0106 & 1.0359 & 0.0513 \\ 0.0170 & 0.0513 & 0.9922 \end{bmatrix},$$

$$R = \begin{bmatrix} -0.1615 & 0.8221 & -0.2426 \\ -0.0404 & -0.5613 & -1.7498 \end{bmatrix},$$

$$K = \begin{bmatrix} -0.1606 & 0.8093 & -0.2836 \\ -0.0057 & -0.4557 & -1.7398 \end{bmatrix}.$$

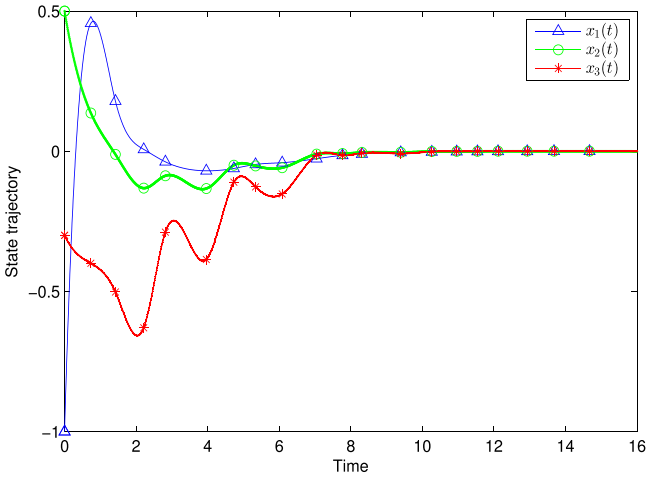

FIGURE 6 State trajectories of systems with control input.

Figure 6 shows the state trajectories of systems with control input in which the effectiveness of the approach is also verified.

Case 2. Some eigenvalues of matrix G are complex-value.

Consider the following mass spring system [42].

$$\begin{cases} \dot{x}_1(t) = x_2(t) \\ \dot{x}_2(t) = -\frac{k}{m}x_1(t) - \frac{c}{m}x_2(t) + \frac{1}{m}u(t) \end{cases}, \tag{15}$$

where $m = 1, k = c = 2$. By $x^T(t) = \begin{bmatrix} x_1^T(t) & x_2^T(t) \end{bmatrix}$, the system (15) can be described as

$$\dot{x}(t) = \begin{bmatrix} 0 & 1 \\ -2 & -2 \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u(t).$$

The roots of the minimal polynomial of G are $\lambda_1 = -1 + i$, $\lambda_2 = -1 - i$, and $\lambda_3 = 0$, with multiplicities $l_1 = 1$, $l_2 = 1$ and $l_3 = 1$. By (1), the corresponding confluent Vandermonde matrix V_G is obtained as

$$V_G = \begin{bmatrix} 1.0000 & 1.0000 & 1.0000 \\ -1.0000 + 1.0000i & -1.0000 - 1.0000i & 0.0000 \\ -2.0000i & 2.0000i & 0.0000 \end{bmatrix}.$$

It is assumed that the normal time interval $T = 0.8$ and the sampling error ρ_k obeys uniform distribution between -0.4 and 0.4. By $\mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\} = \int_{-\infty}^{+\infty} \pi^H(\delta)\pi(\delta)f(\delta)d\delta$, we have

$$\mathbb{E}\left\{\pi^H(\delta)\pi(\delta)\right\} = \begin{bmatrix} 1.1101 & 0.9864 + 0.2129i & 0.9991 + 0.0533i \\ 0.9864 - 0.2129i & 1.1101 & 0.9991 - 0.0533i \\ 0.9991 - 0.0533i & 0.9991 + 0.0533i & 1.0000 \end{bmatrix}.$$

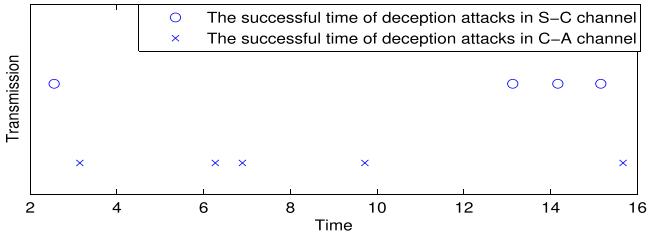

FIGURE 7 Moments of deception attack.

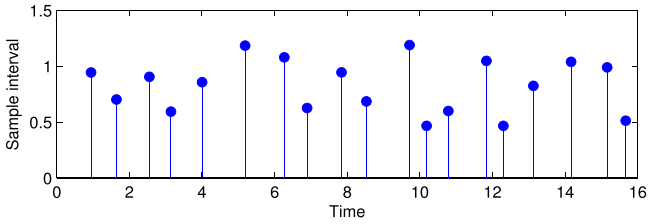

FIGURE 8 Noisy sampling intervals with $\rho_k \sim U(-0.4, 0.4)$.

Then, with (2) and V_G, we derive that

$$U_g = \begin{bmatrix} 0.0125 + 0.0113i & 0.0125 - 0.0113i & -0.0238 \\ 0.0569 - 0.2311i & 0.0569 + 0.2311i & -0.1607 \\ 1.0222 - 0.0914i & 1.0222 + 0.0914i & 0.9867 \end{bmatrix},$$

$$U_g V_G^{-1} = \begin{bmatrix} -0.0238 & -0.0362 & -0.0238 \\ -0.1607 & -0.2177 & 0.0067 \\ 0.9867 & -0.0355 & 0.0280 \end{bmatrix}.$$

The deception attacks rates of S-C channel and C-A channel are assumed to be $\varsigma = 0.3$, $\theta = 0.3$ respectively. F_1 and F_2 are given as

$$F_1 = \begin{bmatrix} 0.0000 & -0.0200 \\ 0.3000 & 0.0000 \end{bmatrix}, F_2 = \begin{bmatrix} 0.0000 & 0.1500 \end{bmatrix}.$$

The sampling intervals and deception attack moments are also depicted in Figures 7 and 8.

Solving the inequality (8), we can obtain $\mathcal{Q}$, R and the designed controller K as follows

$$\mathcal{Q} = \begin{bmatrix} 0.9482 & -0.0257 \\ -0.0257 & 1.0468 \end{bmatrix}, \quad R = \begin{bmatrix} 0.4187 & -0.3584 \end{bmatrix},$$

$$K = \begin{bmatrix} 0.4326 & -0.3317 \end{bmatrix}.$$

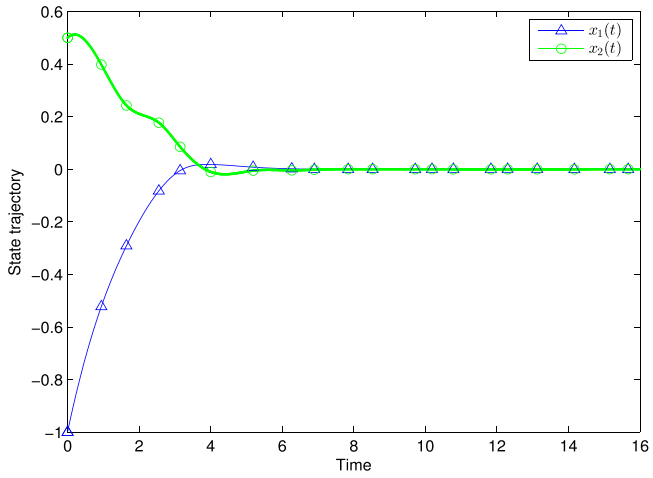

FIGURE 9 State trajectories of systems with control input.

The simulation results are presented in Figure 9 with the initial value $x(0) = \begin{bmatrix}-1 & 0.5\end{bmatrix}^T$. It verifies the effectiveness of the proposed approach.

5 | CONCLUSIONS

The stabilization analysis and controller design problems for networked systems with stochastic sampling and two-channel deception attacks have been investigated in this paper. First, a general matrix decomposition approach has been presented which is applicable in scenarios where the system matrix A contains complex-value eigenvalues. Subsequently, we have established a discrete stochastic framework for networked system which considers the joint effects of sampling errors and two-channel deception attacks. By the general matrix decomposition approach, the expectation operations for coupling matrices with high nonlinearity and randomness have been decoupled. Then, a stabilization controller has been constructed to ensure the exponential mean-square stability of the resulting discrete stochastic system. Finally, the effectiveness of the proposed approach has been validated through three simulation examples.

AUTHOR CONTRIBUTIONS

Yizhen Li: Investigation; writing—original draft; software. **Zhipei Hu**: Conceptualization; project administration; writing—review & editing. **Feiqi Deng**: Methodology; supervision. **Yongkang Su**: Software; writing—review & editing. **Guangjie Li**: Funding acquisition; writing—review & editing.

ACKNOWLEDGEMENTS

This research was partially supported by the Basic and Applied Basic Research of Guangzhou Basic Research Program under Grant 202201010250, in part by the Guangdong Basic and Applied Basic Research Foundation under Grants 2023A1515011025 and 2023A1515012781, and in part by the National Natural Science Foundation of China Under Grant 62333006.

CONFLICT OF INTEREST STATEMENT

The authors declare no potential conflict of interests.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Yizhen Li https://orcid.org/0009-0001-9778-6999
Feiqi Deng https://orcid.org/0000-0002-0257-5647

REFERENCES

1. Rana, M.M., Li, L., Su, S.W.: Cyber attack protection and control of microgrids. IEEE/CAA J. Autom. Sin. 5(2), 602–609 (2017)
2. Chin, W.L., Lee, C.H., Jiang, T.: Blind false data attacks against ac state estimation based on geometric approach in smart grid communications. IEEE Trans. Smart Grid 9(6), 6298–6306 (2017)
3. Hu, Z., Luo, T., Yang, R., Deng, F.: Stabilization of networked control systems subject to consecutive packet dropouts: The random clock offsets case. IEEE Trans. Control Network Syst. 10(1), 285–294 (2022)
4. Ding, D., Wang, Z., Lam, J., Shen, B.: Finite-horizon $\mathcal{H}_\infty$ control for discrete time-varying systems with randomly occurring nonlinearities and fading measurements. IEEE Trans. Autom. Control 60(9), 2488–2493 (2014)
5. Cao, L., Jiang, X., Zhao, Y., Wang, S., You, D., Xu, X.: A survey of network attacks on cyber-physical systems. IEEE Access 8, 44219–44227 (2020)
6. Cui, Y., Liu, Y., Zhang, W., Alsaadi, F.E.: Sampled-based consensus for nonlinear multiagent systems with deception attacks: The decoupled method. IEEE Trans. Syst. Man Cybern.: Syst. 51(1), 561–573 (2018)
7. Ding, D., Wang, Z., Han, Q.L., Wei, G.: Security control for discrete-time stochastic nonlinear systems subject to deception attacks. IEEE Trans. Syst. Man Cybern.: Syst. 48(5), 779–789 (2016)
8. Hu, Z., Su, Y.: Stabilization of networked systems with communication constraints: The random sampling periods case. Automatica 149, 110806 (2023)
9. Wang, D., Wang, Z., Shen, B., Alsaadi, F.E.: Security-guaranteed filtering for discrete-time stochastic delayed systems with randomly occurring sensor saturations and deception attacks. Int. J. Robust Nonlinear Control 27(7), 1194–1208 (2017)
10. Ding, D., Han, Q.L., Ge, X., Wang, J.: Secure state estimation and control of cyber-physical systems: A survey. IEEE Trans. Syst. Man Cybern.: Syst. 51(1), 176–190 (2020)
11. Hu, Z., Chen, K., Deng, F., Luo, S., Hu, S.: $\mathcal{H}_\infty$ controller design for networked systems with two-channel packet dropouts and fdi attacks. IEEE Trans. Cybern. 54(3), 1661–1670 (2023)
12. Wu, Z., Xiong, J., Xie, M.: Improved event-triggered control for networked control systems subject to deception attacks. J. Franklin Inst. 358(4), 2229–2252 (2021)
13. Cao, Z., Niu, Y., Song, J.: Finite-time sliding-mode control of markovian jump cyber-physical systems against randomly occurring injection attacks. IEEE Trans. Autom. Control 65(3), 1264–1271 (2019)
14. Liu, S., Song, Y., Wei, G., Huang, X.: Rmpc-based security problem for polytopic uncertain system subject to deception attacks and persistent disturbances. IET Control Theory Appl. 11(10), 1611–1618 (2017)
15. Zhao, D., Wang, Z., Wei, G., Han, Q.L.: A dynamic event-triggered approach to observer-based pid security control subject to deception attacks. Automatica 120, 109128 (2003)
16. Liu, X., Zhou, X., Xiang, B.: Adaptive event-triggered dynamic output feedback control for networked control systems under hybrid attacks. IET Control Theory Appl. 18(1), 1–13 (2024)

17. Hu, Z., Deng, F., Su, Y., Zhang, J., Hu, S.: Security control of networked systems with deception attacks and packet dropouts: A discrete-time approach. J. Franklin Inst. 358(16), 8193–8206 (2021)
18. Pang, Z.H., Liu, G.P., Zhou, D., Hou, F., Sun, D.: Two-channel false data injection attacks against output tracking control of networked systems. IEEE Trans. Ind. Electron. 63(5), 3242–3251 (2016)
19. Song, H., Shi, P., Zhang, W.A., Lim, C.C., Yu, L.: Distributed $\mathcal{H}_\infty$ estimation in sensor networks with two-channel stochastic attacks. IEEE Trans. Cybern. 50(2), 465–475 (2020)
20. Zhao, T., Zhang, K., Dian, S.: Security control of interval type-2 fuzzy system with two-terminal deception attacks under premise mismatch. Nonlinear Dyn. 102, 431–453 (2020)
21. Hu, Z., Zhang, J., Deng, F., Fan, Z., Qiu, L.: A discretization approach to sampled-data stabilization of networked systems with successive packet losses. Int. J. Robust Nonlinear Control 31(10), 4589–4601 (2021)
22. Varma, V.S., de Oliveira, A.M., Postoyan, R., Morărescu, I.C., Daafouz, J.: Energy-efficient time-triggered communication policies for wireless networked control systems. IEEE Trans. Autom. Control 65(10), 4324–4331 (2019)
23. Hu, Z., Yang, R., Li, X., Su, Y.: A probability theory approach to stability analysis of networked sampled-data systems with consecutive packet dropouts. IEEE Trans. Circuits Syst. II Express Briefs 69(2), 429–433 (2021)
24. Hu, Z., Chen, K., Su, Y., Deng, F., Hu, S., Zou, A.M.: Stochastic analysis and synthesis of networked systems with consecutively lost packets. IEEE Trans. Syst. Man Cybern.: Syst. 54(4), 2205–2212 (2024)
25. Jiang, F., Xie, D., Cao, M.: Dynamic consensus of double-integrator multi-agent systems with aperiodic impulsive protocol and time-varying delays. IET Control Theory Appl. 11(16), 2879–2885 (2017)
26. Chen, K., Song, H., Hu, Z., Deng, F.: Saturated $\mathcal{H}_\infty$ control of networked systems under stochastic transmission delays: The random sampling periods case. Int. J. Robust Nonlinear Control 34(6), 3798–3811 (2024)
27. Shen, B., Tan, H., Wang, Z., Huang, T.: Quantized/saturated control for sampled-data systems under noisy sampling intervals: A confluent vandermonde matrix approach. IEEE Trans. Autom. Control 62(9), 4753–4759 (2017)
28. Hu, Z., Deng, F., Xing, M., Li, J.: Modeling and control of itô stochastic networked control systems with random packet dropouts subject to time-varying sampling. IEEE Trans. Autom. Control 62(8), 4194–4201 (2017)
29. Peng, C., Zhang, J.: Event-triggered output-feedback $\mathcal{H}_\infty$ control for networked control systems with time-varying sampling. IET Control Theory Appl. 9(9), 1384–1391 (2015)
30. Hu, Z., Ren, H., Shi, P.: Synchronization of complex dynamical networks subject to noisy sampling interval and packet loss. IEEE Trans. Neural Networks Learn. Syst. 33(8), 3216–3226 (2022)
31. Kurniawan, E., Cao, Z., Man, Z.: Design of robust repetitive control with time-varying sampling periods. IEEE Trans. Ind. Electron. 61(6), 2834–2841 (2013)
32. Hu, Z., Song, H., Ren, H., Su, Y., Deng, F.: Stabilization of networked control systems subject to noisy sampling intervals and stochastic time-varying delays. IEEE Trans. Control Network Syst. 9(3), 1271–1280 (2022)
33. Zhang, C.K., Jiang, L., He, Y., Wu, H., Wu, M.: Stability analysis for control systems with aperiodically sampled data using an augmented lyapunov functional method. IET Control Theory Appl. 7(9), 1219–1226 (2013)
34. Hu, Z., Ren, H., Deng, F., Li, H.: Stabilization of sampled-data systems with noisy sampling intervals and packet dropouts via a discrete-time approach. IEEE Trans. Autom. Control 67(6), 3204–3211 (2021)
35. Lou, W., Fang, Y.: A multipath routing approach for secure data delivery. In: 2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No. 01CH37277). IEEE, Piscataway (2001)
36. Zhang, H., Cheng, P., Shi, L., Chen, J.: Optimal denial-of-service attack scheduling with energy constraint. IEEE Trans. Autom. Control 60(11), 3023–3028 (2015)
37. Guan, Y., Ge, X.: Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. IEEE Trans. Signal Inf. Process. Networks 4(1), 48–59 (2017)
38. Sandberg, H., Gupta, V., Johansson, K.H.: Secure networked control systems. Annu. Rev. Control Rob. Auton. Syst. 5, 445–464 (2022)
39. Liu, J., Wei, L., Xie, X., Yue, D.: Distributed event-triggered state estimators design for sensor networked systems with deception attacks. IET Control Theory Appl. 13(17), 2783–2791 (2019)
40. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Sec. (TISSEC) 14(1), 1–33 (2011)
41. Hu, Z., Shi, P., Zhang, J., Deng, F.: Control of discrete-time stochastic systems with packet loss by event-triggered approach. IEEE Trans. Syst. Man Cybern.: Syst. 51(2), 755–764 (2021)
42. Liu, J., Wang, Y., Zha, L., Xie, X., Tian, E.: An event-triggered approach to security control for networked systems using hybrid attack model. Int. J. Robust Nonlinear Control 31(12), 5796–5812 (2021)

How to cite this article: Li, Y., Hu, Z., Deng, F., Su, Y., Li, G.: A general matrix decomposition approach with application to stabilization of networked systems with stochastic sampling and two-channel deception attacks. IET Control Theory Appl. 1–10 (2024). https://doi.org/10.1049/cth2.12676