Security Control for Discrete-time Stochastic Nonlinear Systems Subject to Deception Attacks

Derui Ding, Zidong Wang, *Fellow, IEEE*, Qing-Long Han, *Senior Member* and Guoliang Wei

***Abstract*—This paper is concerned with the security control problem with quadratic cost criterion for a class of discrete-time stochastic nonlinear systems subject to deception attacks. A definition of security in probability is adopted to account for the transient dynamics of controlled systems. The purpose of the problem under consideration is to design a dynamic output feedback controller such that the prescribed security in probability is guaranteed while obtaining an upper bound of the quadratic cost criterion. First of all, some sufficient conditions with the form of matrix inequalities are established in the framework of the input-to-state stability in probability (ISSiP). Then, an easy-solution version on above inequalities is proposed by carrying out the well-known matrix inverse lemma to obtain both the controller gain and the upper bound. Furthermore, the main results are shown to be extendable to the case of discrete-time stochastic linear systems. Finally, two simulation examples are utilized to illustrate the usefulness of the proposed controller design scheme.**

***Index Terms*—Discrete-time stochastic nonlinear systems; Deception attacks; Security in probability; Security control.**

I. Introduction

In the past two decades, the networked control systems (NCSs) have received an ever-increasing interest from researchers due to their extensive applications in various practical areas, such as traffic management, robot control, mobile sensor networks and remote control. In contrast with many distinct advantages, the limited bandwidth of the communication channel inevitably leads to various network induced phenomena which could seriously degrade the addressed system performances. Some representative results have been published in [42] for systems with transmission delays, [14], [32] for systems with missing measurements, [16], [21] for systems with signal quantization, and [10], [11] for systems with randomly occurring uncertainties (ROUs). It should be pointed out that the issues of network security are largely ignored despite its frequent occurrence in networked systems.

This work was supported in part by the Royal Society of the UK, the National Natural Science Foundation of China under Grants 61329301, 61573246 and 61374039, the Shanghai Rising-Star Program of China under Grant 16QA1403000, the Program for Capability Construction of Shanghai Provincial Universities under Grant 15550502500, and the Alexander von Humboldt Foundation of Germany.

D. Ding and G. Wei are with the Shanghai Key Lab of Modern Optical System, Department of Control Science and Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China. (Email: deruiding2010@usst.edu.cn)

Z. Wang is with the Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom. (Email: Zidong.Wang@brunel.ac.uk)

Q.-L. Han is with the School of Software and Electrical Engineering, Swinburne University of Technology, John Street, Hawthorn, Melbourne, VIC 3122, Australia.

Network security is of utmost importance in modern society and therefore receives ever-increasing attention in recent years [6], [7], [24], [25], [33], [37], [40], [44]. In the networked scenario, the exchanged data can be easily exploited by adversaries due to the open network links among sensors, controllers and actuators. A cyber-attack can be regarded as methods, processes, or means used to maliciously attempt to reduce network reliability. According to their implementation types, the cyber-attacks can be generally classified into the Denial-of-Service (DoS) attacks [22], the replay attacks [45] and the deception attacks [5], [13]. Furthermore, via the techniques of dynamic programming or Lyapunov stability theory, some preliminary results concerning security control problems have been reported in the literature, see [1], [12], [22] for the case of DoS attacks and [2], [26], [34] for the case of deception attacks. In addition, from the viewpoint of defenders (for plants), the attacks possess *random nature* since the successes of the attacks largely depends on the *detection ability* of protection equipment or software, the *communication protocols* and the *network conditions* (e.g. network load, network congestion, network transmission rate) that are typically randomly fluctuated. For instance, the secure message in multipath routing protocol with a (T, N) secret sharing scheme can not be recovered if the number of shares is less than T [23]. Recently, some interesting results have been reported in [1], [13] where the random nature of attacks is governed by Bernoulli processes or Markov processes. However, it is still an open and non-trivial work to investigate the security in probability for more general networked control systems. The main challenging could be how to develop an appropriate methodology to analyze the transient dynamics of closed-loop systems subject to both the stochastic nature of addressed systems and the interference signals transmitted by adversaries.

On the other hand, nonlinearities are ubiquitous in practice and therefore the control problem for nonlinear systems has attracted considerable research attention in the past two decades, see [31] for more details. Unfortunately, when the nonlinearities and deception attacks come together for NCSs, the security control issue has become quite intractable due primarily to lack of appropriate methodology. For instance, although significant progress has been made for the input-to-state stability (ISS) theory of continuous-time stochastic nonlinear systems [15], [20], [35], the results for their discrete-time counterparts have been very few. Furthermore, it is desirable to design a controller which not only achieves the security but also guarantees other performance requirements such as the minimization of a quadratic cost function [28].

Note that it is a challenge to determine the extremum of cost functions for nonlinear systems even if the corresponding theoretical basis has been established via the Pontryagin maximum principle or dynamic programming method [4], [43]. Instead, a more realistic way is to seek a suboptimal controller to achieve a bound or approximate value of the given quadratic cost function via matrix inequalities [17] or neural-network-based approaches [41]. It is worth pointing out that, in most available literature concerning suboptimal control issues with a quadratic cost index, the non-Gaussian exogenous disturbances have been overlooked and therefore their effects cannot be taken into adequate consideration. The main reason could be that the desired conditions in the form of Hamilton-Jacobi inequalities or general matrix inequalities cannot be easily derived by exploiting developed approaches. Very recently, a novel average quadratic cost function, which can be utilized to evaluate the impact from disturbances on the cost index, has been proposed in [27] to carry out the guaranteed cost control issue for stochastic linear systems. Unfortunately, to the best of the authors' knowledge, such a cost-guaranteed problem for stochastic nonlinear systems has not been properly investigated yet, not to mention the case where the security requirement is also a major concern. It is, therefore, the purpose of this paper to shorten such a gap.

Towards this end, this paper focuses on the security control problem for a class of discrete-time stochastic nonlinear systems subject to deception attacks. First of all, sufficient conditions in form of matrix inequalities are established to guarantee the prescribed security by employing the discrete-time version of input-to-state stability in probability (ISSiP). Furthermore, a desired upper bound for quadratic cost function is proposed by implementing maximum operation and the control gains can be simultaneously obtained in terms of the solution of a set of matrix inequalities. The main contribution of this paper is threefold: *1) the paper deals with, for the first time, the security control problem with quadratic cost criterion for general stochastic nonlinear systems; 2) in view of ISSiP theory combined with maximum operation, sufficient conditions with the form of matrix inequalities are developed to guarantee the predefined security in probability; 3) both the desired controller gains and the upper bound on evaluated quadratic cost are dependent on the solution of matrix inequalities.*

The rest of this paper is organized as follows. A class of discrete-time stochastic nonlinear systems subject to deception attacks is presented In Section II. By adopting the input-to-state stability in probability, some sufficient conditions are established in Section III to guarantee the desired security performance, while obtain an upper bound of the average quadratic cost criterion. Based on that, controller gains can be obtained successfully for the case of discrete-time stochastic linear systems by solving a set of matrix inequalities with a nonlinear inequality constraint. In Section IV, two examples are presented to demonstrate the effectiveness of the main results. Finally, conclusions are drawn in Section V.

Notation The notation used here is fairly standard except where otherwise stated. $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ denote, respectively, the n-dimensional Euclidean space and the set of all $n\times m$ real matrices. I denotes the identity matrix of compatible dimensions. The notation $X \geq Y$ (respectively, $X > Y$), where X and Y are symmetric matrices, means that $X - Y$ is positive semi-definite (respectively, positive definite). A^T represents the transpose of A. $\lambda_{\max}(A)$ and $\lambda_{\min}(A)$ denote the maximum and minimum eigenvalue of A, respectively. For matrices $A \in \mathbb{R}^{m\times n}$ and $B \in \mathbb{R}^{p\times q}$, their Kronecker product is a matrix in $\mathbb{R}^{mp\times nq}$ denoted by $A \otimes B$. $\mathbb{E}\{x\}$ stands for the expectation of the stochastic variable x. $||x||$ describes the Euclidean norm of a vector x. $\mathrm{diag}\{\cdots\}$ stands for a block-diagonal matrix. $\mathbb{I}_{\mathscr{A}}$ denotes the indicator function of set $\mathscr{A}$. γ^{-1} means the inverse function of the monotone function γ. A function $\gamma : \mathbb{R}^+ \to \mathbb{R}^+$ is said to be of class $\mathscr{K}$, if it is a continuous strictly increasing function with $\gamma(0) = 0$, and is said to be of class $\mathscr{K}_\infty$, if $\gamma \in \mathscr{K}$ with $\gamma(r) \to \infty$ as $r \to \infty$. Finally, a function $\sigma : \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}^+$ is said to be of class $\mathscr{KL}$ if the mapping $\sigma(s, k)$ is of class $\mathscr{K}$ for each fixed k and is decreasing to zero as $k \to \infty$ for each fixed s.

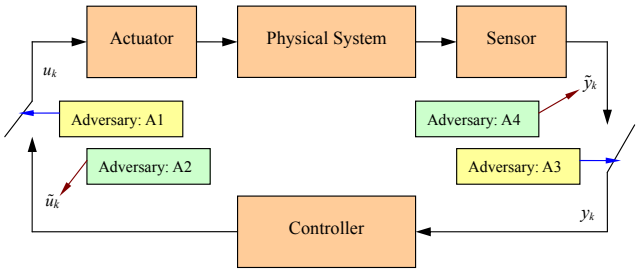


Fig. 1. Attacks on networked control systems [3].

II. Problem Description and Some Preliminaries

Consider the following discrete-time stochastic nonlinear system subject to deception attacks

$$\begin{cases} x_{k+1} = f_1(x_k) + g(x_k)u_k + h_1(x_k)w_k \\ \tilde{y}_k = f_2(x_k) + h_2(x_k)w_k \\ u_k = \tilde{u}_k + \alpha_k r_k \\ y_k = \tilde{y}_k + \sigma_k v_k \end{cases} \tag{1}$$

where $x_k \in \mathbb{R}^{n_x}$, $\tilde{y}_k \in \mathbb{R}^{n_y}$, $y_k \in \mathbb{R}^{n_y}$, $\tilde{u}_k \in \mathbb{R}^{n_u}$ and $u_k \in \mathbb{R}^{n_u}$ are, respectively, the state vectors, the sensor measurements, the *received signals* by the controller subject to attacks, the controller outputs and the actuator inputs subject to attacks. $r_k \in \mathbb{R}^{n_u}$ and $v_k \in \mathbb{R}^{n_y}$ stand for the signals sent by adversaries, and w_k is a one-dimensional, zero-mean Gaussian white noise sequence with $\mathbb{E}\{w_k^2\} = 1$. The stochastic variables α_k and σ_k are two mutually independent Bernoulli-distributed white sequences taking values on 0 or 1 with the following probabilities

$$\begin{aligned} &\mathrm{Prob}\{\alpha_k = 0\} = 1 - \bar{\alpha}, \quad \mathrm{Prob}\{\alpha_k = 1\} = \bar{\alpha} \\ &\mathrm{Prob}\{\sigma_k = 0\} = 1 - \bar{\sigma}, \quad \mathrm{Prob}\{\sigma_k = 1\} = \bar{\sigma}. \end{aligned}$$

The nonlinear functions $f_1 : \mathbb{R}^{n_x} \to \mathbb{R}^{n_x}$, $f_2 : \mathbb{R}^{n_x} \to \mathbb{R}^{n_y}$, $h_1 : \mathbb{R}^{n_x} \to \mathbb{R}^{n_x}$, $h_2 : \mathbb{R}^{n_x} \to \mathbb{R}^{n_y}$ and $g : \mathbb{R}^{n_x} \to \mathbb{R}^{n_u}$ are smooth matrix-valued functions.

Remark 1: Generally speaking, network attacks can be divided into the Denial-of-Service (DoS) attacks and the deception attacks which are shown in Fig. 1. For DoS attacks, the adversary ($A1$ or $A3$) prevents the controller from receiving sensor measurements or the actuators from receiving control commands, that is, $v_k = -\tilde{y}_k$ or $r_k = -\tilde{u}_k$. For deception attacks, the adversary ($A2$ or $A4$) sends false information $v_k = -\tilde{y}_k + \zeta_{2k}$ or $r_k = -\tilde{u}_k + \zeta_{1k}$ to controllers or actuators where ζ_{1k} and ζ_{2k} are the arbitrary bounded energy signals sent by the adversaries.

Remark 2: As discussed in the Introduction, the attack possesses the *random nature* due to the application of *protection equipment or software*, the *communication protocols* and the *network conditions* (e.g. network load, network congestion, network transmission rate). For instance, the false data sent by deception attackers could be identified by using some hardware, software tools, or algorithms (e.g. χ^2 detectors) which leads to a failing attack. In recent years, such a nature for DoS attacks has been addressed by using a Bernoulli distributed process with known statistical information. However, the random nature for deception is overlooked. As such, in this paper, two independent stochastic variables obeying the given Bernoulli distributions are utilized to govern this kind of attack phenomenon.

The dynamic output feedback controller for plant (1) is described by

$$\begin{cases} \hat{x}_{k+1} = f_c(\hat{x}_k) + l_c(\hat{x}_k)y_k \\ \tilde{u}_k = u_c(\hat{x}_k) \end{cases} \tag{2}$$

where $\hat{x}_k$ with $\hat{x}_0 = 0$ is the state estimate, and the matrix-valued functions $f_c : \mathbb{R}^{n_x} \to \mathbb{R}^{n_x}$, $l_c : \mathbb{R}^{n_x} \to \mathbb{R}^{n_y}$ and $u_c : \mathbb{R}^{n_x} \to \mathbb{R}^{n_u}$ are the controller parameters to be determined.

In this paper, the deception attacks r_k and v_k are, respectively, $-u_c(\hat{x}_k)+\zeta_{1k}$ and $-\tilde{y}_k+\zeta_{2k}$ where ζ_{1k} and ζ_{1k} are the bounded energy signals satisfying $||\zeta_{1k}|| + ||\zeta_{2k}|| \leq \varrho$. Here, ϱ is a known positive scalar. By denoting $\eta_k = [\ x_k^T \quad \hat{x}_k^T\ ]^T$, $\zeta_k = [\ \zeta_{1k}^T \quad \zeta_{2k}^T\ ]^T$ and substituting (2) into (1), one has the following closed-loop system

$$\begin{aligned} \eta_{k+1} = {} & \mathcal{F}_1(\eta_k) + (\bar{\sigma} - \sigma_k)\mathcal{F}_2(\eta_k) \\ & + (1-\bar{\alpha})\mathcal{G}_1(\eta_k)u_c(\mathcal{T}\eta_k) \\ & + (\bar{\alpha} - \alpha_k)\mathcal{G}_1(\eta_k)u_c(\mathcal{T}\eta_k) \\ & + \mathcal{H}_1(\eta_k)w_k + (\bar{\sigma} - \sigma_k)\mathcal{H}_2(\eta_k)w_k \\ & + \Lambda^{\alpha\sigma}\mathcal{G}_2(\eta_k)\zeta_k + \Lambda_k^{\alpha\sigma}\mathcal{G}_2(\eta_k)\zeta_k \end{aligned} \tag{3}$$

where

$$\begin{aligned} \mathcal{F}_1(\eta_k) &= \begin{bmatrix} f_1(x_k) \\ f_c(\hat{x}_k) + (1-\bar{\sigma})l_c(\hat{x}_k)f_2(x_k) \end{bmatrix} \\ \mathcal{F}_2(\eta_k) &= [\ 0 \quad f_2^T(x_k)l_c^T(\hat{x}_k)\ ]^T \\ \mathcal{H}_1(\eta_k) &= [\ h_1^T(x_k) \quad (1-\bar{\sigma})h_2^T(x_k)l_c^T(\hat{x}_k)\ ]^T \\ \mathcal{H}_2(\eta_k) &= [\ 0 \quad h_2^T(x_k)l_c^T(\hat{x}_k)\ ]^T \\ \mathcal{G}_1(\eta_k) &= [\ g^T(x_k) \quad 0\ ]^T,\ \mathcal{G}_2(\eta_k) = \mathrm{diag}\{g(x_k), 0\} \\ \mathcal{T} &= [\ 0 \quad I\ ],\quad \Lambda^{\alpha\sigma} = \mathrm{diag}\{\bar{\alpha},\ \bar{\sigma}\} \otimes I, \\ \Lambda_k^{\alpha\sigma} &= \mathrm{diag}\{\alpha_k - \bar{\alpha},\ \sigma_k - \bar{\sigma}\} \otimes I. \end{aligned}$$

Furthermore, associated with the above closed-loop system, consider a quadratic cost functional of the form

$$\mathcal{J}(u_c) = \limsup_{N\to\infty} \frac{1}{2N} \sum_{k=0}^{N} \mathbb{E}\Big\{ \eta_k^T \mathcal{Q}\eta_k + u_c^T(\mathcal{T}\eta_k)\mathcal{R}u_c(\mathcal{T}\eta_k) \Big| \mathscr{F}_0 \Big\} \tag{4}$$

where $\mathcal{Q} \in \mathbb{R}^{2n_x \times 2n_x}$ and $\mathcal{R} \in \mathbb{R}^{n_u \times n_u}$ are two given positive-definite weighting matrices.

Before proceeding further, we introduce the following definitions.

Definition 1: [8] Let the positive scalar ε be given. The system (3) is said to be input-to-state stable with probability $1-\varepsilon$ if there exist functions $\varphi \in \mathscr{KL}$ and $\gamma \in \mathscr{K}$ such that the system dynamic η_k satisfies

$$\mathrm{Prob}\big\{ ||\eta_k|| \leq \varphi(||\eta_0||, k) + \gamma(\|\zeta_k\|_\infty) \big\} \geq 1 - \varepsilon \tag{5}$$

for $\forall k \geq 0$ and $\forall \eta_0 \in \mathbb{R}^{2n_x} \backslash \{0\}$ where $\|\zeta_k\|_\infty := \sup_k\{||\zeta_k||\}$.

Definition 2: Given a security parameter $\vartheta > 0$ and a positive scalar $\varepsilon > 0$, the system (1) subject to deception attacks is secure with probability $1-\varepsilon$ if the system dynamic x_k satisfies

$$\mathrm{Prob}\big\{ ||x_k|| \leq \vartheta \big\} \geq 1 - \varepsilon, \quad \forall k \geq 0. \tag{6}$$

Definition 3: Let the security parameter $\vartheta > 0$ be given. The system (1) subject to deception attacks is said to be ε-securable if there exist three matrix-valued functions f_c, l_c and u_c in the dynamic output feedback controller (2) such that the security requirement $||x_k|| \leq \vartheta$ can be satisfied with probability $1-\varepsilon$.

In this paper, we aim to design the controller parameters f_c, l_c and u_c for the dynamic output feedback controller (2) such that the closed-loop system (3) is secure with probability $1-\varepsilon$ and an upper bounded is obtained for the given quadratic cost functional (4).

III. Main Results

In this section, by resorting to the stochastic analysis approach, some sufficient conditions are provided to guarantee the desired security while obtaining an upper bound of the addressed quadratic cost criterion. Furthermore, the obtained results are extended to the case of discrete-time stochastic linear systems with state-dependent noises. The following three lemmas will be used in deriving our main results.

Lemma 1: [8] Let the positive scalar ε be given. The closed-loop system (3) is input-to-state stable with probability $1-\varepsilon$ if there exist a positive definite function $\mathcal{V} : \mathbb{R}^n \to \mathbb{R}$ (called an ISSiP-Lyapunov function), two $\mathscr{K}_\infty$ class functions $\underline{\nu}$ and $\bar{\nu}$, and two $\mathscr{K}$ class functions $\tilde{\chi}$ and $\tilde{\nu}$ such that, for all $\eta_k \in \mathbb{R}^{2n_x} \setminus \{0\}$, the following two inequalities hold

$$\underline{\nu}(||\eta_k||) \leq \mathcal{V}(\eta_k) \leq \bar{\nu}(||\eta_k||) \tag{7}$$

$$\mathbb{E}\{\mathcal{V}(\eta_{k+1})\big|\mathscr{F}_k\} - \mathcal{V}(\eta_k) \leq \tilde{\chi}(\|\zeta_k\|_\infty) - \tilde{\nu}(||\eta_k||). \tag{8}$$

Furthermore, if (7) and (8) hold, then the functions φ and γ in Definition 1 can be, respectively, selected as

$$\varphi(\cdot, k) = \sqrt{\underline{\nu}^{-1}(\varepsilon^{-1}\phi^k\bar{\nu}(\cdot))}$$

and

$$\gamma(\cdot)=\sqrt{\underline{\nu}^{-1}\big(\varepsilon^{-1}\big(\bar{\nu}(\tilde{\nu}^{-1}(\tilde{\chi}(\cdot)))+\tilde{\chi}(\cdot)\big)\big)}$$

where ϕ is a suitable scalar satisfying $0<\phi<1$.

Lemma 2: [38] Let $\mathscr{F}_0$ be a σ sub-field of $\mathscr{F}_1$ and X be an integrable random variable. The following is true

$$\mathbb{E}\{\mathbb{E}\{X|\mathscr{F}_0\}|\mathscr{F}_1\}=\mathbb{E}\{X|\mathscr{F}_0\}=\mathbb{E}\{\mathbb{E}\{X|\mathscr{F}_1\}|\mathscr{F}_0\}.$$

Lemma 3: [36] (Matrix Inverse Lemma) Let X, Y, U and V be given matrices with appropriate dimensions. If X, Y and $Y^{-1}+VX^{-1}U$ are invertible, then the following holds

$$(X+UYV)^{-1}=X^{-1}-X^{-1}U(Y^{-1}+VX^{-1}U)^{-1}VX^{-1}.$$

The following theorem provides a sufficient condition on security control with predefined probability $1-\varepsilon$. In addition, under the given parameters, an upper bound of quadratic cost is obtained at the same time.

Theorem 1: Assume that scalars ε and ϑ, matrices $\mathcal{Q}$ and $\mathcal{R}$, and the controller parameters f_c, l_c and u_c are known. The stochastic nonlinear system (1) with the dynamic output feedback controller (2) is secure with probability $1-\varepsilon$ and the quadratic cost functional (4) has the upper bound $\mathcal{J}^*=0.5(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2$, if there are two positive definite matrices $\mathcal{P}$ and $\mathcal{W}$, and three positive scalars ν, χ and κ such that, for all nonzero $\eta\in\mathbb{R}^{2n_x}$, matrix inequalities

$$\begin{cases}\Gamma_1(\eta)<-\nu||\eta||^2 & \text{(9a)}\\ \Gamma_2(\eta)<\chi I & \text{(9b)}\\ \Pi_0(\eta)<\mathcal{W} & \text{(9c)}\\ \Pi_2(\eta)<0 & \text{(9d)}\end{cases}$$

and

$$\begin{aligned}&||x_0||\sqrt{\varepsilon^{-1}\lambda_{\min}^{-1}(\mathcal{P})\lambda_{\max}(\mathcal{P})}\\&\quad+\varrho\sqrt{\varepsilon^{-1}\chi\lambda_{\min}^{-1}(\mathcal{P})\big(\nu^{-1}\lambda_{\max}(\mathcal{P})+1\big)}\le\vartheta\end{aligned}\tag{10}$$

hold, where

$$\begin{aligned}\mathcal{A}(\eta)&=\mathcal{F}_1(\eta)+(1-\bar{\alpha})\mathcal{G}_1(\eta)u_c(\mathcal{T}\eta)\\ \mathcal{M}_1&=\text{diag}\{I,\ 0\},\ \mathcal{M}_2:=\text{diag}\{0,\ I\}\\ \Gamma_0(\eta)&=\mathcal{A}^T(\eta)\mathcal{P}\mathcal{A}(\eta)+\tilde{\sigma}\mathcal{F}_2^T(\eta)\mathcal{P}\mathcal{F}_2(\eta)-\eta^T\mathcal{P}\eta\\&\quad+\tilde{\alpha}u_c^T(\mathcal{T}\eta)\mathcal{G}_1^T(\eta)\mathcal{P}\mathcal{G}_1(\eta)u_c(\mathcal{T}\eta)\\&\quad+\mathcal{H}_1^T(\eta)\mathcal{P}\mathcal{H}_1(\eta)+\tilde{\sigma}\mathcal{H}_2^T(\eta)\mathcal{P}\mathcal{H}_2(\eta)\\ \Gamma_1(\eta)&=\Gamma_0(\eta)+\tilde{\sigma}\kappa\mathcal{F}_2^T(\eta)\mathcal{P}\mathcal{F}_2(\eta)+\kappa\mathcal{A}^T(\eta)\mathcal{P}\mathcal{A}(\eta)\\&\quad+\tilde{\alpha}\kappa u_c^T(\mathcal{T}\eta)\mathcal{G}_1^T(\eta)\mathcal{P}\mathcal{G}_1(\eta)u_c(\mathcal{T}\eta)\\ \Gamma_2(\eta)&=(1+\kappa^{-1})\mathcal{G}_2^T(\eta)\Big((\Lambda^{\alpha\sigma})^T\mathcal{P}\Lambda^{\alpha\sigma}\\&\quad+\tilde{\alpha}\mathcal{M}_1^T\mathcal{P}\mathcal{M}_1+\tilde{\sigma}\mathcal{M}_2^T\mathcal{P}\mathcal{M}_2\Big)\mathcal{G}_2(\eta)\\ \Pi_0(\eta)&=\mathcal{G}_2^T(\eta)\Big((\Lambda^{\alpha\sigma})^T\mathcal{P}\Lambda^{\alpha\sigma}\\&\quad+\tilde{\alpha}\mathcal{M}_1^T\mathcal{P}\mathcal{M}_1+\tilde{\sigma}\mathcal{M}_2^T\mathcal{P}\mathcal{M}_2\Big)\mathcal{G}_2(\eta)\\ \Pi_1(\eta)&=\mathcal{A}^T(\eta)\mathcal{P}\Lambda^{\alpha\sigma}\mathcal{G}_2(\eta)-\tilde{\sigma}\mathcal{F}_2^T(\eta)\mathcal{P}\mathcal{M}_2\mathcal{G}_2(\eta)\\&\quad-\tilde{\alpha}u_c^T(\mathcal{T}\eta)\mathcal{G}_1^T(\eta)\mathcal{P}\mathcal{M}_1\mathcal{G}_2(\eta)\\ \Pi_2(\eta)&=\Gamma_0(\eta)-\nu||\eta||^2+\eta^T\mathcal{Q}\eta+u_c^T(\mathcal{T}\eta)\mathcal{R}u_c(\mathcal{T}\eta)\\&\quad+\Pi_1(\eta)\big(\mathcal{W}-\Pi_0(\eta)\big)^{-1}\Pi_1^T(\eta).\end{aligned}$$

Proof: First, it can be calculated that

$$\begin{aligned}\mathbb{E}\big\{(\bar{\alpha}-\alpha_k)\mathcal{P}\Lambda_k^{\alpha\sigma}\big\}&=-\tilde{\alpha}\mathcal{P}\mathcal{M}_1\\ \mathbb{E}\big\{(\bar{\sigma}-\sigma_k)\mathcal{P}\Lambda_k^{\alpha\sigma}\big\}&=-\tilde{\sigma}\mathcal{P}\mathcal{M}_2.\end{aligned}$$

In what follows, choose the Lyapunov function $\mathcal{V}(\eta_k)=\eta_k^T\mathcal{P}\eta_k$. We can easily check that the condition (7) is true when selecting functions $\underline{\nu}(||\eta_k||)=\lambda_{\min}(\mathcal{P})||\eta_k||^2$ and $\bar{\nu}(||\eta_k||)=\lambda_{\max}(\mathcal{P})||\eta_k||^2$. By calculating the difference of $V(\eta_k)$ along the trajectory of the closed-loop system (3) and taking the mathematical expectation, one has

$$\begin{aligned}&\mathbb{E}\{\mathcal{V}(\eta_{k+1})-\mathcal{V}(\eta_k)|\mathscr{F}_k\}\\&=\mathbb{E}\Big\{\eta_{k+1}^T\mathcal{P}\eta_{k+1}-\eta_k^T\mathcal{P}\eta_k|\mathscr{F}_k\Big\}\\&=\mathcal{F}_1^T(\eta_k)\mathcal{P}\mathcal{F}_1(\eta_k)+2\mathcal{F}_1^T(\eta_k)\mathcal{P}\Lambda^{\alpha\sigma}\mathcal{G}_2(\eta_k)\zeta_k\\&\quad+2(1-\bar{\alpha})\mathcal{F}_1^T(\eta_k)\mathcal{P}\mathcal{G}_1(\eta_k)u_c(\mathcal{T}\eta_k)\\&\quad+\tilde{\sigma}\mathcal{F}_2^T(\eta_k)\mathcal{P}\mathcal{F}_2(\eta_k)-2\tilde{\sigma}\mathcal{F}_2^T(\eta_k)\mathcal{P}\mathcal{M}_2\mathcal{G}_2(\eta_k)\zeta_k\\&\quad+(1-\bar{\alpha})u_c^T(\mathcal{T}\eta_k)\mathcal{G}_1^T(\eta_k)\mathcal{P}\mathcal{G}_1(\eta_k)u_c(\mathcal{T}\eta_k)\\&\quad+2(1-\bar{\alpha})u_c^T(\mathcal{T}\eta_k)\mathcal{G}_1^T(\eta_k)\mathcal{P}\Lambda^{\alpha\sigma}\mathcal{G}_2(\eta_k)\zeta_k\\&\quad-2\tilde{\alpha}u_c^T(\mathcal{T}\eta_k)\mathcal{G}_1^T(\eta_k)\mathcal{P}\mathcal{M}_1\mathcal{G}_2(\eta_k)\zeta_k\\&\quad+\mathcal{H}_1^T(\eta_k)\mathcal{P}\mathcal{H}_1(\eta_k)+\tilde{\sigma}\mathcal{H}_2^T(\eta_k)\mathcal{P}\mathcal{H}_2(\eta_k)\\&\quad+\zeta_k^T\mathcal{G}_2^T(\eta_k)(\Lambda^{\alpha\sigma})^T\mathcal{P}\Lambda^{\alpha\sigma}\mathcal{G}_2(\eta_k)\zeta_k\\&\quad+\tilde{\alpha}\zeta_k^T\mathcal{G}_2^T(\eta_k)\mathcal{M}_1^T\mathcal{P}\mathcal{M}_1\mathcal{G}_2(\eta_k)\zeta_k\\&\quad+\tilde{\sigma}\zeta_k^T\mathcal{G}_2^T(\eta_k)\mathcal{M}_2^T\mathcal{P}\mathcal{M}_2\mathcal{G}_2(\eta_k)\zeta_k-\eta_k^T\mathcal{P}\eta_k\\&=\Gamma_0(\eta_k)+2\Pi_1(\eta_k)\zeta_k+\zeta_k^T\Pi_0(\eta_k)\zeta_k.\end{aligned}\tag{11}$$

Applying the element inequality $2a^Tb\le\kappa a^Ta+\kappa^{-1}b^Tb$ to the term $2\Pi_1(\eta_k)\zeta_k$ yields

$$\begin{aligned}&2\Pi_1(\eta_k)\zeta_k\\&=2\mathcal{A}^T(\eta_k)\mathcal{P}\Lambda^{\alpha\sigma}\mathcal{G}_2(\eta_k)\zeta_k-2\tilde{\sigma}\mathcal{F}_2^T(\eta_k)\mathcal{P}\mathcal{M}_2\mathcal{G}_2(\eta_k)\zeta_k\\&\quad-2\tilde{\alpha}u_c^T(\mathcal{T}\eta_k)\mathcal{G}_1^T(\eta)\mathcal{P}\mathcal{M}_1\mathcal{G}_2(\eta_k)\zeta_k\\&\le\kappa\mathcal{A}^T(\eta_k)\mathcal{P}\mathcal{A}(\eta_k)+\tilde{\alpha}\kappa u_c^T(\mathcal{T}\eta_k)\mathcal{G}_1^T(\eta_k)\mathcal{P}\mathcal{G}_1(\eta_k)u_c(\mathcal{T}\eta_k)\\&\quad+\tilde{\sigma}\kappa\mathcal{F}_2^T(\eta_k)\mathcal{P}\mathcal{F}_2(\eta_k)+\kappa^{-1}\zeta_k^T\mathcal{G}_2^T(\eta_k)\Big((\Lambda^{\alpha\sigma})^T\mathcal{P}\Lambda^{\alpha\sigma}\\&\quad+\tilde{\alpha}\mathcal{M}_1^T\mathcal{P}\mathcal{M}_1+\tilde{\sigma}\mathcal{M}_2^T\mathcal{P}\mathcal{M}_2\Big)\mathcal{G}_2(\eta_k)\zeta_k.\end{aligned}\tag{12}$$

Furthermore, taking the above equality into consideration, (11) results in

$$\begin{aligned}&\mathbb{E}\{\mathcal{V}(\eta_{k+1})-\mathcal{V}(\eta_k)|\mathscr{F}_k\}\\&\le\Gamma_1(\eta_k)+\zeta_k^T\Gamma_2(\eta_k)\zeta_k\le-\nu||\eta_k||^2+\chi||\zeta_k||_\infty^2\end{aligned}\tag{13}$$

which means that the second condition (8) from Lemma 1 can be also guaranteed. Therefore, the closed-loop system (3) is input-to-state stable with probability $1-\varepsilon$.

Now, let us select

$$\begin{aligned}\varphi(||\eta_0||,0)&=\sqrt{\varepsilon^{-1}\lambda_{\min}^{-1}(\mathcal{P})\lambda_{\max}(\mathcal{P})}||\eta_0||\\ \gamma(||\zeta_k||_\infty)&=\sqrt{\varepsilon^{-1}\chi\lambda_{\min}^{-1}(\mathcal{P})\big(\nu^{-1}\lambda_{\max}(\mathcal{P})+1\big)}||\zeta_k||_\infty.\end{aligned}$$

It can be found from (10) that

$$\begin{aligned}||x_k||\le||\eta_k||&\le\varphi(||\eta_0||,k)+\gamma(\|\zeta_k\|_\infty)\\&\le\varphi(||\eta_0||,0)+\gamma(\|\zeta_k\|_\infty)\\&=\varphi(||x_0||,0)+\gamma(\|\zeta_k\|_\infty)\le\vartheta\end{aligned}\tag{14}$$

which means

$$\text{Prob}\big\{||x_k|| \le \vartheta\big\} \ge 1-\varepsilon, \quad \forall k \ge 0.$$

As such, it is easily concluded that the closed-loop system (3) is secure with probability $1-\varepsilon$.

Having obtained the analysis results about the security, we are now in a position to investigate the quadratic cost functional (4). For this purpose, denote

$$\begin{aligned}\zeta_k^* &= \big(\mathcal{W}-\Pi_0(\eta_k)\big)^{-1}\Pi_1^T(\eta_k),\\ \Xi_1(\eta_k) &= \Gamma_0(\eta_k)+\eta_k^T\mathcal{Q}\eta_k+u_c^T(\mathcal{T}\eta_k)\mathcal{R}u_c(\mathcal{T}\eta_k)-\nu||\eta_k||^2.\end{aligned}$$

By utilizing the properties of the conditional expectation, one can show that

$$\begin{aligned}
&\mathbb{E}\Big\{2\mathcal{V}(\eta_{k+1})-2\mathcal{V}(\eta_k)\\
&\quad+\eta_k^T\mathcal{Q}\eta_k+u_c^T(\mathcal{T}\eta_k)\mathcal{R}u_c(\mathcal{T}\eta_k)\Big|\mathscr{F}_k\Big\}\\
&=\mathbb{E}\Big\{\Big[2\mathcal{V}(\eta_{k+1})-2\mathcal{V}(\eta_k)+\eta_k^T\mathcal{Q}\eta_k\\
&\quad+u_c^T(\mathcal{T}\eta_k)\mathcal{R}u_c(\mathcal{T}\eta_k)\Big]\mathbb{I}_{||\zeta_k||\le\varrho}\Big|\mathscr{F}_k\Big\}\\
&\le\mathbb{E}\Big\{\Big[\mathcal{V}(\eta_{k+1})-\mathcal{V}(\eta_k)-\nu||\eta_k||^2+\chi||\zeta_k||_\infty^2\\
&\quad+\eta_k^T\mathcal{Q}\eta_k+u_c^T(\mathcal{T}\eta_k)\mathcal{R}u_c^T(\mathcal{T}\eta_k)\Big]\mathbb{I}_{||\zeta_k||\le\varrho}\Big|\mathscr{F}_k\Big\}\\
&=\mathbb{E}\Big\{\Big[\Gamma_0(\eta_k)-\nu||\eta_k||^2+2\Pi_1(\eta_k)\zeta_k\\
&\quad+\zeta_k^T\big(\Pi_0(\eta_k)-\mathcal{W}\big)\zeta_k+u_c^T(\mathcal{T}\eta_k)\mathcal{R}u_c(\mathcal{T}\eta_k)\\
&\quad+\eta_k^T\mathcal{Q}\eta_k+\zeta_k^T\mathcal{W}\zeta_k+\chi||\zeta_k||_\infty^2\Big]\mathbb{I}_{||\zeta_k||\le\varrho}\Big|\mathscr{F}_k\Big\} \qquad (15)\\
&\le\max_{||\zeta_k||\le\varrho}\Big\{\Gamma_0(\eta_k)-\nu||\eta_k||^2+2\Pi_1(\eta_k)\zeta_k\\
&\quad+\zeta_k^T\big(\Pi_0(\eta_k)-\mathcal{W}\big)\zeta_k+\eta_k^T\mathcal{Q}\eta_k\\
&\quad+u_c^T(\mathcal{T}\eta_k)\mathcal{R}u_c(\mathcal{T}\eta_k)+\zeta_k^T\mathcal{W}\zeta_k+\chi||\zeta_k||_\infty^2\Big\}\\
&\le\max_{||\zeta_k||\le\varrho}\Big\{\Xi_1(\eta_k)+2\Pi_1(\eta_k)\zeta_k-\zeta_k^T\big(\mathcal{W}-\Pi_0(\eta_k)\big)\\
&\quad\times\zeta_k\Big\}+(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2\\
&\le\max_{\zeta_k}\Big\{\Pi_2(\eta_k)-(\zeta_k-\zeta_k^*)^T\big(\mathcal{W}-\Pi_0(\eta_k)\big)\\
&\quad\times(\zeta_k-\zeta_k^*)\Big\}+(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2\\
&\le\Pi_2(\eta_k)+(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2.
\end{aligned}$$

Furthermore, it follows from (15) and Lemma 2 that

$$\begin{aligned}
&\sup\sum_{k=0}^{N}\mathbb{E}\Big\{\eta_k^T\mathcal{Q}\eta_k+u_c^T(\mathcal{T}\eta_k)\mathcal{R}u_c(\mathcal{T}\eta_k)\Big|\mathscr{F}_0\Big\}\\
&\le\sup\sum_{k=0}^{N}\mathbb{E}\Big\{\Pi_2(\eta_k)+(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2\\
&\quad-2\mathbb{E}\big\{\mathcal{V}(\eta_{k+1})-\mathcal{V}(\eta_k)|\mathscr{F}_k\big\}\Big|\mathscr{F}_0\Big\} \qquad (16)\\
&\le 2\mathcal{V}(\eta_0)+(N+1)(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2\\
&\quad-\inf\Big\{2\mathbb{E}\big\{\mathcal{V}(\eta_{N+1})|\mathscr{F}_0\big\}\Big\}\\
&\le 2\mathcal{V}(\eta_0)+(N+1)(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2
\end{aligned}$$

which implies

$$\begin{aligned}
\mathcal{J}(u_c)&\le\limsup_{N\to\infty}\frac{1}{2N}\Big(2\mathcal{V}(\eta_0)+(N+1)(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2\Big)\\
&=\frac{(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2}{2}.
\end{aligned}$$

The proof is complete.

Remark 3: The developed result in Theorem 1 includes a nonlinear constraint dependent on initial state, which intuitively describes the security bound. In addition, by exploiting the difference $2\mathcal{V}(\eta_{k+1})-2\mathcal{V}(\eta_k)$ to (15), the condition of security (9a) is skillfully embedded into the analysis of the quadratic cost functional index (4). Such an approach is of importance to gain an upper bound of $\mathcal{J}(u_c)$.

From the purpose of implementation, a linear time-invariant controller is usually employed in real-world systems. Therefore, we are interested to expose that the above developed result can be specialized to the systems with the linear output feedback controller which is of the form

$$\begin{cases}\hat{x}_{k+1}=F_c\hat{x}_k+L_cy_k\\ \tilde{u}_k=K\hat{x}_k\end{cases} \qquad (17)$$

where controller parameters F_c, L_c and K need to be determined. By replacing $f_c(\hat{x}_k)$, $l_c(\hat{x}_k)$ and $u_c(\hat{x}_k)$ with $F_c\hat{x}_k$, L_c and $K\hat{x}_k$, respectively, one has the following theorem.

Theorem 2: Assume that scalars ε and ϑ, matrices $\mathcal{Q}$ and $\mathcal{R}$, and parameters F_c, L_c and K are known. The stochastic nonlinear system (1) with the dynamic output feedback controller (17) is secure with probability $1-\varepsilon$ and the quadratic cost functional (4) has the upper bound $\mathcal{J}^*=0.5(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2$, if there exist two positive definite matrices $\mathcal{P}$ and $\mathcal{W}$, and three positive scalars ν, χ and κ such that, for all nonzero $\eta=[\,x^T,\,\hat{x}^T\,]^T\in\mathbb{R}^{2n_x}$, matrix inequalities

$$\begin{cases}\bar{\Gamma}_1(\eta)<-\nu||\eta||^2 & (18a)\\ \bar{\Gamma}_2(\eta)<\chi I & (18b)\\ \bar{\Pi}_0(\eta)<\mathcal{W} & (18c)\\ \bar{\Pi}_2(\eta)<0 & (18d)\\ I\otimes\mathcal{P}^{-1}-\mathscr{G}_2(\eta)\mathcal{W}^{-1}\mathscr{G}_2^T(\eta)>0 & (18e)\end{cases}$$

and

$$\begin{aligned}&||x_0||\sqrt{\varepsilon^{-1}\lambda_{\min}^{-1}(\mathcal{P})\lambda_{\max}(\mathcal{P})}\\ &\quad+\varrho\sqrt{\varepsilon^{-1}\chi\lambda_{\min}^{-1}(\mathcal{P})\big(\nu^{-1}\lambda_{\max}(\mathcal{P})+1\big)}\le\vartheta\end{aligned} \qquad (19)$$

hold, where

$$\begin{aligned}
\bar{\mathcal{A}}(\eta) =& \begin{bmatrix} f_1(x)+(1-\bar{\alpha})g(x)K\hat{x} \\ F_c\hat{x}+(1-\bar{\sigma})L_cf_2(x) \end{bmatrix} \\
\bar{\mathcal{G}}_1(\eta) =& \begin{bmatrix} g^T(x) & 0 \end{bmatrix}^T,\ \bar{\mathcal{G}}_2(\eta) = \text{diag}\{g(x), L_c\} \\
\bar{\mathcal{F}}_2(\eta) =& \begin{bmatrix} 0 & f_2^T(x)L_c^T \end{bmatrix}^T,\ \bar{\mathcal{H}}_2(\eta) = \begin{bmatrix} 0 & h_2^T(x)L_c^T \end{bmatrix}^T \\
\bar{\mathcal{H}}_1(\eta) =& \begin{bmatrix} h_1^T(x) & (1-\bar{\sigma})h_2^T(x)L_c^T \end{bmatrix}^T, \\
\mathscr{A}(\eta) =& \begin{bmatrix} \bar{\mathcal{A}}^T(\eta) & \sqrt{\tilde{\alpha}}\eta^T\mathcal{T}^TK^T\mathcal{G}_1^T(\eta) & \sqrt{\tilde{\sigma}}\bar{\mathcal{F}}_2^T(\eta) \end{bmatrix}^T \\
\mathscr{G}(\eta) =& \begin{bmatrix} \bar{\mathcal{G}}_2^T(\eta)(\Lambda^{\alpha\sigma})^T & -\sqrt{\tilde{\alpha}}\bar{\mathcal{G}}_2^T(\eta)\mathcal{M}_1^T & -\sqrt{\tilde{\sigma}}\bar{\mathcal{G}}_2^T(\eta)\mathcal{M}_2^T \end{bmatrix}^T \\
\bar{\Gamma}_1(\eta) =& (1+\kappa)\mathscr{A}^T(\eta)(I\otimes\mathcal{P})\mathscr{A}(\eta) - \eta^T\mathcal{P}\eta \\
& + \bar{\mathcal{H}}_1^T(\eta)\mathcal{P}\bar{\mathcal{H}}_1(\eta) + \tilde{\sigma}\bar{\mathcal{H}}_2^T(\eta)\mathcal{P}\bar{\mathcal{H}}_2(\eta) \\
\bar{\Gamma}_2(\eta) =& (1+\kappa^{-1})\mathscr{G}^T(\eta)(I\otimes\mathcal{P})\mathscr{G}(\eta) \\
\bar{\Pi}_0(\eta) =& \mathscr{G}^T(\eta)(I\otimes\mathcal{P})\mathscr{G}(\eta),\ \tilde{\alpha} = \bar{\alpha}(1-\bar{\alpha}) \\
\bar{\Pi}_1(\eta) =& \mathscr{A}^T(\eta)(I\otimes\mathcal{P})\mathscr{G}(\eta),\ \tilde{\beta} = \bar{\beta}(1-\bar{\beta})
\end{aligned}$$

$$\begin{aligned}
\bar{\Pi}_2(\eta) =& \mathscr{A}^T(\eta)\big((I\otimes\mathcal{P})^{-1} - \mathscr{G}(\eta)\mathcal{W}^{-1}\mathscr{G}^T(\eta)\big)^{-1} \\
& \times \mathscr{A}(\eta) - \eta^T\mathcal{P}\eta - \nu\eta^T\eta + \bar{\mathcal{H}}_1^T(\eta)\mathcal{P}\bar{\mathcal{H}}_1(\eta) \\
& + \tilde{\sigma}\bar{\mathcal{H}}_2^T(\eta)\mathcal{P}\bar{\mathcal{H}}_2(\eta) + \eta^T\mathcal{T}^TK\mathcal{R}K\mathcal{T}\eta + \eta^T\mathcal{Q}\eta.
\end{aligned}$$

Proof: Based on Theorem 1, it suffices to show that (9a)-(9d) are satisfied for the stochastic nonlinear system (1) with the dynamic output feedback controller (17).

First, taking (17) into consideration, one has

$$\begin{aligned}
\Gamma_0(\eta) =& \bar{\mathcal{A}}^T(\eta)\mathcal{P}\bar{\mathcal{A}}(\eta) + \tilde{\sigma}\bar{\mathcal{F}}_2^T(\eta)\mathcal{P}\bar{\mathcal{F}}_2(\eta) - \eta^T\mathcal{P}\eta \\
& + \tilde{\alpha}\eta^T\mathcal{T}^TK^T\bar{\mathcal{G}}_1^T(\eta)\mathcal{P}\bar{\mathcal{G}}_1(\eta)K\mathcal{T}\eta \\
& + \bar{\mathcal{H}}_1^T(\eta)\mathcal{P}\bar{\mathcal{H}}_1(\eta) + \tilde{\sigma}\bar{\mathcal{H}}_2^T(\eta)\mathcal{P}\bar{\mathcal{H}}_2(\eta) \\
=& \mathscr{A}^T(\eta)(I\otimes\mathcal{P})\mathscr{A}(\eta) - \eta^T\mathcal{P}\eta \\
& + \bar{\mathcal{H}}_1^T(\eta)\mathcal{P}\bar{\mathcal{H}}_1(\eta) + \tilde{\sigma}\bar{\mathcal{H}}_2^T(\eta)\mathcal{P}\bar{\mathcal{H}}_2(\eta), \\
\Gamma_1(\eta) =& \Gamma_0(\eta) + \tilde{\sigma}\kappa\bar{\mathcal{F}}_2^T(\eta)\mathcal{P}\bar{\mathcal{F}}_2(\eta) + \kappa\bar{\mathcal{A}}^T(\eta)\mathcal{P}\bar{\mathcal{A}}(\eta) \\
& + \tilde{\alpha}\kappa\eta^T\mathcal{T}^TK^T\bar{\mathcal{G}}_1^T(\eta)\mathcal{P}\bar{\mathcal{G}}_1(\eta)K\mathcal{T}\eta, \\
\Gamma_2(\eta) =& (1+\kappa^{-1})\bar{\mathcal{G}}_2^T(\eta)\Big((\Lambda^{\alpha\sigma})^T\mathcal{P}\Lambda^{\alpha\sigma} \\
& + \tilde{\alpha}\mathcal{M}_1^T\mathcal{P}\mathcal{M}_1 + \tilde{\sigma}\mathcal{M}_2^T\mathcal{P}\mathcal{M}_2\Big)\bar{\mathcal{G}}_2(\eta) \\
=& (1+\kappa^{-1})\mathscr{G}^T(\eta)(I\otimes\mathcal{P})\mathscr{G}(\eta).
\end{aligned} \tag{20}$$

Obviously, the inequalities (9a) and (9b) in Theorem 1 follow directly from (18a) and (18b), respectively.

Similarly, it can be found that

$$\begin{aligned}
\Pi_0(\eta) =& \mathscr{G}^T(\eta)(I\otimes\mathcal{P})\mathscr{G}(\eta), \\
\Pi_1(\eta) =& \bar{\mathcal{A}}^T(\eta)\mathcal{P}\Lambda^{\alpha\sigma}\bar{\mathcal{G}}_2(\eta) - \tilde{\sigma}\bar{\mathcal{F}}_2^T(\eta)\mathcal{P}\mathcal{M}_2\bar{\mathcal{G}}_2(\eta) \\
& - \tilde{\alpha}\eta^T\mathcal{T}^TK^T\bar{\mathcal{G}}_1^T(\eta)\mathcal{P}\mathcal{M}_1\bar{\mathcal{G}}_2(\eta) \\
=& \mathscr{A}^T(\eta)(I\otimes\mathcal{P})\mathscr{G}(\eta).
\end{aligned} \tag{21}$$

On the other hand, it follows that

$$\begin{aligned}
\Pi_4(\eta) =& \Pi_1(\eta)\big(\mathcal{W} - \Pi_0(\eta)\big)^{-1}\Pi_1^T(\eta) \\
=& \mathscr{A}^T(\eta)(I\otimes\mathcal{P})\mathscr{G}(\eta)\Big(\mathcal{W} - \mathscr{G}^T(\eta) \\
& \times (I\otimes\mathcal{P})\mathscr{G}(\eta)\Big)^{-1}\mathscr{G}^T(\eta)(I\otimes\mathcal{P})\mathscr{A}(\eta).
\end{aligned} \tag{22}$$

In light of (18e), based on Lemma 3, $\Pi_4(\eta)$ is equivalent to

$$\begin{aligned}
\Pi_4(\eta) =& \mathscr{A}^T(\eta)\Big((I\otimes\mathcal{P})^{-1} - \mathscr{G}(\eta)\mathcal{W}^{-1}\mathscr{G}^T(\eta)\Big)^{-1} \\
& \times \mathscr{A}(\eta) - \mathscr{A}^T(\eta)(I\otimes\mathcal{P})\mathscr{A}(\eta),
\end{aligned} \tag{23}$$

and therefore, it follows from (20) and (23) that

$$\begin{aligned}
\Pi_2(\eta) =& \mathscr{A}^T(\eta)\Big((I\otimes\mathcal{P})^{-1} - \mathscr{G}(\eta)\mathcal{W}^{-1}\mathscr{G}^T(\eta)\Big)^{-1} \\
& \times \mathscr{A}(\eta) - \eta^T\mathcal{P}\eta - \nu\eta^T\eta \\
& + \bar{\mathcal{H}}_1^T(\eta)\mathcal{P}\bar{\mathcal{H}}_1(\eta) + \tilde{\sigma}\bar{\mathcal{H}}_2^T(\eta)\mathcal{P}\bar{\mathcal{H}}_2(\eta) \\
& + \eta^T\mathcal{T}^TK\mathcal{R}K\mathcal{T}\eta + \eta^T\mathcal{Q}\eta.
\end{aligned} \tag{24}$$

It is not difficult to see from (21) and (24) that the inequalities (9c) and (9d) in Theorem 1 follow directly from (18c) and (18d). As such, it can be concluded from Theorem 1 that the desired security for the closed-loop system (3) are achieved and the cost functional (4) has the bound $\mathcal{J}^* = 0.5(\chi + \lambda_{\max}(\mathcal{W}))\varrho^2$, which completes the proof.

Now, we are in a position to extend the developed results to the case of discrete-time stochastic linear systems with state-dependent noises

$$\begin{cases} x_{k+1} = Ax_k + Bu_k + Dx_kw_k \\ \tilde{y}_k = Cx_k + Ex_kw_k \end{cases} \tag{25}$$

where A, B, C, D and E are constant matrices with appropriate dimensions. It is assumed that B is of column full rank.

Subsequently, by selecting $\chi = (1+\kappa^{-1})\lambda_{\max}(\mathcal{W})$, one has that (18b) holds if (18c) is true. Furthermore, by replacing $f_1(x_k)$, $g(x_k)$, $f_2(x_k)$, $h_1(x_k)$ and $h_2(x_k)$ with Ax_k, B, Cx_k, Dx_k and Ex_k, respectively, the following theorem can be obtained immediately from Theorem 2.

Theorem 3: Assume that scalars ε and ϑ, matrices $\mathcal{Q}$ and $\mathcal{R}$, and parameters F_c, L_c and K are known. The discrete-time stochastic linear system (25) with the dynamic output feedback controller (17) is secure with probability $1-\varepsilon$ and the quadratic cost functional (4) has the upper bound $\mathcal{J}^* = 0.5(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2$, if there exist two positive definite matrices $\mathcal{P}$ and $\mathcal{W}$, and two positive scalars ν and κ such that matrix inequalities

$$\begin{cases} \Upsilon_1 < 0 & \text{(26a)} \\ \Upsilon_2 < 0 & \text{(26b)} \\ \Upsilon_3 < 0 & \text{(26c)} \\ \Upsilon_4 > 0 & \text{(26d)} \end{cases}$$

with the nonlinear constraint

$$\begin{aligned}
& ||x_0||\sqrt{\varepsilon^{-1}\lambda_{\min}^{-1}(\mathcal{P})\lambda_{\max}(\mathcal{P})} \\
& \quad + \varrho\sqrt{\varepsilon^{-1}\chi\lambda_{\min}^{-1}(\mathcal{P})\big(\nu^{-1}\lambda_{\max}(\mathcal{P})+1\big)} \le \vartheta
\end{aligned} \tag{27}$$

hold, where

$$\mathcal{S}_1 = \begin{bmatrix} A & (1-\bar{\alpha})BK \\ (1-\bar{\sigma})L_cC & F_c \end{bmatrix},\ \mathcal{S}_6 = \begin{bmatrix} B & 0 \\ 0 & L_c \end{bmatrix}$$
$$\mathcal{S}_2 = \begin{bmatrix} 0 & 0 \\ \sqrt{\bar{\sigma}}L_cC & 0 \end{bmatrix},\ \mathcal{S}_3 = \begin{bmatrix} 0 & \sqrt{\bar{\alpha}}BK \\ 0 & 0 \end{bmatrix}$$
$$\mathcal{S}_4 = \begin{bmatrix} D & 0 \\ (1-\bar{\sigma})L_cE & 0 \end{bmatrix},\ \mathcal{S}_5 = \begin{bmatrix} 0 & 0 \\ \sqrt{\bar{\sigma}}L_cE & 0 \end{bmatrix}$$
$$\bar{\mathscr{A}} = \begin{bmatrix} \mathcal{S}_1^T & \mathcal{S}_3^T & \mathcal{S}_2^T \end{bmatrix}^T,\ \chi = (1+\kappa^{-1})\lambda_{\max}(\mathcal{W})$$
$$\bar{\mathscr{G}} = \begin{bmatrix} (\Lambda^{\alpha\sigma})^T & -\sqrt{\bar{\alpha}}\mathcal{M}_1^T & -\sqrt{\bar{\sigma}}\mathcal{M}_2^T \end{bmatrix}^T\mathcal{S}_6$$
$$\Upsilon_1 = (1+\kappa)\bar{\mathscr{A}}^T(I\otimes\mathcal{P})\bar{\mathscr{A}} - \mathcal{P} + \mathcal{S}_4^T\mathcal{P}\mathcal{S}_4 + \mathcal{S}_5^T\mathcal{P}\mathcal{S}_5 + \nu I$$
$$\Upsilon_2 = \bar{\mathscr{G}}^T(I\otimes\mathcal{P})\bar{\mathscr{G}} - \mathcal{W},\ \Upsilon_4 = (I\otimes\mathcal{P})^{-1} - \bar{\mathscr{G}}\mathcal{W}^{-1}\bar{\mathscr{G}}^T$$
$$\Upsilon_3 = \bar{\mathscr{A}}^T(I\otimes\mathcal{P})\bar{\mathscr{A}} - \mathcal{P} - \nu I + \mathcal{S}_4^T\mathcal{P}\mathcal{S}_4 + \mathcal{S}_5^T\mathcal{P}\mathcal{S}_5 + \mathcal{T}^TK\mathcal{R}K\mathcal{T} + \mathcal{Q}.$$

Finally, for the discrete-time stochastic linear systems with state-dependent noises, the desired controller gains can be obtained via the following corollary.

Theorem 4: Let the positive scalars ε and ϑ, and the positive definite matrices $\mathcal{Q}$ and $\mathcal{R}$ be given. Assume that there exist two positive definite matrices $\mathcal{P}$ and $\mathcal{W}$, seven matrices $\tilde{F}_c$, $\tilde{L}_c$, $\bar{K}$, Θ_{11}, Θ_{12}, Θ_{22} and Λ, and two positive scalars ν and κ satisfying the following parameter-dependent matrix inequalities

$$\begin{cases} \begin{bmatrix} -\mathcal{P} & * \\ \Xi_1 & -\mathcal{P}_{\mathcal{N}} \end{bmatrix} < 0, & \text{(28a)} \\ \begin{bmatrix} -\mathcal{W} & * \\ \Xi_2 & -\mathcal{P}_{\mathcal{N}} \end{bmatrix} < 0 & \text{(28b)} \\ \begin{bmatrix} \Xi_0 & * & * & * \\ \Xi_3 & -\mathcal{P}_{\mathcal{N}} & * & * \\ 0 & \Xi_4 & -\mathcal{W} & * \\ \bar{K}\mathcal{T} & 0 & 0 & \mathcal{R}-\Theta_{11}-\Theta_{11}^T \end{bmatrix} < 0 & \text{(28c)} \\ \begin{bmatrix} -\mathcal{P}_{\mathcal{N}} & * \\ \Xi_2^T & -\mathcal{W} \end{bmatrix} < 0 & \text{(28d)} \end{cases}$$

and

$$||x_0||\sqrt{\varepsilon^{-1}\lambda_{\min}^{-1}(\mathcal{P})\lambda_{\max}(\mathcal{P})} + \varrho\sqrt{\varepsilon^{-1}\chi\lambda_{\min}^{-1}(\mathcal{P})\big(\nu^{-1}\lambda_{\max}(\mathcal{P})+1\big)} \le \vartheta \quad (29)$$

where

$$\mathcal{P}_{\mathcal{N}} = I\otimes(\mathcal{N}+\mathcal{N}'-\mathcal{P}),\ \tilde{\kappa} = 1+\kappa$$
$$\bar{\mathcal{S}}_1 = \begin{bmatrix} \Theta\mathcal{M}A + (1-\bar{\sigma})\tilde{L}_cC & (1-\bar{\alpha})\tilde{K} + \tilde{F}_c \\ (1-\bar{\sigma})\tilde{L}_cC & \tilde{F}_c \end{bmatrix}$$
$$\bar{\mathcal{S}}_2 = \begin{bmatrix} \sqrt{\bar{\sigma}}\tilde{L}_cC & 0 \\ \sqrt{\bar{\sigma}}\tilde{L}_cC & 0 \end{bmatrix},\ \bar{\mathcal{S}}_3 = \begin{bmatrix} 0 & \sqrt{\bar{\alpha}}\tilde{K} \\ 0 & 0 \end{bmatrix}$$
$$\bar{\mathcal{S}}_4 = \begin{bmatrix} \Theta\mathcal{M}D + (1-\bar{\sigma})\tilde{L}_cE & 0 \\ (1-\bar{\sigma})\tilde{L}_cE & 0 \end{bmatrix},\ \Theta = \begin{bmatrix} \Theta_{11} & \Theta_{12} \\ 0 & \Theta_{22} \end{bmatrix}$$
$$\bar{\mathcal{S}}_5 = \begin{bmatrix} \sqrt{\bar{\sigma}}\tilde{L}_cE & 0 \\ \sqrt{\bar{\sigma}}\tilde{L}_cE & 0 \end{bmatrix},\ \bar{\mathcal{S}}_6 = \begin{bmatrix} \Theta\mathcal{M}B & \tilde{L}_c \\ 0 & \tilde{L}_c \end{bmatrix}$$
$$\mathcal{N} = \begin{bmatrix} \Theta\mathcal{M} & \Lambda \\ 0 & \Lambda \end{bmatrix},\ \mathcal{M} = \begin{bmatrix} (B^TB)^{-1}B^T \\ (B^{\perp})^T \end{bmatrix}$$
$$\Xi_0 = \mathcal{P} + \nu I - \mathcal{Q},\ \chi = (1+\kappa^{-1})\lambda_{\max}(\mathcal{W})$$
$$\Xi_1 = \begin{bmatrix} \tilde{\kappa}\bar{\mathcal{S}}_1^T & \tilde{\kappa}\bar{\mathcal{S}}_3^T & \tilde{\kappa}\bar{\mathcal{S}}_2^T & \bar{\mathcal{S}}_4^T & \bar{\mathcal{S}}_5^T \end{bmatrix}^T$$
$$\Xi_2 = \begin{bmatrix} (\Lambda^{\alpha\sigma})^T & -\sqrt{\bar{\alpha}}\mathcal{M}_1^T & -\sqrt{\bar{\sigma}}\mathcal{M}_2^T \end{bmatrix}^T\bar{\mathcal{S}}_6$$
$$\Xi_3 = \begin{bmatrix} \bar{\mathcal{S}}_1^T & \bar{\mathcal{S}}_2^T & \bar{\mathcal{S}}_3^T & \bar{\mathcal{S}}_4^T & \bar{\mathcal{S}}_5^T \end{bmatrix}^T$$
$$\Xi_4 = \begin{bmatrix} \Xi_2 & 0 & 0 \end{bmatrix}^T,\ \tilde{K} = [\bar{K}^T \quad 0]^T.$$

In this case, by designing controller gains $F_c = \Lambda^{-1}\tilde{F}_c$, $L_c = \Lambda^{-1}\tilde{L}_c$ and $K = \Theta_{11}^{-1}\bar{K}$, the discrete-time stochastic linear system (25) with the dynamic output feedback controller (17) is secure with probability $1-\varepsilon$. Furthermore, the quadratic cost functional (4) has the upper bound $\mathcal{J}^* = 0.5(\chi + \lambda_{\max}(\mathcal{W}))\varrho^2$.

Proof: First, with the help of the Schur Complement Lemma, the inequalities (26a) and (26c) are, respectively, equivalent to

$$\begin{bmatrix} -\mathcal{P} & * \\ \tilde{\Xi}_1 & -I\otimes\mathcal{P}^{-1} \end{bmatrix} < 0 \quad (30)$$

and

$$\begin{bmatrix} \Xi_0 & * & * & * \\ \tilde{\Xi}_3 & -I\otimes\mathcal{P}^{-1} & * & * \\ 0 & \tilde{\Xi}_4 & -\mathcal{W} & * \\ K\mathcal{T} & 0 & 0 & -\mathcal{R}^{-1} \end{bmatrix} < 0 \quad (31)$$

where

$$\tilde{\Xi}_1 = \begin{bmatrix} (1+\kappa)\mathcal{S}_1^T & (1+\kappa)\mathcal{S}_3^T & (1+\kappa)\mathcal{S}_2^T & \mathcal{S}_4^T & \mathcal{S}_5^T \end{bmatrix}^T$$
$$\tilde{\Xi}_2 = \begin{bmatrix} (\Lambda^{\alpha\sigma})^T & -\sqrt{\bar{\alpha}}\mathcal{M}_1^T & -\sqrt{\bar{\sigma}}\mathcal{M}_2^T \end{bmatrix}^T\mathcal{S}_6$$
$$\tilde{\Xi}_3 = \begin{bmatrix} \bar{\mathcal{S}}_1^T & \mathcal{S}_3^T & \mathcal{S}_2^T & \mathcal{S}_4^T & \mathcal{S}_5^T \end{bmatrix}^T,\ \tilde{\Xi}_4 = \begin{bmatrix} \tilde{\Xi}_2 & 0 & 0 \end{bmatrix}^T.$$

Denote $\tilde{F}_c = \Lambda F_c$, $\tilde{L}_c = \Lambda L_c$, and $\bar{K} = \Theta_{11}K$. It follows from (28c) that $\mathcal{N}$ and Θ_{11} are invertible. Furthermore, pre- and post-multiplying the inequality (30) by $\mathrm{diag}\{I, I\otimes\mathcal{N}\}$ and $\mathrm{diag}\{I, I\otimes\mathcal{N}^T\}$, and the inequality (31) by $\mathrm{diag}\{I, I\otimes\mathcal{N}, I, \Theta_{11}\}$ and $\mathrm{diag}\{I, I\otimes\mathcal{N}^T, I, \Theta_{11}^T\}$, respectively, result in

$$\begin{bmatrix} -\mathcal{P} & * \\ \Xi_1 & -I\otimes(\mathcal{N}\mathcal{P}^{-1}\mathcal{N}^T) \end{bmatrix} < 0 \quad (32)$$

and

$$\begin{bmatrix} \Xi_0 & * & * & * \\ \Xi_3 & -I\otimes(\mathcal{N}\mathcal{P}^{-1}\mathcal{N}^T) & * & * \\ 0 & \Xi_4 & -\mathcal{W} & * \\ K\mathcal{T} & 0 & 0 & -\Theta_{11}\mathcal{R}^{-1}\Theta_{11}^T \end{bmatrix} < 0. \quad (33)$$

Because of

$$\begin{aligned}&\mathcal{N}+\mathcal{N}^T-\mathcal{N}\mathcal{P}^{-1}\mathcal{N}^T-\mathcal{P}\\&\quad=-(\mathcal{P}-\mathcal{N})\mathcal{P}^{-1}(\mathcal{P}-\mathcal{N})^T\le 0\\&\Theta_{11}+\Theta_{11}^T-\Theta_{11}\mathcal{R}^{-1}\Theta_{11}^T-\mathcal{R}\\&\quad=-(\mathcal{R}-\Theta_{11})\mathcal{R}^{-1}(\mathcal{R}-\Theta_{11})^T\le 0\end{aligned}$$

it can be shown that the inequalities (32) and (33) (equivalent to (26a) and (26c)) can be satisfied if (28a) and (28c) hold. Similarly, we can obtain that (26b) and (26d)) can be satisfied if (28b) and (28d) are true. As such, it can be concluded from Theorem 3 that the desired security is achieved and the quadratic cost functional (4) has the upper bound $\mathcal{J}^*=0.5(\chi+\lambda_{\max}(\mathcal{W}))\varrho^2$ for the addressed system (25), which completes the proof.

Remark 4: In Theorem 4, the system parameters, the desired security probability ε and the weighting matrices $\mathcal{Q}$ and $\mathcal{R}$ in the quadratic cost function (4) are all reflected in a set of parameter-dependent matrix inequalities. Obviously, the inequality (28a) with fixed parameter $\tilde{\kappa}$ will reduce to a linear matrix inequality, and therefore this parameter offers additional flexibility with possibility to improve the security performance.

Remark 5: In this paper, the impact on both the security performance and the average cost of the state and control input is examined from the statistical information of deception attacks. This paper considerably enlarges the scope of our earlier result [9]. In comparison, the developed results have the following two distinguishing features: 1) more general dynamic output feedback controllers are deigned to match up with the corresponding stochastic nonlinear systems; and 2) a quadratic cost is further investigated while guaranteeing the security in probability.

IV. Simulation Examples

To illustrate the effectiveness of the proposed results, two numerical examples are given in this section.

Example 1: The first example concerns the following discrete-time stochastic nonlinear system:

$$\begin{cases}x_{k+1}=\dfrac{1}{3}x_k\sin(x_k)+\dfrac{1}{2}u_k+\dfrac{1}{15}x_k\cos(x_k)w_k,\\ \tilde{y}_k=\dfrac{1}{2}x_k+\dfrac{1}{15}x_k\sin(x_k)w_k,\end{cases}$$

with the initial condition $x_0=0.4$. Give the probability $\bar{\alpha}=\bar{\sigma}=0.05$ and $\varepsilon=0.25$, the security parameter $\vartheta=14$, the bound of disturbance input $\varrho=0.05$, and the weighting matrices $\mathcal{Q}=0.05I$ and $\mathcal{R}=0.05I$. According to Theorem 2, it can be seen that the controller (17) with parameters $F_c=-0.4$, $L_c=0.25$ and $K=0.8$ is a suitable dynamic output feedback controller for the above stochastic nonlinear system. Here, the other parameters satisfying the conditions in Theorem 2 can be selected as $\mathcal{P}=\mathrm{diag}\{0.9,0.9\}$, $\mathcal{W}=1$, $\nu=0.31$, $\Lambda=0.77$ and $\kappa=0.45$. Furthermore, the permitted upper bound $\mathcal{J}^*$ is 0.0355.

Example 2: The second example considers the discrete-time stochastic linear system (25) with

$$A=\begin{bmatrix}-1.00 & 2.00\\ -0.20 & -0.65\end{bmatrix},\ D=\begin{bmatrix}0.007 & -0.005\\ 0.010 & 0.006\end{bmatrix}$$
$$B=\begin{bmatrix}2.00 & 0\end{bmatrix}^T,\ C=\begin{bmatrix}0.50 & -0.50\end{bmatrix}$$
$$E=\begin{bmatrix}0.025 & -0.025\end{bmatrix}$$

and the initial condition $x_0=\begin{bmatrix}0.40 & -0.20\end{bmatrix}$. Then, the other corresponding parameters are the same with the above example. By using the Matlab software (with the YALMIP 3.0), a set of solutions to matrix inequalities (28a)-(28d) in Theorem 4 is obtained as follows:

$$\mathcal{P}=\begin{bmatrix}0.7259 & -0.0931 & 0.4192 & -0.0209\\ -0.0931 & 4.3751 & -0.2098 & 1.5271\\ 0.4192 & -0.2098 & 0.4163 & 0.0446\\ -0.0209 & 1.5271 & 0.0446 & 0.9762\end{bmatrix}$$
$$\mathcal{W}=\begin{bmatrix}1.6361 & 0.0264\\ 0.0264 & 1.6569\end{bmatrix},\ \Theta=\begin{bmatrix}1.0401 & -0.0741\\ 0 & 7.9006\end{bmatrix}$$
$$\Lambda=\begin{bmatrix}0.4483 & 0.0413\\ -0.1545 & 1.8515\end{bmatrix},\ \tilde{L}_c=\begin{bmatrix}0.7331\\ -0.1372\end{bmatrix}$$
$$\tilde{F}_c=\begin{bmatrix}0.3026 & 0.0386\\ -0.4109 & -0.7702\end{bmatrix},\ \tilde{K}=\begin{bmatrix}-0.4253\\ 0.3224\end{bmatrix}^T$$
$$\nu=0.0405,\quad \kappa=0.05.$$

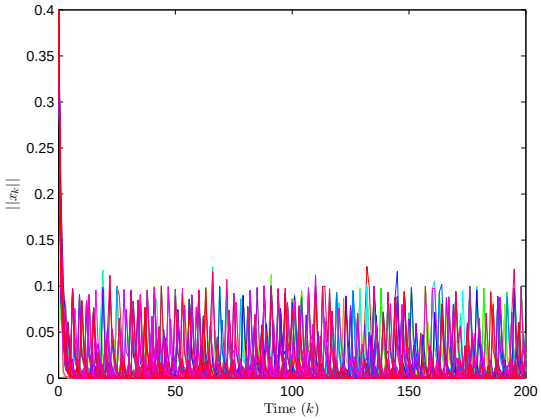
It can be checked that the condition (27) is satisfied. Furthermore, the permitted upper bound $\mathcal{J}^*$ is 0.7370 and the desired control parameters are

$$F_c=\begin{bmatrix}0.6901 & 0.1234\\ -0.1643 & -0.4057\end{bmatrix},\ L_c=\begin{bmatrix}1.6300\\ 0.0618\end{bmatrix}$$
$$K=\begin{bmatrix}-0.4089 & 0.3100\end{bmatrix}.$$

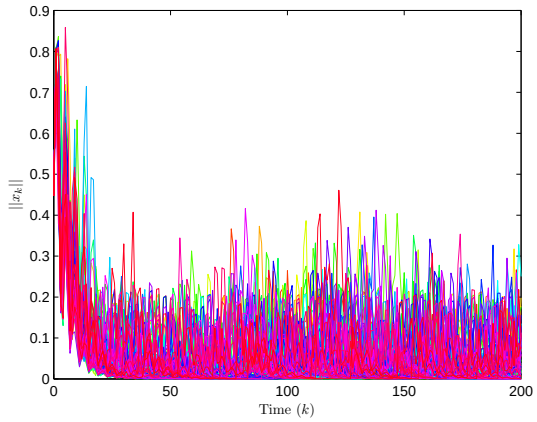
In the simulations, the exogenous disturbance inputs are selected as $\zeta_{1,k}=0.2\cos(k)$ and $\zeta_{2,k}=0.2\sin(k)$. The simulation results for Example 1 and Example 2 are shown in Figs. 2∼4. Specially, Fig. 2 plots the dynamic trajectories of $||x_k||$ for 100 independent simulation trials, which effectively checks the *security in probability* for the employed examples. In addition, Fig. 3 and Fig. 4 depict both the dynamic trajectory of $||x_k||$ and attack times for a simulation trial, which vividly reflects the impact from deception attacks. The simulation results have confirmed that the designed controller performs very well.

V. Conclusions

In this paper, we have dealt with the security control problem with a predefined quadratic cost for discrete-time stochastic nonlinear systems subject to deception attacks. A definition of security in probability has been employed to reasonably account for the transient dynamics of the closed-loop systems. Sufficient conditions with the form of matrix inequalities have been established by means of the input-to-state stability in probability (ISSiP). Furthermore, an easy-solution version on above inequalities has been developed by carrying out the well-known matrix inverse lemma. Specially, the controller parameters and the desired upper bound have been characterized via the solution of matrix inequalities with a nonlinear inequality constraint. Further research topics can be focused on security issues for general time-delayed systems

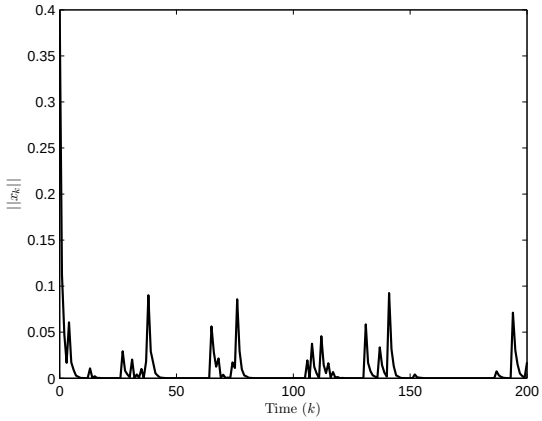


(a) The dynamic trajectory of $||x_k||$ (Example 1).

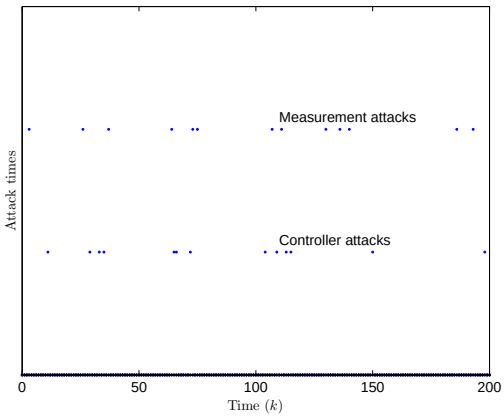


(b) The dynamic trajectory of $||x_k||$ (Example 2).

Fig. 2. The dynamic trajectories (100 independent simulation trials).



(a) The dynamic trajectory of $||x_k||$.



(b) Attack times.

Fig. 3. The dynamic trajectory and the attack times for Example 1.

or switched systems [29], [30] subject to various cyber attacks with/without event-triggered communication protocols [18], [19], [39].

REFERENCES

[1] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems", *Automatica*, vol. 49, no. 1, pp. 186-192, Jan. 2013.

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

[3] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under a class of denial-of-service attack models", In: *Proceedings of the 2011 American Control Conference*, San Francisco, CA, USA, pp. 643-648, 2011.

[4] F. Borrelli, M. Baotić, A. Bemporad, and M. Morari, "Dynamic programming for constrained optimal control of discrete-time linear hybrid systems", *Automatica*, vol. 41, no. 10, pp. 1709-721, Oct. 2005.

[5] A. A. Cárdenas, S. Amin, and S. S. Sastry, "Secure control: Towards survivable cyber-physical systems", In: *Proceedings of the 1st International Workshop on Cyber-Physical Systems*, pp. 495-500, Beijing, China, Jun. 2008.

[6] D. Ding, Y. Shen, Y. Song, and Y. Wang, "Recursive state estimation for discrete time-varying stochastic nonlinear systems with randomly occurring deception attacks", *International Journal of General Systems*, vol. 45, no. 5, pp. 548-560, 2016.

[7] D. Ding, G. Wei, S. Zhang, Y. Liu, and F. E. Alsaadi, "On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors", *Neurocomputing*. DOI: 10.1016/j.neucom.2016.09.009.

[8] D. Ding, Z. Wang, B. Shen, G. Wei, Event-triggered consensus control for discrete-time stochastic multi-agent systems: The input-to-state stability in probability", *Automatica*, vol. 62, pp. 284-291, Nov. 2015.

[9] D. Ding, Z. Wang, and Hongli Dong, "Dynamic output feedback control for discrete-time stochastic nonlinear systems with adversaries", In: *Proceedings of the 33st Chinese Control Conference*, pp. 5428-5432, Nanjing, China, Jul. 2014.

[10] H. Dong, Z. Wang, X. Bu, and F. E. Alsaadi, "Distributed fault estimation with randomly occurring uncertainties over sensor networks", *International Journal of General Systems*, vol. 45, no. 5, pp. 619-632, 2016.

[11] Y. Yu, H. Dong, Z. Wang, W. Ren, and F. E. Alsaadi, "Design of non-fragile state estimators for discrete time-delayed neural networks with parameter uncertainties", *Neurocomputing*, vol. 182, pp. 18-24, Mar. 2016.

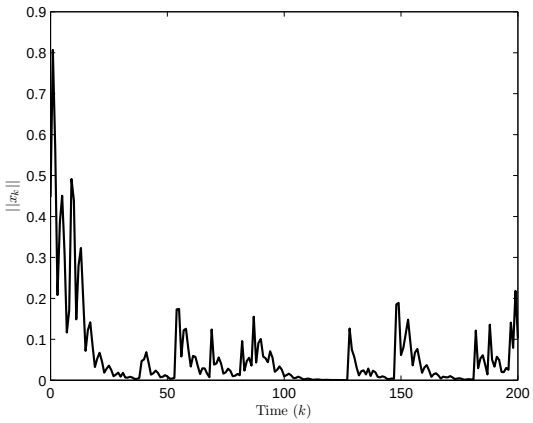
[12] H. Foroush and S. Martínez, "On event-triggered control of linear systems under periodic Denial-of-Service jamming attacks", In: *Proceedings of the the 51st IEEE Conference on Decision and Control*, Hawaii, USA, pp. 2551-2256, Dec. 2012.

[13] J. Hu, S. Liu, D. Ji, and S. Li, "On co-design of filter and fault estimator against randomly occurring nonlinearities and randomly occurring deception attacks", *International Journal of General Systems*, vol. 45, no. 5, pp. 619-632, 2016.

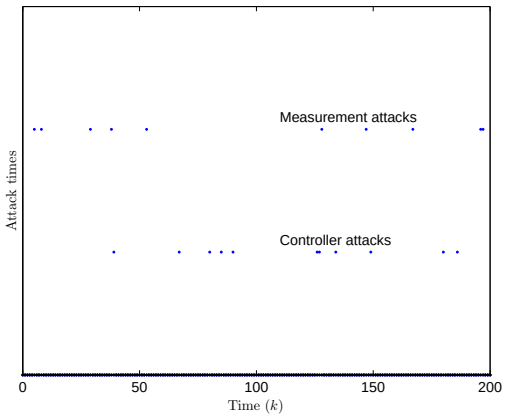
[14] J. Hu, Z. Wang, S. Liu, and H. Gao, "A variance-constrained approach to recursive state estimation for time-varying complex networks with missing measurements", *Automatica*, vol. 64, pp. 155-162, Feb. 2016.

[15] L. Huang and X. Mao, "On input-to-state stability of stochastic retarded systems with Markovian switching", *IEEE Transactions on Automatic Control*, vol. 54, no. 8, pp. 1898-1902, Aug. 2009.

[16] H. R. Karimi, "Robust $\mathcal{H}_\infty$ filter design for uncertain linear systems over network with network-induced delays and output quantization", *Modeling, Identification and Control*, vol. 30, no. 1, pp. 27-37, 2009.



(a) The dynamic trajectory of $||x_k||$.



(b) Attack times.

Fig. 4. The dynamic trajectory and the attack times for Example 2.

[17] S. Kek, K. Teo, and A. A. Ismail, "An integrated optimal control algorithm for discrete-time nonlinear stochastic system", *International Journal of Control*, vol. 83, no. 12, pp. 2536-2545, Dec. 2010.

[18] Q. Li, B. Shen, J. Liang, and H. Shu, "Event-triggered synchronization control for complex networks with uncertain inner coupling", *International Journal of General Systems*, vol. 44, no. 2, Jan. 2015, pp. 212-225.

[19] Q. Li, B. Shen, Y. Liu, F. E. Alsaadi, "Event-triggered $\mathcal{H}_\infty$ state estimation for discrete-time stochastic genetic regulatory networks with Markovian jumping parameters and time-varying delays", *Neurocomputing*, vol. 174, pp. 912-920, Jan. 2016.

[20] S. Liu and J. Zhang, "Output-feedback control of a class of stochastic nonlinear systems with linearly bounded unmeasurable states", *International Journal of Robust and Nonlinear Control*, vol. 18, no. 6, pp. 665-687, Apr. 2008.

[21] S. Liu, G. Wei, Y. Song, and Y. Liu, "Error-constrained reliable tracking control for discrete time-varying systems subject to quantization effects", *Neurocomputing*, vol. 174, pp. 897-905, Jan. 2016.

[22] M. Long, , C.-H. Wu and J. Y. Hung, "Denial of service attacks on network-based control systems: impact and mitigation", *IEEE Transactions on Industrial Informatics*, vol. 1, no. 2, pp. 85-96, May 2005.

[23] W. Lou and Y. Fang, "A multipath routing approach for secure data delivery", In: *Communications for Network-Centric Operations: Creating the Information Force*, MILCOM, McLean, VA, USA, pp. 1467-1473, Oct. 2001.

[24] R. Mitchell and I.-R. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications", *IEEE Transactions on Systems, Man and Cybernetics - Systems*, vol. 44, no. 5, pp. 593-604, May 2014.

[25] P. Palensky, E. Widl and A. Elsheikh, "Simulating cyber-physical energy systems: challenges, tools and methods", *IEEE Transactions on Systems, Man and Cybernetics - Systems*, vol. 44, no. 3, pp. 318-326, Mar. 2014.

[26] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks", *IEEE Transactions on Control Systems Technology*, vol. 20, no. 5, pp. 1334-1342, Sep. 2012.

[27] I. R. Petersen, "Guaranteed cost control of stochastic uncertain systems with slope bounded nonlinearities via the use of dynamic multipliers", *Automatica*, vol. 47, no. 2, pp. 411-417, Feb. 2011.

[28] M. Rabi, C. Ramesh, and K. H. Johansson, "Separated design of encoder and controller for networked linear quadratic optimal control", *SIAM Journal on Control and Optimization*, vol. 54, no. 2, pp. 662-689, 2016

[29] G. Rajchakit, "Switching design for the robust stability of nonlinear uncertain stochastic switched discrete-time systems with interval time-varying delay", *Journal of Computational Analysis & Applications*, vol. 16, no. 1, pp. 10-19, Jun. 2014.

[30] G. Rajchakit, "Robust stability and stabilization of nonlinear uncertain stochastic switched discrete-time systems with interval time-varying delays", *Applied Mathematics & Information Sciences*, vol. 6, no. 3, pp. 555-565, Sep. 2012.

[31] B. Shen, Z. Wang, H. Shu, and G. Wei, "Robust $\mathcal{H}_\infty$ finite-horizon filtering with randomly occurred nonlinearities and quantization effects", *Automatica*, vol. 46, no. 11, pp. 1743-1751, Nov. 2010.

[32] Z. Shu, J. Lam, and J. Xiong, "Non-fragile exponential stability assignment of discrete-time linear systems with missing data in actuators", *IEEE Transactions on Automatic Control*, vol. 54, no. 3, pp. 625-630, Mar. 2009.

[33] C.-K. Tham and T. Luo, "Sensing-driven energy purchasing in smart grid cyber-physical system", *IEEE Transactions on Systems, Man and Cybernetics-Systems*, vol. 43, no. 4, pp. 773-784, Jul. 2013.

[34] A. Teixeira, H. Sandberg, and K. H. Johansson, "Networked control systems under cyber attacks with applications to power networks", In: *Proceedings of the 2010 American Control Conference*, Baltimore, MD, USA, pp. 3690-3696, Jun. 2010.

[35] J. Tsinias, "Stochastic input to state stability and application to global feedback stabilization", *International Journal of Control*, vol. 71, no. 5, pp. 907-930, 1998.

[36] D. J. Tylavsky and G. R. L. Sohie, "Generalization of the matrix inversion lemma", *Proceeding of the IEEE*, vol. 74(7): 1050-1052, Jul. 1986.

[37] A. Vempaty, L. Tong, and P. Varshney, "Distributed inference with Byzantine data: State-of-the-art review on data falsification attacks", *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 65-75, Jan. 2013.

[38] J. Wang, *F*oundations of modern probability, Fudan University Press, Shanghai, China, 2005.

[39] G. Wei, S. Liu, L. Wang, and Y. Wang, "Event-based distributed set-membership filtering for a class of time-varying non-linear systems over sensor networks with saturation effects", *International Journal of General Systems*, vol. 45, no. 5, pp. 532-547, J2016.

[40] L. Wang, S. Ren, B. Korel, K. Kwiat and E. Salerno, "Improving system reliability against rational attacks under given resources", *IEEE Transactions on Systems, Man and Cybernetics-Systems*, vol. 44, no. 4, pp. 446-456, Apr. 2014

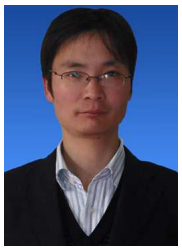
[41] H. Xu, Q. Zhao, and S. Jagannathan, "Finite-horizon near-optimal output feedback neural network control of quantized nonlinear discrete-time systems with input constraint", *IEEE Transactions on Neural Networks and Learning Systems*, vol. 26, no. 8, pp. 1776-1788, Aug. 2015.

[42] F. Yang, Z. Wang, Y. S. Hung, and M. Gani, "$\mathcal{H}_\infty$ control for networked systems with random communication delays", *IEEE Transactions on Automatic Control*, vol. 51, no. 3, pp. 511-518, Mar. 2006.

[43] J. Yong and X. Zhou, *Stochastic controls: Hamiltonian systems and HJB equations*, Springer, New York, 1999.

[44] J. Zhang, R. S. Blum, X. Lu, and D. Conus, "Asymptotically optimum distributed estimation in the presence of attacks", *IEEE Transactions on Singnal Processing*, vol. 63, no. 5, pp. 1086-1101, Mar. 2015.

[45] M. Zhu, and S. Martinez, "On the performance analysis of resilient networked control systems under replay attacks", *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 804-808, Mar. 2014.



Derui Ding received both the B.Sc. degree in Industry Engineering in 2004 and the M.Sc. degree in Detection Technology and Automation Equipment in 2007 from Anhui Polytechnic University, Wuhu, China, and the Ph.D. degree in Control Theory and Control Engineering in 2014 from Donghua University, Shanghai, China. From July 2007 to December 2014, he was a teaching assistant and then a lecturer in the Department of Mathematics, Anhui Polytechnic University, Wuhu, China.

He is currently an associate professor with the Department of Control Science and Engineering, University of Shanghai for Science and Technology, Shanghai, China. From June 2012 to September 2012, he was a research assistant in the Department of Mechanical Engineering, the University of Hong Kong, Hong Kong. From March 2013 to March 2014, he was a visiting scholar in the Department of Information Systems and Computing, Brunel University London, UK. His research interests include nonlinear stochastic control and filtering, as well as multi-agent systems and sensor networks. He has published around 20 papers in refereed international journals. He is a very active reviewer for many international journals.

Zidong Wang (SM'03-F'14) was born in Jiangsu, China, in 1966. He received the B.Sc. degree in mathematics in 1986 from Suzhou University, Suzhou, China, and the M.Sc. degree in applied mathematics in 1990 and the Ph.D. degree in electrical engineering in 1994, both from Nanjing University of Science and Technology, Nanjing, China.

He is currently Professor of Dynamical Systems and Computing in the Department of Information Systems and Computing, Brunel University London, U.K. From 1990 to 2002, he held teaching and research appointments in universities in China, Germany and the UK. Prof. Wang's research interests include dynamical systems, signal processing, bioinformatics, control theory and applications. He has published more than 300 papers in refereed international journals. He is a holder of the Alexander von Humboldt Research Fellowship of Germany, the JSPS Research Fellowship of Japan, William Mong Visiting Research Fellowship of Hong Kong.

Prof. Wang serves (or has served) as the Editor-in-Chief for Neurocomputing and an Associate Editor for 12 international journals, including IEEE Transactions on Automatic Control, IEEE Transactions on Control Systems Technology, IEEE Transactions on Neural Networks, IEEE Transactions on Signal Processing, and IEEE Transactions on Systems, Man, and Cybernetics - Part C. He is a Fellow of the IEEE, a Fellow of the Royal Statistical Society and a member of program committee for many international conferences.

Qing-Long Han (M'09-SM'13) received the B.Sc. degree in mathematics from Shandong Normal University, Jinan, China, in 1983, and the M.Sc. and Ph.D. degrees in Control Engineering and Electrical Engineering from East China University of Science and Technology, Shanghai, China, in 1992 and 1997, respectively.

From September 1997 to December 1998, he was a Post-doctoral Researcher Fellow with the Laboratoire d'Automatique et d'Informatique Industielle (now renamed as Laboratoire d'Informatique et d'Automatique pour les Systémes), Ecole Sup érieure d'Ing'enieurs de Poitiers (now renamed as Ecole Nationale Supérieure d'Ingé nieurs de Poitiers), Universit é de Poitiers, France. From January 1999 to August 2001, he was a Research Assistant Professor with the Department of Mechanical and Industrial Engineering at Southern Illinois University at Edwardsville, USA. From September 2001 to December 2014, he was Laureate Professor, Associate Dean (Research and Innovation) with the Higher Education Division, and Founding Director of the Centre for Intelligent and Networked Systems at Central Queensland University, Australia. From December 2014 to May 2016, he was Deputy Dean (Research), with the Griffith Sciences, and Professor with the Griffith School of Engineering, Griffith University, Australia. In May 2016, he joined Swinburne University of Technology, Australia, where he is currently Pro Vice-Chancellor (Research Quality) and Distinguished Professor. His research interests include networked control systems, neural networks, time-delay systems, multiagent systems, and complex systems.

Professor Han was appointed Chang Jiang (Yangtze River) Scholar Chair Professor by the Ministry of Education, China, in March 2010. He is one of The World's Most Influential Scientific Minds: 2014, The World's Most Influential Scientific Minds: 2015, and The World's Most Influential Scientific Minds: 2016. He is a Highly Cited Researcher in Engineering according 1153 to Thomson Reuters.

Guoliang Wei received the B.Sc. degree in mathematics from Henan Normal University, Xinxiang, China, in 1997 and the M.Sc. degree in applied mathematics and the Ph.D. degree in control engineering, both from Donghua University, Shanghai, China, in 2005 and 2008, respectively.

He is currently a Professor with the Department of Control Science and Engineering, University of Shanghai for Science and Technology, Shanghai, China. From March 2010 to May 2011, he was an Alexander von Humboldt Research Fellow in the Institute for Automatic Control and Complex Systems, University of Duisburg-Essen, Germany. From March 2009 to February 2010, he was a post doctoral research fellow in the Department of Information Systems and Computing, Brunel University, Uxbridge, UK, sponsored by the Leverhulme Trust of the UK From June to August 2007, he was a Research Assistant at the University of HongKong. From March to May 2008, he was a Research Assistant at the City University of Hong Kong.

His research interests include nonlinear systems, stochastic systems, and bioinformatics. He has published more than 20 papers in refereed international journals. He is a very active reviewer for many international journals.