Security-Guaranteed Filtering for Discrete-Time Stochastic Delayed Systems with Randomly Occurring Sensor Saturations and Deception Attacks

Dong Wang[a], Zidong Wang[b,c], Bo Shen[a,*] and Fuad E. Alsaadi[c]

Abstract

In this paper, the security-guaranteed filtering problem is studied for a class of nonlinear stochastic discrete time-delay systems with randomly occurring sensor saturations (ROSSs) and randomly occurring deception attacks (RODAs). The nonlinearities in systems satisfy the sector-bounded conditions and the time-varying delays are unknown with given lower and upper bounds. A novel measurement output model is proposed to reflect both the ROSSs and the RODAs. A new definition is put forward on the security level with respect to the noise intensity, the energy bound of the false signals, the energy of the initial system state and the desired security degree. We aim at designing a filter such that, in the presence of ROSSs and RODAs, the filtering error dynamics achieves the prescribed level of security. By using the stochastic analysis techniques, a sufficient condition is first derived under which the filtering error system is guaranteed to have the desired security level, and then the filter gain is designed by solving a linear matrix inequality with nonlinear constraints. Finally, a numerical example is provided to demonstrate the feasibility of the proposed filtering scheme.

Index Terms

Security-guaranteed filtering, nonlinear stochastic systems, discrete time-delay systems, randomly occurring sensor saturations, randomly occurring deception attacks.

I. Introduction

In reality, most physical systems are inherently nonlinear and the nonlinearity results in considerable system complexity. In engineering practice such as maneuverable target tracking and mobile robot navigation, one often needs to estimate the true value of states of the nonlinear systems based on some potentially noisy measurement outputs, and such nonlinear filtering problems have been attracting considerable research interest in the past few decades due to their wide application potentials. A number of efficient algorithms have been developed to solve the nonlinear filtering problems, among which the most renowned one is arguably the extended Kalman filtering approach that is applicable to linearized systems with Gaussian noises of known statistics. In addition, the H_∞ and robust filters for nonlinear systems have been paid much attention due to their excellent robustness against

This work was supported in part by the National Natural Science Foundation of China under Grants 61329301 and 61473076, the Shu Guang project of Shanghai Municipal Education Commission and Shanghai Education Development Foundation under Grant 13SG34, the Program for Professor of Special Appointment (Eastern Scholar) at Shanghai Institutions of Higher Learning, the Fundamental Research Funds for the Central Universities, the DHU Distinguished Young Professor Program, and the Alexander von Humboldt Foundation of Germany.

[a] School of Information Science and Technology, Donghua University, Shanghai 200051, China.
[b] Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom.
[c] Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia.
[*] Corresponding author. Email: shenbodh@gmail.com

the exogenous disturbances and parameter uncertainties. For example, the extended Kalman filtering problems for nonlinear system have been investigated in [16], [17]. The H_∞ filter has been designed for systems with affine nonlinearities [1], sector-bounded nonlinearities [25], nonlinear fractional transformations [37] and randomly occurring nonlinear disturbances [10]. In [28], the robust filtering problem has been investigated for a class of discrete-time uncertain stochastic nonlinear time-delay systems with both the probabilistic missing measurements and external stochastic disturbances.

In practice, due to a variety of reasons such as the unmodeled inertia of system components and the finite speeds of the transmitting signals, the time delay has proven to be a pervasive phenomenon with many dynamic systems. In recent years, the study of time-delay systems has attracted much attention and a large number of research results have been reported in the literature, see e.g. [5], [13], [14], [29], [30], [33], [34]. Different types of time-delays (e.g. constant delays, time-varying delays, discrete delays and distributed delays) have been thoroughly investigated in the analysis and control problems by using a variety of methods such as the linear matrix inequality approach, the Lyapunov functional method, the M-matrix theory, the topological degree theory as well as the general inequality techniques. For instance, in [29], time-varying mode-dependent delays have been considered in the robust H_∞ filtering problem. In [13], a robust H_∞ filter has been designed for linear discrete-time uncertain systems with multiple delays in the states by using a delay-dependent approach. Very recently, a reliable filter has been designed in [27] for a class of discrete-time piecewise linear systems with both sensor failures and infinite distributed delays.

As is well known, the filtering performance is highly dependent on the information known *a priori* on the available measurements and the sensors responsible for collecting/transmitting signals play a vitally important role in the filtering process. A particular phenomenon that occurs often to the sensors is the so-called saturation resulting from physical, safety or technological constraints on the components of the system such as battery capacity, power limit and intermittent failures. Sensor saturations are essentially a nonlinear behavior that could lead to poor performances or even instability of the system. In the context of nonlinear filtering, much work has recently been done to attenuate the effects from the sensor saturation phenomenon or packet losses on the overall filtering performance, see. e.g. [15], [22], [26], [31], [32], [35], [36]. For example, the H_∞ filter has been designed in [26] for systems with both sensor saturations and missing measurements. In [15], the probability-guaranteed H_∞ finite-horizon filtering problem has been investigated for a class of nonlinear time-varying systems with sensor saturations.

With rapid development of communication networks, many components of physical systems (e.g. actuators, sensors and state estimators) are required to share a common communication link [6]–[9], [11], [19], [20]. Due to the strong opening-up property of a shared network, the data received by sensors may be transmitted over the network without security protections. As such, attackers can arbitrarily intercept, tamper or retransmit the data transmitted in the network and hence destabilize the plant or steer the plant to their desired operating points. Therefore, the attack behaviours for physical systems have attracted much attention in recent years, and some preliminary results related to this emerging topic of research have been reported in the literature, see e.g. [2], [3], [12], [21], [24], [38]. It should be pointed out that, deception attacks (or false data injection attacks) are considered to be the most dangerous attack behaviours since attackers can inject the malicious data in order to degrade or even deteriorate the performance of systems. For example, in [2], a defending mechanism against false data injection attacks has been proposed for state estimation of power system in terms of graphical methods and the main results have then been extended in [3]. Nevertheless, when the system is subject to both sensor saturations and deception attacks in a possibly random way, the corresponding security-guaranteed filtering problem has not been investigated yet, not to mention the case when nonlinearities and time-delays are also present. It is, therefore, the main motivation of this paper to shorten such a gap.

The contributions of the paper are summarized as follows. 1) A new research problem of security-guaranteed filter

design is proposed for nonlinear stochastic discrete time-delay systems with randomly occurring sensor saturations as well as deception attacks. 2) A novel model for measurement outputs is put forward to account for the sensor saturations and the deception attacks that are randomly occurring according to two sets of Bernoulli distributed white sequences. 3) In order to quantify the security degree, we introduce a new concept of mean square security domain. 4) A sufficient condition is derived under which the filtering error dynamics achieves the desired degree of security and then the desired filter gain is obtained by solving a linear matrix inequality with nonlinear constraints.

This paper is organized as follows. Security-guaranteed filtering problem for nonlinear stochastic discrete time-delay systems with randomly occurring sensor saturations as well as deception attacks is presented in Section II, where we propose a novel model for measurement outputs and a new concept of mean-square security domain to describe this issue. Then, in Section III, with the help of the stochastic analysis techniques, a sufficient condition is derived to make the filtering error dynamics to achieve the desired degree of security and the desired filter gain is obtained subsequently. Finally, an illustrative example is presented to show the effectiveness of the filtering scheme proposed in Section IV.

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. The notation $X\geq Y$ (respectively, $X>Y$), where X and Y are real symmetric matrices, means that $X-Y$ is positive semi-definite (respectively, positive definite). M^T represents the transpose of the matrix M. I denotes the identity matrix of compatible dimension. diag$\{\cdots\}$ stands for a block-diagonal matrix. $\mathbb{N}^+$ indicates the positive integer set. $\lambda_{\max}(A)$ and $\lambda_{\min}(A)$ denote the maximum and minimum eigenvalue of A, respectively. $\mathbb{E}\{x\}$ stands for the expectation of the stochastic variable x. $\|x\|$ describes the Euclidean norm of a vector x. In symmetric block matrices, "$*$" is used to denote a term induced by symmetry. Matrices, if they are not explicitly specified, are assumed to have compatible dimensions.

II. Problem Formulation

Consider the following discrete-time nonlinear stochastic system with time delays

$$\begin{aligned} x(k+1) =& Ax(k)+A_dx(k-d(k))+Bf(x(k))+B_df_d(x(k-d(k)))+D_1w(k),\\ x(j) =& \varphi(j),\quad j=-d_M,-d_M+1,\ldots,-1,0, \end{aligned} \tag{1}$$

where $x(k)\in\mathbb{R}^{n_x}$ is the state vector, $w(k)\in\mathbb{R}$ is a zero-mean Gaussian white noise sequence with $\mathbb{E}w^2(k)\leq\delta^2$, A, A_d, B, B_d, and D_1 are known real constant matrices with appropriate dimensions. $\varphi(j)$ ($j=-d_M,-d_M+1,\ldots,-1,0$) are the initial conditions, which are assumed to be independent of the process $\{w(k)\}_{k\in\mathbb{N}^+}$.

The nonlinear functions $f:\mathbb{R}^{n_x}\to\mathbb{R}^{n_x}$ and $f_d:\mathbb{R}^{n_x}\to\mathbb{R}^{n_x}$ satisfy the following sector-bounded conditions:

$$\begin{aligned} [f(x)-K_1x]^T[f(x)-K_2x]\leq&0,\\ [f_d(x)-T_1x]^T[f_d(x)-T_2x]\leq&0, \end{aligned} \tag{2}$$

where K_1, K_2, T_1 and T_2 are known real matrices of appropriate dimensions. $K=K_1-K_2$ and $T=T_1-T_2$ are symmetric positive definite matrices.

For the system (1), the positive integer $d(k)$ denotes the time-varying delay satisfying

$$d_m\leq d(k)\leq d_M,\quad k\in\mathbb{N}^+, \tag{3}$$

where the lower bound d_m and the upper bound d_M are known positive integers.

The sensor measurement model with randomly occurring saturations and deception attacks is described by

$$\begin{aligned}\tilde{y}(k) =&\alpha(k)\sigma(Cx(k)) + (1-\alpha(k))Cx(k) + D_2 w(k),\\ y(k) =&\tilde{y}(k) + \beta(k)v(k),\\ v(k) =&-\tilde{y}(k) + \xi(k),\end{aligned} \tag{4}$$

where $\tilde{y}(k) \in \mathbb{R}^{n_y}$ is the measurement outputs with randomly occurring sensor saturations (ROSSs), $y(k) \in \mathbb{R}^{n_y}$ is the received measurement outputs with randomly occurring deception attacks (RODAs), $v(k) \in \mathbb{R}^{n_y}$ stands for the signal sent by adversaries with the non-zero $\xi(k) \in \mathbb{R}^{n_y}$ satisfying

$$\| \xi(k) \| \leq \delta_1. \tag{5}$$

for a given positive scalar δ_1. C and D_2 are known real constant matrices with appropriate dimensions.

Remark 1: When launching deception attacks, the attackers inject malicious data in order to degrade or deteriorate the system performances. In (4), the external signals (injected false data) sent by the adversaries are just $v(k)$ and the attackers do not need to know the exact information about $\tilde{y}(t)$. The reason for us to rewrite $v(k)$ as $v(k) = -\tilde{y}(k) + \xi(k)$ is just for the analysis convenience. Note that the "deception function" $\xi(k)$ is assumed to satisfy the boundedness condition (5) for the specific class of deception attacks considered in this paper.

The saturation function $\sigma(\cdot)$ is defined as

$$\sigma(u) = \begin{bmatrix}\sigma(u_1) & \sigma(u_2) & \dots & \sigma(u_{n_y})\end{bmatrix}^T, \quad \forall u \in \mathbb{R}^{n_y} \tag{6}$$

where $\sigma(u_i) = \text{sign}(u_i)\min\{\underline{u}_i, |u_i|\}$ for $i = 1, 2, \cdots, n_y$. Here, sign$(\cdot)$ denotes the signum function and $\underline{u}_i$ is the saturation level. From the definition of saturation function $\sigma(\cdot)$, there exists a diagonal matrix Λ satisfying $0 \leq \Lambda < I$ and

$$[\sigma(u) - \Lambda u]^T [\sigma(u) - u] \leq 0. \tag{7}$$

The stochastic variables $\alpha(k)$ and $\beta(k)$ are two mutually independent Bernoulli distributed white sequences taking values on 0 or 1 with the following probabilities

$$\begin{aligned}\text{Prob}\{\alpha(k) = 0\} =&1 - \bar{\alpha}, \quad \text{Prob}\{\alpha(k) = 1\} = \bar{\alpha},\\ \text{Prob}\{\beta(k) = 0\} =&1 - \bar{\beta}, \quad \text{Prob}\{\beta(k) = 1\} = \bar{\beta},\end{aligned} \tag{8}$$

where $\bar{\alpha} \in [0, 1)$ and $\bar{\beta} \in [0, 1)$ are two known constants.

Remark 2: In reality, the physical parameters of a networked environment (e.g. network load, network congestion, network transmission rate) are typically randomly fluctuated and, from the defenders' perspective, the attacks successfully passing through the detectors may occur intermittently or randomly. In other words, the successes of the attacks are largely dependent on the randomly changing network conditions and the given value of $\bar{\beta}$ represents the success rate for launched attacks that can be estimated through statistical tests or specified according to the security requirements.

Based on the measurements mentioned before, the following filter structure is adopted

$$\begin{aligned}\hat{x}(k+1) &= F\hat{x}(k) + Ny(k),\\ \hat{x}(j) &= 0, \quad j = -d_M, -d_M + 1, \dots, -1, 0,\end{aligned} \tag{9}$$

where $\hat{x}(k) \in \mathbb{R}^{n_x}$ is the state estimate, F and N are the filter parameters to be determined. $\hat{x}(j)$ $(j = -d_M, -d_M + 1, \dots, -1, 0)$ are the estimates of initial states.

By letting the filtering error $e(k)=x(k)-\hat{x}(k)$, it follows from (1), (4) and (9) that

$$\begin{aligned} e(k+1)=&Fe(k)+[A-(1-\alpha(k))(1-\beta(k))NC-F]x(k)+A_dx(k-d(k))\\ &-[\alpha(k)(1-\beta(k))N]\sigma(Cx(k))+[D_1-(1-\beta(k))ND_2]w(k)\\ &+Bf(x(k))+B_df_d(x(k-d(k)))-\beta(k)N\xi(k). \end{aligned} \tag{10}$$

It is easily seen that the initial errors satisfy $e(j)=x(j)=\varphi(j)$ $(j=-d_M,-d_M+1,\ldots,-1,0)$.

We introduce the following definition.

Definition 1: Let the positive constant scalars δ, δ_1, δ_2 and δ_3 be given. The filtering error system (10) is said to be $(\delta,\delta_1,\delta_2,\delta_3)$-*secure* if, when $\mathbb{E}w^2(k)\le\delta^2$, $\|\xi(k)\|\le\delta_1$ and $\sup\limits_{-d_M\le i\le 0}\mathbb{E}\|\varphi(i)\|^2\le\delta_2^2$, one has $\mathbb{E}\|e(k)\|^2\le\delta_3^2$ for all $k\ge d_M+1$.

In this paper, our main purpose is to design a filter for system (1) with measurement outputs described by (4) such that the filtering error system (10) is $(\delta,\delta_1,\delta_2,\delta_3)$-secure.

Remark 3: In the framework of H_∞ filtering, the exogenous disturbances are usually assumed to satisfy the energy-bounded conditions. In other words, the signals intensity from the outside will decrease gradually to zero as time tends to infinity. Such an assumption is, however, unsuitable for the deception attacks because the adversaries would launch uninterrupted attacks with non-zero intensities. In the presence of persistent attacks with non-zero intensities, it is only possible to ensure the boundedness (as opposed to the conventional zero-equilibrium in H_∞ filtering) of the filtering error which is essentially the requirement of the so-called security-guaranteed filtering. As such, instead of the energy-bounded condition, a norm-bounded condition is imposed on the external attack signals so as to make it possible to guarantee the boundedness (security) of the filtering errors.

III. Main Results

In this section, we first derive a sufficient condition under which the filtering error system (10) is $(\delta,\delta_1,\delta_2,\delta_3)$-secure in the presence of both ROSSs and RODAs. Based on the obtained condition, the design method of the desired filter is then given.

For the convenience of the manipulation, we set $\eta(k)=\begin{bmatrix}x^T(k) & e^T(k)\end{bmatrix}^T$, and then the dynamic system (1) and the filtering error system (10) can be combined into an augmented system as follows:

$$\begin{aligned} \eta(k+1)=&\bar{A}\eta(k)+\tilde{A}_d\eta(k-d(k))+\tilde{B}f(H_1\eta(k))+\tilde{B}_df_d(H_1\eta(k-d(k)))\\ &+\bar{D}w(k)+\bar{E}\sigma(CH_1\eta(k))-\beta(k)H_2N\xi(k) \end{aligned} \tag{11}$$

where

$$\begin{aligned} &\bar{A}=\begin{bmatrix}A & 0\\ A-(1-\alpha(k))(1-\beta(k))NC-F & F\end{bmatrix},\quad H_1=\begin{bmatrix}I & 0\end{bmatrix},\\ &\tilde{A}_d=\begin{bmatrix}A_d & 0\\ A_d & 0\end{bmatrix},\quad \tilde{B}=\begin{bmatrix}B\\ B\end{bmatrix},\quad \tilde{B}_d=\begin{bmatrix}B_d\\ B_d\end{bmatrix},\quad H_2=\begin{bmatrix}0\\ I\end{bmatrix},\\ &\bar{D}=\begin{bmatrix}D_1\\ D_1-(1-\beta(k))ND_2\end{bmatrix},\quad \bar{E}=\begin{bmatrix}0\\ -\alpha(k)(1-\beta(k))N\end{bmatrix}. \end{aligned}$$

The following lemma will be used in the proof of our main result in this paper.

Lemma 1: [4] Given constant matrices S_1, S_2 and S_3, where $S_1=S_1^T$ and $S_2=S_2^T>0$, then $S_1+S_3S_2^{-1}S_3^T<0$ if and only if

$$\begin{bmatrix}S_1 & S_3\\ S_3^T & -S_2\end{bmatrix}<0\quad\text{or}\quad\begin{bmatrix}-S_2 & S_3^T\\ S_3 & S_1\end{bmatrix}<0. \tag{12}$$

In the following theorem, a sufficient condition is provided under which the filtering error system (10) is $(\delta, \delta_1, \delta_2, \delta_3)$-secure.

Theorem 1: Let the positive scalars $\delta, \delta_1, \delta_2, \delta_3$ and the filter gains F, N be given. The filtering error system (10) is $(\delta, \delta_1, \delta_2, \delta_3)$-secure if there exist positive definite matrices P_1, P_2 and positive scalars ε_1, ε_2, ε_3, ε_4, ε_5 satisfying the following inequalities

$$\begin{cases} \Xi = \Phi_{11} + \Phi_{12}\Phi_{22}\Phi_{12}^T < 0 \\ \max\left\{ \dfrac{\zeta(r_0)}{\lambda_{\min}(P_1)}, \dfrac{\theta^2 r_0}{\lambda_{\min}(P_1)(r_0-1)} \right\} \le \delta_3^2 \end{cases} \tag{13}$$

where

$$\Phi_{11} = \begin{bmatrix} (d_M - d_m + 1)P_2 - P_1 + \Omega & 0 & -\varepsilon_3 R_2 & 0 & -\varepsilon_2 Q_2 & 0 & 0 \\ * & -P_2 - \varepsilon_5 S_1 & 0 & 0 & 0 & -\varepsilon_5 S_2 & 0 \\ * & * & -\varepsilon_3 I & 0 & 0 & 0 & 0 \\ * & * & * & -\varepsilon_4 I & 0 & 0 & 0 \\ * & * & * & * & -\varepsilon_2 I & 0 & 0 \\ * & * & * & * & * & -\varepsilon_5 I & 0 \\ * & * & * & * & * & * & -\varepsilon_1 I \end{bmatrix},$$

$$\Phi_{12} = \begin{bmatrix} \tilde{A} & \tilde{A}_d & \tilde{E} & 0 & \tilde{B} & \tilde{B}_d & -\bar{\beta} H_2 N \\ 0 & 0 & 0 & \tilde{D} & 0 & 0 & 0 \end{bmatrix}^T,$$

$$\tilde{A} = \begin{bmatrix} A & 0 \\ A - (1-\bar{\alpha})(1-\bar{\beta})NC - F & F \end{bmatrix},$$

$$\tilde{D} = \begin{bmatrix} D_1 \\ D_1 - (1-\bar{\beta})ND_2 \end{bmatrix}, \quad \tilde{E} = \begin{bmatrix} 0 \\ -\bar{\alpha}(1-\bar{\beta})N \end{bmatrix},$$

$$Q_1 = (H_1^T K_1^T K_2 H_1 + H_1^T K_2^T K_1 H_1)/2, \quad Q_2 = -H_1^T (K_1^T + K_2^T)/2,$$

$$S_1 = (H_1^T T_1^T T_2 H_1 + H_1^T T_2^T T_1 H_1)/2, \quad S_2 = -H_1^T (T_1^T + T_2^T)/2,$$

$$R_1 = H_1^T C^T \Lambda C H_1, \quad R_2 = -H_1^T C^T (\Lambda + I)/2,$$

$$\Omega = -\varepsilon_3 R_1 - \varepsilon_2 Q_1, \quad \Phi_{22} = \operatorname{diag}\{P_1, P_1\}, \quad \theta = \sqrt{\varepsilon_1 \delta_1^2 + \varepsilon_4 \delta^2},$$

and the constant $r_0 > 1$ in (13) is the solution to the following equation

$$-\lambda_{\min}(-\Xi) r_0 + (r_0 - 1)\lambda_{\max}(P_1) + 2r_0(d_M - d_m + 1)\lambda_{\max}(P_2)(r_0^{d_M} - 1) = 0, \tag{14}$$

and $\zeta(r_0)$ is given as follows

$$\zeta(r_0) = 2(\mu + \nu)\delta_2^2, \tag{15}$$

where

$$\begin{aligned} \mu &= d_M \lambda_{\max}(P_2)(r_0^{d_M} - 1)(d_M - d_m + 1), \\ \nu &= d_M \max(\lambda_{\max}(P_1), (d_M - d_m + 1)\lambda_{\max}(P_2)). \end{aligned} \tag{16}$$

Proof: Construct the following energy-like functional

$$V(k) = V_1(k) + V_2(k) + V_3(k), \tag{17}$$

where

$$\begin{aligned} V_1(k) =&\eta^T(k)P_1\eta(k),\\ V_2(k) =& \sum_{i=k-d(k)}^{k-1} \eta^T(i)P_2\eta(i),\\ V_3(k) =& \sum_{j=k-d_M+1}^{k-d_m}\sum_{i=j}^{k-1}\eta^T(i)P_2\eta(i). \end{aligned} \tag{18}$$

The mathematical expectation of the difference of the energy-like functional along the system (11) is calculated as follows:

$$\begin{aligned} &\mathbb{E}\{\Delta V(k)\}\\ =&\mathbb{E}\{\Delta V_1(k)\}+\mathbb{E}\{\Delta V_2(k)\}+\mathbb{E}\{\Delta V_3(k)\}\\ =&\mathbb{E}\left\{\eta^T(k+1)P_1\eta(k+1)-\eta^T(k)P_1\eta(k)+(d_M-d_m+1)\eta^T(k)P_2\eta(k)-\eta^T(k-d(k))P_2\eta(k-d(k))\right\}\\ =&\mathbb{E}\{\eta^T(k)(\tilde{A}^TP_1\tilde{A}+(d_M-d_m+1)P_2-P_1)\eta(k)+\eta^T(k-d(k))(\tilde{A}_d^TP_1\tilde{A}_d-P_2)\eta(k-d(k))\\ &+f^T(H_1\eta(k))\tilde{B}^TP_1\tilde{B}f(H_1\eta(k))+f_d^T(H_1\eta(k-d(k)))\tilde{B}_d^TP_1\tilde{B}_df_d(H_1\eta(k-d(k)))+w^T(k)\tilde{D}^TP_1\tilde{D}w(k)\\ &+\sigma^T(CH_1\eta(k))\tilde{E}^TP_1\tilde{E}\sigma(CH_1\eta(k))+\bar{\beta}^2\xi^T(k)N^TH_2^TP_1H_2N\xi(k)+2\eta^T(k)\tilde{A}^TP_1\tilde{A}_d\eta(k-d(k))\\ &+2\eta^T(k)\tilde{A}^TP_1\tilde{B}f(H_1\eta(k))+2\eta^T(k)\tilde{A}^TP_1\tilde{B}_df_d(H_1\eta(k-d(k)))+2\eta^T(k)\tilde{A}^TP_1\tilde{D}w(k)\\ &+2\eta^T(k)\tilde{A}^TP_1\tilde{E}\sigma(CH_1\eta(k))-2\bar{\beta}\eta^T(k)\tilde{A}^TP_1H_2N\xi(k)+2\eta^T(k-d(k))\tilde{A}_d^TP_1\tilde{B}f(H_1\eta(k))\\ &+2\eta^T(k-d(k))\tilde{A}_d^TP_1\tilde{B}_df_d(H_1\eta(k-d(k)))+2\eta^T(k-d(k))\tilde{A}_d^TP_1\tilde{D}w(k)+2\eta^T(k-d(k))\tilde{A}_d^TP_1\tilde{E}\sigma(CH_1\eta(k))\\ &-2\bar{\beta}\eta^T(k-d(k))\tilde{A}_d^TP_1H_2N\xi(k)+2f^T(H_1\eta(k))\tilde{B}^TP_1\tilde{B}_df_d(H_1\eta(k-d(k)))+2f^T(H_1\eta(k))\tilde{B}^TP_1\tilde{D}w(k)\\ &+2f^T(H_1\eta(k))\tilde{B}^TP_1\tilde{E}\sigma(CH_1\eta(k))-2\bar{\beta}f^T(H_1\eta(k))\tilde{B}^TP_1H_2N\xi(k)+2f_d^T(H_1\eta(k-d(k)))\tilde{B}_d^TP_1\tilde{D}w(k)\\ &+2f_d^T(H_1\eta(k-d(k)))\tilde{B}_d^TP_1\tilde{E}\sigma(CH_1\eta(k))-2\bar{\beta}f_d^T(H_1\eta(k-d(k)))\tilde{B}_d^TP_1H_2N\xi(k)\\ &+2w^T(k)\tilde{D}^TP_1\tilde{E}\sigma(CH_1\eta(k))-2\bar{\beta}w^T(k)\tilde{D}^TP_1H_2N\xi(k)-2\bar{\beta}\tilde{E}^T\sigma^T(CH_1\eta(k))P_1H_2N\xi(k)\} \end{aligned} \tag{19}$$

By noting (2), (5), (7), (10) and $\mathbb{E}w^2(k) \leq \delta^2$, it can be obtained further that

$$
\begin{aligned}
&\mathbb{E}\{\Delta V(k)\}\\
\leq&\mathbb{E}\{\eta^T(k)(\tilde{A}^T P_1 \tilde{A} + (d_M - d_m + 1)P_2 - P_1)\eta(k) + \eta^T(k-d(k))(\tilde{A}_d^T P_1 \tilde{A}_d - P_2)\eta(k-d(k))\\
&+ f^T(H_1\eta(k))\tilde{B}^T P_1 \tilde{B} f(H_1\eta(k)) + f_d^T(H_1\eta(k-d(k)))\tilde{B}_d^T P_1 \tilde{B}_d f_d(H_1\eta(k-d(k))) + w^T(k)\tilde{D}^T P_1 \tilde{D} w(k)\\
&+ \sigma^T(CH_1\eta(k))\tilde{E}^T P_1 \tilde{E}\sigma(CH_1\eta(k)) + \bar{\beta}^2 \xi^T(k) N^T H_2^T P_1 H_2 N \xi(k) + 2\eta^T(k)\tilde{A}^T P_1 \tilde{A}_d \eta(k-d(k))\\
&+ 2\eta^T(k)\tilde{A}^T P_1 \tilde{B} f(H_1\eta(k)) + 2\eta^T(k)\tilde{A}^T P_1 \tilde{B}_d f_d(H_1\eta(k-d(k))) + 2\eta^T(k)\tilde{A}^T P_1 \tilde{D} w(k)\\
&+ 2\eta^T(k)\tilde{A}^T P_1 \tilde{E}\sigma(CH_1\eta(k)) - 2\bar{\beta}\eta^T(k)\tilde{A}^T P_1 H_2 N \xi(k) + 2\eta^T(k-d(k))\tilde{A}_d^T P_1 \tilde{B} f(H_1\eta(k))\\
&+ 2\eta^T(k-d(k))\tilde{A}_d^T P_1 \tilde{B}_d f_d(H_1\eta(k-d(k))) + 2\eta^T(k-d(k))\tilde{A}_d^T P_1 \tilde{D} w(k) + 2\eta^T(k-d(k))\tilde{A}_d^T P_1 \tilde{E}\sigma(CH_1\eta(k))\\
&- 2\bar{\beta}\eta^T(k-d(k))\tilde{A}_d^T P_1 H_2 N \xi(k) + 2f^T(H_1\eta(k))\tilde{B}^T P_1 \tilde{B}_d f_d(H_1\eta(k-d(k))) + 2f^T(H_1\eta(k))\tilde{B}^T P_1 \tilde{D} w(k)\\
&+ 2f^T(H_1\eta(k))\tilde{B}^T P_1 \tilde{E}\sigma(CH_1\eta(k)) - 2\bar{\beta} f^T(H_1\eta(k))\tilde{B}^T P_1 H_2 N \xi(k) + 2f_d^T(H_1\eta(k-d(k)))\tilde{B}_d^T P_1 \tilde{D} w(k)\\
&+ 2f_d^T(H_1\eta(k-d(k)))\tilde{B}_d^T P_1 \tilde{E}\sigma(CH_1\eta(k)) - 2\bar{\beta} f_d^T(H_1\eta(k-d(k)))\tilde{B}_d^T P_1 H_2 N \xi(k)\\
&+ 2w^T(k)\tilde{D}^T P_1 \tilde{E}\sigma(CH_1\eta(k)) - 2\bar{\beta} w^T(k)\tilde{D}^T P_1 H_2 N \xi(k) - 2\bar{\beta}\tilde{E}^T\sigma^T(CH_1\eta(k)) P_1 H_2 N \xi(k)\}\\
&+ \varepsilon_1(\delta_1^2 - \xi^T(k)\xi(k)) - \varepsilon_2[f(H_1\eta(k)) - K_1 H_1\eta(k)]^T[f(H_1\eta(k)) - K_2 H_1\eta(k)]\\
&- \varepsilon_3[\sigma(CH_1\eta(k)) - \Lambda CH_1\eta(k)]^T[\sigma(CH_1\eta(k)) - CH_1\eta(k)] + \varepsilon_4(\delta^2 - w^T(k)w(k))\\
&- \varepsilon_5[f_d(H_1\eta(k-d(k))) - T_1 H_1\eta(k-d(k))]^T[f_d(H_1\eta(k-d(k))) - T_2 H_1\eta(k-d(k))]\}\\
=&\mathbb{E}\left\{\phi^T(k)\Xi\phi(k) + \theta^2\right\},
\end{aligned}
\tag{20}
$$

where

$$
\phi(k) = \begin{bmatrix}\eta^T(k) & \eta^T(k-d(k)) & \sigma^T(CH_1\eta(k)) & w^T(k) & f^T(H_1\eta(k)) & f_d^T(H_1\eta(k-d(k))) & \xi^T(k)\end{bmatrix}^T.
$$

By considering (13), it is easily known that

$$
\mathbb{E}\{\Delta V(k)\} \leq -\lambda_{\min}(-\Xi)\mathbb{E}\{\|\eta(k)\|^2\} + \theta^2. \tag{21}
$$

On the other hand, according to the definition of the energy-like functional $V(k)$, it is seen that

$$
V(k) \leq \lambda_{\max}(P_1)\mathbb{E}\{\|\eta(k)\|^2\} + \lambda_{\max}(P_2)(d_M - d_m + 1)\sum_{i=k-d_M}^{k-1}\mathbb{E}\{\|\eta(i)\|^2\}. \tag{22}
$$

Now we introduce a scalar $r > 1$ and it follows from (21) and (22) that

$$
\begin{aligned}
&\mathbb{E}\{r^{k+1}V(k+1)\} - \mathbb{E}\{r^k V(k)\}\\
=&r^{k+1}\mathbb{E}\{\Delta V(k)\} + r^{k+1}\mathbb{E}\{V(k)\} - r^k\mathbb{E}\{V(k)\}\\
\leq&r^{k+1}[-\lambda_{\min}(-\Xi)\mathbb{E}\{\|\eta(k)\|^2\} + \theta^2] + r^k(r-1)\mathbb{E}\{V(k)\}\\
\leq&a(r)r^k\mathbb{E}\{\|\eta(k)\|^2\} + b(r)\sum_{i=k-d_M}^{k-1} r^k\mathbb{E}\{\|\eta(i)\|^2\} + r^{k+1}\theta^2
\end{aligned}
\tag{23}
$$

where

$$
\begin{aligned}
a(r) &= -\lambda_{\min}(-\Xi)r + (r-1)\lambda_{\max}(P_1),\\
b(r) &= (d_M - d_m + 1)(r-1)\lambda_{\max}(P_2).
\end{aligned}
$$

For any integer $T \geq d_M + 1$, summing up both sides of (23) from 0 to $T-1$ with respect to k yields

$$\begin{aligned}&\mathbb{E}\{r^T V(T)\} - \mathbb{E}\{V(0)\}\\ \leq& a(r)\sum_{k=0}^{T-1} r^k \mathbb{E}\{\|\eta(k)\|^2\} + \frac{r(1-r^T)}{1-r}\theta^2 + b(r)\sum_{k=0}^{T-1}\sum_{i=k-d_M}^{k-1} r^k \mathbb{E}\{\|\eta(i)\|^2\}.\end{aligned} \tag{24}$$

The last term in (24) can be computed as

$$\begin{aligned}&\sum_{k=0}^{T-1}\sum_{i=k-d_M}^{k-1} r^k \mathbb{E}\{\|\eta(i)\|^2\}\\ \leq& \left(\sum_{i=-d_M}^{-1}\sum_{k=0}^{i+d_M} + \sum_{i=0}^{T-d_M-1}\sum_{k=i+1}^{i+d_M} + \sum_{i=T-d_M}^{T-1}\sum_{k=i+1}^{T-1}\right) r^k \mathbb{E}\{\|\eta(i)\|^2\}\\ \leq& \frac{r^{d_M}-1}{r-1}\sum_{i=-d_M}^{-1}\mathbb{E}\{\|\eta(i)\|^2\} + \frac{r(r^{d_M}-1)}{r-1}\sum_{i=0}^{T-1} r^i \mathbb{E}\{\|\eta(i)\|^2\}\\ &+ \frac{r(r^{d_M-1}-1)}{r-1}\sum_{i=0}^{T-1} r^i \mathbb{E}\{\|\eta(i)\|^2\}.\end{aligned} \tag{25}$$

Substituting (24) and (25), we have

$$\begin{aligned}&\mathbb{E}\{r^T V(T)\} - \mathbb{E}\{V(0)\}\\ \leq& \frac{r(1-r^T)}{1-r}\theta^2 + \frac{b(r)(r^{d_M}-1)d_M}{r-1}\sup_{-d_M\leq i\leq 0}\mathbb{E}\{\|\eta(i)\|^2\}\\ &+ \xi(r)\sum_{k=0}^{T-1} r^k \mathbb{E}\{\|\eta(k)\|^2\},\end{aligned} \tag{26}$$

where

$$\xi(r) = a(r) + \frac{2rb(r)(r^{d_M}-1)}{r-1}.$$

Since $\xi(1) = -\lambda_{\min}(-\Xi) < 0$ and $\lim_{r\to\infty}\xi(r) = +\infty$, there exists a scalar $r_0 > 1$ such that $\xi(r_0) = 0$. Hence, we find a scalar $r_0 > 1$ such that

$$\begin{aligned}&\mathbb{E}\{r_0^T V(T)\} - \mathbb{E}\{V(0)\}\\ \leq& \frac{r_0(1-r_0^T)}{1-r_0}\theta^2 + \frac{b(r_0)(r_0^{d_M}-1)d_M}{r_0-1}\sup_{-d_M\leq i\leq 0}\mathbb{E}\{\|\eta(i)\|^2\}.\end{aligned} \tag{27}$$

Noting

$$\begin{aligned}&\sup_{-d_M\leq i\leq 0}\mathbb{E}\{\|\eta(i)\|^2\}\\ =& \sup_{-d_M\leq i\leq 0}\mathbb{E}\{\|x(i)\|^2 + \|e(i)\|^2\}\\ \leq& \sup_{-d_M\leq i\leq 0}\mathbb{E}\{\|x(i)\|^2\} + \sup_{-d_M\leq i\leq 0}\mathbb{E}\{\|e(i)\|^2\} \leq 2\delta_2^2,\end{aligned} \tag{28}$$

$$\mathbb{E}\{r_0^T V(T)\} \geq \lambda_{\min}(P_1) r_0^T \mathbb{E}\{\|\eta(T)\|^2\} \geq \lambda_{\min}(P_1) r_0^T \mathbb{E}\{\|e(T)\|^2\}, \tag{29}$$

and

$$\mathbb{E}\{V(0)\} \leq d_M \max\left(\lambda_{\max}(P_1), (d_M - d_m + 1)\lambda_{\max}(P_2)\right)\sup_{-d_M\leq i\leq 0}\mathbb{E}\{\|\eta(i)\|^2\}, \tag{30}$$

we have

$$\begin{aligned}\mathbb{E}\{\|e(T)\|^2\} &\leq \frac{(r_0^T-1)\theta^2}{r_0^{T-1}(r_0-1)\lambda_{\min}(P_1)}+\frac{\zeta(r_0)}{r_0^T\lambda_{\min}(P_1)}\\ &= r_0^{-T}\left[\frac{\zeta(r_0)}{\lambda_{\min}(P_1)}-\frac{\theta^2 r_0}{\lambda_{\min}(P_1)(r_0-1)}\right]+\frac{\theta^2 r_0}{\lambda_{\min}(P_1)(r_0-1)}\\ &\leq \max\left\{\frac{\zeta(r_0)}{\lambda_{\min}(P_1)},\frac{\theta^2 r_0}{\lambda_{\min}(P_1)(r_0-1)}\right\}.\end{aligned} \tag{31}$$

By noting (13), it can be obtained that $\mathbb{E}\{\|e(T)\|^2\}\leq\delta_3^2$ which, from Definition 1, implies that the filtering error system (10) is $(\delta,\delta_1,\delta_2,\delta_3)$-secure and therefore the proof of Theorem 1 is complete. ■

Remark 4: It should be mentioned that, the aim of constructing a Lyapunov functional is to analyze the stability for systems according to the traditional Lyapunov stability theory. In Theorem 1, however, we are interested in the boundedness (rather than the stability) of the filter errors and the proposed energy-like functional is employed to deduce the boundedness conditions.

According to the analysis conducted in Theorem 1, a solution to the secure filtering problem with ROSSs and RODAs is obtained in the following theorem. For the convenience of design, the positive definite matrix P_1 is taken as $P_1=\mathrm{diag}\{P_{11},P_{22}\}$ where P_{11} and P_{22} are positive definite matrices.

Theorem 2: Let the positive scalars $\delta,\delta_1,\delta_2,\delta_3$ be given. If there exist positive definite matrices $P_1=\mathrm{diag}\{P_{11},P_{22}\}$, P_2, matrices X, Y and positive scalars ε_1, ε_2, ε_3, ε_4, ε_5 satisfying the following inequalities

$$\begin{cases}\Pi=\begin{bmatrix}\Pi_{11}&\Pi_{12}\\ *&\Pi_{22}\end{bmatrix}<0\\ \max\left\{\dfrac{\zeta(r_0)}{\lambda_{\min}(P_1)},\dfrac{\theta^2 r_0}{\lambda_{\min}(P_1)(r_0-1)}\right\}\leq\delta_3^2\end{cases} \tag{32}$$

where

$$\Pi_{11}=\begin{bmatrix}(d_M-d_m+1)P_2-P_1+\Omega & 0 & -\varepsilon_3R_2 & 0 & -\varepsilon_2Q_2 & 0 & 0\\ * & -P_2-\varepsilon_5S_1 & 0 & 0 & 0 & -\varepsilon_5S_2 & 0\\ * & * & -\varepsilon_3I & 0 & 0 & 0 & 0\\ * & * & * & -\varepsilon_4I & 0 & 0 & 0\\ * & * & * & * & -\varepsilon_2I & 0 & 0\\ * & * & * & * & * & -\varepsilon_5I & 0\\ * & * & * & * & * & * & -\varepsilon_1I\end{bmatrix},$$

$$\Pi_{12}=\begin{bmatrix}\hat{A}&P_1\tilde{A}_d&\hat{E}&0&P_1\tilde{B}&P_1\tilde{B}_d&-\bar{\beta}H_2Y\\ 0&0&0&\hat{D}&0&0&0\end{bmatrix}^T,\quad \Pi_{22}=\mathrm{diag}\{-P_1,-P_1\},$$

$$\hat{A}=\begin{bmatrix}P_{11}A & 0\\ P_{22}A-(1-\bar{\alpha})(1-\bar{\beta})YC-X & X\end{bmatrix},$$

$$\hat{D}=\begin{bmatrix}P_{11}D_1\\ P_{22}D_1-(1-\bar{\beta})YD_2\end{bmatrix},\quad \hat{E}=\begin{bmatrix}0\\ -\bar{\alpha}(1-\bar{\beta})Y\end{bmatrix},$$

and the constant $r_0>1$ in (32) becomes the solution to the following equation

$$-\lambda_{\min}(-\Pi)r_0+(r_0-1)\lambda_{\max}(P_1)+2r_0(d_M-d_m+1)\lambda_{\max}(P_2)(r_0^{d_M}-1)=0, \tag{33}$$

then, the filtering error system (10) is $(\delta,\delta_1,\delta_2,\delta_3)$-secure. In this case, the filter gain matrices are given by

$$\begin{aligned}F&=P_{22}^{-1}X,\\ N&=P_{22}^{-1}Y.\end{aligned} \tag{34}$$

Proof: From Lemma 1, it is known that $\Xi < 0$ is equivalent to

$$\Phi = \begin{bmatrix} \Phi_{11} & \Phi_{12} \\ * & -\Phi_{22}^{-1} \end{bmatrix} < 0. \tag{35}$$

Pre- and post-multiplying the inequality (35) by $\mathrm{diag}\{I, \Phi_{22}\}$, we can obtain

$$\hat{\Phi} = \begin{bmatrix} \Phi_{11} & \hat{\Phi}_{12} \\ * & \hat{\Phi}_{22} \end{bmatrix} < 0, \tag{36}$$

where

$$\begin{aligned} \hat{\Phi}_{12} =& \begin{bmatrix} P_1\tilde{A} & P_1\tilde{A}_d & P_1\tilde{E} & 0 & P_1\tilde{B} & P_1\tilde{B}_d & -\bar{\beta}P_1H_2N \\ 0 & 0 & 0 & P_1\tilde{D} & 0 & 0 & 0 \end{bmatrix}^T, \\ \hat{\Phi}_{22} =& \mathrm{diag}\{-P_1, -P_1\}. \end{aligned} \tag{37}$$

By setting $X = P_{22}F$ and $Y = P_{22}N$, it is easily seen that $\Pi < 0$ is exactly as the same as inequality (36) which means that the conditions in Theorem 1 are satisfied and the rest of the proof of Theorem 2 follows Theorem 1 directly. ■

Until now, we have analyzed security issue for the filtering error system with randomly occurring both sensor saturations and deception attacks, and obtained a sufficient condition which ensures the $(\delta, \delta_1, \delta_2, \delta_3)$-security of the filtering error system. In Theorem 2, the design method of the desired filter has been given.

Remark 5: In Theorems 1-2, the security-guaranteed filtering problem is solved for a class of nonlinear stochastic discrete time-delay systems with ROSSs and RODAs. The new concept of $(\delta, \delta_1, \delta_2, \delta_3)$-security is proposed to reflect the degree of security against the noise intensity, the energy bound of the false signals and the energy of the initial system state, all of which are included in the main results in addition to the sector-bound of the nonlinearities as well as the bounds of the time-delays. An energy-like functional is constructed to derive the delay-dependent security criteria and the corresponding solvability conditions for the desired filter gains are expressed in terms of the feasibility of few linear matrix inequalities (LMIs) that can be solved using available software package.

Remark 6: It is worth mentioning that this paper is not concerned with the attack detection issue. However, no matter how strong the attack is, a security-guaranteed filter can be always obtained by using the proposed design approach.

IV. Illustrative Examples

In this section, a numerical simulation example is given to show the effectiveness of the filtering methods proposed in this paper. The parameters of the nonlinear stochastic discrete time-delay system (1) are given as follows

$$\begin{aligned} &A = \begin{bmatrix} 0.5 & 0.02 \\ 0.01 & 0.6 \end{bmatrix}, \quad A_d = \begin{bmatrix} 0.05 & 0 \\ 0 & 0.03 \end{bmatrix}, \quad B = \begin{bmatrix} 0.02 & 0.1 \\ 0 & 0.05 \end{bmatrix}, \\ &B_d = \begin{bmatrix} 0.01 & 0 \\ 0 & 0.02 \end{bmatrix}, \quad D_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad d_m = 1, \quad d_M = 5. \end{aligned}$$

The nonlinear functions are chosen to be

$$\begin{aligned} f(x(k)) &= \mathrm{sign}(x(k))\mathrm{log}(\mathrm{sign}(x(k))x(k) + 1), \\ f_d(x(k - d(k))) &= \mathrm{sign}(x(k - d(k)))\mathrm{log}(\mathrm{sign}(x(k - d(k)))x(k - d(k)) + 1). \end{aligned}$$

It is easy to see that functions f and f_d satisfy the sector-bounded conditions (2) with parameters

$$K_1 = T_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad K_2 = T_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The parameters of the measurement output model are taken as

$$C = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad D_2 = 1.$$

Moreover, the sensor saturation parameter is set as $\Lambda = 0.5$ and the probabilities of saturations and deception attacks are assumed to be $\bar{\alpha} = 0.2$ and $\bar{\beta} = 0.3$. The parameters δ, δ_1, δ_2 and δ_3 are taken as 0.3, 0.2, 0.3 and 1.2, respectively.

With the above parameters, the inequality in (32) is solved by using the Matlab software (with the YALMIP 3.0) and, according to (34), the desired filter gains F and N can be obtained as follows

$$F = \begin{bmatrix} -0.0592 & 0.0435 \\ -0.2187 & 0.3780 \end{bmatrix}, \quad N = \begin{bmatrix} 1.0130 \\ 0.6939 \end{bmatrix}.$$

In the simulation, the disturbance from attackers is selected as $\xi(k) = \delta_1$ and the initial values of the state are chosen as $x(-5) = x(-4) = x(-3) = x(-2) = x(-1) = x(0) = \begin{bmatrix} 0.2 & 0.2 \end{bmatrix}^T$. The simulation results are shown in Figs. 1-6. Figs. 1-2 plot the actually occurring time instants of sensor saturations and deception attacks, respectively. Figs. 3-4 depict the state trajectories and their estimates. The norm of filtering errors in the presence of sensor saturations and deception attacks is shown in Fig. 5, from which we can see that the norm is always below the given bound δ_3. Also, the relation between the norm of filtering error and the attack bound is shown in Fig. 6. It can be seen from Fig. 6 that the norm of the filtering error will increase when the attack bound becomes large. The simulation results have demonstrated the effectiveness of the designed filter.

V. Conclusions

In this paper, we have discussed the secure filtering problem for a class of nonlinear stochastic discrete time-delay systems with both ROSSs and RODAs. A novel measurement output model has been provided to describe the ROSSs and RODAs within a unified framework. Then, by using the stochastic analysis techniques, a sufficient condition has been obtained to guarantee the security requirement of the addressed systems. Furthermore, the design method of the desired secure filter gain has been obtained by solving a linear matrix inequality with nonlinear constraints. Finally, a numerical example has been exploited to show the usefulness of the filtering scheme derived in this paper. One of the future research topics would be the extension of our main results to the distributed filtering problems over wireless sensor networks [23].

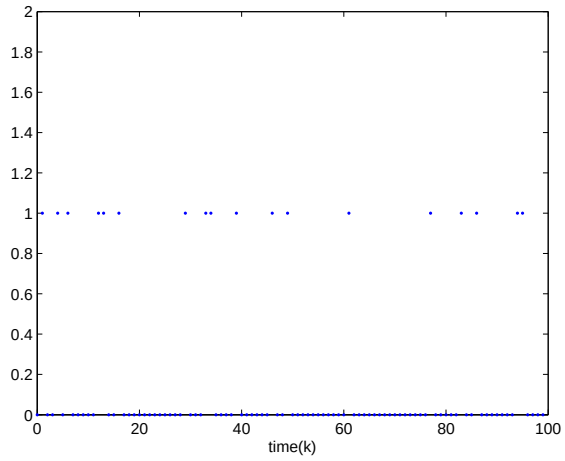

Fig. 1: Occurring of sensor saturations.

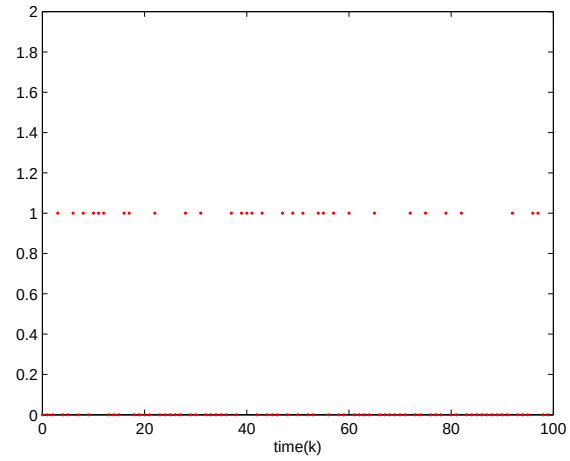

Fig. 2: Occurring of deception attacks.

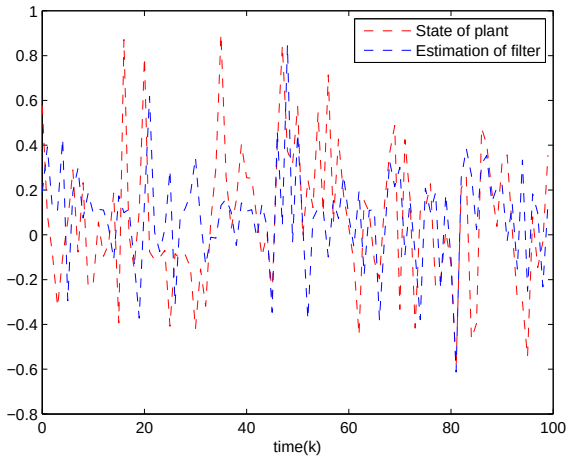

Fig. 3: State $x_1(k)$ and its estimate $\hat{x}_1(k)$.

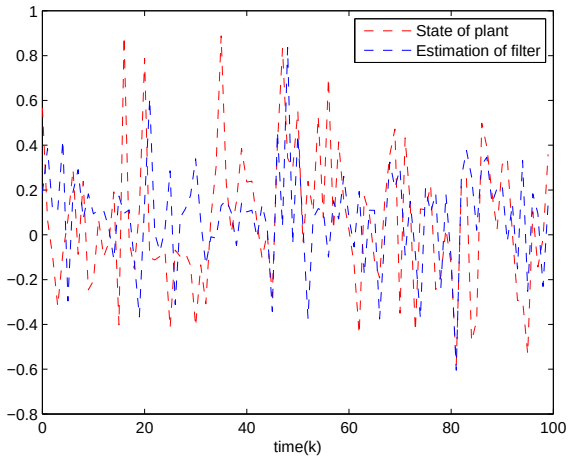

Fig. 4: State $x_2(k)$ and its estimate $\hat{x}_2(k)$.

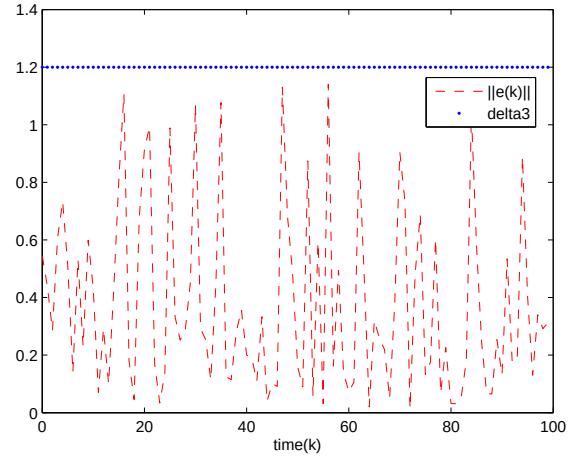

Fig. 5: The norm of filtering errors with both sensor saturations and deception attacks.

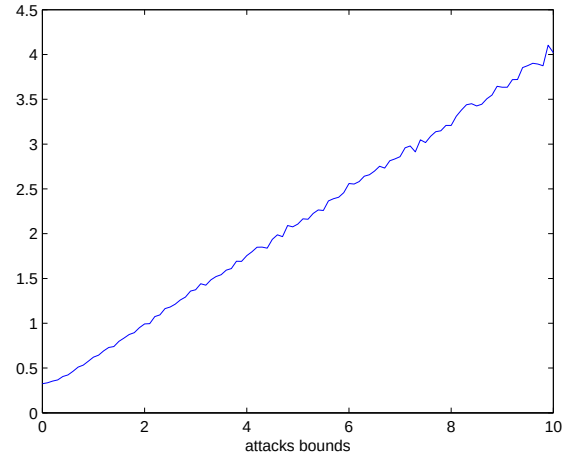

Fig. 6: The average norm of filtering errors.

REFERENCES

[1] M. Basin, S. Elvira-Ceja and E. Sanchez. Mean-square H_∞ filtering for stochastic systems: application to a 2DOF helicopter. *Signal Processing*, vol. 92, no. 3, pp. 801–806, 2012.

[2] S. Bi and Y. Zhang, Graphical methods for defense against false-data injection attacks on power system state estimation, *IEEE Transactions on Smart Grid*, Vol. 5, No. 3, pp. 1216-1227, May. 2014.

[3] S. Bi and Y. Zhang, Using covert topological information for defense against malicious attacks on DC state estimation, *IEEE Journal on Selected Areas in Communications*, Vol. 32, No. 7, pp. 1471-1485, Jul. 2014.

[4] S. Boyd, L. Ghaoui, E. Feron and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*, SIAM: philadelphia, 1994.

[5] R. Caballero-Águila, A. Hermoso-Carazo and J. Linares-Pérez. Optimal state estimation for networked systems with random parameter matrices, correlated noises and delayed measurements. *International Journal of General Systems* vol. 44, no. 2, pp. 142–154, 2015.

[6] D. Ding, Z. Wang, B. Shen and 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, Dec. 2015.

[7] D. Ding, Z. Wang and B. Shen, Recent advances on distributed filtering for stochastic systems over sensor networks, *International Journal of General Systems*, Vol. 43, No. 3-4, pp. 372–386, 2014.

[8] D. Ding, Z. Wang, Fuad E. Alsaadi, and Bo Shen, Receding horizon filtering for a class of discrete time-varying nonlinear systems with multiple missing measurements, *International Journal of General Systems*, Vol. 44, No. 2, pp. 198-211, 2015.

[9] D. Ding, Z. Wang, J. Lam and B. Shen, Finite-Horizon H_∞ control for discrete time-varying systems with randomly occurring nonlinearities and fading measurements, *IEEE Transactions on Automatic Control*, Vol. 60, No. 9, pp. 2488–2493, 2015.

[10] H. Dong, Z. Wang, D. W. C. Ho and H. Gao, Robust H_∞ filtering for markovian jump systems with randomly occurring nonlinearities and sensor saturation: the finite-horizon case, *IEEE Transactions on Signal Processing*, Vol. 59, No. 7, pp. 3048-3057, Jul. 2011.

[11] H. Dong, Z. Wang, F. E. Alsaadi and B. Ahmad, Event-triggered robust distributed state estimation for sensor networks with state-dependent noises, *International Journal of General Systems*, Vol. 44, No. 2, pp. 254-266, 2015.

[12] Z. Feng, G. Hu and G. Wen, Distributed consensus tracking for multi-agent systems under two types of attacks, *International Journal of Robust and Nonlinear Control*, published online, DOI:10.1002/rnc.3342, 2015.

[13] H. Gao and C. Wang, A delay-dependent approach to robust H_∞ filtering for uncertain discrete-time state-delayed systems, *IEEE Transactions on Signal Processing*, Vol. 52, No. 6, pp. 1631-1640, Jun. 2004.

[14] N. Hou, H. Dong, Z. Wang, W. Ren and F. E. Alsaadi, Non-fragile state estimation for discrete Markovian jumping neural networks, *Neurocomputing*, Vol. 179, pp. 238–245, Feb. 2016.

[15] J. Hu, Z. Wang, H. Gao, L. Stergioulas, Probability-guaranteed H_∞ finite-horizon filtering for a class of nonlinear time-varying systems with sensor saturations, *Systems and Control Letters*, Vol. 61, No. 4, pp. 477-484, Apr. 2012.

[16] K. Ito and K. Xiong, Gaussian filters for nonlinear filtering problems, *IEEE Transactions on Automatic Control*, Vol. 45, No. 5, pp. 910-927, May 2000.

[17] S. Julier, J. Uhlmann and H. Durrant-Whyte, A new method for the nonlinear transformation of means and covariances in filters and estimators, *IEEE Transactions on Automatic Control*, Vol. 45, No. 3, pp. 477-482, Mar. 2000.

[18] H. Li and Y. Shi, Robust H_∞ filtering for nonlinear stochastic systems with uncertainties and Markov delays, *Automatica*, Vol. 48, No. 1, pp. 159-166, Jan. 2012

[19] Y. Liu, F. E. Alsaadi, X. Yin and Y. Wang, Robust H_∞ filtering for discrete nonlinear delayed stochastic systems with missing measurements and randomly occurring nonlinearities, *International Journal of General Systems*, Vol. 44, No. 2, pp. 169-181, 2015.

[20] Y. Luo, G. Wei, Y. Liu and X. Ding, Reliable H_∞ state estimation for 2-D discrete systems with infinite distributed delays and incomplete observations, *International Journal of General Systems*, Vol. 44, No. 2, pp. 155-168, 2015.

[21] Y. Mo and B. Sinopoli, Secure estimation in the presence of integrity attacks, *IEEE Transactions on Automatic Control*, Vol. 60, No. 4, pp. 1145-1151, Apr. 2015.

[22] Y. Niu, D. W. C. Ho and C. Li, H_∞ filtering for uncertain stochastic systems subject to sensor nonlinearities, *International Journal of Systems Science*, Vol. 42, No. 5, pp. 737-749, 2011.

[23] V. Ugrinovskii, Distributed robust filtering with H_∞ consensus of estimates, *Automatica*, Vol. 47, No. 1, pp. 1-13, Jan. 2011.

[24] D. Wang, X. Guan, T. Liu, Y. Gu, C. Shen and Z. Xu, Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids, *Energies*, Vol. 7, No. 3, pp. 1517-1538, Mar. 2014.

[25] Z. Wang, Y. Liu and X. Liu, H_∞ filtering for uncertain stochastic time-delay systems with sector-bounded nonlinearities, *Automatica*, Vol. 44, No. 5, pp. 1268-1277, May. 2008.

[26] Z. Wang, B. Shen and X. Liu, H_∞ filtering with randomly occurring sensor saturations and missing measurements, *Automatica*, Vol. 48, No. 3, pp. 556-562, Mar. 2012.

[27] G. Wei, F. Han, L. Wang and Y. Song, Reliable H_∞ filtering for discrete piecewise linear systems with infinite distributed delays, *International Journal of General Systems*, Vol. 43, No. 3-4, pp. 346-358, May. 2014.

[28] G. Wei, Z. Wang and H. Shu, Robust filtering with stochastic nonlinearities and multiple missing measurements, *Automatica*, Vol. 45, No. 3, pp. 836-841, Mar. 2009.

[29] S. Xu, T. Chen and J. Lam, Robust H_∞ filtering for uncertain Markovian jump systems with mode-dependent time delays, *IEEE Transactions on Automatic Control*, Vol. 48, No. 5, pp. 900-907, May. 2003.

[30] F. Yang, H. Dong, Z. Wang, W. Ren and F. E. Alsaadi, A new approach to non-fragile state estimation for continuous neural networks with time-delays, *Neurocomputing*, Vol. 197, pp. 205–211, Jul. 2016.

[31] W. Yang, M. Liu and P. Shi, H_∞ filtering for nonlinear stochastic systems with sensor saturation, quantization and random packet losses, *Signal Processing*, Vol. 92, No. 6, pp. 1387-1396, Jun. 2012.

[32] F. Yang and Y. Li, Set-membership filtering for systems with sensor saturation, *Automatica*, Vol. 45, No. 8, pp. 1896-1902, Aug. 2009.

[33] H. Yang, Z. Wang, H. Shu, F. E. Alsaadi and T. Hayat, Almost sure H_∞ sliding mode control for nonlinear stochastic systems with Markovian switching and time-delays, *Neurocomputing*, Vol. 175, pp. 392-400, Jan. 2016.

[34] 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.

[35] H. Zhang, H. Yan, F. Yang and Q. Chen, Distributed average filtering for sensor networks with sensor saturation, *IET Control Theory and Applications*, Vol. 7, No. 6, pp. 887-893, Apr. 2013.

[36] W. Zhang, G. Feng and L. Yu. Multi-rate distributed fusion estimation for sensor networks with packet losses, *Automatica*, Vol. 48, No. 9, pp. 2016-2028, Sep. 2012.

[37] S. Zhou and J. Lam, H_∞ filtering for systems with delays and time-varying nonlinear parameters, *Circuits, Systems and Signal Processing*, Vol. 29, No. 4, pp. 601-627, Aug. 2010.

[38] S. Zonouz, K. Rogers and R. Berthier, SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures, *IEEE Transactions on Smart Grid*, Vol. 3, No. 4, pp. 1790-1799, Dec. 2012.