Neurocomputing 207 (2016) 708–716

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks☆

Shuai Liu [a], Guoliang Wei [b,*], Yan Song [b], Yurong Liu [c,d]

[a] Business School, University of Shanghai for Science and Technology, Shanghai 200093, People's Republic of China
[b] Department of Control Science and Engineering, Key Laboratory of Modern Optical System, University of Shanghai for Science and Technology, Shanghai 200093, People's Republic of China
[c] Department of Mathematics, Yangzhou University, Yangzhou 225002, People's Republic of China
[d] Communication Systems and Networks (CSN) Research Group, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia

ARTICLE INFO

Article history:
Received 16 January 2016
Received in revised form
10 April 2016
Accepted 24 May 2016
Communicated by Ma Lifeng Ma
Available online 7 June 2016

Keywords:
Stochastic nonlinear system
Extended Kalman filtering
Randomly occurring cyber attack
Stochastic boundedness

ABSTRACT

This paper is concerned with the extended Kalman filtering problem for a class of stochastic nonlinear systems under cyber attacks, wherein the discussed cyber attacks occur in a random way in the data transmission from sensor nodes to remote filter nodes. A novel cyber attack model is established in a unified representation to account for both the false data injection attacks and the denial of service (DoS) attacks. Moreover, a more general nonlinear description that stands for both the deterministic and stochastic nonlinearities is put forward. By virtue of the recurrence on the stochastic analysis approach, the upper bound of filtering error covariance is obtained, and it can be minimized at each time instant via solving an optimization problem. Furthermore, a sufficient condition is provided to ensure the stochastic boundedness of filtering error in the simultaneous presence of randomly occurring cyber attacks and nonlinearities. Eventually, one example is presented to verify the validity of the suggested filtering scheme.

1. Introduction

Kalman filtering, one of the most popular state estimation\ filtering approaches with respect to signal processing, has been proven to be a powerful tool to settle filtering problems since it was first proposed in 1960s. After then, considerable efforts have been devoted to numerous applications such as engineering, biological and economic systems. As is well known, the classical Kalman filtering scheme usually serves as an optimal filtering algorithm in the minimum error covariance sense for the linear systems with the Gaussian noises. In the real world, however, many practical systems involve somewhat nonlinear properties due to their inherent characteristics and the influence of the external environment. In such a case, the traditional Kalman filtering approach is no more valid to handle the nonlinearities, thus it gives rise to the necessary studies in developing some nonlinear filtering technologies so as to close the gap. In the existing literature, there are considerable results on dealing with the estimation problem for nonlinear systems, H_∞ filtering [1–3], variance-constrained filtering [4], set-membership filtering [5], extended Kalman filtering (EKF) [6–9] and so on. With regard to the aforementioned various filtering techniques, EKF is much favorable especially in practical engineering due to its convenient-to-design and easy-to-implement. In consideration of the errors resulting from the linearization process in EKF algorithm, an additional deviation of the system model is introduced, whereas it might lead to the degradation of the filtering performance or even the divergence of the system. To handle such a challenge, Einicke and White [10] presented a new robust design approach for a discrete-time EKF based on the H_∞ norm minimization criterion, in which, it was assumed that the linearization errors were functions of the state estimation errors and the exogenous inputs with the bounded H_∞ norm. Furthermore, in [11], by modelling the linearization errors as a norm-bounded uncertainty term, a novel robust EKF was proposed for discrete-time nonlinear systems with stochastic uncertainties, by which an optimized upper bound of the estimation error covariance could be guaranteed. Similarly, such an approach was adopted to deal with linearization errors under the conditions of the stochastic nonlinearities and multiple missing measurements in [6]. It has been proven out that such a method can

☆This work was supported in part by the National Natural Science Foundation of China under Grants 61573246, 61403254, 61374039, Shanghai Natural Science Foundation of China under Grant 13ZR1428500, Innovation Program of Shanghai Municipal Education Commission 14YZ083, Program for Capability Construction of Shanghai Provincial Universities 15550502500.

* Corresponding author.
E-mail address: guoliang.wei1973@gmail.com (G. Wei).

http://dx.doi.org/10.1016/j.neucom.2016.05.060
0925-2312/© 2016 Elsevier B.V. All rights reserved.

effectively reduce the conservatism by introducing extra degree of freedom. Unfortunately, it is incredibly difficult to obtain the iterative solution of filtering error covariance. Thus, one usually prefers to seek an upper bound for the admissible error covariance by local minimization instead, which is also adopted to deal with the EKF problem via network communication in this paper.

Over the past few decades, the networked communication has gained much attentions because of its overwhelming advantages compared with the traditional point-to-point connection, and it thus has been increasingly applied into various fields [12,13]. Although networked communication works much better on low cost, simple installation and maintenance as well as high reliability, it unavoidably causes the network traffic congestion during the frequent data transmission between components, therefore some network-induced phenomena unexpectedly arise, time delays, signal quantizations, missing measurements, etc. Some efforts have been devoted to dealing with the challenges for networked control systems, see, for example [14–17], and the references therein.

Additionally, security protection has been seldom focused in many achievements on networked systems. Regardless of the system security, data might be broken by the malevolent attacks during the transmission, and then the system performance might be deteriorated. Therefore, system security is an indispensable issue and should receive more and more attention. In typical networked control systems (NCSs), sensors, controllers and actuators are integrated through common network links, which makes the networked systems vulnerable to two severe kinds of security threats known as denial of service (DoS) attacks [18,19] and false data injection (deception) attacks [20–22]. Generally speaking, the main purpose of those attackers is to destroy the data through network communication in order to make the plant instable or drive the system into their expected operation area. In this case, a secure mechanism is necessarily demanded for the defences against the cyber attacks. It should be pointed out that adversary attacks might be prevented and intercepted by the protection devices, that is to say, the attacks usually occur in a random manner. To the best of our knowledge, few results have been obtained on cyber attacks, especially in EKF community, which motives our research on such a challenging issue.

In response to the above discussions, this paper is concerned with the EKF problem for a class of stochastic nonlinear systems subject to randomly occurring cyber attacks. The main challenges for the analysis and synthesis issues can be divided into the following aspects: (1) how to develop a comprehensive system model in a unified presentation so as to account for both the nonlinear perturbations and the randomly occurring mixed cyber attacks; (2) how to deal with the linearization error in a proper manner to reduce the conservatism; (3) how to design the filter parameter with an explicit analytical form to achieve the specified filtering performance; and (4) how to guarantee the exponential boundedness of filtering error for the stochastic nonlinear systems with random attacks.

In this paper, our objective is of dealing with the above challenges. Therefore, the main contributions can be summarized as follows: (1) a novel model is put forward to characterize the mixed cyber attacks by using a set of Bernoulli distributed white sequences; (2) by employing the adjustable term that satisfies the norm bounded uncertainty, the linearization error is effectively handled; (3) an upper bound of filtering error covariance is obtained by solving two coupled algebraic Riccati-like equations, then the filter gain can be obtained by minimizing such an upper bound; and (4) in terms of stochastic boundedness analysis technique, a sufficient condition is established to ensure the exponential boundedness in the mean square for all admissible nonlinearities and randomly occurring cyber attacks.

The rest of this paper is organized as follows. In Section 2, a class of stochastic nonlinear systems subject to randomly occurring cyber attacks is presented. In Section 3, firstly, the upper bound of filtering error covariance is obtained iteratively based on the feasible solutions of the two coupled algebraic Riccati-like equations, and the desired filter parameters are derived via solving a family of optimal problems to minimize such an upper bound. Secondly, the stochastic boundedness of filtering error is ensured in the mean square under some rational assumptions. In Section 4, an illustrative example is applied to show the feasibility of the presented filter design scheme. Finally, we conclude this paper in Section 5.

Notations: The notation employed throughout the paper is fairly standard. The notation $X \geq Y (X > Y)$, where X and Y are real symmetric matrices, is used to represent that $X - Y$ is a positive semi-definite (positive definite) matrix. $\|\cdot\|$ refers to the Euclidean norm in $\mathbb{R}^n$. The shorthand $\mathrm{diag}\{\cdots\}$ represents a block-diagonal matrix. A^T stands for the transpose of A. I represents identity matrix with appropriate dimension. $\mathrm{tr}(\cdot)$ stands for the trace of a matrix. $\mathbb{E}\{x\}$ represents the mathematical expectation of the stochastic variable x. Matrices, if they are not explicitly specified, are assumed to have compatible dimensions.

2. Problem formulation

In this paper, consider the following discrete-time stochastic nonlinear system defined on $k \in [0, N]$:

$$x_{k+1} = f(x_k) + g(x_k, \eta_k) + D_k w_k, \tag{1}$$

$$\tilde{y}_k = h(x_k) + E_k v_k \tag{2}$$

where $x_k \in \mathbb{R}^n$ is the state vector of the target plant, and $\tilde{y}_k \in \mathbb{R}^m$ is the measurement output from sensors. $w_k \in \mathbb{R}^p$ and $v_k \in \mathbb{R}^q$ are zero mean and uncorrelated Gaussian white noise sequences with known variances Q_k and R_k, respectively. $f(x_k)$ and $h(x_k)$ are deterministic nonlinear functions. $\eta_k \in \mathbb{R}$ is a zero mean Gaussian white noise sequence. D_k and E_k are time-varying matrices with compatible dimensions.

In this paper, we mainly consider two kinds of nonlinear functions including deterministic nonlinearities and stochastic nonlinearities. In the following, we give the detailed nonlinear descriptions.

Firstly, the deterministic nonlinear function $h(x_k)$: $\mathbb{R}^n \to \mathbb{R}^n$ is assumed to be continuously differentiable satisfying

$$\| h(x_k)\| \leq a_1 \| x_k \| + a_2 \tag{3}$$

where a_1 and a_2 are some nonnegative real scalars.

Besides, following the similar line in [23,24], the stochastic nonlinear function $g(x_k, \eta_k)$ satisfying $g(0, \eta_k) = 0$ has the statistical properties as follows:

$$\begin{cases} \mathbb{E}\{g(x_k, \eta_k)|x_k\} = 0, \\ \mathbb{E}\{g(x_k, \eta_k)g^T(x_j, \eta_j)|x_k\} = 0, \quad k \neq j, \\ \mathbb{E}\{g(x_k, \eta_k)g^T(x_k, \eta_k)|x_k\} = \sum_{i=1}^{s} \Pi_k^i x_k^T \Gamma_k^i x_k \end{cases} \tag{4}$$

where s is a known nonnegative integer; Π_k^i and Γ_k^i $(i = 1, \ldots, s)$ are positive semidefinite matrices with appropriate dimensions.

Remark 1. As is well known, almost all real-time systems inevitably suffer from the nonlinear disturbances induced by environment changes. So far, a good many efforts have been devoted to describe the nonlinearities in different ways, such as Lipschitz nonlinearities, sector-bounded nonlinearities and stochastic