Automatica 78 (2017) 231–240

Contents lists available at ScienceDirect

Automatica

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

Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks☆

Derui Ding [a,1], Zidong Wang [b], Daniel W.C. Ho [c], Guoliang Wei [a]

[a] Shanghai Key Lab of Modern Optical System, Department of Control Science and Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China

[b] Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, UK

[c] Department of Mathematics, City University of Hong Kong, Kowloon, Hong Kong, China

ARTICLE INFO

Article history:
Received 4 January 2016
Received in revised form
10 June 2016
Accepted 19 November 2016

Keywords:
Sensor networks
Distributed filtering
Recursive filtering
Deception attacks
Uniform quantization

ABSTRACT

This paper is concerned with the distributed recursive filtering problem for a class of discrete time-delayed stochastic systems subject to both uniform quantization and deception attack effects on the measurement outputs. The target plant is disturbed by the multiplicative as well as additive white noises. A novel distributed filter is designed where the available innovations are from not only the individual sensor but also its neighboring ones according to the given topology. Attention is focused on the design of a distributed recursive filter such that, in the simultaneous presence of time-delays, deception attacks and uniform quantization effects, an upper bound for the filtering error covariance is guaranteed and subsequently minimized by properly designing the filter parameters via a gradient-based method at each sampling instant. Furthermore, by utilizing the mathematical induction, a sufficient condition is established to ensure the asymptotic boundedness of the sequence of the error covariance. Finally, a simulation example is utilized to illustrate the usefulness of the proposed design scheme of distributed filters.

1. Introduction

For a few decades, as one of the most notable algorithms for state estimation problems, the Kalman filtering (KF) technique has been playing an important role in signal processing and system control fields (Basin, Alcorta-Garcia, & Rodriguez-Gonzalez, 2005; Basin & Martinez-Zuniga, 2004; Zeng, Wang, & Zhang, 2016). The KF technique is essentially a maximum-likelihood estimate algorithm for linear models with Gaussian noises under a quadratic performance criterion (Gandhi & Mili, 2010). To cope with nonlinearities and/or uncertainties, there have been a few sub-optimal variants based on the traditional KF algorithm. Examples include, but are not limited to, the robust KF for uncertain systems (Gandhi & Mili, 2010), the extended KF (EKF) or the unscented KF for nonlinear systems (Hu, Chen, & Du, 2014) and the KF/EKF for systems with equality constraints (Simon & Chia, 2002). Recently, the Kalman filtering problem for systems with communication delays has received considerable research interest corresponding to the popularity of the networked systems. In case of the discrete time-delayed systems, the filtering algorithms have been proposed via system augmentation approach in order to utilize the Riccati equation methods (Lu, Xie, Zhang, & Wang, 2007). Different from the discrete-time case, the continuous-time system with delayed measurements can be converted into a nominal system with delay-free measurements via the re-organizing method (Kong, Saif, & Zhang, 2013). It is worth mentioning that the computational burden would become an issue for the augmentation and re-organizing methods especially when the time-delays are relatively large. Obviously, an adequate trade-off between the estimation accuracy and the computational efficiency should be taken into account when dealing with time-delays in the filtering problems.

It is well known that, in networked systems, an analog-to-digital converter is usually adopted to convert the continuous-time analog signal to the corresponding discrete-time digital one. Due primarily to the operation of rounding or truncation, the unavoidable difference between the actual analog value and

☆ The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Brett Ninness under the direction of Editor Torsten Söderström.

E-mail addresses: deruiding2010@usst.edu.cn (D. Ding), Zidong.Wang@brunel.ac.uk (Z. Wang), madaniel@cityu.edu.hk (D.W.C. Ho), guoliang.wei1973@gmail.com (G. Wei).

[1] Fax: +86 21 55271299.

http://dx.doi.org/10.1016/j.automatica.2016.12.026
0005-1098/

converted digital one is customarily referred to as the quantization error or quantization distortion. This kind of errors can be modeled as a bounded unknown disturbance or as an additional random signal obeying *uniform distribution* (Brockett & Liberzon, 2000; Rojas & Lotero, 2015). Up to now, the stabilization and minimum data transmission rate issues with uniform quantization have been investigated by utilizing Lyapunov functions combined with perturbation analysis techniques, see e.g. Brockett and Liberzon (2000). It is worth emphasizing that the quantization errors from uniform quantizers are *non-square summable sequences* that cannot be described by the widely used *state-dependent Lipschitz-like conditions*, Li, Shen, Liang, and Shu (2015) and therefore cannot be handled by the well-known robust design techniques. This may well explain why the results on filter/controller design problems under uniform quantizations have been scattered in comparison with those for logarithmic quantizations.

On the other hand, in parallel with the quiet evolution of sensor network technologies, the distributed filtering problem through sensor networks has gained an ever-increasing interest from researchers in many areas such as signal processing and control engineering, and a number of filtering algorithms have been proposed in the literature, see e.g. Dong, Wang, Alsaadi, and Ahmad (2015), Dong, Wang, and Gao (2013) and Li, Shen, Liu, and Alsaadi (2016) for the distributed H_∞ filtering schemes and (Olfati-Saber, 2007) for the distributed KF methods. In particular, a distributed filtering framework that sheds insightful light on this domain has been established in Olfati-Saber (2007) with the aid of two identical consensus filters for fusion of the sensor data and covariance information. A typical feature with the distributed filters is their collaborative information processing mechanism, that is, the information available on an individual node is not only from its own measurement but also from its neighboring sensors' measurements according to the given topology via open networks. Note that the sensor nodes are usually made of low cost devices with low computing capacity and limited battery power. As such, the sensor networks might be vulnerable to cyber-attacks especially during the signal transmission (Marano, Matta, & Tong, 2009; Zhang, Blum, Lu, & Conus, 2015) and, accordingly, the emerging cyber-security issues have been raised that have quickly attracted much attention, see e.g. Pang and Liu (2012) and Vempaty, Tong, and Varshney (2013).

In the general context of networked control systems, so far, much progress has been made on the security control/filtering problems by employing the techniques of dynamic programming or Lyapunov stability theory, see e.g. Amin, Schwartz, and Shankar Sastry (2013) and Long, Wu, and Hung (2005) for denial-of-service (DoS) attacks and (Ding, Wang, Ho, & Wei, 2016; Ding, Wei, Zhang, Liu, & Alsaadi, 2017; Fawzi, Tabuada, & Diggavi, 2014; Hu, Liu, Ji, & Li, 2016; Pang & Liu, 2012) for deception attacks. However, when it comes to the distributed filtering issues over sensor networks, only a limited number of results have been available in the literature (see e.g. Marano et al., 2009; Vempaty, Ozdemir, Agrawal, Chen, & Varshney, 2013; Zhang et al., 2015). For instance, under binary hypotheses with quantized sensor observations, the optimal attacking distributions have been estimated in Marano et al. (2009) to minimize the detection error exponent and the fraction of Byzantine sensors (i.e. compromised sensors for adversaries). Recently, in Zhang et al. (2015), the identification and categorization issues of attacked sensors have been discussed by utilizing the joint estimation of the statistical description of the attacks and the estimated parameter. Note that most existing results have been concerned with *static target plants* despite the fact that *dynamic target plants* are more often encountered in engineering practice, which is due probably to the difficulties in analyzing the dynamics in collaborative nature and spatial structure when designing distributed filters.

In the research area of cyber-security, the success ratio of the launched attacks has recently become an emerging topic of research from the defenders' perspectives. The launched attacks by the adversaries may not always be successful for mainly three reasons: (1) only a relatively small amount of attacks could pass through the detectors (with anti-attack countermeasures) for systems equipped with protection devices or software; (2) the attacks cannot be persistently (or arbitrarily) launched by the adversaries due to unavoidable limited resource (e.g. energy); and (3) the attacks sent through the networks with limited bandwidth are subject to randomly fluctuated condition changes (e.g. network load, network congestion and network transmission rate) and therefore cannot arrive at the desired end. As such, *from the viewpoint of the defending party*, the successfully occurred cyber-attacks can be understood to be intermittent or random in implementation, and the corresponding issue of intermittently or randomly occurred cyber-attacks have been dealt with in Amin et al. (2013), Zhang et al. (2015) and Zhu and Martinez (2014). For example, the maximal number of succession attacks has been investigated in Zhu and Martinez (2014) where a variation of the receding-horizon control law has been proposed to deal with the replay attacks and analyze the resulting system performance degradation. Nevertheless, the *intermittent or random* nature of the successfully occurred cyber-attacks has not received adequate attention yet for the distributed filtering problem of *dynamic target plants*, not to mention the case where the multiplicative/additive noises (Gershon, Shaked, & Yaesh, 2001) and the uniform quantizations are also the concerns.

Summarizing the above discussions, the focus of this paper is on the parameter design and performance analysis of distributed recursive filtering with uniform quantization and intermittent deception attacks. We endeavor to answer the following questions: (1) how to design a distributed filter effectively fusing the unreliable data corrupted by noises, quantization errors and possible deception attacks? (2) how to develop an efficient filtering algorithm that would help reduce the computation burden resulting from time delays and the large number of sensor nodes? and (3) how to cope with the complicated coupling issues between the filtering errors and observed states in the performance analysis? The main contribution of this paper is threefold: (1) *a novel structure of distributed filters is designed to adequately utilize the available innovations from not only itself (credible measurements) but also its neighboring sensors which could be subject to deception attacks*; (2) *the developed filter design algorithm is of a form suitable for distributed recursive computation in online applications via solving two Riccati-like difference equations; and* (3) *a sufficient condition is proposed to show the asymptotic boundedness of the filtering error covariance through intensive stochastic analysis.*

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 dimension. 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). M^T represents the transpose of M. $\mathbb{E}\{x\}$ stands for the expectation of stochastic variable x. $\|x\|$ describes the Euclidean norm of a vector x. The shorthand $\mathrm{diag}\{M_1, M_2, \ldots, M_n\}$ denotes a block diagonal matrix with diagonal blocks being the matrices $M_1, M_2, \ldots, M_n$.

2. Problem formulation and preliminaries

In this paper, the underlying sensor network has n sensor nodes which are distributed in space according to a fixed network topology represented by a directed graph $\mathscr{G} = (\mathscr{V}, \mathscr{E}, \mathscr{H})$ of order n with the set of nodes $\mathscr{V} = \{1, 2, \ldots, n\}$, the set of edges