Applied Mathematics and Computation 320 (2018) 158–174

Contents lists available at ScienceDirect

Applied Mathematics and Computation

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

Hybrid-driven-based H_∞ filter design for neural networks subject to deception attacks

Jinliang Liu[a,*], Jilei Xia[a], Engang Tian[b], Shumin Fei[c]

[a] College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, Jiangsu 210023, PR China
[b] Institute of Information and Control Engineering Technology, Nanjing Normal University, Nanjing, Jiangsu 210042, PR China
[c] School of Automation, Southeast University, Nanjing, Jiangsu 210096, PR China

ARTICLE INFO

Keywords:
Neural networks
Hybrid triggered scheme
H_∞ filter design
Deception attacks

ABSTRACT

This paper investigates the problem of H_∞ filter design for neural networks with hybrid triggered scheme and deception attacks. In order to make full use of the limited network resources, a hybrid triggered scheme is introduced, in which the switching between the time triggered scheme and the event triggered scheme obeys Bernoulli distribution. By considering the effect of hybrid triggered scheme and deception attacks, a mathematical model of H_∞ filtering error system is constructed. The sufficient conditions that can ensure the stability of filtering error system are given by using Lyapunov stability theory and linear matrix inequality (LMI) techniques. Moreover, the explicit expressions are provided for the designed filter parameters that is in terms of LMIs. Finally, a numerical example is employed to illustrate the design method.

1. Introduction

Nowadays, neural networks have been triumphantly applied in many areas such as image processing, associative storage, signal optimization, large volume of high speed data processing. Over the last decades, rapidly increasing attention has been paid to the research of neural networks, and a great number of achievements have been obtained by researchers [1–5]. Due to the certain theory meaning and application value of filter design for neural networks, the research on filter design for delayed neural networks has attracted extensive attention in recent years [6–9]. In [7], the authors investigate the resilient finite-time filtering problem for discrete-time uncertain Markov jump neural networks with packet dropouts. The authors in [8] investigate the robust H_∞ filtering problem for neural delay differential systems with parametric uncertainties. In literature [9], the authors are concerned with H_∞ filter design for a class of neural network systems with event-triggered communication scheme and quantization.

During the past few decades, time triggered scheme (periodic sampling) that is applied for the sensor sampling in the analysis and design of control systems has been widely studied by lots of researchers [10,11]. For example, a model of networked control systems is constructed by taking the effects of network-induced delay and data dropout into consideration in [11]. Based on the constructed model of networked control systems above, the design of robust H_∞ controllers for uncertain networked control systems is investigated in [11]. However, if all sampling data is delivered via the network, it will result in plenty of waste for the limited network resources. To avoid the drawbacks of periodic sampling, many researchers propose

* Corresponding author.
E-mail address: liujinliang@vip.163.com (J. Liu).

https://doi.org/10.1016/j.amc.2017.09.007
0096-3003/

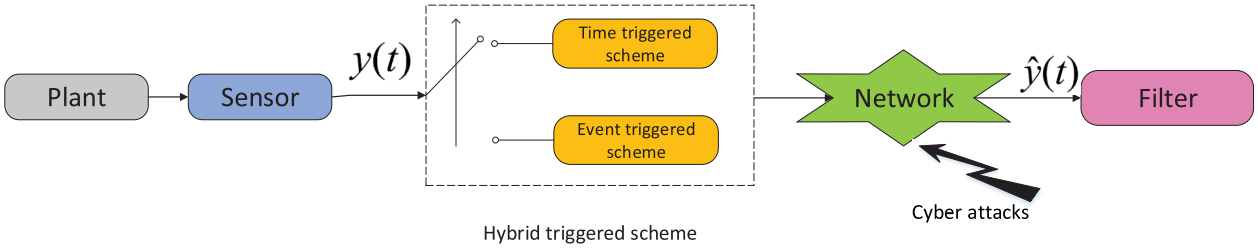

Fig. 1. The structure of hybrid-driven-based H_∞ filter for neural networks subject to deception attacks.

event triggered schemes to reduce the burden of network and enhance the efficiency of transmission. For example, a new event triggered scheme is proposed in [12] to investigate the problem of event-triggered controller design for networked control systems. The basic idea of event triggered scheme in [12] is that whether the pre-designed condition is violated or not can be the key rule of transmission for newly sampling data, in other words, it only be delivered when newly sampling data violates the pre-designed conditions. Based on the research achievement in [12], large numbers of researchers have arisen interest in the investigation of event triggered scheme and obtained fruitful achievements [13–16]. For instance, the authors in [13] investigate the problem of event-triggered state estimation for complex network systems with quantization. A decentralized event triggering communication scheme for large-scale systems is investigated in [14] under network environments. The authors of [15] are devoted to the design of H_∞ event-triggered filter for a class of T-S fuzzy systems. Drawing lessons from existing researches on the event-triggered scheme in [12], the authors in [17] propose a new hybrid triggered scheme, in which the stochastic switching between the time triggered scheme and event triggered scheme is described by a variable obeying Bernoulli distribution. On the basis of hybrid triggered scheme in [17], the problem of reliable control for hybrid-driven T-S fuzzy systems with actuator faults and probabilistic nonlinear perturbations is investigated in [18]. In this paper, inspired by the proposed hybrid triggered scheme in [17], an H_∞ filter design is investigated with hybrid triggered scheme and deception attacks.

Cyber attacks are aggressive behaviors aiming at destroying communication systems, real sampling data, networked infrastructures and devices. As is described in [19], Denial of Service attacks, replay attacks and deception attacks are three categories of cyber attacks. One of the most important attack modes on the safety of network is the deception attacks that include an incorrect sensor measurement or a mistaken identity of the receiving equipment. In view of the significance of network security, the risks of deception attacks should not be ignored any more with the fast development of network. On the basis of the deception attacks mentioned above, more and more researchers are devoting to the exploration of deception attacks [19–21]. For example, the attack scheduling problem for a class of stochastic linear systems with χ_2 detectors is studied in [19]. The authors investigate 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 in [20]. A novel event based distributed estimator is proposed in [21] to defend against the false injection attack. Based on the deception attacks proposed in [19], this paper is concerned with hybrid-driven-based H_∞ filter design for neural networks subject to deception attacks.

Motivated by the observations above, this paper addresses the issue of H_∞ filter design for neural networks with hybrid-triggered scheme and deception attacks. The hybrid triggered scheme that consists of time triggered scheme and event triggered scheme is introduced to reduce the pressure of network bandwidth. A mathematical model of H_∞ filtering error system is constructed by taking the effect of hybrid triggered scheme and deception attacks into consideration. Sufficient conditions that can guarantee the stability of filtering error system for neural networks are obtained by using Lyapunov stability theory and LMI techniques. Moreover, the parameters of the filter are obtained in explicit expression. A simulation example is provided to show the usefulness of the proposed method.

This paper is organized as follows. In Section 2, a filtering error system is considered for the neural networks with hybrid triggered scheme and deception attacks. Section 3 gives sufficient conditions which can guarantee the stability of filtering error system for neural networks. A numerical example is given in Section 4 to show the usefulness of the proposed method. The conclusion is drawn in the final part.

Notation: R^n and $R^{n\times m}$ denote the n-dimensional Euclidean space, and the set of $n\times m$ real matrices; Matrix $X>0$, for $X\in R^{n\times n}$ means that the matrix X is real symmetric positive definite. I is the identity matrix of appropriate dimension. In addition, T stands for the transpose of matrix. For a matrix B and two symmetric matrices A and C, $\left[\begin{smallmatrix} A & * \\ B & C \end{smallmatrix}\right]$ denotes a symmetric matrix, where $*$ denotes the entries implied by symmetry.

2. System description

In this paper, a hybrid-driven-based H_∞ filter design for neural networks subject to deception attacks is investigated. As is shown in Fig. 1, supposing that the sampling data is transmitted in a non-ideal networked environment, the hybrid triggered scheme is introduced to reduce the pressure of network bandwidth. The neural networks with n neurons is given