Neurocomputing 000 (2018) 1–15

Contents lists available at ScienceDirect

Neurocomputing

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

Quantized state estimation for neural networks with cyber attacks and hybrid triggered communication scheme

Jinliang Liu[a], Jilei Xia[a], Jie Cao[a,*], Engang Tian[b]

[a] College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, Jiangsu 210023, China
[b] Institute of Information and Control Engineering Technology, Nanjing Normal University, Nanjing, Jiangsu 210042, China

ARTICLE INFO

Article history:
Received 12 November 2017
Revised 25 December 2017
Accepted 10 February 2018
Available online xxx

Communicated by Prof. Wei Guoliang

Keywords:
Neural networks
Hybrid triggered scheme
State estimation
Cyber attacks

ABSTRACT

This paper is concerned with the issue of quantized state estimation for neural networks with cyber attacks and hybrid triggered communication scheme. In order to reduce the pressure of the network transmission and save the network resources, the hybrid triggered scheme and quantization are introduced. The hybrid triggered scheme consists of time triggered scheme and event triggered scheme, in which the stochastic switch is described by a variable satisfying Bernoulli distribution. First, by taking the effect of hybrid triggered scheme and quantization into consideration, a mathematical model for estimating the state of neural networks is constructed. Second, by using linear matrix inequality (LMI) techniques and Lyapunov stability theory, the sufficient conditions are given which can ensure the stability of estimating error system under hybrid triggered scheme, and the designing algorithm of desired state estimator is also presented in terms of LMIs. Finally, a numerical example is given to show the usefulness of the proposed approach.

1. Introduction

In recent years, the dynamic behaviors of neural networks have been paid increasing attention due to their potential applications in automation, image recognition, data compression and large volume of high speed data processing. It is well known that understanding the neuron states is an indispensable step to apply the neural networks and realize the desired performance in practical application. A large number of researchers have made great achievements in the neuron state estimation problem [1–4]. In [1], the authors investigate the variance-constrained state estimation problem for a class of networked multi-rate systems with network-induced probabilistic sensor failures and measurement quantization. The authors in [2] concentrate on the problem of stochastic finite-time state estimation for discrete time-delay neural networks with Markovian jumps. In literature [3], the authors consider the problem of state estimation with guaranteed performance for a class of switching fuzzy neural networks.

Over the past few decades, time triggered scheme (periodic sampling) is intensively applied for systems modeling in conventional control systems [5–7]. In [5], the authors consider the robust H_∞ filtering problem for a class of uncertain nonlinear time-delay stochastic systems. In view of the limited network resources, the drawback of time triggered scheme which contains the transmitting of large repetitive signals is prominent day by day. To avoid the shortcoming of time triggered scheme, another triggered scheme named event triggered scheme is proposed, which is used to deal with many issues of data transmission for networked control systems. For example, a novel event triggered scheme, which is used to reduce the communication load of the network, is proposed in [8] to investigate the problem of H_∞ controllers design for networked control systems with network-induced delay. Different from the time triggered scheme, the main idea of event triggered scheme mentioned above is that whether the settled threshold is violated or not can be the key rule of newly sampling data transmission. Based on the proposed event triggered scheme in [8], a large number of scholars concentrate on the investigations of event triggered scheme and have obtained abundant research results [9–12]. For example, an adaptive event-triggered communication scheme is proposed in [9] which is applied for a class of networked Takagi–Sugeno (T–S) fuzzy control systems. In [10], the problem of event-triggered reliable H_∞ filtering for networked systems with multiple sensor distortions is investigated. The authors in [11] are devoted to the design of event-triggered non-fragile state estimator for delayed neural networks subject to randomly occurring sensor nonlinearity. On the basis of the proposed event triggered scheme in [8], another triggered scheme named hybrid triggered scheme is proposed in [13], which is used to

* Corresponding author.
E-mail addresses: liujinliang@vip.163.com (J. Liu), caojie690929@163.com (J. Cao).

https://doi.org/10.1016/j.neucom.2018.02.060
0925-2312/

investigate the design of hybrid driven controller for networked control systems with network-induced delays. Inspired by the work mentioned above, some researchers make a further study about hybrid triggered scheme [14–17]. The authors in [14] are devoted to the reliable controller design for hybrid-driven nonlinear systems via T–S fuzzy model with probabilistic actuator faults and probabilistic nonlinear perturbations. The problem of H_∞ filter design for neural networks is investigated in [15] with hybrid triggered scheme and deception attacks. The hybrid-triggered H_∞ filtering problem is considered for networked systems under stochastic cyber attacks in [16]. In this paper, the hybrid triggered scheme is introduced to investigate the state estimation for neural networks with cyber attacks.

Recently, the quantitative processing has drawn much attention which is an effective way to save the network resources besides the event triggered scheme mentioned above. In networked control systems, the quantitative processing which contains the compression and decompression of sampling data aims at reducing the pressure of transmission and save network resources. Motivated by the merit of quantization mentioned above, many researchers have taken the effect of quantization into consideration for networked systems [18–20]. The problem of H_∞ output feedback control for event-triggered Markovian jump system is investigated in [18] with measured output quantizations. In [19], an event-driven networked control systems has been studied subject to quantization and packet losses. The authors in [20] investigate the dynamic output-feedback control problem for a class of discrete-time nonlinear stochastic systems with uniform quantization effects. In this paper, due to the quantitative processing which can reduce the pressure of network transmission in networked systems, the quantization is introduced in the investigation of state estimation for neural networks. To the best of authors' knowledge, the state estimation for neural networks with hybrid triggered scheme and quantization has not been investigated yet, which is the motivation of this paper.

The insertion of network has posed many conveniences in data transmission, but it also brings a lot of challenges such as packet losses, nonlinear disturbance and network-induced delay. In addition, another offensive behavior named cyber attacks aims at destroying data transmission system, real-time sampling data, communication infrastructures and networked devices. According to descriptions in [21,22], cyber attacks, which include an inaccurate sampling data and misidentification of the receiving devices, have generated greater threats to the safety of network. Given the importance of network security, enough attention should be paid to the risks of the cyber attacks. In recent years, large numbers of researchers are devoted to the investigations of cyber attacks and have obtained abundant research results [23–25]. For example, a novel approach of state filtering scheme and the sensor scheduling co-design for cyber–physical systems subject to random deception attacks is investigated in [23]. The authors in [24] investigate online deception attack strategy against remote state estimation with sensor-to-estimator communication rate constraint. A novel distributed state estimator with an event-triggered scheme is proposed in [25] to defend against false data injection attack. Drawing lessons from the existing achievements about cyber attacks, this paper is concerned with the design of state estimator for neural networks under hybrid triggered scheme subject to cyber attacks.

Motivated by the observations above, this paper is concerned with state estimation for neural networks with hybrid triggered scheme and quantization subject to cyber attacks. The hybrid triggered scheme and quantization are introduced to reduce the pressure of network transmission. Cyber attacks are also considered to make the state estimation for neural networks closer to the working condition of the actual system. Finally, a numerical example is given to show the usefulness of the proposed method.

This paper is organized as follows. In Section 2, a mathematical model of the estimating error system is constructed by taking the effects of hybrid triggered scheme and cyber attacks into consideration. Sufficient conditions which can guarantee stability of the estimating error system are established and a state estimator design method is provided in Section 3. A numerical example is given in Section 4 to show the usefulness of the proposed method. The conclusion is given in the final part.

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

2. System description

This paper is concerned with state estimation for neural networks with hybrid triggered scheme and quantization subject to cyber attacks. As is shown in Fig. 1, the hybrid triggered scheme and quantization are introduced to reduce the pressure of network transmission. A random variable which satisfies Bernoulli distribution is employed to describe the stochastic switch between the time triggered scheme and event triggered scheme in the hybrid triggered scheme. Consider the following neural networks with time-varying delays and n neurons [4,26,27]:

$$\begin{cases}\dot{x}(t) = -Ax(t) + W_0 g(x(t)) + W_1 g(x(t-\phi(t)))\\ y(t) = Cx(t)\end{cases} \tag{1}$$

where $x(t)=[x_1(t),x_2(t),\cdots,x_n(t)]^T\in\mathbb{R}^n$ is the state vector of neural networks and $y(t)=[y_1(t),y_2(t),\ \cdots,y_r(t)]^T\in\mathbb{R}^r$ is the measurement output; $A=diag\{a_1,a_2,\cdots,a_n\}$ is a diagonal matrix with positive entries $a_i>0$; W_0 and W_1 are the connection weight matrix and the delayed connection weight matrix, respectively; C is a given constant matrix of appropriate dimensions. $g(x(t)) = [g_1(x_1(t)),g_2(x_2(t)),\cdots,g_n(x_n(t))]^T$ denotes the neuron activation function, and $\phi(t)$ denotes the time-varying bounded state delay satisfying $\phi(t)\in[\phi_m,\phi_M]$, where ϕ_m and ϕ_M are the lower and upper bounds of $\phi(t)$.

In order to estimate the state of neural network system (1), the following state estimation system [28,29] is introduced:

$$\begin{cases}\dot{\hat{x}}(t) = -A\hat{x}(t) + K(\tilde{y}(t)-\hat{y}(t))\\ \hat{y}(t) = C\hat{x}(t)\end{cases} \tag{2}$$

where $\hat{x}(t)\in\mathbb{R}^n$ is the estimated state vector and K is the estimator gain matrix to be determined. $\tilde{y}(t)$ is the actual input of the estimator and $\hat{y}(t)$ is the estimated measurement output.

In this paper, the state estimation for neural networks is investigated with hybrid triggered scheme and quantization subject to stochastic cyber attacks. The structure of the state estimator is shown in Fig. 1. The sensor measurements are sampled at time kh with a period h.

As is shown in Fig. 1, when "time triggered scheme" is chosen, by using the similar arguments in [30], the actual input of the estimator can be written as follows without considering the effect of quantization.

$$y_1(t) = Cx(t_k h),\quad t\in[t_k h+\tau_{t_k}, t_{k+1}h+\tau_{t_{k+1}}) \tag{3}$$

where h is the sampling period, $t_k h$ is the instant that the sampled data is transmitting, τ_{t_k} is the corresponding network-induced delay. Similar to [31], define the network allowable equivalent delay $\tau(t)=t-t_k h$, Eq. (3) can be written as follows

$$y_1(t) = Cx(t-\tau(t)) \tag{4}$$

Please cite this article as: J. Liu et al., Quantized state estimation for neural networks with cyber attacks and hybrid triggered communication scheme, Neurocomputing (2018), https://doi.org/10.1016/j.neucom.2018.02.060