Research on $H_{\infty}$ Controller of Cyber Attacks and Eventtriggering Mechanism

Linqi Chen, Yan Gao, Jianwu Ma and Fengjiao Gu

School of Electronics and Electricity, Shanghai University of Engineering and Technology, Shanghai, 20160, China
e-mail: 1095855736@qq.com, gy@sues.edu.cn, 1596673894@qq.com, 2548746829@qq.com

ABSTRACT: Aiming at the limited network bandwidth and various cyber attacks, the $H_{\infty}$ neural network controller triggered by discrete events is studied. In order to further improve the utilization of network bandwidth, the event triggering mechanism is improved by taking advantage of the advantages of event triggering in network transmission. At the same time, due to various uncertain and deliberate network attacks, data tampering and packet loss problems are caused. A new neural network control system model is established based on the attack mode obeying Bernoulli probability and dynamic integration. By using Lyapunov function, sufficient conditions are obtained to ensure the asymptotic stability of the closed-loop system, which meets the requirements of $H_{\infty}$. Finally, a numerical example is given to verify the validity of the results.

1. Introduction

In recent years, the successful application of neural networks in signal processing, image processing and other scenarios has made the application of neural networks attract the attention of a large number of researchers. The neural network controller has also developed rapidly in the field of network transmission, and the performance of the network system has been greatly improved. However, problems such as data packet loss and network security still exist. Faced with the above problems, how to make full use of the network for data transmission, save network energy, and ensure data security is still an important research topic.

So far, many new results have been published to solve the problem of network control. Among them, for limited bandwidth transmission, a periodic trigger mechanism (time trigger mechanism) is proposed, but when transmitting, a large number of redundant signals will be generated, resulting in waste of resources and congestion of network transmission, resulting in network performance decline. To solve this problem, an event triggering mechanism was proposed. By designing functions and thresholds to control unnecessary data transmission [3-8], the network bandwidth is fully utilized, thereby saving network resources and being applied to other controllers. For example: in [11], the feedback controller is designed using the event trigger mechanism, in [14], the event trigger mechanism is applied to the fuzzy neural network system. The improvement of the event triggering mechanism is also varied, and this article improves the event triggering mechanism based on the existing event triggering mechanism combined with the actual.

For a variety of network control systems, network security is a hot topic. The modification or loss of data may have unexpected consequences and cause catastrophic persecution of human beings. Therefore, it is necessary to study network security issues. To study network security issues, you must
understanding network attacks. Network attacks refer to using communication links and sending wrong control signals to operators. Generally speaking, network attacks mainly include denial of service attacks and spoofing attacks. In [2, 3], a Bernoulli deceptive network attack is applied, but if this attack does not match the controller, it may become a periodic interference signal that blocks the communication channel. Soon, integral dynamic network attacks appeared, but there are few literatures that combine multiple attacks and act on neural network controllers.

Under the above considerations, the neural network controller is reconstructed using Bernoulli-compliant network attacks and integral dynamic network attacks [1, 2], combined with an improved event triggering mechanism. For each sensor, this paper improves the event-triggered transmission scheme to determine the local transmission signal, reducing the consumption of communication resources. For cumulative dynamic attack scenarios, this paper proposes an integration function that satisfies the given constraints. Considering various factors and adding multiple time delays to the system, a novel Lyapunov function is constructed, which proves that the system is closed-loop stable, and the appropriate controller gain and trigger parameters are solved through the LMI toolbox. Finally, an example illustrates the feasibility of this article.

2. Problem formulation and preliminaries

2.1. Problem Description

The neural network controller is designed according to Figure 1. Under time lag and cyber attacks, sensors and corresponding controllers can ensure data reliability when transmitting data over the network. The time-delay network model applied in this paper is as follows:

\[
\begin{align*}
\dot{x}(t) &= Ax(t) + Bu(t) + Eg\left(x\left(t - \eta\left(t\right)\right)\right) + D\omega(t) \\
z(t) &= C x(t)
\end{align*}
\] (1)

Where \(x(t) = [x_1(t), x_2(t), \ldots, x_n(t)]^T\) represents state variables of \(n\) neurons, \(u(t)\) is the input of the model, \(z(t)\) is the output variable. \(g(t) = [g_1(x_1(t)), g_2(x_1(t)), \ldots, g_n(x_1(t))]\) represents activation function of the network, \(\eta(t)\) Changes in network latency and meets \(0 \leq \eta(t) \leq \eta_0; \eta_0\) is the maximum delay constant, \(A\) is a symmetric matrix, \(B, C, D\) is a real matrix of appropriate dimensions.

2.2. Event triggering mechanism

The event trigger mechanism uses the following model:

\[
\ell_i^T(t) \Xi \ell_i^T(t) \leq \theta_i x_i^T\left(t_{i+1}, h\right) \Xi x_i^T\left(t_{i+1}, h\right)
\] (2)

\(\theta_i\in[0,1], \Xi > 0\) is a positive definite weighting matrix (\(\Xi = 0\) changes time trigger). The event trigger mechanism consists of two parts: register, comparator. The register is used to record the latest sampled data status \(x_i(t_i)\). Set the sampling interval \(\delta h\), The comparator judges whether the data satisfies the above-mentioned trigger condition on the status of the current sampled data \(x_i(t_i + \delta h)\), the number of triggers is expressed in the following way:
\[ \{ t_i, t_{i+1}, \ldots \} \subseteq \{ h, 2h, \ldots, n_1 h \}, t_i, h = t_i h + j h. \] Through the buffer to record the time stamp output by the controller, \( j h \) represents timestamp of its maximum sampling interval, by Zero-order holder \( \{ t_i h, \dot{t}_i h, \ddot{t}_i h, \dddot{t}_i h \} \) can be divided into the following:

\[ \bigcup_{j=0}^{M} \mathcal{Y}_j, \quad \mathcal{Y}_j = \left[ t_i h + j h + \tau_{q_i}, t_i h + j h + \tau_{q_i + 1} \right) \quad j^\prime = 0, 1, \ldots, j^\prime_M = t_i^\prime - t_i^\prime - 1 \quad (3) \]

Definition: \( \tau_i = t_i h - \dot{t}_i h - \ddot{t}_i h \), \( \alpha_1 \in [0, 1] \), \( \beta_1 \in [0, 1] \), \( \alpha(t) \in [0, 1] \), \( \beta(t) \in [0, 1] \), \( K \) represents the gain of the controller, \( f(x(t-d(t))) \) and \( \int_{t=d(t)}^{t} g(x(s)) \) represents the type of non-linear and integral cyber attacks, as follows:

\[ f(x) = \left[ f_1(x_1), f_2(x_2), \ldots, f_n(x_n) \right] \] \( g(x) = \left[ g_1(x_1), g_2(x_2), \ldots, g_n(x_n) \right] \quad (6) \]

\[ d(t) \in \{ 0, d_u \}, \quad v(t) \in \{ 0, v_m \} \]

\[ \alpha(t_k) = 1 \] represents network is normal, there is no network attack; \( \alpha(t_k) = 0 \) and \( \beta(t_k) = 1 \) represent The Bernoulli attack occurred; \( \alpha(t_k) = 0 \) and \( \beta(t_k) = 0 \) represent An integral cyber attack has occurred.

3. Model establishment and assumptions

3.1. Model establishment

Randomly generated network attacks may affect the conditions for event triggering, and further cause the controller to make wrong judgments. Therefore, in the \( t_i h + \tau_{q_i}, \dot{t}_i h, \ddot{t}_i h \), combining formulas (1) and (6) obtain the following control model:

\[ u(t) = \omega(t_k)Kx(t_k h) + \varphi(t_k)BKf(x(t)) + \gamma(t_k)BKf(t-d(t)) + \mathcal{E}g(x(t)) + \mathcal{D} (7) \]

Considering the definition of \( \tau(t) \) and \( a(t) \), the model can be rewritten on the basis of (7):

\[ \dot{x}(t) = Ax(t) + \omega(t)BKx(t_k h) + \varphi(t_k)BKf(x(t)) + \gamma(t_k)BKf(t-d(t)) + \mathcal{E}g(x(t)) + \mathcal{D} w(t) \]

\[ + \left[ \omega(t_k) - \omega(t) \right] BK \left[ x(t - \tau(t)) + e(t) \right] + \left[ \varphi(t_k) - \varphi(t) \right] BKf(x(t-d(t))) + \mathcal{E}g(x(t)) + \mathcal{D} w(t) \] \quad (8)
\( \phi, \phi, \phi, \phi \) are known constant and represent upper and lower boundaries of a cyber attack.

**Lemma 1:**

For \( v_i \geq 0 \) \((i = 1, 2)\), there is a diagonal matrix that satisfies:

\[
\begin{bmatrix}
-x(t)^	op & V_i \phi_i^+ & V_i \phi_i^- & x(t)^	op \\
-x(t) & \phi_i^+ V_i & -V_i & x(t)
\end{bmatrix} \geq 0,
\]

\[
\phi_i = \text{diag} \left\{ \phi_1^+, \phi_2^+, \ldots, \phi_n^+ \right\}
\]

\[
\phi_i^- = \text{diag} \left\{ \phi_1^-, \phi_2^-, \ldots, \phi_n^- \right\}
\]

**Lemma 2:**

For any constant matrix \( R, M \in \mathbb{R}^{m \times n} \) and \( \begin{bmatrix} R^* & M \end{bmatrix} \geq 0 \), the following inequalities can be obtained:

\[
\tau(t) \int_{t-	au(t)}^{t} \dot{x}^\top(s) R \dot{x}(s) ds \leq \dot{\xi}^\top(t) \Psi \dot{\xi}(t) \quad \dot{x}^\top(t) = x^\top(t) + x^\top(t - \tau(t)) + \tau(t)
\]

\[
\Psi = \begin{bmatrix} -R & * \\ -R - M & -2R + M + M^\top & * \\ M & R - M & * \end{bmatrix}
\]

**Lemma 3:**

Positive matrix \( P, Q \) satisfy the following inequality:

\[
(R - e_i^\top P) R_k^{-1} (R_k - e_i^\top P) \geq 0 \quad -PR_k^{-1} P \leq -2e_i P + e_i^\top R_k
\]

**Lemma 4:**

For column full rank matrix \( M \in \mathbb{R}^{m \times n} \), through singular value decomposition: \( M = USV^\top \), \( U, V \) are orthogonal matrices, \( S \in \mathbb{R}^{m \times n} \) is diagonal matrix of positive real numbers. If \( P \in \mathbb{R}^{n \times n} \) and \( P = \text{diag} \{ P_1, P_2 \} U^\top \), there must be a constant matrix \( X \in \mathbb{R}^{n \times n} \), making \( PM = MX \). There must be a \( X \), making \( PBK = BXK \).

**Definition:** \( Y = UX \).

### 4. Main results

Using the LMI toolbox and combining with the above lemma are to obtain sufficient conditions to ensure the progressive stability of the closed-loop system (7).

**Theory:** \( \alpha, \beta, \theta, \bar{T}, \bar{A}, \bar{P}, \bar{Q}, \bar{R}, \bar{M}, \bar{Q} \) are known. If \( P, R, R, R, Q, Q, Q \) are positive definite matrix, \( M, M, M, M \) are proper dimension matrix, \( \Xi, \nu_i, U_i, U_i \) is diagonal matrix and there is a matrix \( \gamma \), The closed-loop system (7) is asymptotically stable.

\[
\begin{bmatrix} I & * \\ 0 & * \end{bmatrix} < 0
\]

\[
\begin{bmatrix} R_k^a & * \\ M_k^a & R_k^a \end{bmatrix} > 0, a = 1, 2, 3
\]

Where

\[
\Pi_{11} = \begin{bmatrix} T_1 & \ast & \ast \\ -Q_1 \ast \ast & \ast \end{bmatrix}
\]

\[
\Pi_{22} = \begin{bmatrix} -Q_2 \ast \ast & \ast \\ 0 \ast \ast & \ast \end{bmatrix}
\]

\[
\Pi_{12} = \begin{bmatrix} -Q_2 \ast \ast & \ast \\ 0 \ast \ast & \ast \end{bmatrix}
\]

\[
\Pi_{11} = \begin{bmatrix} T_1 & \ast & \ast \\ -Q_1 \ast \ast & \ast \end{bmatrix}
\]

\[
\Pi_{22} = \begin{bmatrix} -Q_2 \ast \ast & \ast \\ 0 \ast \ast & \ast \end{bmatrix}
\]

\[
\Pi_{12} = \begin{bmatrix} -Q_2 \ast \ast & \ast \\ 0 \ast \ast & \ast \end{bmatrix}
\]
Through Lemma 1, the following constraints can be imposed on the attack network function

\[ V(x(t)) = V_1(x(t)) + V_2(x(t)) \]  

along the time trajectory \( t \), expect the derivative of \( v(x(t)) \):

\[
E[V'(x(t))] = 2x'(t)P_k x(t) + \int_{t-vu}^{t} x'(s)Q_k x(s) ds + \int_{t-vu}^{t} x'(s)Q_k x(s) ds \\
+ \int_{t-vu}^{t} x'(s)Q_k x(s) ds + \tau_u \int_{t-vu}^{t} x'(v)R_k x(v) dvds \\
+ d_u \int_{t-vu}^{t} \int_{s-vy}^{s} x'(v)R_k x(v) dvds + v_u \int_{t-vu}^{t} \int_{v-y}^{v} x'(v)R_k x(v) dvds
\]

\[
V_2(x(t)) = \int_{t-vu}^{t} g(x(s))s, g(x(s)) dvds
\]

along the time trajectory \( t \), expect the derivative of \( v(x(t)) \):

\[
E[V'(x(t))] = 2x'(t)P_k x(t) + \int_{t-vu}^{t} x'(s)Q_k x(s) ds + \int_{t-vu}^{t} x'(s)Q_k x(s) ds \\
+ \int_{t-vu}^{t} x'(s)Q_k x(s) ds + \tau_u \int_{t-vu}^{t} x'(v)R_k x(v) dvds \\
+ d_u \int_{t-vu}^{t} \int_{s-vy}^{s} x'(v)R_k x(v) dvds + v_u \int_{t-vu}^{t} \int_{v-y}^{v} x'(v)R_k x(v) dvds
\]

\[
V_2(x(t)) = \int_{t-vu}^{t} g(x(s))s, g(x(s)) dvds
\]

along the time trajectory \( t \), expect the derivative of \( v(x(t)) \):

\[
E[V'(x(t))] = 2x'(t)P_k x(t) + \int_{t-vu}^{t} x'(s)Q_k x(s) ds + \int_{t-vu}^{t} x'(s)Q_k x(s) ds \\
+ \int_{t-vu}^{t} x'(s)Q_k x(s) ds + \tau_u \int_{t-vu}^{t} x'(v)R_k x(v) dvds \\
+ d_u \int_{t-vu}^{t} \int_{s-vy}^{s} x'(v)R_k x(v) dvds + v_u \int_{t-vu}^{t} \int_{v-y}^{v} x'(v)R_k x(v) dvds
\]

\[
V_2(x(t)) = \int_{t-vu}^{t} g(x(s))s, g(x(s)) dvds
\]
Combining (2), (7)-(11), Lemma 3 and Lemma 4 can lead to the following conclusions:

\[
E \{ \mathcal{V} (x(t)) \} \leq 2x^T(t)P\dot{x}(t) + x^T(t)(Q_1 + Q_2 + Q_3)\dot{x}(t) - x^T(t - \tau_u)Q_1\dot{x}(t - \tau_u) - x^T(t - d_u)Q_2\dot{x}(t - d_u) - x^T(t - d_u)Q_3\dot{x}(t - d_u) - \int_{-\tau_u}^{0} x^T(s)R_1\dot{x}(s)ds - \int_{-d_u}^{0} x^T(s)R_2\dot{x}(s)ds - \int_{-d_u}^{0} x^T(s)R_3\dot{x}(s)ds
\]

Where

\[
\zeta = [x^T(t) x^T(t - \tau(t)) x^T(t - d(t)) x^T(t - d(u)) x^T(t - v(t)) x^T(t - v_u(t))]
\]

\[
f(x(t - d(t))) g(x(t)) g^T(x(t - v(t))) \left( \int_{-\tau(t)}^{0} g(x(s))ds \right)^T e^T(t) o^T(t)
\]

From Schur's theorem, (13) can be obtained:

\[
E \{ \mathcal{V} (x(t)) \} < r^2\omega^T(t)\omega(t) - z^T(t)z(t)
\]

### 5. Numerical Analysis

An example is used to validate the above theory, and the results are as follows:

\[
A = \begin{bmatrix} 0.1 & 0 & 0 \\ 0 & 0.2 & 0 \end{bmatrix}, \quad C = \text{diag}(0.1, 0.1, 0.1), \quad D = \begin{bmatrix} 0.1 & 0.1 & 0.1 \end{bmatrix}
\]

When \(\omega(t) = 0\), \(\rho(t) = 1\), if only the network attack function \(f(x)\) is considered, it is the network attack problem mainly studied in [2]. This paper further studies the attack problem. The following are the experimental results of two random attack triggers and controller states \(x(t)\). According to Lemma 1, bring in this fixed value:

\[
\phi_i = \text{diag} \{ 0, 0, 0 \}, \quad \phi_i = \text{diag} \{ 0.02, 0.02, 0.02 \}, \quad \phi_i = \text{diag} \{ 0.015, 0.03, 0.015 \}
\]

The following parameters are known:

\[
\bar{\alpha} = 0.8, \quad \bar{\theta} = 0.8, \quad \tau_u = 0.5, \quad d_u = 0.5, \quad v_u = 0.5, \quad e_1 = 1, \quad e_2 = 1, \quad \epsilon = 0.1, \quad \theta = 0.1, \quad h = 0.1
\]

We can get (8) controller gain and event trigger matrix through LMI toolbox combined with the above known conditions:

\[
K = \begin{bmatrix} 5.9709 & 0 & 0 \\ 0 & 3.9676 & 0 \end{bmatrix}, \quad \Xi = \begin{bmatrix} 5.9709 & 0 & 0 \\ 0 & 3.9676 & 0 \end{bmatrix}
\]

Figures 1 to 3 show the sensor release interval. The three sensors transmit measured values: 82,79,30, and the average transmission rate is 12.73%: (1500 sample measurements). Figure 4 shows the state of the controller. Compared with [2], the controller is still stable under various attack methods, and the transmission rate is still stable.
6. Conclusions

In this paper, we use time-delay neural network to study the problem of event-triggered control for the problem of limited bandwidth and two kinds of random network attacks. Through improved event triggering to avoid unnecessary network transmission, reduce bandwidth burden, increase the type of network attack, a new network controller is constructed, and a stability analysis is performed through a novel Lyapunov function, which proves the progressive stability of the closed-loop system. Finally, an example is used to verify the reliability of the results through the LMI toolbox, and the transmission of each sensor data is obtained. In this paper, although event triggering and network attack are improved, and new controllers are proposed based on a variety of time-delay neural networks, how to remove the upper and lower boundary constraints of network attack functions, and the combination of adaptive event triggering and the model are the main contents of my future research.

Acknowledgments

I thank my parents and girlfriend for their understanding and support. I hope that my parents are healthy and my girlfriend has a successful career. At the same time, I also thank my tutor for his guidance in the thesis and the research environment provided by the school, which made me go further and further in the research.

References

[1] Wei, L., Liu, J. (2017) Stabilization for networked control systems under stochastic cyber-attacks. The 36th China Control Association., Da Lian. pp. 1414-1419.
[2] Zha, L., Tian, E., Xie, X., Gu, Z., Cao, J. (2018) Decentralized event-triggered H∞ control for neural networks subject to cyber-attacks. Information Sciences., 457-458: 141–155.
[3] Fu, A., Manuel, M. (2018) Decentralized periodic event-triggered control with quantization and asynchronous communication. Automatica., 94: 294-199.
[4] Zhang, H., Zhang H., Wang Z. (2019) Unmanned vehicle path following predictive control based on event triggering. Control and Decision., 34: 2421-2427.
[5] Gao, H., Song, Y., Wen, C.Y. (2020) Event-triggered adaptive neural network controller for uncertain nonlinear system. Information Sciences., 506: 0250-0255.

[6] Liang, J., Hua, H., Hu, Y. (2011) Network-Based H∞ Filtering for Linear Systems with Randomly Varying Sensor Delay. Journal of Donghua University (English Edition.), 28: 400-404.

[7] Jiang, C., Liu, M. (2015) A class of event-driven networked H∞ filter design. Journal of Suzhou University of Science and Technology., 32: 51-56.

[8] Wang, Y., Ren, W. (2018) Non-fragile H∞ state estimation triggered by fuzzy neural network events. Journal of System Simulation., 30: 2335-2344.

[9] Li, Q., Wang, Z., Sheng, W., Alsaadi, F. E., Alsaadi, F. E. (2019) Dynamic event-triggered mechanism for H∞ non-fragile state estimation of complex networks under randomly occurring sensor saturations. Information Sciences., 509: 304-316.

[10] Liu, D., Yang, G. (2019) Decentralized event-triggered output feedback control for a class of interconnected large-scale systems. ISA Transactions., 93: 156-164.

[11] Wang, T., Qiu, J., Gao, H. (2019) Adaptive neural network control of stochastic nonlinear system based on event trigger mechanism. Journal of Automation., 45 (01): 226-233.

[12] Wang, Y., Zheng, W., Zhang, H. (2017) Dynamic event-based control of nonlinear stochasticsystems. IEEE Trans. Automat. Contr., 62: 6544–6551.

[13] Han, F., Wei, G., Ding, D., Song, Y. (2017) Finite-horizon bounded H∞ synchronisation and state estimation for discrete-time complexnetworks: localperformanceanalysis. IET Control Theory Appl., 11(6): 827–837.

[14] Huang, H., Huang, T. (2017) Multi-agent leadership following consistency under event trigger mechanism. Computer Engineering and Applications., 53 (06): 29-33.

[15] Lam, H., Leung, F. (2006) Design and stabilization of sampled-data neural-network-based control systems. IEEE Trans. Syst., Man, Part B (Cybernetics), 36 (5): 995–1005.

[16] Fridman, E., Seuret, A., Richard, J. (2004) Robust sampled-data stabilization of linear systems: an input delay approach. Automatica., 40(8): 1441–1446.

[17] Chao, G., Hong, W., Liu, Y., Ju, H.P. (2017) Further results on stabilization of neural-network-based systems using sampled-data control. Nonlinear Dynamics., 90 (3): 2209-2219.

[18] Hu, S., Yue, D., Xie X. (2018) Stabilization of Neural-Network-Based Control Systems via Event-Triggered Control With Nonperiodic Sampled Data. IEEE Transactions on Neural Networks and Learning Systems., 29 (3): 573-585.

[19] Wang, I., Shen, Y., Ding, Z. (2015) Finite time stabilization of delayed neural networks. Neural Netw., 70: 74-80.

[20] Zha, L., Fang, J. A., Liu, J., Tian, E. (2018) Event-triggered non-fragile state estimation for delayed neural networks with randomly occurring sensor nonlinearity. Neurocomput., 273: 1-8.