electronics

MDPI

Article

Secure Change Control for Supply Chain Systems via Dynamic Event Triggered Using Reinforcement Learning under DoS Attacks

Lingling Fan, Bolin Zhang *, Shuangshuang Xiong and Qingkui Li

Department of Control Engineering, School of Automation, Beijing Information Science & Technology University, Beijing 100192, China; linglingfan@bistu.edu.cn (L.F.); shuangshx@bistu.edu.cn (S.X.); sdlqk01@bistu.edu.cn (Q.L.)

* Correspondence: 2021020351@bistu.edu.cn

Abstract: In this paper, a distributed secure change control scheme for supply chain systems is presented under denial-of-service (DoS) attacks. To eliminate the effect of DoS attacks on supply chain systems, a secure change compensation is designed. A distributed policy iteration method is established to approximate the coupled Hamilton–Jacobi–Isaacs (HJI) equations. Based on the established reinforce–critic–actor (RCA) structure using reinforcement learning (RL), the reinforced signals, performance indicators, and disturbance input are proposed to update the traditional time-triggered mechanism, and the control input is proposed to update the dynamic event-triggered mechanism (DETM). Stability is guaranteed based on the Lyapunov method under secure change control. The simulation results for supply chain systems show the effectiveness of the secure change control scheme and verify the results.

Keywords: denial-of-service (DoS) attacks; secure change control scheme; supply chain systems; dynamic event-triggered mechanism (DETM); reinforcement learning (RL); reinforce–critic–actor (RCA)

check for updates

Citation: Fan, L.; Zhang, B.; Xiong, S.; Li, Q. Secure Change Control for Supply Chain Systems via Dynamic Event Triggered Using Reinforcement Learning under DoS Attacks. *Electronics* **2024**, *13*, 1136. https://doi.org/10.3390/electronics13061136

Academic Editor: Luca Patanè

Received: 13 February 2024
Revised: 13 March 2024
Accepted: 18 March 2024
Published: 20 March 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The production and manufacturing of enterprises are closely connected, thus forming a multi-connected network supply chain system, which is usually a complex network system composed of manufacturers, distributors, and retailers [1]. The control of the supply chain production inventory system has always been an important task of enterprise management. The supply chain production inventory system is designed by the traditional single-level sub-chain system, but for large enterprises, the production inventory system is a network system composed of multi-level sub-chains, which is more in line with the research on modern supply chain systems. Therefore, multi-agent is widely used in research on supply chain systems [2–4]. The control theory has been widely used in supply chain management. In [5,6], the supply chain is controlled by synovial control. In [7], the dynamic supply chain is designed via fuzzy robust control. In [8,9], the multi-agent supply chain is tracked and controlled at a fixed time. In addition, distributed model predictive control has been applied to supply chain inventory management [10,11]. However, the modern supply chain inventory system is faced with many challenges, such as the difficulty in accurately obtaining system dynamics information and accurately constructing system structure, etc. Therefore, there is an urgent need to develop data-driven methods that rely only on data instead of models. In addition, unexpected network attacks will seriously damage the normal production operation of enterprises and damage the security of the system. How to develop a security scheme to deal with major network events, and realizing the security control of the supply chain production and inventory system is an important means to prevent enterprises from suffering heavy economic losses.

From the perspective of control research on supply chain production inventory systems, firstly, based on the precise mathematical dynamics model of the system [12], all

designs are based on the static mechanism model and [13] matrix inequalities are used to optimize and solve the controller, but this method relies on the precise dynamics information of the system. Secondly, with the rapid development of information technology, the manufacturing industry is developing rapidly towards intelligent production and manufacturing [14]. From the perspective of the agent, the inventory–production–modeling integrated architecture of the supply chain system is presented in [15]. Intelligent manufacturing is composed of interconnected enterprises, machines, and human and physical systems through the basic network of the industrial Internet. This enables comprehensive sensing, dynamic transmission, and real-time analysis of industrial data and then intelligent control and scientific decision-making to improve the efficient allocation of manufacturing resources. During the operation of supply chain systems, a large amount of input and process data are generated, which are recorded and kept by the system equipment for the subsequent data-driven design [16]. The operation and execution of the current large-scale intelligent industrial system and machinery and equipment ensure the smooth circulation of the large-scale industrial Internet. The accurate transmission of the Internet equipment determines the normal operation of the machine equipment, and the machine equipment and the industrial Internet transmission information medium are usually connected through the data; for large enterprises, the network structure is more complex, data transmission is extremely large and dense, and the transmission equipment requirements are higher. Therefore, determining how to save transmission data resources for enterprises and reduce the pressure of communication load is an important problem to be solved in the supply chain system, and it is also an important task of this study.

With the development of big data, artificial intelligence, and digital twins, modern supply chain systems have become intelligent systems integrating production equipment, robots, and the industrial Internet [17]. The intelligent system of a large-scale network will be subject to unexpected external events, which will lead to supply chain disruption. Therefore, change control in the face of emergencies has become an important issue in supply chain design. The authors of [18] developed a recovery control algorithm for supply chain disruptions. For a non-linear supply chain system, in [19], faced with the influence of demand disturbance and unexpected events, the feasible solution of the Takagi–Sugeno fuzzy system is given by using linear matrix inequality. However, network security events will lead to supply chain system transmission interruption; these security events will directly attack the information data of the system and destroy the security operation of the whole supply chain system, resulting in major security accidents. Therefore, the problem of security change control has been paid more and more attention by enterprises. It has become an important task of the inventory control of supply chain systems to design security change plans for the system and ensure that the system can respond to emergencies quickly and in a timely manner. At present, secure change control has been widely explored and studied in the field of multi-agent. For aperiodic persistent network attacks [20], an estimator is established to compensate for the state under network attacks, and a double-ended event-triggered mechanism is proposed to ensure the consistency of system security. A new adaptive dynamic event-triggered mechanism was proposed and the maximum duration of a network attack was deduced to achieve security consensus in [21]. Model-free adaptive control is applied to the secure control as an effective data-driven method. For an aperiodic network attack, the compensation scheme under network attack is given by [22]. For periodic network attacks, an emergency compensation scheme was proposed at the time of network attacks and an observer was used to estimate the output in [23]. Adaptive dynamic programming (ADP) has been widely developed and studied for solving optimal controllers. RL has been utilized to tackle the optimal control problem for multi-agent systems, such as tracking control [24,25]. After this, refs. [26,27] both unitized event-triggered ADP to address optimal control problems. Although the adaptive dynamic programming technique can be used to approach the optimal controller in the above paper, the external disturbance is not considered enough. For the supply chain system, the external uncertain demand is usually unknown, and it will gradually

amplify along the reverse direction of the product side of the system, which is the bullwhip effect. Therefore, weakening the adverse impact of the bullwhip effect on the supply chain system has become another important task in the design of this system. Effective methods to weaken the bullwhip effect are proposed in [28,29]. However, ADP is rarely applied to the design of supply chain systems, and a large number of studies have found that the dynamic event triggering method can reduce the communication load pressure and save the communication load between supply chains. Therefore, we studied the supply chain inventory control based on the combination of adaptive dynamic planning technology and the dynamic event triggering mechanism.

The previous works focused on supply chain systems under DoS attacks can be used to detect and mitigate the impact through Machine Learning (ML), Deep Learning (DL), and reinforcement learning. In the attack detection for supply chain systems, leverage evolutionary and DL approaches to detect cyber-attacks in a cloud-based Supply Chain Management environment are proposed in [30]. A Machine Learning approach for network anomaly detection and constructing data-driven models to detect distributed DoS attacks on industry is presented in [31]. A federated learning-based efficient detection model named DFF-SC4N is addressed in [32] to identify intrusions from supply chain 4.0 networks. In the prediction detection for supply chain systems, Logistic Regression, Decision Tree, Naïve Bayes, and Random Forest classification algorithms are considered to learn a dataset for performance accuracies and threat predictions based on the CSC resilience design principles in [33]. However, RL is the only ML technique that can learn without any dataset. It is considered that supply chain systems only have initial permission or arbitrary data, so secure control for supply chain systems can be achieved.

Inspired by the large amount of research mentioned above, we carried out the following work. Firstly, the problem of the bullwhip effect caused by uncertain market demand is considered, and the idea of a zero-sum differential game is introduced into the supply chain system. Secondly, a goal-heuristic dynamic programming adaptive reinforcement learning method combined with the dynamic event triggering mechanism is designed. The dynamic event-triggering mechanism is then compared with a static event-triggering scheme [34,35]. The dynamic triggering scheme is adopted to further reduce the number of triggers. Finally, due to the packet loss caused by DoS attacks, an emergency compensation scheme is designed to realize the security change control of the supply chain systems, and a Lyapunov proof based on emergency compensation under DoS attacks is given. The simulation results fully demonstrate the effectiveness of the proposed method. The contributions of this paper are as follows:

(1) For the supply chain production inventory system, the production input and uncertain demand are regarded as two sides of a zero-sum game. Based on the HJI equation, the RCA network online learning structure is established.
(2) On this basis, a dynamic event-triggered mechanism is proposed, and appropriate internal parameters of the dynamic event-triggered mechanism are selected to reduce the number of iterations of the neural network, so as to realize the dynamic event triggering tracking control of each sub-chain of the supply chain to the main chain.
(3) A secure change control scheme under DoS attack is proposed to ensure the normal operation of the supply chain production inventory system. The simulation analysis carried out proves that the proposed security change scheme can achieve effective change control.

The structure of the rest of this paper is organized as follows. Section 2 provides some preliminary knowledge. In Section 3, the dynamic event triggering mechanism and stability analysis are given. The learning structure of the neural network is presented in Section 4, the proposed method is verified by simulation, and Section 5 provides the summary and future research direction of this paper.

2. Preliminaries

2.1. Algebraic Graph Theory

In this paper, we consider a communication topology $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ consisting of a vertex set $\mathcal{V} = \{v_1, v_2, \cdots, v_N\}$. $\mathcal{E} \in \mathcal{V} \times \mathcal{V}$ is an edge set, which indicates that v_i can obtain state information directly from v_j. $\mathcal{A} = [a_{ij}]$ is a weighted adjacency matrix with element a_{ij}, $a_{ij} > 0$ if and only if $(v_i, v_j) \in \mathcal{E}$, and $a_{ij} = 0$ otherwise. The in-degree matrix defines a diagonal matrix $\mathcal{D} = \text{diag}\{d_1, d_2, \cdots, d_n\}$ with $d_i \in \sum_{j \in N_i} a_{ij}$, and the Laplacian matrix L can be defined as $L = \mathcal{D} - \mathcal{A}$. The connected matrix of the leader is defined as a diagonal matrix $\mathcal{B} = diag\{b_1, b_2, \cdots, b_n\}$ where $b_i > 0$ if v_i can receive the information leader and $b_i = 0$ otherwise.

2.2. Problem Formulation

We consider a supply chain system consisting of N subchains and a chain leader. The dynamics are described as:

$$\begin{cases} x_i(k+1) = Ax_i(k) + Bu_i(k) + D\hat{\omega}_i(k) \\ y_i(k) = Cx_i(k) \end{cases} \tag{1}$$

where $i = 1, 2, \cdots, N$, $x_i(k) \in R^n$ is the production inventory status for the subchain i at k. $u_i(k) \in R^n$ is the productivity for the subchain i at k. $\hat{\omega}_i \in R^n$ is the market demand for subchain i at k, and $d_i \in R^n$ is the constant market. The production inventory, productivity, and market can be regarded as the state variable, the control input, and external disturbances for control theory. A, B, and D represent the unknown system matrix.

The chain leader is the tracking target of the other subchains. The dynamics of the chain leader are described as:

$$x_0(k+1) = Ax_0(k) + Dd_i \tag{2}$$

where $x_0(k) \in R^n$ is the production inventory status for the chain leader at k.

Definition 1. *The design goal of the supply chain production inventory system is to design a distributed minimum control strategy $u_i(k)$ and maximum disturbance strategy $\omega_i(k)$, so that the inventory status of all subchains can follow the inventory status of the chain leader $x_i(0)$, that is:*

$$\lim_{k \to \infty} \|x_i(k) - x_0(k)\| = 0 \tag{3}$$

Definition 2. *For the supply chain production inventory system, there exists a bullwhip suppression parameter, which makes the following bullwhip effect suppression conditions valid, that is:*

$$\sum_{k=0}^{\infty} e_i^T(k) Q_{ii} e_i(k) + \sum_{k=0}^{\infty} u_i^T(k) R_{ii} u_i(k) \leq \gamma^2 \sum_{k=0}^{\infty} \omega_i^T(k) T_{ii} \omega_i(k) \tag{4}$$

Assumption 1. *The directed communication topology contains a spanning tree with the root node.*

Assumption 2. *There exists a positive constant m such that:*

$$\|f_i\left(e_i(k), u_i\left(k_s^i\right), \omega_i(k)\right)\| \leq m\|e_i(k)\| + m\|\epsilon_i(k)\| \tag{5}$$

Lemma 1. ([24]). *According to Assumption 1, $L + \mathcal{B}$ is a positive definite matrix (non-singular). Then, the consensus error is bounded by:*

$$\|\xi(k)\| \leq \|e(k)\| / \lambda_{\min}(L + \mathcal{B}) \tag{6}$$

where $\lambda_{\min}(L+\mathcal{B})$ *is the minimum singular value of* $(L+\mathcal{B})$.

The local neighborhood error of subchain i is defined as:

$$e_i(k) = \sum_{j \in N_i} a_{ij}\big(x_i(k) - x_j(k)\big) + b_i(x_i(k) - x_0(k)) \tag{7}$$

The global consensus error vector is given by:

$$e(k) = ((L+\mathcal{B}) \otimes I_n)(x(k) - \overline{x}_0(k)) \tag{8}$$

where $e(k) = \left[e_1^T(k), e_2^T(k), \ldots, e_N^T(k)\right]^T \in R^{Nn}$, $x(k) = \left[x_1^T(k), x_2^T(k), \ldots, x_N^T(k)\right]^T \in R^{Nn}$, $\overline{x}_0(k) = (1 \otimes I_n)x_0(k) \in R^{Nn}$.

Then, the global synchronization error vector is written as:

$$\xi(k) = x(k) - \overline{x}_0(k) \tag{9}$$

where $\xi(k) = \left[\xi_1^T(k), \xi_2^T(k), \ldots, \xi_N^T(k)\right]^T \in R^{Nn}$.

The dynamic of the local neighborhood error for subchain i is obtained as:

$$\begin{aligned} e_i(k+1) &= Ae_i(k) + (d_i + b_i)Bu_i(k) - \sum_{j \in N_i} Bu_j(k) \\ &+ (d_i + b_i)D\omega_i(k) - \sum_{j=1}^{N} a_{ij}D\omega_j(k) \\ &= f_i(e_i(k), u_i(k), \omega_i(k)) \end{aligned} \tag{10}$$

3. Results

3.1. The Secure Change Consensus Control Scheme

The purpose of DoS attacks is to decrease the supply chain systems' performance by blocking the useful information transmitted between the sensor and the controller. DoS attacks cause packet dropouts in communication channels, resulting in production equipment being unable to operate normally. The supply chain systems cannot be designed according to the objective control scheme. The structure of the secure change control for supply chain systems is shown in Figure 1. The data packets received by the controller can be transformed into the following form:

$$\tilde{e}_{di}(k) = \alpha_i(k)e_i(k) \tag{11}$$

where $\alpha_i(k)$ represents whether the DoS attacks are successful in the communication channels. If the DoS attacks are successful, $\alpha_i(k) = 1$; otherwise, $\alpha_i(k) = 0$. The probability of DoS attacks conforms to a Bernoulli distribution, $P\{\alpha_i(k) = 1\} = \beta_i$,$P\{\alpha_i(k) = 0\} = 1 - \beta_i$.

To eliminate the effects of DoS attacks, the secure change scheme is designed as:

$$\tilde{e}_{di}(k) = (1 - \alpha_i(k))e_i(k) + \alpha_i(k)e_i(k-1) \tag{12}$$

The internal dynamic variable $\tilde{\theta}_{di}(k)$ under the secure change satisfies

$$\tilde{\theta}_{di}(k) = (1 - \alpha_i(k))\theta_i(k) + \alpha_i(k)\theta_i(k-1) \tag{13}$$

To improve the tracking performance of the supply chain system, the local internal performance signals can be described as:

$$\begin{aligned} &P_i(e_i(k), u_i(k), u_{-i}(k), \omega_i(k), \omega_{-i}(k)) \\ &= \sum_{m=k}^{\infty} \alpha^{m-k} r_i(e_i(m), u_i(m), u_{-i}(m), \omega_i(m), \omega_{-i}(m)) \end{aligned} \tag{14}$$

where $\alpha \in (0,1)$ is the discount factor, $u_{-i}(k) = \{u_j(k)|j \in N_i\}$ is the control input of the i subchain's neighbors, and $\hat{\omega}_{-i}(k) = \{\hat{\omega}_j(k)|j \in N_i\}$ is the disturbance input of the i subchain's neighbors. The external reinforcement signal is given by:

$$\begin{aligned} r_i(e_i(k), u_i(k), u_{-i}(k), \omega_i(k), \omega_i(k)) = e_i^T(k)Q_{ii}e_i(k) + u_i^T(k)R_{ii}u_i(k) \\ + \sum_{j\in N_i} u_j^T(k)R_{ij}u_j(k) - \gamma^2\omega_i^T(k)T_{ii}\omega_i(k) \\ -\gamma^2 \sum_{j\in N_i} \omega_j^T(k)T_{ij}\omega_j(k) \end{aligned} \tag{15}$$

where $R_{ii} > 0$, $R_{ij} > 0$, $T_{ii} > 0$, $T_{ij} > 0$ are all positive symmetric weighting matrices.

Then, the local performance function can be defined as:

$$\begin{aligned} J_i(e_i(k), u_i(k), u_{-i}(k), \omega_i(k), \omega_{-i}(k)) = \sum_{l=k}^{\infty} \{e_i^T(k)Q_{ii}e_i(k) + u_i^T(k)R_{ii}u_i(k) \\ + \sum_{j\in N_i} u_j^T(k)R_{ij}u_j(k) - \gamma^2 \sum_{j\in N_i} \omega_j^T(k)T_{ij}\omega_j(k) \\ -\gamma^2\omega_i^T(k)T_{ii}\omega_i(k)\} \end{aligned} \tag{16}$$

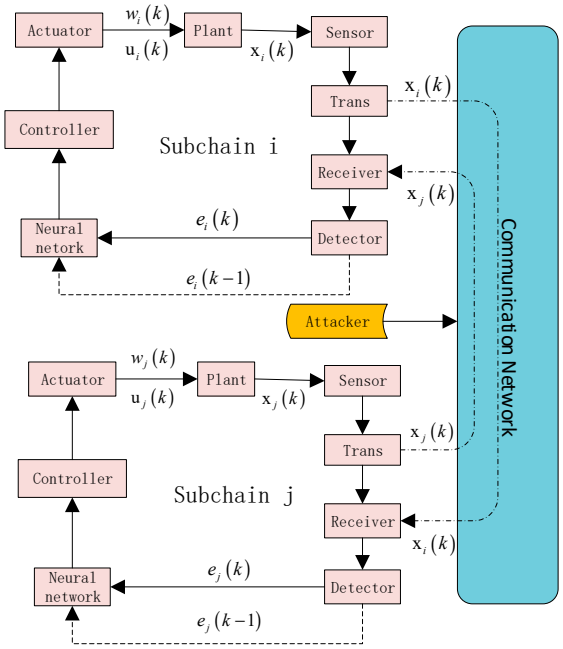

Figure 1. The structure of the secure change control for supply chain systems.

Given the admissible control input u_i and disturbance input ω_i, we define the local value function $V_i(e_i(k))$ as:

$$V_i(e_i(k)) = \sum_{t=k}^{\infty} \eta^{t-k} P_i\big(e_i(t), u_i(t), u_{-i}(t), \omega_i(t), \omega_{-j}(t)\big) \tag{17}$$

where $\eta \in (0,1)$ is the discount factor.

According to Equation (16), the Bellman equation is given by:

$$V_i(e_i(k)) = P_i(u_i(k), u_{-i}(k), \omega_i(k), \omega_{-i}(k)) + \eta V_i(e_i(k+1)) \tag{18}$$

Based on the Bellman optimality principle, the optimal value function $V_i^*(e_i(k))$ of subchain i satisfies the following HJI equation:

$$\begin{aligned} V_i^*(e_i(k)) &= \min_{u_i}\max_{\omega_i}\{P_i(e_i(k),u_i(k),u_{-i}(k),\omega_i(k),\omega_{-i}(k)) + \eta V_i^*(e_i(k+1))\} \\ &= \max_{\omega_i}\min_{u_i}\{P_i(e_i(k),u_i(k),u_{-i}(k),\omega_i(k),\omega_{-i}(k)) + \eta V_i^*(e_i(k+1))\} \end{aligned} \tag{19}$$

where the local internal reinforcement signals can be rewritten as:

$$\begin{aligned} &P_i(e_i(k),u_i(k),u_{-i}(k),\omega_i(k),\omega_{-i}(k)) \\ &= r_i(e_i(k),u_i(k),u_{-i}(k),\omega_i(k),\omega_{-i}(k)) \\ &+\alpha P_i(e_i(k+1),u_i(k+1),u_{-i}(k+1),\omega_i(k+1),\omega_{-i}(k+1)) \end{aligned} \tag{20}$$

Then, the optimal control pair can be expressed as:

$$u_i^*(k) = \arg\min_{u_i}\{P_i(e_i(k),u_i(k),u_{-i}(k),\omega_i(k),\omega_{-i}(k)) + \eta V_i^*(e_i(k+1))\} \tag{21}$$

$$\omega_i^*(k) = \arg\max_{\omega_i}\{P_i(e_i(k),u_i(k),u_{-i}(k),\omega_i(k),\omega_{-i}(k)) + \eta V_i^*(e_i(k+1))\} \tag{22}$$

For subchain i, we denote $\{k_s^i\}_{s=0}^{\infty}$ as the incrementally triggering sequence.
The local neighbor error is rewritten by:

$$e_i(k) = e_i\left(k_s^i\right) \tag{23}$$

The control input of subchain i is rewritten by:

$$u_i(k) = u_i\left(k_s^i\right), k \in \left[k_s^i, k_{s+1}^i\right) \tag{24}$$

Then, we define the error variable $\epsilon_i(k)$ as:

$$\epsilon_i(k) = e_i\left(k_s^i\right) - e_i(k), k \in \left[k_s^i, k_{s+1}^i\right) \tag{25}$$

Once the event is triggered, $\epsilon_i(k) = 0$.
According to the HJI equation under the dynamic event-triggered mechanism, the optimal control pair can be rewritten as:

$$\begin{aligned} V_i^*(e_i(k)) &= \min_{u_i}\max_{\omega_i}\{P_i(e_i(k),u_i(k_s^i),u_{-i}(k),\omega_i(k),\omega_{-i}(k)) + \eta V_i^*(e_i(k+1))\} \\ &= \max_{\omega_i}\min_{u_i}\{P_i(e_i(k),u_i(k_s^i),u_{-i}(k),\omega_i(k),\omega_{-i}(k)) + \eta V_i^*(e_i(k+1))\} \end{aligned} \tag{26}$$

The optimal control input under the dynamic event-triggered mechanism is rewritten as:

$$u_i^*(k) = \arg\min_{u_i}\left\{P_i\left(e_i(k),u_i\left(k_s^i\right),u_{-i}(k),\omega_i(k),\omega_{-i}(k)\right) + \eta V_i^*(e_i(k+1))\right\} \tag{27}$$

The optimal disturbance input under the traditional time-triggered mechanism is rewritten as:

$$\omega_i^*(k) = \arg\max_{\omega_i}\left\{P_i\left(e_i(k),u_i\left(k_s^i\right),u_{-i}(k),\omega_i(k),\omega_{-i}(k)\right) + \eta V_i^*(e_i(k+1))\right\} \tag{28}$$

3.2. Stability Analysis

For subchain i, the dynamic event-triggered mechanism is given by:

$$2m^2\|\epsilon_i(k)\|^2 \le \left(1-2m^2\right)\|e_i(k)\|^2 + \rho_i\theta_i(k) \tag{29}$$

where $0 < \rho_i < 1$, $0 < m < \frac{\sqrt{2}}{2}$, and $\theta_i(k)$ satisfy:

$$\theta_i(k+1) = (1-\lambda_i)\theta_i(k) + \xi_i\left(\left(1-2m^2\right)\|e_i(k)\|^2 - \left(2m^2\right)\|\epsilon_i(k)\|^2\right) \tag{30}$$

where $0 < (1-\xi_i)\rho_i < \lambda_i < 1, 0 < \xi_i < 1$.

Lemma 2. *For the dynamic event-triggered mechanism, it satisfies*:

$$\theta_i(k) > 0 \tag{31}$$

Proof of Lemma 2. According to (28) and (29), one has

$$\left(2m^2\right)\|\epsilon_i(k)\|^2 - \left(1-2m^2\right)\|e_i(k)\|^2 \leq \rho_i\theta_i(k) \tag{32}$$

Based on (29), one has

$$\theta_i(k+1) \geq (1-\lambda_i-\xi_i\rho_i)\theta_i(k) \geq, \ldots, \geq (1-\lambda_i-\xi_i\rho_i)^{k+1}\theta_i(0) \geq (1-\rho_i)^{k+1}\theta_i(0) \tag{33}$$

It is clear that $\theta_i(0) > 0$, $(1-\lambda_i-\xi_i\rho_i) > 0$; therefore, $\theta_i(k) > 0$. This completes the proof. □

Theorem 1. *Suppose that Assumption 1 and Assumption 2 hold. Supply chain systems (1) and (2) could achieve secure change consensus under the dynamic event-triggered mechanisms (28) and (29) under DoS attacks.*

Proof of Theorem 1. In order to guarantee the stability of the designed systems, consider the following Lyapunov function for $k \in \left[k_s^i, k_{s+1}^i\right)$

$$L_i(k) = L_{1i}(k) + L_{2i}(k) \tag{34}$$

where $L_{1i}(k) = \tilde{e}_{di}^T(k)\tilde{e}_{di}(k)$, $L_{2i}(k) = \tilde{\theta}_{di}(k)$. □

(1) If DoS attacks do not occur at two continuous sampling times k and times $k+1$, it is assumed that $\alpha_i(k) = \alpha_i(k+1) = 0$

The difference of $L_{1i}(k)$ can be calculated as follows:

$$\begin{aligned} \Delta L_{1i}(k) &= L_{1i}(k+1) - L_{1i}(k) \\ &= e_i^T(k+1)e_i(k+1) - e_i^T(k)e_i(k) \\ &\leq \left(\|e_i(k+1)\|^2 - \|e_i(k)\|^2\right) \end{aligned} \tag{35}$$

According to Assumption 2 and the Cauchy–Schwarz inequality equation, one has

$$\begin{aligned} \Delta L_{1i}(k) &= L_{1i}(k+1) - L_{1i}(k) \\ &\leq \|e_i(k+1)\|^2 - \|e_i(k)\|^2 \\ &\leq (m\|e_i(k)\| + m\|\epsilon_i(k)\|)^2 - \|e_i(k)\|^2 \\ &\leq 2m^2\|e_i(k)\|^2 + 2m^2\|\epsilon_i(k)\|^2 - \|e_i(k)\|^2 \end{aligned} \tag{36}$$

The difference of $L_{2i}(k)$ can be calculated as follows:

$$\begin{aligned} \Delta L_{2i}(k) &= L_{2i}(k+1) - L_{2i}(k) \\ &= \theta_i(k+1) - \theta_i(k) \\ &= -\lambda_i\theta_i(k) + \xi_i\left(\left(1-2m^2\right)\|e_i(k)\|^2 - \left(2m^2\right)\|\epsilon_i(k)\|^2\right) \end{aligned} \tag{37}$$

Then,

$$\begin{aligned}\Delta L_i(k) &= \Delta L_{1i}(k) + \Delta L_{2i}(k)\\ &\le (1-\xi_i)\left(2m^2\|\epsilon_i(k)\|^2 - \left(1-2m^2\right)\|e_i(k)\|^2\right) - \lambda_i\theta_i(k)\end{aligned} \tag{38}$$

According to the dynamic event-triggered mechanism, it can be rewritten as:

$$\begin{aligned}\Delta L_i(k) &= \Delta L_{1i}(k) + \Delta L_{2i}(k)\\ &\le (1-\xi_i)\left(2m^2\|\epsilon_i(k)\|^2 - \left(1-2m^2\right)\|e_i(k)\|^2\right) - \lambda_i\theta_i(k)\\ &\le (1-\xi_i)\rho_i\theta_i(k) - \lambda_i\theta_i(k)\\ &\le [(1-\xi_i)\rho_i - \lambda_i]\theta_i(k)\\ &< 0\end{aligned} \tag{39}$$

The secure consensus for the supply chain system is achieved.

(2) If DoS attacks occur at sampling time k and do not occur at sampling time $k+1$, it is assumed that $\alpha_i(k) = 0$, $\alpha_i(k+1) = 1$.

The difference of $L_{1i}(k)$ can be calculated as follows:

$$\begin{aligned}\Delta L_{1i}(k) &= e_{di}^T(k+1)e_{di}(k+1) - e_{di}^T(k)e_{di}(k)\\ &= e_i^T(k)e_i(k) - e_i^T(k)e_i(k)\\ &= 0\end{aligned} \tag{40}$$

The difference of $\Delta L_{2i}(k)$ can be calculated as follows:

$$\begin{aligned}\Delta L_{2i}(k) &= \theta_{di}(k+1) - \theta_{di}(k)\\ &= \theta_i(k) - \theta_i(k)\\ &= 0\end{aligned} \tag{41}$$

The secure consensus for the supply chain systems is achieved.

(3) If DoS attacks do not occur at sampling time k and occur at sampling time $k+1$, it is assumed that $\alpha_i(k) = 1$, $\alpha_i(k+1) = 0$. We discuss two situations in the next section.

When the triggering mechanisms are satisfied at $k-1$, the difference of $\Delta L_{1i}(k)$ can be calculated as follows:

$$\begin{aligned}\Delta L_{1i}(k) &= e_i^T(k+1)e_i^T(k+1) - e_i^T(k-1)e_i^T(k-1)\\ &\le \left(m\|e_i(k)\| + m\|\epsilon_i(k)\|\right)^2 - \|e_i(k-1)\|^2\\ &\le 2m^2\|e_i(k)\|^2 + 2m^2\|\epsilon_i(k)\|^2 - \|e_i(k-1)\|^2\\ &\le \left(2m^2-1\right)\|e_i(k)\|^2 + 2m^2\|\epsilon_i(k)\|^2 + \|e_i(k)\|^2 - \|e_i(k-1)\|^2\\ &\le \left(2m^2-1\right)\|e_i(k)\|^2 + 2m^2\|\epsilon_i(k)\|^2 + \left(2m^2-1\right)\|e_i(k-1)\|^2 + 2m^2\|\epsilon_i(k-1)\|^2\end{aligned} \tag{42}$$

The difference of $\Delta L_{2i}(k)$ can be calculated as follows:

$$\begin{aligned}\Delta L_{2i}(k) &= L_{2i}(k+1) - L_{2i}(k)\\ &= \theta_i(k+1) - \theta_i(k-1)\\ &= \theta_i(k+1) - \theta_i(k) + \theta_i(k) - \theta_i(k-1)\\ &= -\lambda_i\theta_i(k) + \xi_i\left(\left(1-2m^2\right)\|e(k)\|^2 - \left(2m^2\right)\|\epsilon_i(k)\|^2\right)\\ &-\lambda_i\theta_i(k-1) + \xi_i\left(\left(1-2m^2\right)\|e(k-1)\|^2 - \left(2m^2\right)\|\epsilon_i(k-1)\|^2\right)\\ &= -\lambda_i\theta_i(k) + \xi_i\left(\left(1-2m^2\right)\|e_i(k)\|^2 - \left(2m^2\right)\|\epsilon_i(k)\|^2\right)\\ &-\lambda_i\theta_i(k-1) + \xi_i\left(\left(1-2m^2\right)\|e(k-1)\|^2 - \left(2m^2\right)\|\epsilon_i(k-1)\|^2\right)\end{aligned} \tag{43}$$

Therefore, combining (42) and (43) can further give:

$$\begin{aligned}\Delta L_i(k) &= \Delta L_{1i}(k) + \Delta L_{2i}(k)\\ &\le ((1-\xi_i)\rho_i - \lambda_i)\theta_i(k) + ((1-\xi_i)\rho_i - \lambda_i)\theta_i(k-1)\end{aligned} \tag{44}$$

According to $0 < (1-\xi_i)\rho_i < \lambda_i$ and $\theta_i(k) > 0$, $\theta_i(k-1) > 0$, one can obtain $\Delta L_i(k) < 0$. The secure consensus for the supply chain system is achieved.

When the triggering mechanisms are dissatisfied at $k-1$, the difference of $\Delta L_{1i}(k)$ can be calculated as follows:

$$\begin{aligned}\Delta L_{1i}(k) &= e_i^T(k+1)e_i^T(k+1) - e_i^T(k-1)e_i^T(k-1)\\ &\le (m\|e_i(k)\| + m\|\epsilon_i(k)\|)^2 - \|e_i(k-1)\|^2\\ &\le 2m^2\|e_i(k)\|^2 + 2m^2\|\epsilon_i(k)\|^2 - \|e_i(k-1)\|^2\\ &\le \left(2m^2-1\right)\|e_i(k)\|^2 + 2m^2\|\epsilon_i(k)\|^2 + \|e_i(k)\|^2 - \|e_i(k-1)\|^2\\ &\le \left(2m^2-1\right)\|e_i(k)\|^2 + 2m^2\|\epsilon_i(k)\|^2 + \left(2m^2-1\right)\|e_i(k-1)\|^2 + 2m^2\|\epsilon_i(k-1)\|^2\end{aligned} \tag{45}$$

The difference of $\Delta L_{2i}(k)$ can be calculated as follows:

$$\begin{aligned}\Delta L_{2i}(k) &= L_{2i}(k+1) - L_{2i}(k)\\ &= \theta_i(k+1) - \theta_i(k-1)\\ &= \theta_i(k+1) - \theta_i(k) + \theta_i(k) - \theta_i(k-1)\\ &= -\lambda_i\theta_i(k) + \xi_i\Big(\left(1-2m^2\right)\|e(k)\|^2 - \left(2m^2\right)\|\epsilon_i(k)\|^2\Big)\\ &-\lambda_i\theta_i(k-1) + \xi_i\Big(\left(1-2m^2\right)\|e(k-1)\|^2 - \left(2m^2\right)\|\epsilon_i(k-1)\|^2\Big)\\ &= -\lambda_i\theta_i(k) + \xi_i\Big(\left(1-2m^2\right)\|e_i(k)\|^2 - \left(2m^2\right)\|\epsilon_i(k)\|^2\Big)\\ &-\lambda_i\theta_i(k-1) + \xi_i\Big(\left(1-2m^2\right)\|e(k-1)\|^2 - \left(2m^2\right)\|\epsilon_i(k-1)\|^2\Big)\end{aligned} \tag{46}$$

It is noted that $\|\epsilon_i(k-1)\|^2 = 0$; thus, the Lyapunov function $\Delta L_i(k)$ is calculated as:

$$\begin{aligned}\Delta L_i(k) &= \Delta L_{1i}(k) + \Delta L_{2i}(k)\\ &\le ((1-\xi_i)\rho_i - \lambda_i)\theta_i(k) - \lambda_i\theta_i(k-1) + (1-\xi_i)\left(2m^2-1\right)\|e_i(k-1)\|^2\end{aligned} \tag{47}$$

Since $0 < (1-\xi_i)\rho_i < \lambda_i$, $\lambda_i > 0$, $0 < \xi_i < 1$, $0 < m < \frac{\sqrt{2}}{2}$, we have $\Delta L_i(k) < 0$, and the secure consensus control for supply chain systems could be achieved.

(4) If DoS attacks occur at two continuous sampling times k and $k+1$, it is assumed that $\alpha_i(k) = \alpha_i(k+1) = 1$. We also discuss two situations in the next section.

When the triggering mechanisms are satisfied at $k-1$, the difference of $\Delta L_{1i}(k)$ can be calculated as follows:

$$\begin{aligned}\Delta L_{1i}(k) &= e_i^T(k)e_i(k) - e_i^T(k-1)e_i(k-1)\\ &\le \left(2m^2-1\right)\|e_i(k-1)\|^2 + 2m^2\|\epsilon_i(k)\|^2\end{aligned} \tag{48}$$

The difference of $\Delta L_{2i}(k)$ can be calculated as follows

$$\begin{aligned}\Delta L_{2i}(k) &= \theta_i(k) - \theta_i(k-1)\\ &= -\lambda_i\theta_i(k-1) + \xi_i\Big(\left(1-2m^2\right)\|e_i(k-1)\|^2 - \left(2m^2\right)\|\epsilon_i(k-1)\|^2\Big)\end{aligned} \tag{49}$$

From (43) and (44), it follows that:

$$\begin{aligned}\Delta L_i(k) &= \Delta L_{1i}(k) + \Delta L_{2i}(k)\\ &\le ((1-\xi_i)\rho_i - \lambda_i)\theta_i(k-1)\end{aligned} \tag{50}$$

Based on $0 < (1-\xi_i)\rho_i < \lambda_i$ and $\theta_i(k-1) > 0$, it yields that $\Delta L_i(k) < 0$. The secure consensus for the supply chain system is achieved. Thus, this completes the proof.

When the triggering mechanisms are dissatisfied at $k-1$, the difference of $\Delta L_{1i}(k)$ can be calculated as follows.

$$\begin{aligned}\Delta L_{1i}(k) &= e_i^T(k)e_i(k) - e_i^T(k-1)e_i(k-1)\\ &\le \left(2m^2-1\right)\|e_i(k-1)\|^2 + 2m^2\|\epsilon_i(k-1)\|^2\end{aligned} \tag{51}$$

The difference of $\Delta L_{2i}(k)$ can be calculated as follows:

$$\begin{aligned}\Delta L_{2i}(k) &= \theta_i(k) - \theta_i(k-1)\\ &= -\lambda_i\theta_i(k-1) + \xi_i\Big(\left(1-2m^2\right)\|e_i(k-1)\|^2 - \left(2m^2\right)\|\epsilon_i(k-1)\|^2\Big)\end{aligned} \tag{52}$$

Since $\|\epsilon_i(k-1)\|^2 = 0$, the difference of $\Delta L_i(k)$ can thus be calculated as follows:

$$\begin{aligned}\Delta L_i(k) &= \theta_i(k) - \theta_i(k-1)\\ &= -\lambda_i\theta_i(k-1) - (1-\xi_i)\Big(\left(1-2m^2\right)\|e_i(k-1)\|^2\Big)\end{aligned} \tag{53}$$

Based on $\theta_i(k-1) > 0$, it yields that $\Delta L_i(k) < 0$. The secure consensus for the supply chain systems is achieved. Thus, this completes the proof.

3.3. Neural Network-Based Dynamic Event-Triggered Mechanism under DoS Attacks

The RCA structure is shown in Figure 2. It can be seen that all training processes use our methods, and the learning process is introduced in the next section.

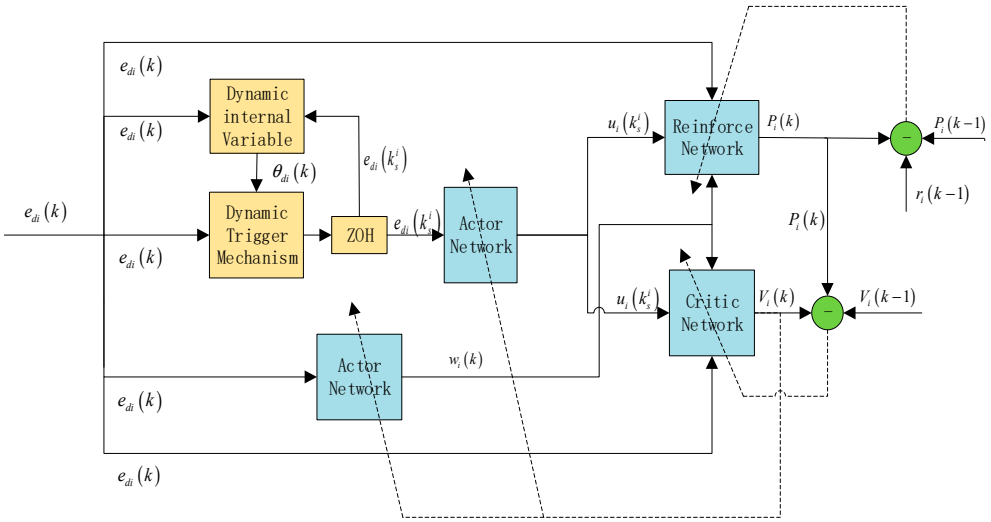

Figure 2. The RCA structure of the secure change control for supply chain systems.

3.3.1. Reinforce NN Learning Network Secure Change Design

For subchain i, we define the local internal reinforcement approximates as:

$$\hat{P}_i(\tilde{Z}_{gi}(k)) = \psi_{gi}\Big(W_{g2i}^T \cdot \psi_{gi}\Big(W_{g1i}^T \cdot \tilde{Z}_{gi}(k)\Big)\Big) \tag{54}$$

where $\tilde{Z}_{gi}(k)$ is the reinforced network secure change; it consists of $\tilde{e}_{di}(k)$, $u_i(k_s^i)$, $u_{-i}(k_s^i)$, $\omega_i(k)$, and $\omega_{-i}(k)$. W_{g1i} denotes the weights between the input layer and the hidden layer, and W_{g2i} denotes the weights between the hidden layer and the output layer.

When training the reinforced NN, the error function of the reinforced NN is defined as:

$$\tilde{\delta}_{gi}(k) = \alpha\hat{P}_i(\tilde{Z}_{gi}(k)) - \hat{P}_i(\tilde{Z}_{gi}(k-1)) + \tilde{r}_i(k-1) \tag{55}$$

The loss function is to minimize the following objective function:

$$\tilde{E}_{gi}(k) = \frac{1}{2}\tilde{\delta}_{gi}^{T}(k)\tilde{\delta}_{gi}(k) \tag{56}$$

The weights W_{g2i} updating the rules for subchain i are expressed as:

$$W_{g2i}(k+1) = W_{g2i}(k) - \mu_{gi}\left(\frac{\partial \tilde{E}_{gi}}{\partial W_{g2i}}\right) \tag{57}$$

Based on the chain backpropagation rules, we derive:

$$\begin{aligned} W_{g2i}(k+1) &= W_{g2i}(k) - \mu_{gi}\left(\frac{\partial \tilde{E}_{gi}(k)}{\partial \tilde{\delta}_{gi}(k)}\frac{\partial \tilde{\delta}_{gi}(k)}{\partial \hat{P}_i\left(\tilde{Z}_{gi}(k)\right)}\frac{\partial \hat{P}_i\left(\tilde{Z}_{gi}(k)\right)}{\partial W_{g2i}(k)}\right) \\ &= W_{g2i}(k) - \tfrac{1}{2}\mu_{gi}\alpha\tilde{\delta}_{gi}(k)\left(1 - \hat{P}_i^2\left(\tilde{Z}_{gi}(k)\right)\right)\phi_{gi}(k) \end{aligned} \tag{58}$$

where $0 < \mu_{gi} < 1$ is the learning rate of the reinforced NN, $\phi_{gi}(k) = \psi_{gi}\left(W_{g1i}^{T} \cdot \tilde{Z}_{gi}(k)\right)$.

3.3.2. Critic NN Learning Network Secure Change Design

For subchain i, we define the critic network approximates as:

$$\hat{V}_i\left(\tilde{Z}_{ci}(k)\right) = W_{c2i}^{T}\psi_{ci}\left(W_{c1i}^{T} \cdot \tilde{Z}_{ci}(k)\right) \tag{59}$$

where $\tilde{Z}_{ci}(k)$ is the critic network secure change; it consists of $\tilde{e}_{di}(k)$, $u_i\left(k_s^i\right)$, $u_{-i}\left(k_s^i\right)$, $\omega_i(k)$, $\omega_{-i}(k)$, and $\hat{P}_i\left(\tilde{Z}_{gi}(k)\right)$. W_{c1i} denotes the weights between the input layer and the hidden layer, and W_{c2i} denotes the weights between the hidden layer and the output layer.

The error of the critic network is obtained:

$$\tilde{\delta}_{gi}(k) = \alpha\hat{P}_i\left(\tilde{Z}_{gi}(k)\right) - \hat{P}_i\left(\tilde{Z}_{gi}(k-1)\right) + \tilde{r}_i(k-1) \tag{60}$$

The objective function of the critic network to be minimized is:

$$\tilde{E}_{ci}(k) = \frac{1}{2}\tilde{\delta}_{ci}^{T}(k)\tilde{\delta}_{ci}(k) \tag{61}$$

The weights W_{c2i} updating the rules for subchain i are given by:

$$W_{c2i}(k+1) = W_{c2i}(k) - \mu_{ci}\left(\frac{\partial \tilde{E}_{ci}(k)}{\partial W_{c2i}(k)}\right) \tag{62}$$

Based on the chain backpropagation rules, we derive:

$$\begin{aligned} W_{c2i}(k+1) &= W_{c2i}(k) - \mu_{ci}\left(\frac{\partial \tilde{E}_{ci}(k)}{\partial \tilde{\delta}_{ci}(k)}\frac{\partial \tilde{\delta}_{ci}(k)}{\partial \hat{V}_i\left(\tilde{Z}_{ci}(k)\right)}\frac{\partial \hat{V}_i\left(\tilde{Z}_{ci}(k)\right)}{\partial W_{c2i}(k)}\right) \\ &= W_{c2i}(k) - \mu_{ci}\eta\tilde{\delta}_{ci}(k)\psi_{ci}\left(W_{c1i}^{T} \cdot \tilde{Z}_{ci}(k)\right) \end{aligned} \tag{63}$$

where $0 < \mu_{ci} < 1$ is the learning rate of the reinforced NN.

3.3.3. Actor NN Learning Network Secure Change Design

For subchain i, we define the optimal control input under the dynamic event-triggered mechanism as:

$$\hat{u}_i(k) = \psi_{ai}\left(W_{a2i}^{T} \cdot \psi_{ai}\left(W_{a1i}^{T} \cdot \tilde{Z}_{ai}(k)\right)\right) \tag{64}$$

where $\tilde{Z}_{ai}(k)$ is the actor network secure change for optimal control input; it consists of $e_{di}\left(k_s^i\right)$. W_{a1i} denotes the weights between the input layer and the hidden layer, and W_{a2i} denotes the weights between the hidden layer and the output layer.

The error of the actor network secure change for optimal control input is obtained:

$$\delta_{ai}(k) = \hat{V}_i\left(\tilde{Z}_{ci}(k)\right) - U_c \tag{65}$$

The objective function of the actor network to be minimized is:

$$\tilde{E}_{ai}(k) = \frac{1}{2}\tilde{\delta}_{ai}^T(k)\tilde{\delta}_{ai}(k) \tag{66}$$

The weights W_{c2i} updating the rules for subchain i are expressed as:

$$W_{a2i}(k+1) = W_{a2i}(k) - \mu_{ai}\left(\frac{\partial \tilde{E}_{ai}(k)}{\partial W_{a2i}(k)}\right) \tag{67}$$

Based on the chain backpropagation rules, we derive:

$$\begin{aligned} &W_{a2i}(k+1) = W_{a2i}(k) - \mu_{ai}\left(\frac{\partial \tilde{E}_{ai}(k)}{\partial \hat{V}_i\left(\tilde{Z}_{ci}(k)\right)}\frac{\partial \hat{V}_i\left(\tilde{Z}_{ci}(k)\right)}{\partial \hat{u}_i(k)}\frac{\partial \hat{u}_i(k)}{\partial W_{a2i}(k)}\right) \\ &= W_{a2i}(k) - \tfrac{1}{4}\mu_{ai}\phi_{ai}(k)W_{c2i}^T(k)C_1(k)\left(1-\hat{u}_i^2(k)\right)\left[W_{c2i}^T(k)\psi_{ci}\left(W_{c1i}^T\cdot\tilde{Z}_{ci}(k)\right)\right] \end{aligned} \tag{68}$$

where $0 < \mu_{ai} < 1$ is the learning rate of the actor network secure change for optimal control input, $\phi_{ai}(k) = \psi_{ai}\left(W_{a1i}^T\cdot\tilde{Z}_{ai}(k)\right)$, $C_1(k) = \partial\psi_{ci}\left(W_{c1i}^T\cdot\tilde{Z}_{ci}(k)\right)/\partial\hat{u}_i(k)$.

For subchain i, we define the worst-case disturbance input under the traditional time-triggered mechanism as:

$$\hat{\omega}_i(k) = \psi_{ai}\left(W_{d2i}^T\cdot\psi_{ai}\left(W_{d1i}^T\cdot\tilde{Z}_{di}(k)\right)\right) \tag{69}$$

where $\tilde{Z}_{di}(k)$ is the actor network secure change for the worst-case disturbance input; it consists of $\tilde{e}_{di}(k)$. W_{d1i} denotes the weights between the input layer and the hidden layer, and W_{d2i} denotes the weights between the hidden layer and the output layer.

The error function of the actor network secure change for the worst-case disturbance input and objective function are the same results as in (57) and (58).

The weights W_{d2i} updating the rules for subchain i are expressed as:

$$W_{d2i}(k+1) = W_{d2i}(k) - \mu_{di}\left(\frac{\partial \tilde{E}_{di}(k)}{\partial W_{d2i}(k)}\right) \tag{70}$$

Based on the chain backpropagation rules, we derive:

$$\begin{aligned} &W_{d2i}(k+1) = W_{d2i}(k) - \mu_{di}\left(\frac{\partial \tilde{E}_{ai}(k)}{\partial \hat{V}_i\left(\tilde{Z}_{ci}(k)\right)}\frac{\partial \hat{V}_i\left(\tilde{Z}_{ci}(k)\right)}{\partial \hat{\omega}_i(k)}\frac{\partial \hat{\omega}_i(k)}{\partial W_{d2i}(k)}\right) \\ &= W_{d2i}(k) - \tfrac{1}{4}\mu_{di}\phi_{di}(k)W_{c2i}^T(k)C_2(k)\left(1-\hat{\omega}_i^2(k)\right)\left[W_{c2i}^T(k)\psi_{ci}\left(W_{c1i}^T\cdot\tilde{Z}_{ci}(k)\right)\right] \end{aligned} \tag{71}$$

where $0 < \mu_{ai} < 1$ is the learning rate of the actor network secure change for the worst-case disturbance input, $\phi_{di}(k) = \psi_{di}\left(W_{d1i}^T\cdot\tilde{Z}_{di}(k)\right)$, $C_2(k) = \partial\psi_{ci}\left(W_{c1i}^T\cdot\tilde{Z}_{ci}(k)\right)/\partial\hat{\omega}_i(k)$.

4. Simulation

In this section, we consider a supply chain system to testify to the validity of the proposed results. We consider a supply chain system with four subchains and one chain leader. The system matrices are $A = \begin{bmatrix} 0.7 & 0 \\ 0 & 0.8 \end{bmatrix}$, $B = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$, and $D = \begin{bmatrix} 0 \\ -1 \end{bmatrix}$. The topology of the communication network is illustrated in Figure 3. The four subchains are denoted 1 2 3 4 and one chain leader is 0.

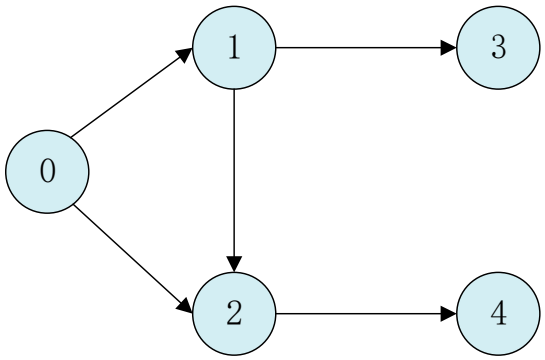

Figure 3. The topology of the communication network.

We can obtain the edge matrix with $a_{21} = a_{31} = a_{42} = 1$ and the pinning gain with $b_1 = b_2 = 1$, $b_3 = b_4 = 0$. The weight matrices are selected as $Q_{ii} = I_{2\times 2}$, $R_{21} = R_{31} = R_{42} = 1$, $R_{11} = R_{22} = R_{33} = R_{44} = 1$. We set the initial production inventory status as $x_0(0) = [1.5, 1.5]^T$, $x_1(0) = [1, 1]^T$, $x_2(0) = [1, 1.2]^T$, $x_3(0) = [0.5, 1.2]^T$, and $x_4(0) = [0.8, 0.9]^T$. The initial productions are chosen as $u_1(0) = [0.3, 0.1]^T$, $u_2(0) = [0.5, 0.2]^T$, $u_3(0) = [0.1, 0.3]^T$, and $u_4(0) = [0.2, 0.4]^T$. The initial demand market is chosen as $\omega_i(0) = 0.1$. The attenuation level of the bullwhip effect γ is chosen as $\gamma = 1$ and the constant demand market $d = 0.1$.

In the training process, we select the discount factors $\alpha = \eta = 0.9$ and the learning rates $\mu_{gi} = \mu_{ci} = \mu_{ai} = \mu_{di} = 0.04$. Next, we choose dynamic event-triggered parameters $m^2 = 0.1$, $\lambda_i = 0.2$, $\rho_i = 0.1$, and $\xi_i = 0.3$ and the initial internal dynamic variable $\theta_1(0) = 1$, $\theta_2(0) = 2$, $\theta_3(0) = 3$, and $\theta_4(0) = 4$. The parameters of DoS attacks are chosen as $\beta_i = \beta_2 = \beta_3 = \beta_4 = 0.5$. The initial weights are selected randomly in $(0, 1)$.

The results are shown in Figures 4 and 5. The production inventory status of the four subchains and chain leaders under the proposed secure change control scheme can be seen.

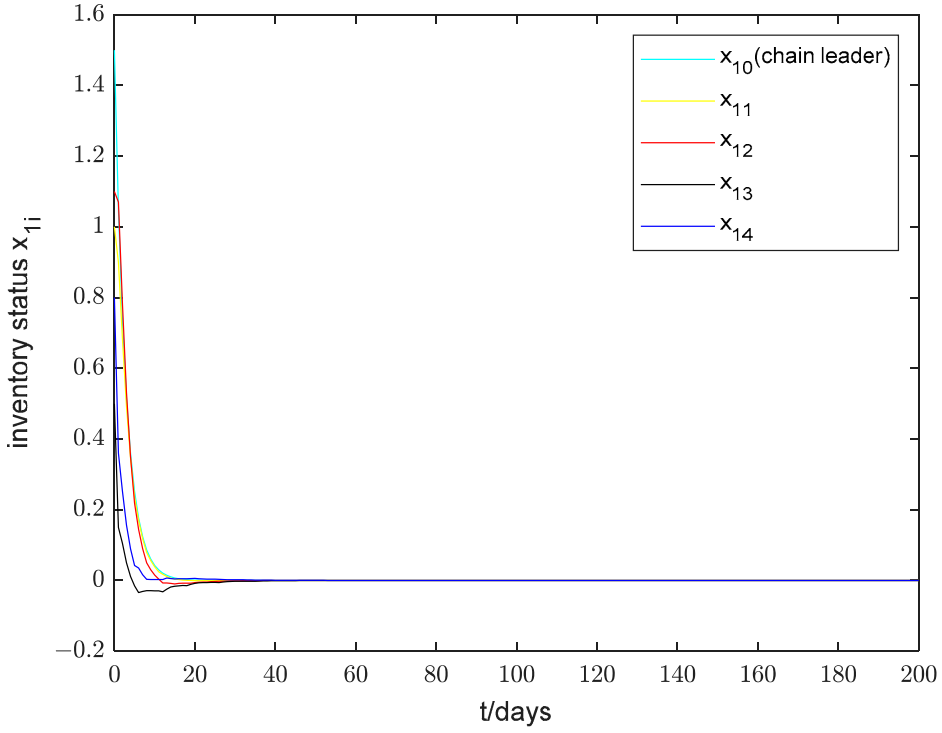

Figure 4. The production inventory status x_{1i}.

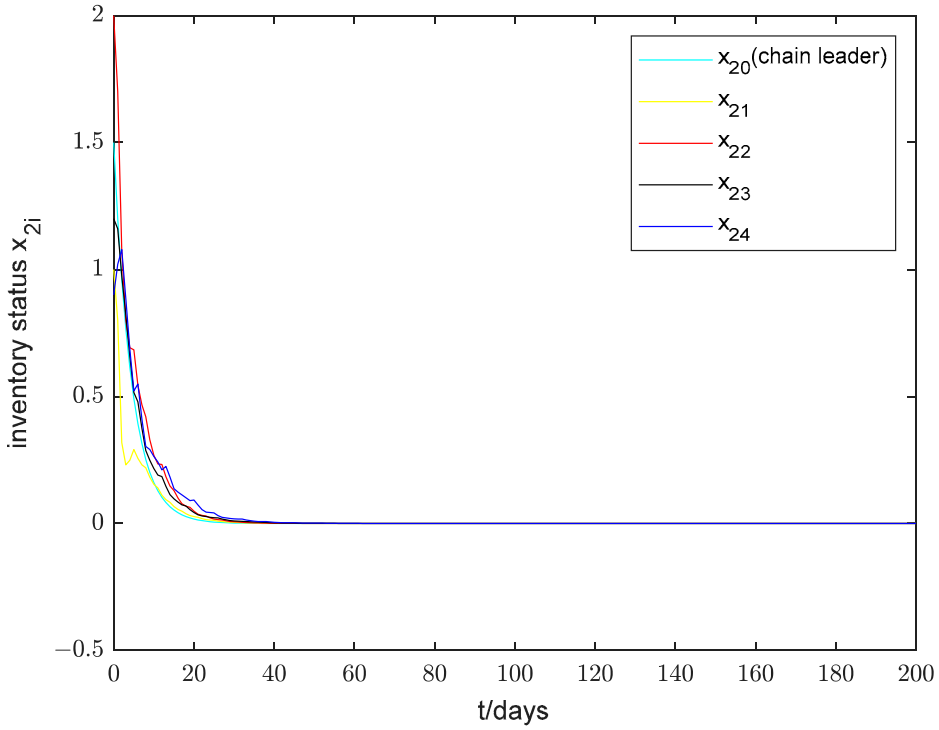

Figure 5. The production inventory status x_{2i}.

The weight curves of the reinforced neural network, the critic neural network, and the actor neural network are shown in Figures 6–9. It can be observed that the weights are convergent at $k = 5$ a day. Due to the supply chain system still operating using the RCA structure under DoS attacks, the subchains cannot track the supply leaders. Thus, in Figures 4 and 5, it can be seen that the production inventory status of all subchains and supply leaders demonstrates that synchronization is achieved around $k = 60$ a day under DoS attacks.

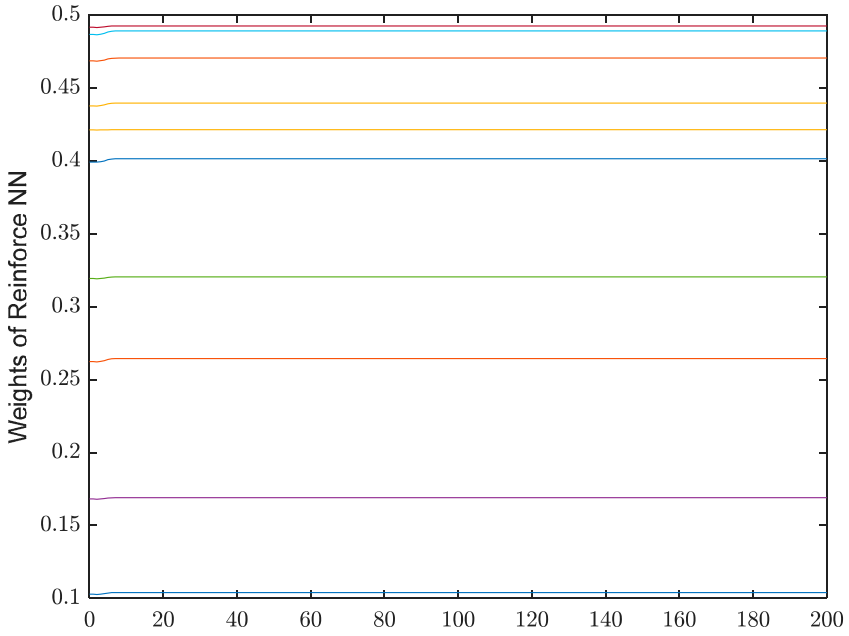

Figure 6. The curves of the weights W_{g2}.

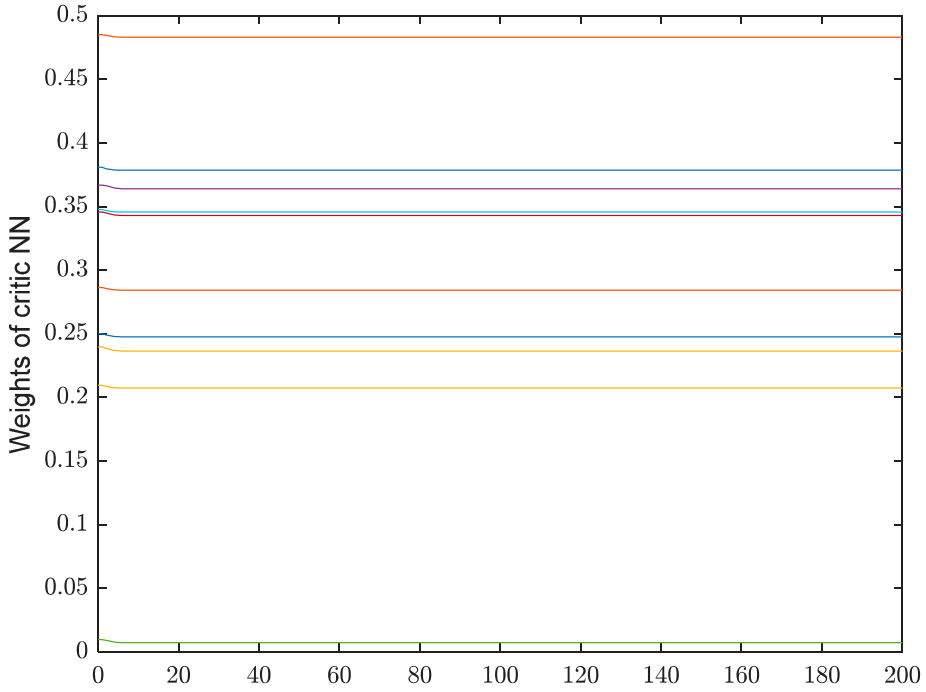

Figure 7. The curves of the weights W_{c2}.

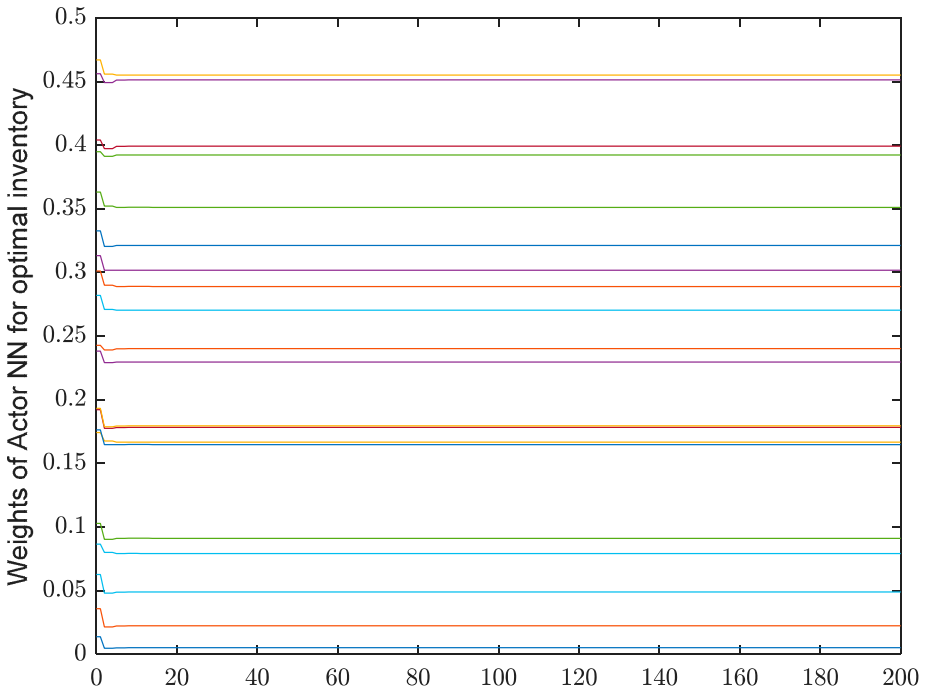

Figure 8. The curves of the weights W_{a21}.

Figures 10 and 11 depict that the inventory status errors eventually converge to zero around $k = 60$ a day. It can be seen that the internal dynamic variable θ_i is always positive and convergent in Figure 12. The trigger instants of the four subchains are shown in Figure 13. The trajectories of triggering errors $\|\varepsilon_i(k)\|^2$ along with the dynamic event-triggering threshold are shown in Figure 14. The instants under DoS attacks can be seen in Figure 15a,b.

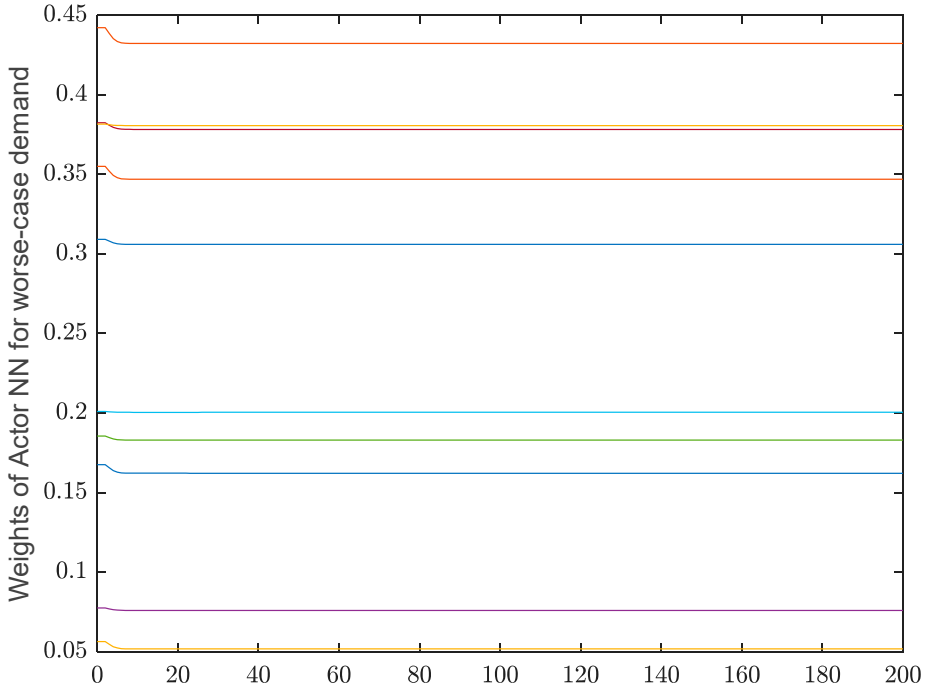

Figure 9. The curves of the weights W_{d21}.

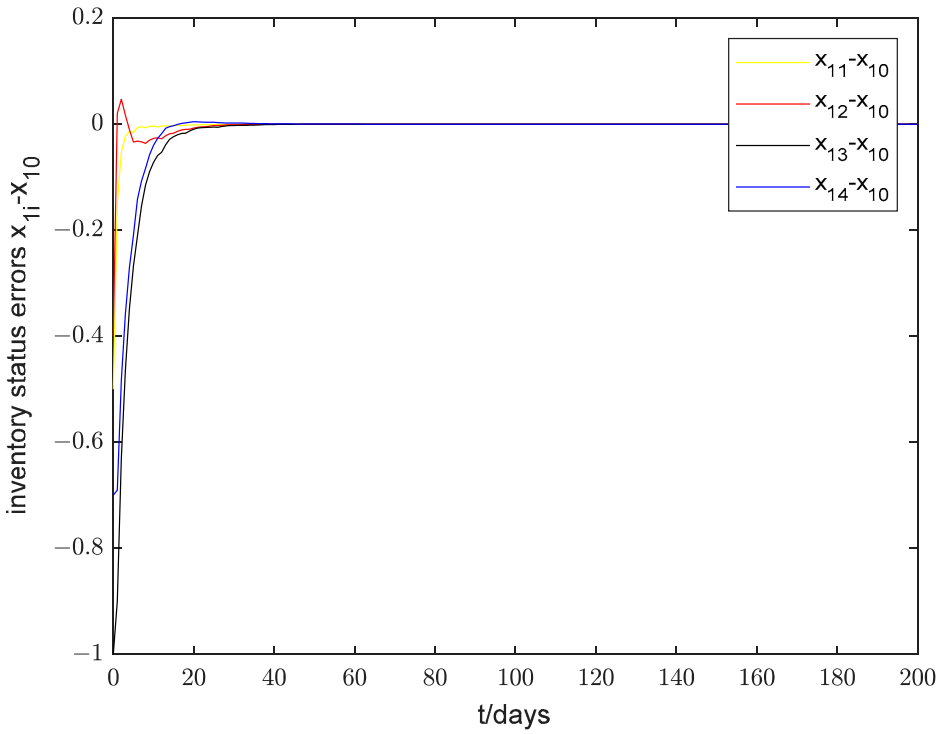

Figure 10. The inventory status errors of x_{1i}.

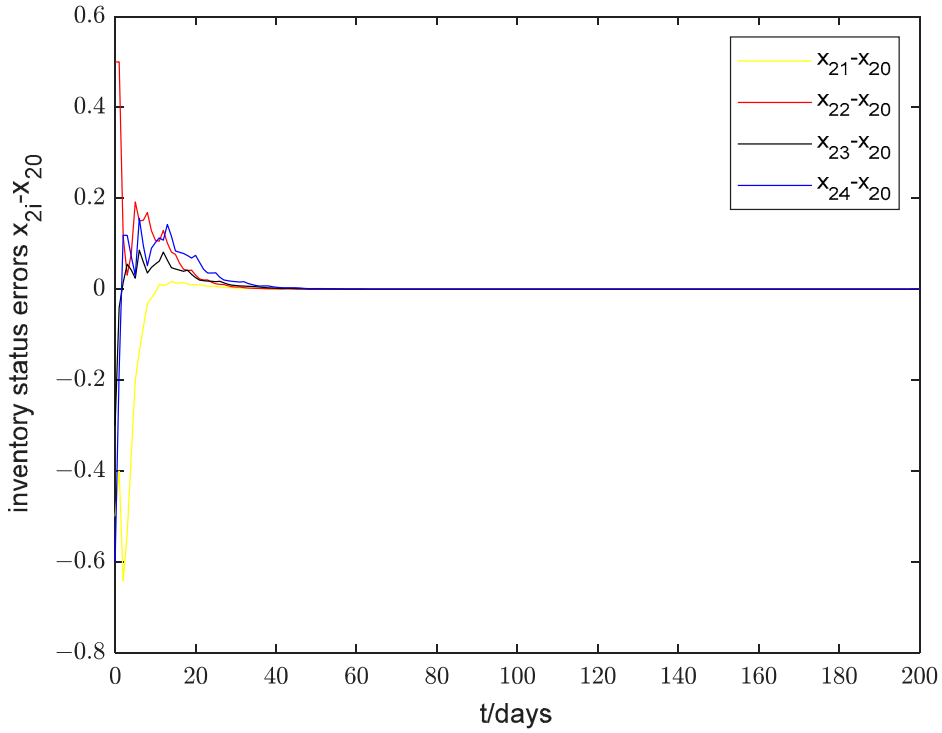

Figure 11. The inventory status errors of x_{2i}.

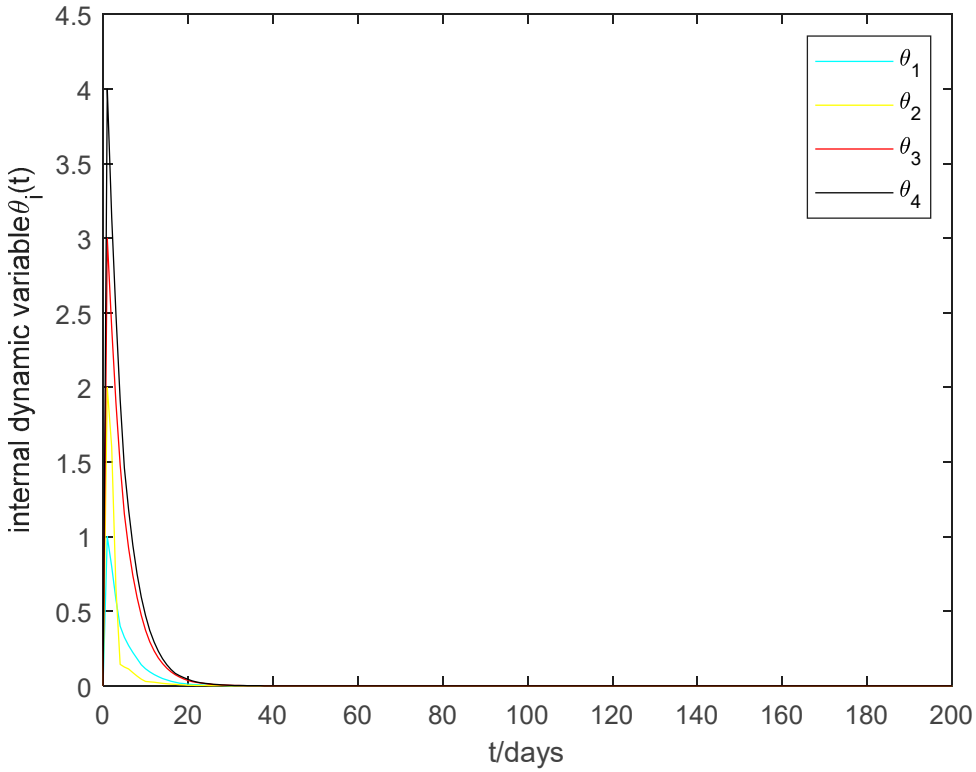

Figure 12. The internal dynamic variable θ_i.

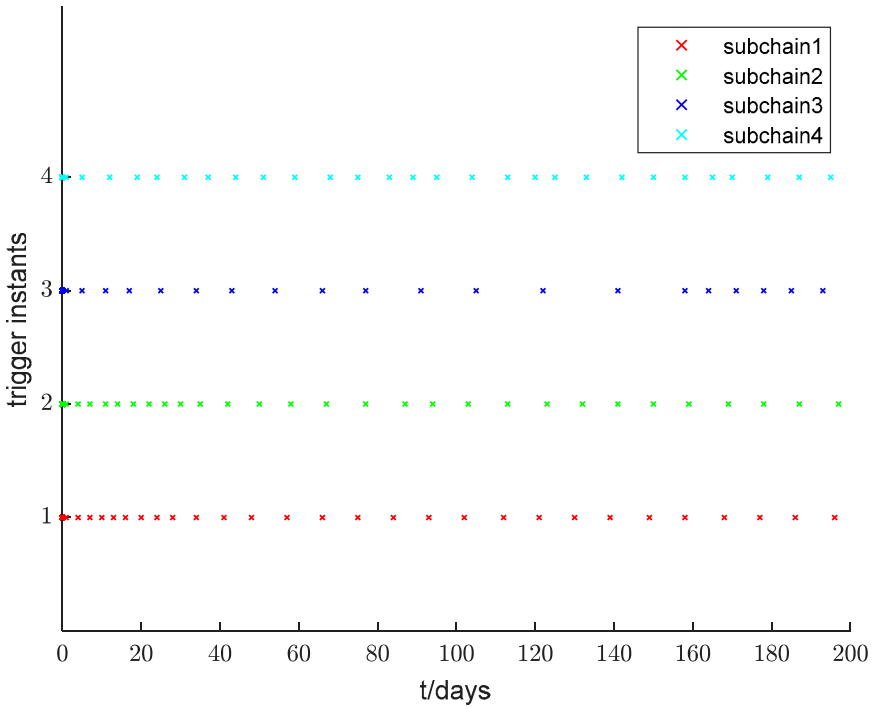

Figure 13. The trigger instants of the four subchains.

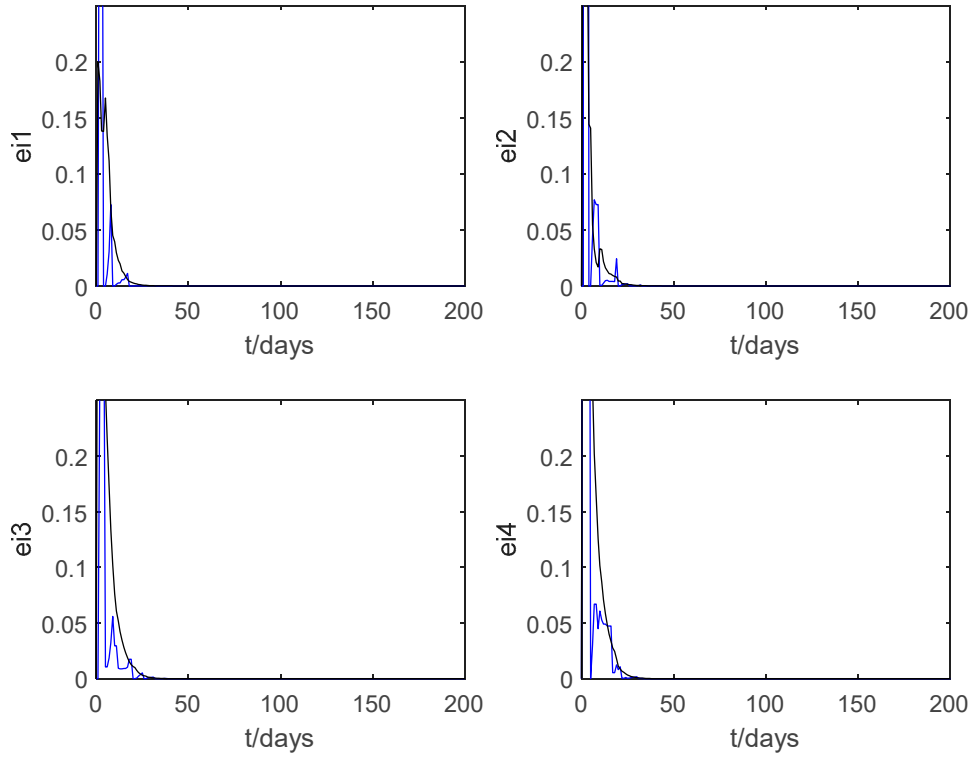

Figure 14. The trajectories of triggering errors $\|\varepsilon_i(k)\|^2$ along with the dynamic event-triggering threshold.

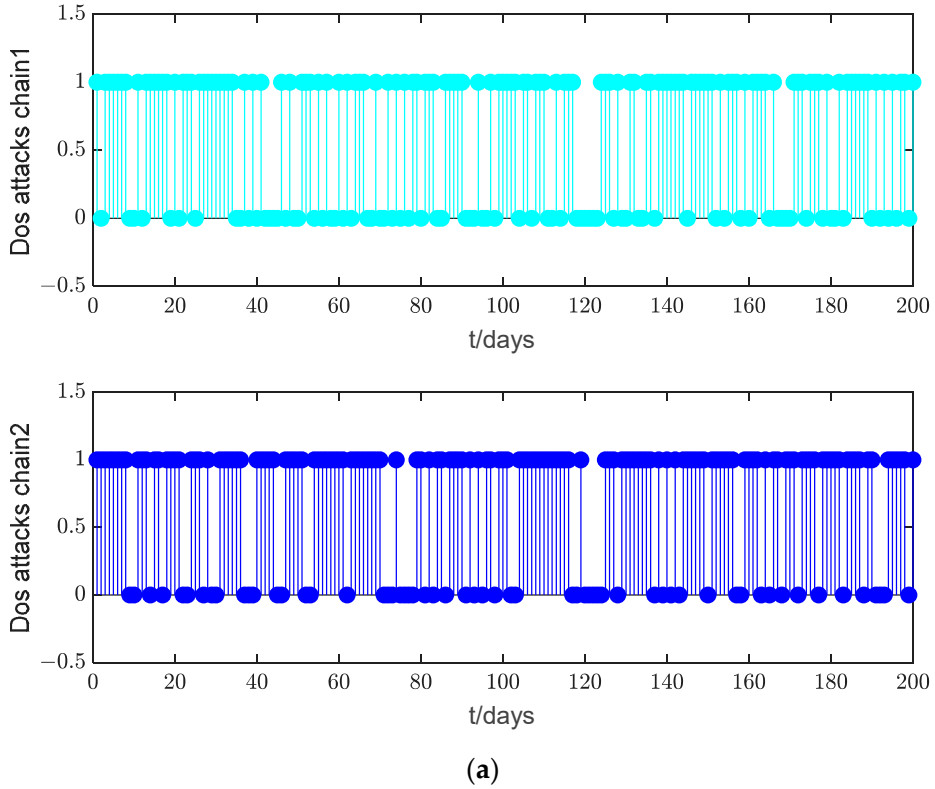

Figure 15. (**a**). DoS attack instants of subchains 1 and 2. (**b**). DoS attack instants of subchains 3 and 4.

5. Conclusions

In this paper, supply chain systems are provided by a new data-driven method based on the established RCA structure. The problems of unknown demand and the

dynamic model can be solved by this method under Dos attacks. The secure change control problem for supply chain systems under DoS attacks is solved under the dynamic event-triggered mechanism. The proposed method requires no system model information, only the inventory status, production input, and disturbance input. Firstly, to alleviate the influence of DoS attacks, a structure of secure change control for supply chain systems is designed. A secure change mechanism is used to store the latest received data packets based on the structure. Then, a dynamic event-triggered mechanism is proposed for supply chain systems using RL. In addition, an RCA structure of secure change control for supply chain systems is provided. The dynamic event-triggered mechanism is applied to reduce the number of production input updates. The stability proof is provided by using the Lyapunov function under DoS attacks. Finally, the simulation results verify that the subchains can be tracked by the chain leaders using an RCA structure under DoS attacks. The weight curves of the network are eventually convergent.

It is worth noting that the proposed method can be applied not only to linear supply chain systems to achieve secure change tracking control but also to non-linear supply chain systems. However, considering that actual supply chain systems' DoS attacks are usually aperiodic and unpredictable, supply chain systems' aperiodic denial of service attacks under network attack events may be developed and studied in future work.

Author Contributions: Conceptualization, L.F. and Q.L.; methodology, B.Z.; software, B.Z.; validation, Q.L., S.X. and L.F.; formal analysis, B.Z. and L.F.; writing—original draft preparation, B.Z.; writing—review and editing, L.F. and B.Z.; visualization, S.X.; supervision, Q.L.; project administration, L.F. and Q.L.; funding acquisition, L.F., S.X. and Q.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Key Research and Development Program of China (No.2020YFB1708200) and in part by the Project of Cultivation for Young Topnotch Talents of Beijing Municipal Institutions under Grant BPHR202203231 and the R&D Program of Beijing Municipal Education Commission (KM202210009011). The corresponding author of this paper is Lingling Fan. This work was supported by the National Natural Science Foundation (NNSF) of China under Grant 62103057.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare that there are no conflicts of interest.

References

1. Gharaei, A.; Jolai, F. A multi-agent approach to the integrated production scheduling and distribution problem in multi-factory supply chain. *Appl. Soft Comput.* **2018**, *65*, 577–589. [CrossRef]
2. Yang, N.; Ding, Y.; Leng, J.; Zhang, L. Supply chain information collaborative simulation model integrating multi-agent and system dynamics. *Promet-Traffic Transp.* **2022**, *34*, 711–724. [CrossRef]
3. Henriques, R.d.S. Multi-agent system approach applied to a manufacturer's supply chain using global objective function and learning concepts. *J. Intell. Manuf.* **2019**, *30*, 1009–1019. [CrossRef]
4. Dharmapriya, S.; Kiridena, S.; Shukla, N. Multiagent Optimization Approach to Supply Network Configuration Problems with Varied Product-Market Profiles. *IEEE Trans. Eng. Manag.* **2022**, *69*, 2707–2722. [CrossRef]
5. Xu, X.; Lee, S.-D.; Kim, H.-S.; You, S.-S. Management and optimisation of chaotic supply chain system using adaptive sliding mode control algorithm. *Int. J. Prod. Res.* **2021**, *59*, 2571–2587. [CrossRef]
6. Cuong, T.N.; Kim, H.-S.; Nguyen, D.A.; You, S.-S. Nonlinear analysis and active management of production-distribution in nonlinear supply chain model using sliding mode control theory. *Appl. Math. Model.* **2021**, *97*, 418–437. [CrossRef]
7. Zhang, S.; Zhang, C.; Zhang, S.; Zhang, M. Discrete Switched Model and Fuzzy Robust Control of Dynamic Supply Chain Network. *Complexity* **2018**, *2018*, 3495096. [CrossRef]
8. Sun, T.-C.; Yousefpour, A.; Karaca, Y.; Alassafi, M.O.; Ahmad, A.M.; Li, Y.-M. Dynamical investigation and distributed consensus tracking control of a variable-order fractional supply chain network using a multi-agent neural network-based control method. *Fractals-Complex Geom. Patterns Scaling Nat. Soc.* **2022**, *30*, 2240168. [CrossRef]
9. Shi, L.; Guo, W.; Wang, L.; Bekiros, S.; Alsubaie, H.; Alotaibi, A.; Jahanshahi, H. Stochastic Fixed-Time Tracking Control for the Chaotic Multi-Agent-Based Supply Chain Networks with Nonlinear Communication. *Electronics* **2023**, *12*, 83. [CrossRef]
10. Fu, D.; Zhang, H.T.; Dutta, A.; Chen, G. A Cooperative Distributed Model Predictive Control Approach to Supply Chain Management. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *50*, 4894–4904. [CrossRef]

11. Fu, D.; Zhang, H.T.; Yu, Y.; Ionescu, C.M.; Aghezzaf, E.H.; Keyser, R.D. A Distributed Model Predictive Control Strategy for the Bullwhip Reducing Inventory Management Policy. *IEEE Trans. Ind. Inform.* **2019**, *15*, 932–941. [CrossRef]
12. Boccadoro, M.; Martinelli, F.; Valigi, P. Supply Chain Management by H-Infinity Control. *IEEE Trans. Autom. Sci. Eng.* **2008**, *5*, 703–707. [CrossRef]
13. Li, Q.K.; Lin, H.; Tan, X.; Du, S. H∞ Consensus for Multiagent-Based Supply Chain Systems under Switching Topology and Uncertain Demands. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *50*, 4905–4918. [CrossRef]
14. Wang, Q.; Shang, J. Analysis of the quality improvement path of supply chain management under the background of Industry 4.0. *Int. J. Technol. Manag.* **2023**, *91*, 1–18. [CrossRef]
15. Long, Q.; Zhang, W. An integrated framework for agent based inventory-production-transportation modeling and distributed simulation of supply chains. *Inf. Sci.* **2014**, *277*, 567–581. [CrossRef]
16. Liu, C.; Cai, W.; Zhang, C.; Wei, F. Data-driven intelligent control system in remanufacturing assembly for production and resource efficiency. *Int. J. Adv. Manuf. Technol.* **2023**, *128*, 3531–3544. [CrossRef]
17. Xu, L.; Mak, S.; Brintrup, A. Will bots take over the supply chain? Revisiting agent-based supply chain automation. *Int. J. Prod. Econ.* **2021**, *241*, 108279. [CrossRef]
18. Chen, J.; Kang, H.; Wang, H. A Product-Design-Change-Based Recovery Control Algorithm for Supply Chain Disruption Problem. *Electronics* **2023**, *12*, 2552. [CrossRef]
19. Wei, Z.; Liu, Y.; Wu, Y.; Chen, W.; Li, Q.-K. T-S fuzzy model based event-triggered change control for product and supply chain systems. *Int. J. Syst. Sci.* **2023**, *55*, 426–439. [CrossRef]
20. Yang, Y.; Li, Y.; Yue, D.; Tian, Y.C.; Ding, X. Distributed Secure Consensus Control with Event-Triggering for Multiagent Systems under DoS Attacks. *IEEE Trans. Cybern.* **2021**, *51*, 2916–2928. [CrossRef] [PubMed]
21. Du, S.; Sheng, H.; Ho, D.W.C.; Qiao, J. Secure Consensus of Multiagent Systems with DoS Attacks via Fully Distributed Dynamic Event-Triggered Control. *IEEE Trans. Syst. Man Cybern. Syst.* **2023**, *53*, 6588–6597. [CrossRef]
22. Ma, Y.S.; Che, W.W.; Deng, C.; Wu, Z.G. Model-Free Adaptive Resilient Control for Nonlinear CPSs with Aperiodic Jamming Attacks. *IEEE Trans. Cybern.* **2023**, *53*, 5949–5956. [CrossRef]
23. Ma, Y.S.; Che, W.W.; Deng, C.; Wu, Z.G. Distributed Model-Free Adaptive Control for Learning Nonlinear MASs under DoS Attacks. *IEEE Trans. Neural Netw. Learn. Syst.* **2023**, *34*, 1146–1155. [CrossRef]
24. Zhang, H.; Jiang, H.; Luo, Y.; Xiao, G. Data-Driven Optimal Consensus Control for Discrete-Time Multi-Agent Systems with Unknown Dynamics Using Reinforcement Learning Method. *IEEE Trans. Ind. Electron.* **2017**, *64*, 4091–4100. [CrossRef]
25. Zhong, X.; He, H. GrHDP Solution for Optimal Consensus Control of Multiagent Discrete-Time Systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *50*, 2362–2374. [CrossRef]
26. Li, T.; Yang, D.; Xie, X.; Zhang, H. Event-Triggered Control of Nonlinear Discrete-Time System with Unknown Dynamics Based on HDP(λ). *IEEE Trans. Cybern.* **2022**, *52*, 6046–6058. [CrossRef]
27. Peng, Z.; Luo, R.; Hu, J.; Shi, K.; Ghosh, B.K. Distributed Optimal Tracking Control of Discrete-Time Multiagent Systems via Event-Triggered Reinforcement Learning. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2022**, *69*, 3689–3700. [CrossRef]
28. Ponte, B.; Pino, R.; de la Fuente, D. Multiagent Methodology to Reduce the Bullwhip Effect in a Supply Chain. In Proceedings of the International Joint Conference on Computational Intelligence (IJCCI), Barcelona, Spain, 5–7 October 2012; pp. 1–21.
29. Wang, X.; Ding, D.; Ge, X.; Han, Q.L. Supplementary Control for Quantized Discrete-Time Nonlinear Systems under Goal Representation Heuristic Dynamic Programming. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *35*, 3202–3214. [CrossRef]
30. Chauhdary, S.H.; Alkatheiri, M.S.; Alqarni, M.A.; Saleem, S. An efficient evolutionary deep learning-based attack prediction in supply chain management systems. *Comput. Electr. Eng.* **2023**, *109*, 108768. [CrossRef]
31. Abosuliman, S.S. Deep learning techniques for securing cyber-physical systems in supply chain 4.0. *Comput. Electr. Eng.* **2023**, *107*, 108637. [CrossRef]
32. Khan, I.A.; Moustafa, N.; Pi, D.; Hussain, Y.; Khan, N.A. DFF-SC4N: A Deep Federated Defence Framework for Protecting Supply Chain 4.0 Networks. *IEEE Trans. Ind. Inform.* **2023**, *19*, 3300–3309. [CrossRef]
33. Yeboah-Ofori, A.; Swart, C.; Opoku-Boateng, F.A.; Islam, S. Cyber resilience in supply chain system security using machine learning for threat predictions. *Contin. Resil. Rev.* **2022**, *4*, 1–36. [CrossRef]
34. Song, R.; Liu, L.; Xia, L.; Lewis, F.L. Online Optimal Event-Triggered H∞ Control for Nonlinear Systems with Constrained State and Input. *IEEE Trans. Syst. Man Cybern. Syst.* **2023**, *53*, 131–141. [CrossRef]
35. Zhang, Y.; Zhao, B.; Liu, D.; Zhang, S. Event-Triggered Control of Discrete-Time Zero-Sum Games via Deterministic Policy Gradient Adaptive Dynamic Programming. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *52*, 4823–4835. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.