Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

Robustness Of Interdependent Supply Chain Networks Considering Disruption Propagation

Lei Zhang, Jian Zhou, Yizhong Ma

School of Economics and Management, Nanjing University of Science and Technology, Nanjing, Jiangsu 210094, China

Keywords: interdependent supply chain network, robustness, disruption propagation, network structure

---

Failure mode analyses play a crucial role in ensuring the robustness of interdependent supply chain networks (ISCNs). However, most existing research focuses on a single failure mode for ISCNs, which may not accurately represent real-world ISCNs. This paper proposes a new disruption propagation model with four failure modes regarding ISCNs. In this paper, A weight-directed ISCN model is first developed to investigate the process of disruption propagation. Then, we conduct case studies of synthetic networks and a European supply chain network and evaluate the impact of network structures and interdependent patterns on the robustness of ISCNs. The simulation results show that adjusting these factors can enhance network performance more effectively.

Traditionally, Supply chain networks (SCNs) were often seen as isolated logistics networks, and SCNs' interaction with other types of network systems is rarely considered. However, due to the evolution of information technology, data platforms in communication networks are widely used to gather and process the data on production and transportation within logistics networks. It sends control signals to maintain the normal operation of logistics networks. As a result, SCNs have developed into interdependent supply chain networks (ISCNs) (Ivanov and Dolgui, 2021; Panetto et al. 2019), which can be modelled as a combination of a weighted undirected cyber-supply network (CSN) and a weighted directed physical-supply network (PSN). The network structures and interdependent patterns impact the robustness of ISCNs. Most research has focused on a single network structure and interdependent pattern. However, in practice, there are many different types of network structures, such as Erdos-Renyi (ER) networks and Barabasi-Albert (BA) networks. The interdependent patterns include random links (RL), assortative links (AL), and disassortative links (DL). To study the robustness of ISCN, it is important to consider different network structures and interdependency patterns.

Generally, Failure modes in ISCNs can be categorized into four types: overload failures, underload failures, loss-dependence failures (i.e., if a node in a subnetwork is connected to a failed node in another subnetwork, the node will fail), and isolation failures (i.e., if a node isolates from the largest connected component of an ISCN, then the node fails) (Shi et al., 2022). It is worth pointing out that most studies on the disruption propagation models consider four failure modes separately. However, in real-world ISCNs, four failure modes can occur simultaneously. For example, the disruption of Venezuela's power supply network in 2019 triggered mixed cascading failures with overload, underload, loss-dependency, and isolation failures, causing the network to collapse. However, in most existing studies about ISCNs, these four failure modes are rarely considered together.

A PSN is a weighted directed network, and a CSN is a weighted undirected network in this paper. The PSN and CSN models are represented as follows:

$$G^P = (V^P, E^P, W^P, L^P(0), A^P, B^P), \tag{1}$$

$$G^C = (V^C, E^C, W^C, L^C(0), C^C), \tag{2}$$

where G^P and G^C represent a PSN and a CSN, respectively. $V^P = V^C = \{v_i^{P/C} \mid i = 1, 2, ..., N^{P/C}\}$ is the set of nodes. $E^P = E^C = \{e_{ij}^{P/C} = 1 \text{ or } 0, i, j = 1, 2, ..., N^{P/C}\}$ is the set of connectivity links, $W^P = W^C = \{w_{ij}^{P/C} \mid e_{ij}^{P/C} = 1, i, j = 1, 2, ..., N^{P/C}\}$ is the set of connectivity link weights. $L^P(0) = L^C(0) = \{L_i^{P/C}(0) \mid i = 1, 2, ..., N^{P/C}\}$ indicates the set of initial loads on each node. $A^P = \{A_i^P \mid i = 1, 2, ..., N^P\}$ and $B^P = \{B_i^P \mid i = 1, 2, ..., N^P\}$ are the sets of upper and lower bounds on capacity in a PSN, respectively. $C^C = \{C_i^C \mid i = 1, 2, ..., N^C\}$ denotes the capacity of each node in the CSN.

The disruption propagation process with four failure modes is depicted in Fig. 1. In stage 1. We randomly interrupt a node in the CSN. The initial disruption propagates to neighboring nodes along the network link. If the load of the PSN node is less than its capacity, then it will be removed due to underload failure (indicated as brown). If the load of the CSN node is greater than its capacity, then it will be removed due to overload failure (marked in blue). Loss-dependence failures are shown in green, and isolation failures are shown in yellow.

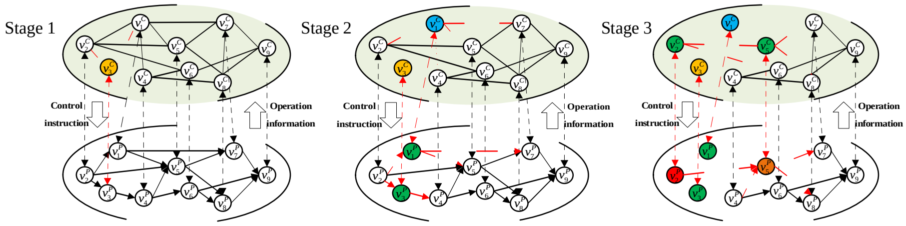

Fig. 1. The disruption propagation process of an ISCN.

The following robustness metric is used to evaluate the performance loss after a disruption,

$$R = (G_{LCC}^{C'} + G_{LWCC}^{P'}) / (N^C + N^P), \tag{3}$$

where $G_{LCC}^{C'}$ is the size of the largest connected component (LCC) in the CSN, and $G_{LWCC}^{P'}$ denotes the size of the largest weakly connected component (LWCC) in the PSN.

We set the number of nodes and average degrees of CSN and PSN to be equal, 400 and 4. Four attack types are used to simulate the disruption propagation, including random attacks on PSNs (RAP), intentional attacks on PSNs (IAP), random attacks on CSNs (RAC), and intentional attacks on CSNs (IAC).

Table 1 The simulation results of ISCN robustness considering disruption propagation for three network structures.

	ER-ER	ER-BA	BA-BA
RAC	[0.9750, 0.9004, 0.8078, 0.6219, 0.2536]	[0.9750, 0.9008, 0.7792, 0.5631,0.2684]	[0.9750, 0.9015, 0.7560, 0.5229, 0.3012]
RAP	[0.9750, 0.9031, 0.8104, 0.6284, 0.2703]	[0.9750, 0.9055, 0.8006, 0.6045,0.2922]	[0.9750, 0.9036, 0.8079, 0.6052, 0.3221]
IAC	[0.9750, 0.8370, 0.4639, 0.0096, 0]	[0.9750, 0.8397, 0.4601, 0.0215, 0]	[0.9750, 0.3104, 0.0005, 0, 0]
IAP	[0.9750, 0.8014, 0.5309, 0.0534, 0]	[0.9750, 0.2646, 0.0076, 0, 0]	[0.9750, 0.2924, 0.0123, 0, 0]

Table 2 The simulation results of ISCN robustness considering disruption propagation for three interdependent patterns.

		ER-ER	ER-BA	BA-BA
RAP	RL	[0.9750, 0.9031, 0.8104, 0.6284, 0.2703]	[0.9750, 0.9055, 0.8006, 0.6045,0.2922]	[0.9750, 0.9036, 0.8079, 0.6052, 0.3221]
	AL	[0.9750, 0.9213, 0.8765, 0.8224, 0.7394]	[0.9750, 0.9150, 0.8759, 0.8208,0.7417]	[0.9750, 0.9218, 0.8846, 0.8329, 0.7519]
	DL	[0.9750, 0.8994, 0.6642, 0.1552. 0.0019]	[0.9750, 0.8977, 0.4244, 0.1224,0.0064]	[0.9750, 0.8994, 0.7064, 0.3355, 0.0485]
IAP	RL	[0.9750, 0.8014, 0.5309, 0.0534, 0]	[0.9750, 0.2646, 0.0076, 0, 0]	[0.9750, 0.2924, 0.0123, 0, 0]
	AL	[0.9750, 0.7617, 0.2967, 0.0009, 0]	[0.9750, 0.2038, 0.0023, 0, 0]	[0.9750, 0.0217, 0, 0, 0]
	DL	[0.9750, 0.8340, 0.5811, 0.0655, 0]	[0.9750, 0.4096, 0.1117, 0.0015, 0]	[0.9750, 0.3459, 0.0649, 0, 0]

Table 1 shows that the robustness of the three network structures under RAP and RAC is BA-BA, BA-ER, and ER-ER in descending order. The robustness of the three network structures under IAP and IAC is ER-ER, BA-ER, and BA-BA in descending order. According to Table 2, the robustness of the three interdependent patterns under IAP is DL, RL, and AL from small to large, while it is the opposite under RAP.

This paper proposes a weighted directed ISCN model. Considering the complexity of the network's internal structure and the uncertainty of the external environment, a disruption propagation model with four failure modes is proposed. The research results show that the BA-BA network with AL coupling pattern under RAC and RAP has the highest resilient network structure. ISCN robustness under edge attack can be discussed in the future.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Nos. 72101116, 71931006).

References

Ivanov, D., Dolgui, A. 2021. A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. Production Planning & Control 32(9), 775-788.

Panetto, H., Iung, B., Ivanov, D., Weichhart, G., Wang, X. 2019. Challenges for the cyber-physical manufacturing enterprises of the future. Annual Reviews in Control 47, 200-213.

Shi, X.Q., Deng, D.S., Long, W., Li, Y.Y., Yu, X.H. 2021. Research on the robustness of interdependent supply networks with tunable parameters. Computers & Industrial Engineering 158, 107431.

Statistical methods in reliability, safety and security