NetSciX2026: International School and Conference on Network Science
February 17^{th}-20^{th}, 2026 - Auckland, New Zealand

Analysis of Dynamic Trade Network Under Attacks

Keywords: Global trade, Dynamic network, Centrality attacks, Network performance

Extended Abstract

In recent years, trade has been an emerging topic across the globe because it significantly contributes to the countries' growth. Over the last decade, global trade has been affected by many unforeseen events. The average trade value growth has experienced a massive decline of 6% in the unit value and 2.6% growth in volume during 2013-15, which is the lowest since 1981 [1]. In 2020, international trade was marred by the largest decline in trade output volume since World War II because of the COVID-19 pandemic [2]. The enterprise export volume has shrunk more than the trade value, which makes it more interesting to consider the study of the enterprise trade volume network. In any trade network, nodes represent the countries; trade between countries indicates links or ties. The study of global trade networks is evolving in various sectors. There are some relevant studies of the trade network, the trade war between the U.S. and China for supply chain semiconductor chip industry [3], characteristics of global semiconductor trade and role of countries in trade [4], trade network of aircraft manufacturing core products supply chain [5], structure and robustness of the international oil and gas trade networks [6, 7], and vulnerability of global arms trade network [8]. However, the above research is limited to the trade industry products under only random or purposeful attacks on the degree or strength of the node, not for both together

This study aims to investigate the enterprise trade networks (unweighted and weighted) under purposeful and random centrality attacks. First, we proposed a numerical simulation to perform centrality attacks on the dynamic enterprise trade networks. Each centrality attack identifies the vulnerable and dominant countries using the centrality measures. After that, this study addresses the measures of trade networks and their performance before, during, and after attacks. This research contributes to the existing literature by utilizing enterprise data to investigate how the structure of enterprise trade networks changes and the contribution of vulnerable nodes to the network under each centrality attack. Then, this study performs a comparative analysis of unweighted and weighted networks under purposeful and random centrality attacks. This study has considered the enterprise trade data from 2012 to 2022, with the participation of 84 to 142 countries and 2336 to 2710 trade ties between them. There are two kinds of participant countries: first, the reference country, from where trade is flowing, and second, the partner country, which is involved in trade with other countries [2].

The research methodology has two stages: simulations and analysis. Numerical simulations are performed to investigate changes in the network metrics of unweighted and weighted networks under the two types of centrality attacks: purposeful and random. Purposeful attacks indicate network scenarios where human intervention exists, like nations facing geopolitical and ideological conflicts, technology failure, and cyber attacks, while random attacks indicate the scenarios in which human intervention is absent, such as natural disasters like climate change and unforeseen events, any pandemic like COVID-19. The purposeful attacks are simulated by sequentially removing the country from the network based on the maximum centrality measures. However, random attacks are simulated by the random elimination of a country from the trade network, no matter whether the node has maximum or minimum centrality for trade volume and trade ties in a network. We computed the five centrality measures, Degree, Closeness, Betweenness, Eigenvector, and PageRank Centrality, which help to investigate the key coun-

tries in trade networks. Moreover, other network properties like Transitivity, which identifies the likelihood that the neighbouring countries are also exporting and importing to each other; Efficiency, which refers to the fast communications and effective utilization of trade volume between the countries; and Density, which indicates the interconnectivity level of countries. The above-discussed properties help to analyze the performance of enterprise networks before and during the centrality attacks.

Results show that World, Germany, Italy, France, UK, and USA have the highest trade volume and are the key country nodes with strong dominance in enterprise networks (unweighted and weighted). Austria, Belgium, Bulgaria, Cyprus, and Czechia have the most exports and imports throughout the years in unweighted networks; those surpass Spain, Germany, France, the UK, and USA, which have the highest trade volume in the network. Moreover, Canada, Israel, Argentina, Switzerland, and other European countries have critical intermediaries in trade ties networks. In contrast, Malta, Cyprus, the World, Israel, Canada, and other European country nodes are considered the most important intermediaries for the trade volume networks. These countries play a critical role as bridges, connecting other countries. Netherlands, Poland, Turkey, Sweden, and Denmark are still emerging countries for economies that play a vital role in the trade networks. The ranking of other countries changes over time due to geopolitical relations and other unforeseen events. The results suggest that enterprise trade networks are vulnerable to purposeful attacks based on node betweenness centrality, highlighting the potential for significant disruption after eliminating key countries. Networks are moderately vulnerable to purposeful attacks based on node strength and closeness centralities. These two attacks highly jeopardise the strength of the network. However, it has been seen that eigenvector centrality increases under the strength attacks, which indicates the domination of countries. The trade networks are less vulnerable to purposeful attacks based on eigenvector and PageRank centrality measures because the network's sustainability is higher against these attacks. Furthermore, trade networks are more stable and sustainable when dealing with random attacks.

This research paper provides valuable insights and suggestions for maintaining trade network stability under unforeseen events. Discussed suggestions might be helpful for policymakers, network planners, and the government to keep a network sustainable and secure, with information on policies for countries and relevant industries. This study does not fully account for current government regulations and changes in trade policy. Future research may build a predictive model to tackle unforeseen events like tariffs, reciprocal tariffs, and other regulations and changes. This will help design a viable network and provide a practical understanding of trade networks to improve trade policies and strategies

References

[1] World Trade Statistical Review. General trends and drivers of world trade in 2015, 2016.

[2] OECD. Balanced trade in services (batis), 2022. Data retrieved from OECD Data Explorer.

[3] Yongli Zhang and Xianduo Zhu. Analysis of the global trade network of the chip industry chain: Does the us-china tech war matter? *Heliyon*, 9(6), 2023.

[4] Long Li, Hua Wang, Zhiyi Li, and Shaodong Hu. Analysis of the structure and robustness of the global semiconductor trade network. *PloS one*, 20(1):e0313162, 2025.

[5] Lanyan Zeng, Hongzhuan Chen, Mingchih Chen, and Xufeng Zhao. Resilience assessment of the aircraft manufacturing core products supply chain: the international trade network perspective. *Annals of Operations Research*, pages 1–39, 2024.

[6] Na Wei, Wen-Jie Xie, and Wei-Xing Zhou. Robustness of the international oil trade network under targeted attacks to economies. *Energy*, 251:123939, 2022.

[7] Xin Sun, Ye Wei, Ying Jin, Wei Song, and Xiaoling Li. The evolution of structural resilience of global oil and gas resources trade network. *Global Networks*, 23(2):391–411, 2023.

[8] Weidong Guo, Debin Du, Tingzhu Li, and Qiang Zhang. The vulnerability of the global arms trade: A network perspective. *Networks and Spatial Economics*, pages 1–20, 2025.