Invulnerability Evaluation of Complex Combat Network Based on Entropy Weight-Analytic Hierarchy Process Method

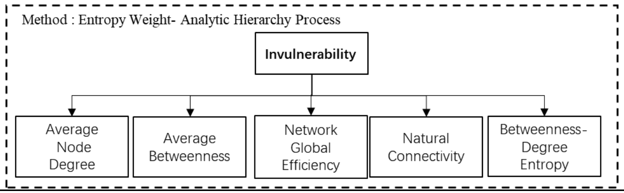
Wenxiu Chen, Hongbo Chen, Chaoxian Wu, Guanjun Wang, Chuankai Zhou

School of Systems Science and Engineering, Sun Yat-Sen University

INTRODUCTION

With the popularization of complex networks, the theoretical significance and value of complex network invulnerability research has become increasingly prominent. At present, the research on invulnerability of complex networks mainly focuses on the network topology and only considers a single feature. Since it's difficult to evaluate the invulnerability of complex combat network in a thoughtful way, this paper proposes a measure of invulnerability for complex combat network based on entropy weight- Analytic Hierarchy Process method. Compared to single indicator, the invulnerability measurement with combined indicators using the proposed method is more effective, and it also provides theoretical suggestions and support for the improvement of the invulnerability of complex combat networks.

NETWORK INVULNERABILITY INDICATORS



Method : Entropy Weight- Analytic Hierarchy Process

Invulnerability

Average Node Degree

Average Betweenness

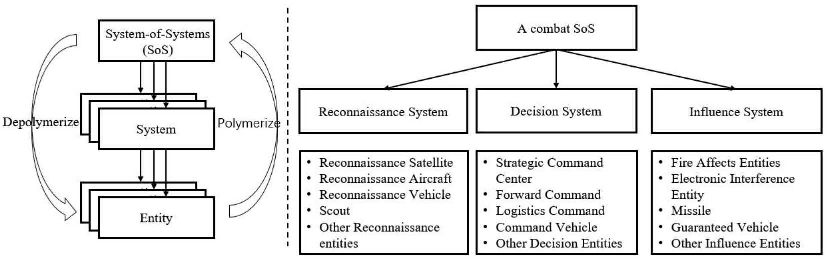
Network Global Efficiency

Natural Connectivity

Betweenness-Degree Entropy

CASE SIMULATION AND ANALYSIS

Assume that there are 7 decision-making nodes, 27 reconnaissance nodes and 27 influence nodes in a complex combat system, so $N = 61$. According to the interaction relationship between entities, the adjacency matrix of the connection relationship between nodes can be constructed, and if there is a connection relationship between two nodes, the value is 1, otherwise it is 0. The built network is shown in fig. 2.



System-of-Systems (SoS)

System

Entity

Depolymerize

Polymerize

A combat SoS

Reconnaissance System

- Reconnaissance Satellite
- Reconnaissance Aircraft
- Reconnaissance Vehicle
- Scout
- Other Reconnaissance entities

Decision System

- Strategic Command Center
- Forward Command
- Logistics Command
- Command Vehicle
- Other Decision Entities

Influence System

- Fire Affects Entities
- Electronic Interference Entity
- Missile
- Guaranteed Vehicle
- Other Influence Entities

Fig. 1. Combat SoS framework

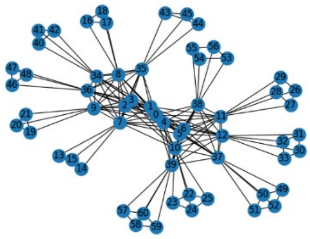


Fig. 2. Complex combat network

It can be found that under the degree-ranked attack, the indicators generally show a downward trend, but the changes between the indicators are quite different. The change of combined invulnerability is within a relatively average and reasonable range of change. In general, the combined invulnerability value can make up for the shortcomings of a single indicator and better reflect the characteristics of network.

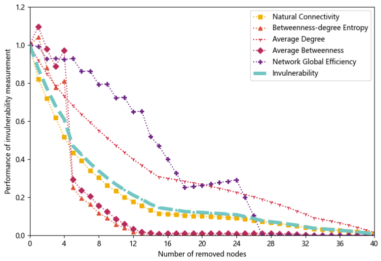


Fig. 3. The performance of invulnerability measure under deliberate attack

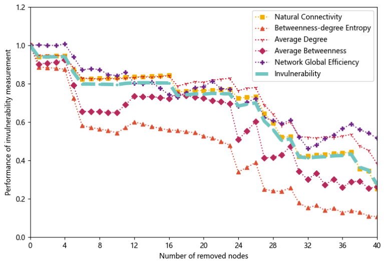


Fig. 4. The performance of invulnerability measure under random attack

When under random attack, the downward trend of all measure is flatter. Compared to degree-ranked attack, random attacks have less destructive impact on the network, the invulnerability value is still in an average range.

CONCLUSION

This paper analyzes invulnerability using all six measures, the simulations result shows that the proposed method is effective for the indicator evaluation and measure of combined invulnerability of complex combat networks. The combined invulnerability provides theoretical suggestions and support for the improvement of invulnerability. In addition, the proposed method can also be extended to application, when the number of invulnerability indicators increases, the proposed method can still be used to establish a multi-hierarchical model for indicators evaluation, and then calculate the combined invulnerability in different attack modes. Meanwhile, the proposed method can also be used to comprehensively evaluate invulnerability of different structures and select a network with best performance.