**Advances in Reliability,
Safety and Security**

ESREL 2024
Collection of Extended Abstracts

A Node Protection Method For Improving The Resilience Of Combat System Under Continuous Attack

Jiuyao Jiang, Hongqian Wu, Renjie Xu, Hang Yang, Yihao Zhang, Jichao Li

College of Systems Engineering, National University of Defense Technology, Changsha, China

Keywords: combat system, resilience assessment, improve resilience, continuous attack, node protection

---

Resilience is a measure of the ability of a system to adapt to changes in conditions, withstand disturbances and recover quickly from them. Improving system resilience through node protection is of great value for keenly recognizing the uncertainty of the battlefield environment, bearing the enemy's precise strikes, and building a combat system that adapts to system operations and fulfills mission requirements. However, most of the current research focuses on the identification of key nodes, and there are fewer studies related to how key nodes are specifically protected. Therefore, this paper investigates how to assign protection strength to different nodes before battle based on resilience.

Firstly, in view of the complex functions of the combat system and equipment and the diverse interactive relationships, the static network structure is modeled based on the concept of OODA loop. For the characteristics of confrontation and dynamic evolution in the combat process, its dynamic simulation is based on NetLogo to describe the combat process.

Secondly, traditional resilience assessments are usually directed at individual perturbations. In contrast, the operational process is in a dramatically changing environment where loss of performance and recovery may occur simultaneously and cannot be clearly delineated into phases. In this paper, a resilience assessment method is constructed for continuous attacks:

$$R = \frac{\int_{t_1}^{t_3} E(t)dt}{E(t_1)*(t_3 - t_1)}, \tag{1}$$

where $E(t)$ is the performance of the system, $E(t_1)$ is the initial performance before the attack, t_3 is the end moment of combat, and t_1 is the beginning moment of combat. The calculation of $E(t)$ improves on the traditional ADC approach (proposed by the Weapon System Effectiveness Industry Advisory Committee, combines the three major elements of availability, dependability and capacity to realize the effectiveness assessment) by integrating multiple aspects of the combat system's structure, combat capabilities, and effects:

$$E_t = \sum_{t=1}^{L} \frac{A_l * D_l * C_l}{n_l\,!}\,. \tag{2}$$

Thirdly, considering the node protection strength and cost resource constraints, the genetic algorithm is used to solve the optimal node protection strategy, the optimization model is shown below:

$$\max R$$
$$\begin{cases} In_i = 0,1,2 \\ \sum_{i=1}^{N} In_i \le C^* \end{cases} \tag{3}$$

Finally, the proposed method is demonstrated and verified with case application. The resilience of the combat system under the optimal node protection policy is first solved. Next, the characteristics of the protected nodes are analyzed in terms of degree, betweenness centrality, and deployment location, respectively, as shown in Figure 1. Finally, a node protection strategy is constructed based on the node importance index and the contribution rate index of the classical complex network, and compared with the resilience value of the strategy solved in this paper, as shown in Figure 2.

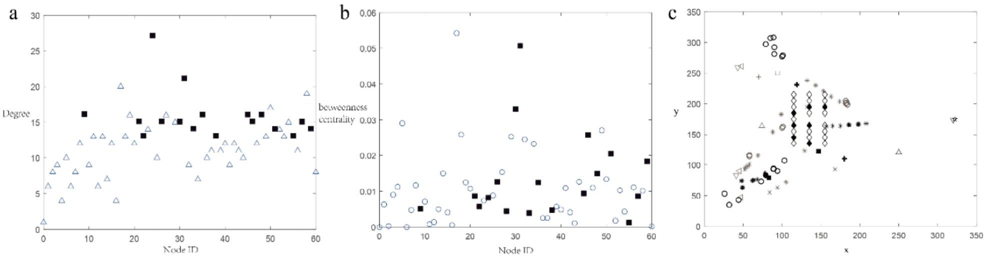

Fig. 1. (a) the difference between equipment degrees; (b) the difference of betweenness centrality between equipment; (c) deployment location of the protected equipment.

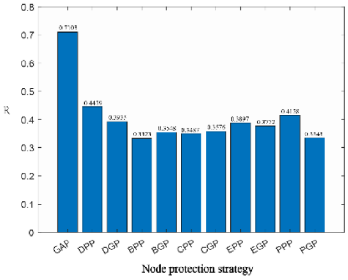

Fig. 2. system resilience under different node protection strategies.

In conclusion, the protection strategy of identifying key nodes directly by relying on the network structure is not fully applicable to combat scenarios, because it ignores the emergence of the network. In addition, the deployment location of the device also has a large impact on the node protection policy.

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China under Grants 72001209, 72071206 and 71690233.

References

Aaron, B. 2005. Boyd‘s OODA loop and the infantry company commander. Military Review 18(1), 17-19.

Levitin, G., Xing, L., Xiang, Y. 2021. Optimizing preventive replacement schedule in standby systems with time consuming task transfers. Reliability Engineering & System Safety 205, 107227.

Liu, K., Zhai, C., Dong, Y. 2021. Optimal restoration schedules of transportation network considering resilience. Structure and Infrastructure Engineering 17(8), 1141-1154.

Liu, X.M., Li, D.Q., Ma, M.Q., et al. 2022. Network resilience, Physics Reports 971, 1-108.

Ma, L.J., Li, J.Q., Lin, Q.Z., et al. 2021. Enhancing robustness and resilience of multiplex networks against node-community cascading failures[J], IEEE Transactions on Systems, Man, and Cybernetics: Systems 52(6), 3808-3821.

Oriol, A., Marco, G., Manlio, D.D., et al. 2024. Robustness and resilience of complex networks, Nature Reviews Physics 6, 114-131.

Xiao, F., Li, J., Wei, B. 2022. Cascading failure analysis and critical node identification in complex networks. Physica A: Statistical Mechanics and its Applications, 127117.