Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

Task Oriented Resilience Assessment Framework For System Of Systems

Xueming Xu, Renjie Xu, Jiahao Liu, Yihao Zhang, Hongqian Wu, Jichao Li, Haiyue Yu, Jiang Jiang[a]

National University of Defense Technology, Chang Sha, China

Keywords: system-of-systems (SoS), resilience assessment, mitigation, task-oriented

System-of-systems (SoS) are inevitably subject to disturbances during task execution, and resilience is a key factor for SoS damage and recovery. System-of-systems resilience (SoSR) assessment has important value for effectively completing tasks and optimizing SoS architecture. However, identifying the most resilient SoS among different ones for the same task is a basic but challenging question. This paper proposes a task-oriented SoSR assessment framework to identify the most resilient SoS. First, we use a heterogeneous information network and meta-path to describe a SoS network architecture composed of different subsystems and the SoS performance model was developed, based on node and link quality. Based on this model, a system-of-system resilience metric (SoSRM) is proposed to describe the ability of the SoS to recover quickly dealing with disruption. Then, we extend further this metric to consider the impact of mitigation measures that exist in practical scenarios. Finally, we demonstrate the feasibility and effectiveness of this framework through a combat SoS case study, which yields useful insights for identifying and designing a more resilient SoS that can successfully accomplish the task.

A SoS refers to a collection of independent and self-contained systems that are interconnected and operate collaboratively to achieve a common objectives or tasks. Resilience refers to the SoS ability to recover its desired level of performance after a disturbance event. This study defines SoSR as: System-of-Systems resilience. Under a specific task objective, negative impacts resulting from disturbance events (node and link removal) are minimized through recovery measures to complete the task as much as possible.

Describing the internal structural composition of a SoS through a network model is a widely recognized approach, we provide the following definitions for heterogeneous information networks and meta-path as Figure 1.

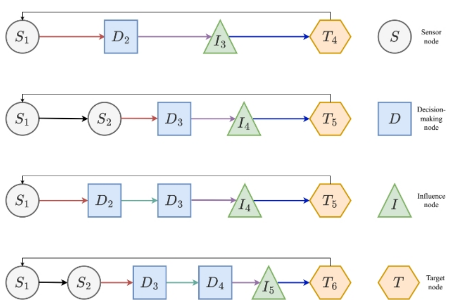

Fig. 1. Schematic of different types of meta-operation loop

The performance of the meta-operation loop is, then, calculated using (1):

$$C_{mp} = \prod_{v_k \in mp} c(v_k) \tag{1}$$

The probability that a meta-operation loop is executable is given by (2)

$$P_{mp} = \prod_{i=1}^{k} p(L_i) \tag{2}$$

The SoS performance model is proposed by considering both node quality and link quality in the temporal dimension, as shown in (3).

$$P(T) = \sum_{mp \in A(MP)} C_{mp}(T) \times p_{mp}(T) \tag{3}$$

Therefore, considering the above, a system resilience index that combines "resilience loss" and "prediction triangle," as represented in (4)

$$\mathfrak{R} = \frac{\int_{T_0}^{T_0+T_u} f(x)dT}{T_u \times f_{max}} \tag{4}$$

The same holds for the links in the SoS. Therefore, the SoSRM considering mitigation is given by

$$\mathfrak{R} = \frac{1}{n+m}\left(\sum_{disruption=1}^{n} \frac{\int_{T_0}^{T_0+max\left\{t_i^{SoS_b}, t_j^{SoS_b}\right\}}\left[\sum_{mp \in A(MP)} C_{mp_{mit}}(T) \times p_{mp_{mit}}(T)\right]dT}{max\left\{t_i^{SoS_b}, t_j^{SoS_b}\right\} \times P_{max\left\{p_0^{SoS_b}\right\}}} + \sum_{disruption=1}^{m} \frac{\int_{T_0}^{T_0+max\left\{t_i^{SoS_b}, t_j^{SoS_b}\right\}}\left[\sum_{mp \in A(MP)} C_{mp_{mit}}(T) \times p_{mp_{mit}}(T)\right]dT}{max\left\{t_i^{SoS_b}, t_j^{SoS_b}\right\} \times P_{max\left\{p_0^{SoS_b}\right\}}}\right) \tag{5}$$

Resilience reflects the comprehensive performance of a SoS and has important value for effectively completing tasks and optimizing the architecture of the SoS. Therefore, comparing the resilience of different SoSs is a challenging job. To address this issue, we propose an integrated task-oriented SoSR assessment framework to identify the most resilient SoS, which has the following merits:

- considering both the nodes and links of the SoS, rather than simply considering one of them, making it more applicable to actual SoS operation;
- combining network topology parameters and network performance parameters as well as considering mitigation for the first time to analyze the SoSR;
- this framework has a certain universality and can adjust the input performance function *f*(*x*), weight coefficients for nodes and links to make it applicable to resilience assessments in fields such as biological SoS and infrastructure SoS.

References

Najjar, W., Gaudiot, J L. 1990. Network Resilience: A Measure of Network Fault Tolerance. IEEE Transactions on Computers 39(2), 174-181.

Moutsinas, G., Guo, W. 2020. Node-Level Resilience Loss in Dynamic Complex Networks. Scientific Reports 10(1), No. 3599.

Cardinale, I., Reggiani, A., Scazzieri, R. 2022. Vulnerability, Resilience and Complex Structures: A connectivity perspective. Networks and Spatial Economics. 22(3), 409-413.

Sun, Q., Li, H., Wang, Y., et al. 2022. Multi-swarm-based cooperative reconfiguration model for resilient unmanned weapon SoS. Reliability Engineering and System Safety 222, No. 108426.

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

Lei, C., Lu, L., Ouyang, Y. 2022. System of Systems Model for Planning Electric Vehicle ChargingInfrastructure in Intercity Transportation Networks Under Emission Consideration. IEEE Transactions on Intelligent Transportation Systems 23(7), 8103-8113.

Gianetto, D.A., Heydari, B. 2015. Catalysts of cooperation in system of systems: The role of diversity and network structure. IEEE Systems Journal 9(1), 303-311.

Xing, P., Huixiong, W., Yanjing, Y., et al. 2019. Resilience based importance measure analysis for SoS. Journal of Systems Engineering and Electronics 30(5), 920-930.

Simulation based methods for reliability, safety and security