Journal of Systems Engineering and Electronics
Vol. 30, No. 5, October 2019, pp.920 – 930

Resilience based importance measure analysis for SoS

PAN Xing[1,*], WANG Huixiong[1], YANG Yanjing[1,2], and ZHANG Guozhong[3]

1. School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China;
2. China Railway Signal and Communication Corporation, Beijing 100070, China;
3. Institute of Systems Engineering, China State Shipbuilding Corporation, Beijing 100036, China

Abstract: In a system of systems (SoS), resilience is an important factor in maintaining the functionality, stability, and enhancing the operation effectiveness. From the perspective of resilience, this paper studies the importance of the SoS, and a resilience-based importance measure analysis is conducted to provide suggestions in the design and optimization of the structure of the SoS. In this paper, the components of the SoS are simplified as four kinds of network nodes: sensor, decision point, influencer, and target. In this networked SoS, the number of operation loops is used as the performance indicator, and an approximate algorithm, which is based on eigenvalue of the adjacency matrix, is proposed to calculate the number of operation loops. In order to understand the performance change of the SoS during the attack and defense process in the operations, an integral resilience model is proposed to depict the resilience of the SoS. From different perspectives of enhancing the resilience, different measures, parameters and the corresponding algorithms for the resilience importance of components are proposed. Finally, a case study on an SoS is conducted to verify the validity of the network modelling and the resilience-based importance analysis method.

Keywords: system of systems (SoS), resilience, network modelling, importance measure analysis, operation loop.

DOI: 10.21629/JSEE.2019.05.10

1. Introduction

In recent years, resilience has aroused interest of more and more researchers from different domains, especially the complex systems [1] and infrastructures [2]. The term ‘resilience’ originates from Greek ‘resilere’, which means ‘bounce back’ [3]. In 1970s, Holling [4] first defined ‘resilience’ in the study of ecology as the ability of an ecosystem to recover to the original balanced status after environmental change or human activities. Since then, the term ‘resilience’ is used to depict the ability that a system or entity can restore its performance or function after a disruptive event, and this definition is already used in different subjects, e.g., ecology [4,5], sociology [6,7], economics [8,9], and engineering [10,11].

In engineering discipline, the resilience of a system is defined as the ability that a system can resist collapse and recover its performance characteristic after a disruptive event, e.g., system malfunction, being attacked [12]. The resilience of a system is strongly related to reliability (the ability to perform the intended function), robustness (the ability to resist malfunctions or external attacks) and recoverability (the ability to recover from malfunctions or external attacks), and thus affects the performance of the system. In system of systems (SoS) theory, resilience is the ability that an SoS restores its weakened performance with its characteristics and structure. For an SoS consisting of several systems, resilience is an important guarantee that a system can remain stable and perform its expected functions. Among the member systems of the SoS, each component has different degrees of importance, which requires a resilience importance measure (RIM) for the SoS, and hence provides a direction for the design and optimization of SoS.

In the research on design and optimization of SoS, the abstraction of the SoS into a network is commonly used in SoS modelling. The last decades have witnessed intensive studies on the network components and the connection among them, especially in the research of network centric warfare (NCW). In NCW, the evolution of an SoS is simplified as the process of decision making and execution. Specifically, the entities of ally are divided into three categories: sensors, decision points, and influencers. Meanwhile, considering the antagonism in systematic operation, the entities of the opponent are abstracted into targets [13,14]. As a matter of fact, the above categorization is constructed on the basis that the operation of an SoS can be seen as a process of decision and action. Therefore, in other domains, e.g., critical infrastructure, transportation system, the components are also abstracted into the above

Manuscript received March 06, 2019.
*Corresponding author.
This work was supported by the National Natural Science Foundation of China (71571004).

four categories. In this study, we follow the above categorization, and use the above four categories of components in the modelling and research on resilience and importance measure analysis.

When analyzing the resilience importance of an SoS, it is a basic method to build a resilience model that analyzes the disruptive events and the influence. As a matter of fact, all systems will encounter different kinds of interference in life circle, thus preventive or resistant strategies are used to guarantee the operational capacity and resistibility against the interference, e.g., intentional attacks, natural disasters, human accidents, and malfunctions. Previous studies have offered insight into these strategies in different types of SoS, e.g., protecting critical system elements [15], operating in degraded mode [16], providing redundancy [17], deploying false targets [18], and launching preventive strikes [19]. The abovementioned strategies improve the survivability of the SoS by different approaches, while the mechanisms of these strategies can be intelligibly subdivided into three categories: predicting the adverse event, deferring its occurrence, and improving the reliability of the SoS [20]. Take the false target deployment as an example, when an approaching threat is detected (predicted), the system will deploy a false target so that the adverse event is excluded (deferred). However, it is sometimes costly and unrealistic to prevent or evade the adverse event; therefore, we hope that the SoS can quickly restore its performance from the disturbing event. Resilience, therein, is a measure to depict such ability of an SoS. Many devastating events have proved the significance of resilience in an SoS, because it is the key factor to diminish the impact brought by the adverse events [21,22]. Generally, there are three characteristics that build up the resilience of the SoS: independence of component functions, redundancy of inter-systematic functions, and self-reconstructive or evolutional functions [23]. Among the above three characteristics, resilience is based on the redundancy of inter-systematic functions, while resilience is accomplished by the self-reconstructive and evolutional functions. In an SoS, when a subsystem failure causes malfunctions, the performance of the SoS can be recovered by recombining the other components. In a word, there are many factors that enable the SoS to resist and restore from adverse events and performance decrease, including redundancy, and reliable or effective recovery measures. This manuscript will focus on the disruptive events, divide the process of performance change into different phases, and study the factors that affect the resilience of SoS.

Analyzing the resilience importance of an SoS is one aspect of importance analysis. Another important issue in the reliability and risk analysis of complex system is the recognition of uncertainty. When analyzing the uncertainty, the measure of importance is to recognize the uncertain component parameters that pose the biggest impact on the overall performance with the help of sensitivity analysis [24]. Importance measurement is an efficient tool to recognize the important input parameters and regulate the uncertainty of system output. Thus, analysts can depict the most influential or critical risk context by importance measure analysis, and, therefore, optimize the design of system and improve the logistic strategy.

In order to determine the importance of system components, previous studies proposed a variety of indexes measuring components importance. The most commonly used indices are Birnbaum measure, failure critical index (FCI), the Fussell-Vesely measure, risk achievement worth (RAW), risk reduction worth (RRW), etc. [25]. In addition, there are derivatives of parameters in system risk, such as the likelihood ratio gradient [26]. Moreover, research on the uncertain importance measure (UIM) method of parameters combined with the probabilistic risk assessment (PRA) method in reliability models is a priority in the field of reliability and safety analysis [27 – 30]. Meanwhile, other UIM indices are researched from different prospectives in reliability, such as time-independent [31,32] or cost-based importance measure [33,34], and logistic support process [35].

The literature above indicates that it is important to conduct importance measure analysis on the system nodes and analyze the design and optimization of the system from the perspective of resilience [36]. Previous studies on importance measure analysis of system or SoS focused on the influence of the accession of a new SoS member, while neglecting the influence of resilience. Focusing on the improvement of resilience, this article proposes a modeling method of SoS network, in which the observe – orient – decide – act (OODA) loop is used to quantify the performance of the system, and the trend of performance change is studied to build the resilience model. Furthermore, an analytical method is proposed to measure the resilience and provide different resilience-based importance indices.

2. OODA-based resilience model

2.1 Two types of resilience model

There are two different types of SoS resilience: time-irrelevant model (i.e., quotient resilience model), and time-relevant model (i.e., integral model) [37]. Fig. 1 illustrates the trends of SoS performance under the two resilience models, where $\varphi(t)$ represents the SoS performance at time t.

(i) Quotient resilience model

In the resilience process, the occurrence of a disruptive event e^j will decrease the performance of SoS, while re-

covery measure can restore the performance. In the quotient resilience model, as shown in Fig. 1(a), the resilience of the SoS is defined as the ratio of the restored performance to the lost performance. Equation (1) provides a concise expression of SoS resilience:

$$R(t) = \varphi_{\text{restored}}(t)/\varphi_{\text{lost}}(t_d) \tag{1}$$

where $R(t)$ represents the resilience of the SoS, $\varphi_{\text{restored}}(t)$ represents the restored performance at time t, i.e., the difference between performance at time t under recovery strategies and the minimum performance under the disruptive event e^j, and $\varphi_{\text{lost}}(t)$ represents the maximum performance loss, i.e., difference between original performance before e^j and minimum performance under e^j.

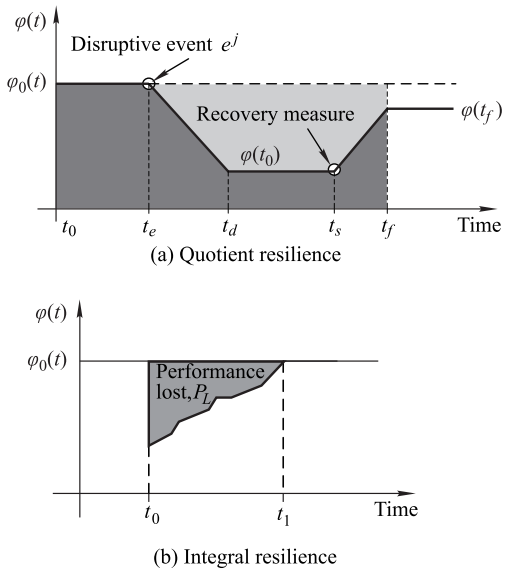

Fig. 1 Trends of SoS performance in the disturbing event under two resilience models

Equation (1) exhibits the ability that an SoS can bounce back to the normal performance after a disruptive event. If the SoS can restore its performance completely, i.e., $\varphi_{\text{restored}}(t) = \varphi_{\text{lost}}(t_d)$, we say the SoS has complete resilience; if the SoS does not restore at all, i.e., $\text{Recovery}(t) = 0$, we say the SoS has no resilience. In this model, resilience is defined as the ratio of restored performance to the lost, thus it is called the quotient resilience model.

In the quotient resilience model, when performance indicator $\varphi(t)$, time of disruptive event e^j, start time of recovery t_s, and end time of recovery t_f are determined, the SoS resilience, equivalent to $R(t)$ in (1), can be represented as

$$R_Q(t|e^j) = \frac{\varphi(t|e^j) - \varphi(t_d|e^j)}{\varphi(t_0) - \varphi(t_d|e^j)}, \quad t > t_s \tag{2}$$

where $R_Q(t|e^j)$ represents the quotient resilience of the SoS at time t after the disruptive event e^j, $\varphi(t|e^j)$ represents the SoS performance at time t, and $\varphi(t_d|e^j)$ represents the SoS performance after the disruptive event e^j.

The denominator in (2) represents the reduced performance of the SoS, and less reduced performance means better SoS resilience; the numerator represents the performance recovered by the recovery measure. Therefore, the denominator and numerator respectively represent the influence of the disruptive event and the recovery measure.

(ii) Integral resilience model

The quotient resilience model can only depict the resilience of the SoS at a certain time, while neglecting the overall effect of SoS resilience during the whole attack-recovery process. Integral resilience model, however, measures the SoS resilience in the process by calculating the accumulated effect of performance over time. Fig. 1(b) illustrates the triangular integral resilience model, which evolves from Fig. 1(a). The resilience triangle, which is the dash area in Fig. 1(b), illustrates the performance loss after the disruptive event. In the integral model, the performance lost in the resilience process can be mathematically represented as

$$R_L = \int_{t_0}^{t_1} [100 - Q(t)]\mathrm{d}t \tag{3}$$

where R_L represents the performance lost in the resilience process, and $Q(t) = 100\varphi(t)/\varphi(t_0)$ represents the quality of SoS performance. When there is no adverse event, $Q(t)$ is assigned to be 100.

In the integral model, a smaller resilience triangle indicates better SoS resilience. To enhance the resilience, the resilience triangle, or the value of R_L should be small. For example, increasing the performance and reducing the time cost in the recovery will result in higher resilience.

In the integral resilience model, the retention amount of performance, instead of the lost amount of performance, is used to depict the SoS resilience. This can be mathematically represented as

$$R_I(t|e^j) = \frac{\int_{t_0}^{t} \varphi(u|e^j)\mathrm{d}u}{\int_{t_0}^{t} \varphi(t_0)\mathrm{d}u}, \quad t > t_s \tag{4}$$

where $R_I(t|e^j)$ represents the integral resilience at time t after the disruptive event e^j, $\varphi(t_0)$ represents the expected performance with no disruptive event, and $\varphi(u|e^j)$ is the SoS performance at time t.

The numerator in (4) is the integral of SoS performance to time during the disruptive event, while the denominator represents the integral of expected SoS performance with

no disruption. The area under the performance curve indicates the accumulated effect of SoS performance over the time.

2.2 Performance measurement of SoS

2.2.1 OODA loop of SoS

According to the above resilience model, a performance indicator $\varphi(t)$ must be defined in the analysis of SoS resilience. Previous studies on the network-based SoS model also defines various measures of network performance. Network efficiency and largest connected component (LCC) are two common performance measurements in the study of complex networks. To some extent, these traditional measurements reflect the performance of the SoS, while they are limited to some certain aspects of the performance [38]. For example, network efficiency focuses more on the ability of the network to transmit information, while LCC neglects the functionality of other connected groups of nodes. In NCW, the operation loop provides a description for the operational process of a weapon SoS by extracting the decision and operation loop in the operational process. More operation loops indicate more alternatives in decision-making, thus will provide higher fighting capacity. Therefore, the number of the operation loop is a comprehensive and popular indicator to measure the performance of an operational SoS.

The OODA loop is a decision cycle known as the Boyd cycle, first proposed by U. S. Air Force Maj. John Boyd [39]. Although the OODA loop originates from the combat process, this theory has been widely used in military, business, public administration, etc., especially in military command and control. In OODA theory, the military operation is divided into four basic activities: observe, orient, decide, and act, and an operation loop is a closed-loop consisting of the four activities: detect the sensor (S) and trace the target (T), and transmit the target information to the decision point (D) [40]; the decision point makes decision and issues the order after analyzing the target information and the operational situation; influencer (I) takes action, after which sensor (S) will detect the target again to affirm the attack; finally, the decision point will decide whether a second action is needed. In modern military theory, an operation is a cyclic process consisting of observation, judgement, and action. Owing to the difference between the reliability and capacity of each component, the performance of different operation loops is not the same, however, a network with more operation loops is able to process more information and launch more strikes in operations, and have more alternatives when some of the SoS components fail. Therefore, we propose that the number of operation loops is suitable for the measurement of the SoS performance.

As a description of decision and action, the operation loop is also significant in complex network: nodes in a network can be classified as four types: sensor, decision point, influencer and target. When these four types of nodes constitute a loop, the corresponding decision and action are finished. Further, the number of OODA loops illustrates the operational efficiency of the network. Therefore, in this study, we take the number of OODA loops as the performance indicator $\varphi(t)$ in the resilience analysis.

2.2.2 OODA loop approximate algorithm

In this study, the number of operation loops is calculated by an approximate algorithm based on eigenvalue of the network adjacency matrix. When the scale of the SoS is very large, the connectivity of the network will be complicated, thus in this study, the number of closed loops is used as an approximation of the number of closed operation loops, i.e., ignoring the sequence of nodes in an operation loop.

An SoS can be simplified as a heterogeneous network consisting of specific components and connection, including sensors, decision points, influencers, and targets. Assume an operational network with N entities, the topology, i.e., connections between entities, can be explicitly represented as an adjacency matrix $\boldsymbol{A} = [a_{ij}]_{N\times N}$, where

$$a_{ij} = \begin{cases} 1, & \text{node } i \text{ is connected to node } j \\ 0, & \text{node } i \text{ is not connected to node } j \end{cases}. \quad (5)$$

We use a simplified SoS example to illustrate the calculation of operation loops. The SoS consists of decision node D_1, sensor nodes S_1 and S_2, influencer nodes I_1 and I_2, and target node T_1. This operational network can be represented as matrix $\boldsymbol{A}$ in Fig. 2. The number of operation loops can be estimated with matrix $\boldsymbol{A}$.

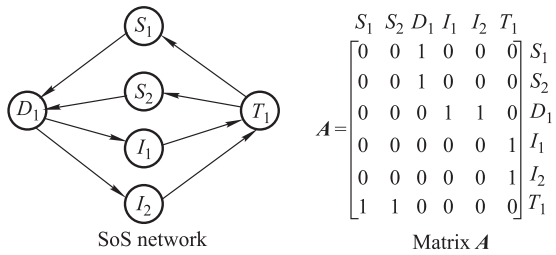

Fig. 2 Simple example of SoS and its corresponding adjacency matrix

In Fig. 2, it is evident that the number of loops that pass through D_1 with the length of 4 is 4. While in large-scale SoS networks, the number of operation loops is large. Since the operation loop is a special case of the closed loop, it is assumed that a large number of closed loops indicates a large number of operation loops. Therefore, the number of closed loops can be used as an estimation to the number of operation loops.

Let n_i^k represent the number of closed loops that pass through node v_i with the length of k, i.e., the number of closed paths that start at v_i and end at v_i with k steps. In matrix $\boldsymbol{A}^k$, the matrix multiplication of $\boldsymbol{A}$s, each element $a_{ij}^{(k)}$ equals the number of paths from node i to node j with k steps, therefore the elements on the primary diagonal in matrix $\boldsymbol{A}^k$ equals the closed loops that pass through v_i with the length of k, i.e., $n_i^k = a_{ii}^{(k)}$.

For the network in Fig. 2, we obtain

$$\boldsymbol{A}^3 = \begin{array}{c} \begin{matrix} S_1 & S_2 & D_1 & I_1 & I_2 & T_1 \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 2 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 \end{bmatrix} \end{array} \begin{matrix} S_1 \\ S_2 \\ D_1 \\ I_1 \\ I_2 \\ T_1 \end{matrix}$$

$$\boldsymbol{A}^4 = \begin{array}{c} \begin{matrix} S_1 & S_2 & D_1 & I_1 & I_2 & T_1 \end{matrix} \\ \begin{bmatrix} 2 & 2 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{bmatrix} \end{array} \begin{matrix} S_1 \\ S_2 \\ D_1 \\ I_1 \\ I_2 \\ T_1 \end{matrix} .$$

The number of operation loops with the length of k can be calculated [41] with

$$S_k = \sum_{i=1}^{N} a_{ii}^k = \mathrm{trace}(\boldsymbol{A}^k) = \sum_{i=1}^{N} \lambda_i^k \tag{6}$$

where λ_1^k, λ_2^k, ..., λ_N^k represent the eigenvalues of matrix $\boldsymbol{A}^k$.

Therefore, the number of all operation loops in the SoS can be calculated by summarizing S_k

$$S = \sum_{k=1}^{\infty} S_k = \sum_{k=1}^{\infty} \sum_{i=1}^{N} \lambda_i^k. \tag{7}$$

To estimate the number of operation loops, we adopt the approximate algorithm proposed by Tan et al. [42], in which a weighted sum $c_k = 1/k!$ is used to eliminate the recalculation of loops with multiplied lengths as well as the influence of the length of the loops. Mathematically,

$$S' = \sum_{k=1}^{\infty} c_k S_k = \sum_{k=1}^{\infty} \sum_{i=1}^{N} \frac{\lambda_i^k}{k!} = \sum_{i=1}^{N} \mathrm{e}^{\lambda_i}. \tag{8}$$

For a large-scale network, the value of S' is very large. Therefore, we rescale S' [42] as

$$\overline{S} = \frac{1}{N} \sum_{i=1}^{N} \mathrm{e}^{\lambda_i}. \tag{9}$$

The above equation provides an approximate method with simple parameters in the matrix, while depicting an important aspect of the performance of the SoS network. Equation (9) is not the exact number of operation loops, though, the weighted sum of closed loops considers the structural properties of the SoS, and hence is more preferable in computational efficiency. Therefore, in this study, $\overline{S}$ is used as a comprehensive indicator to measure the performance of an operational SoS.

2.3 Resilience using OODA loop

In this study, the integral resilience model is used to measure the resilience of the SoS. Considering the number of operation loops during the degeneration and recover process, the resilience of the SoS under a certain disruptive event e^j can be represented as

$$R((t_0, t)|e^j) = \frac{\int_{t_0}^{t} \overline{S}(t)\mathrm{d}(t)}{\int_{t_0}^{t} \overline{S}(t_0)\mathrm{d}(t)} \tag{10}$$

where $R((t_0, t)|e^j)$ represents the integral resilience of the SoS at time t after the disruptive event e^j. $\overline{S}(t_0)$ represents the number of operation loops with no disruptive event. $\overline{S}(t)$ represents the number of operation loops at time t during the mission.

Integral resilience measures the accumulated performance of the time, and the ability of the SoS to perform the expected functions in a time period. In order to measure the accumulative effect of the SoS performance, the resilience at the end of the mission is measured to depict the resilience of the SoS.

Therefore, on the basis of (10), we propose a definition of overall resilience R_h: the ability of an SoS to maintain its expected functionality after a disruptive event e^j. It can be measured by integral resilience at time interval $[t_0, t_m]$:

$$R_h = R((t_0, t_m)|e^j) = \frac{\int_{t_0}^{t_m} \overline{S}(t)\mathrm{d}(t)}{\int_{t_0}^{t_m} \overline{S}(t_0)\mathrm{d}(t)} \tag{11}$$

where $\overline{S}(t_0)$ represents the number of operation loops after the disruptive event e^j, and $\overline{S}(t)$ represents the number of operation loops at time t under the mission circumstance.

3. Importance measure analysis

As introduced above, the mechanisms of strategies to improve the survivability of the system can be divided into three categories: predicting the adverse event, deferring its occurrence, and improving the reliability of the SoS. The three categories actually represent the strategies conducted

in three phases: before, in, and after the disruptive event. Accordingly, in analysis of importance of the SoS components, the measurement changes along with the phase of the strategies. In this section, the importance measures in three phases are introduced respectively.

3.1 Pre-event importance measure

Pre-event importance measure is to analyze the impact of addition of a node before the occurrence of the disruptive event. As shown in Fig. 3, the two curves respectively represent the trend of SoS performance in the resilience process with and without the addition of a new node n_i. The solid line represents the original trend of SoS performance in the resilience process $\overline{S}(t)$, while the dashed line represents the trend after the addition of a new node $\overline{S}_{+n_i}(t)$. When the start time and end time of event $e^j(t_e,\ t_d)$, as well as the start time and end time of recovery measure $(t_s,\ t_f)$ are determined, we obtain the overall resilience of the SoS at time t_m and the pre-event importance indicator.

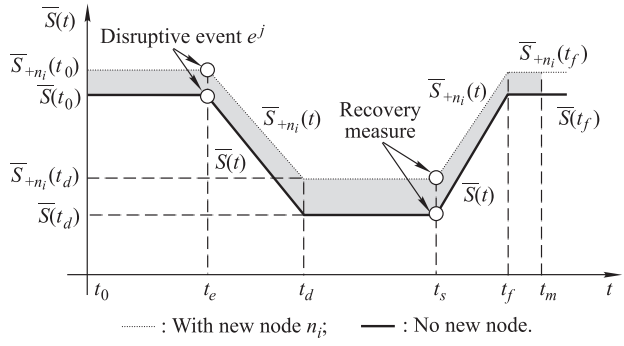

Fig. 3 Trends of SoS performance in pre-event importance measure

Therefore, pre-event RIM can be mathematically represented as

$$C_{+n_i} = \frac{R_{h\_+n_i} - R_h}{R_h} \tag{12}$$

where $R_{n\_+n_i}$ represents the overall resilience towards the disruptive event with new node n_i; R_h represents the situation without new node n_i. Combining (11) and (12), we obtain

$$C_{+n_i} = \frac{R_{h\_+n_i} - R_h}{R_h} = \frac{\int_{t_0}^{t_m} \overline{S}_{+n_i}(t)\mathrm{d}(t)}{\int_{t_0}^{t_m} \overline{S}(t)\mathrm{d}(t)} \cdot \frac{\overline{S}(t_0)}{\overline{S}_{+n_i}(t_0)} - 1. \tag{13}$$

3.2 Middle-event importance measure

Middle-event importance measure is to analyze the impact that a new node is added to the network during the disruptive event. As shown in Fig. 4, the three curves respectively represent the SoS performance after event e^j in three different states of new node n_i: the normal status, no node failure, and no failure on node n_i. The corresponding symbol of the performance under three states is marked in the figure. Note that when failure occurs in fewer nodes, the recovery time will decrease, i.e., $t_f^{N\_n_i} < t_f$.

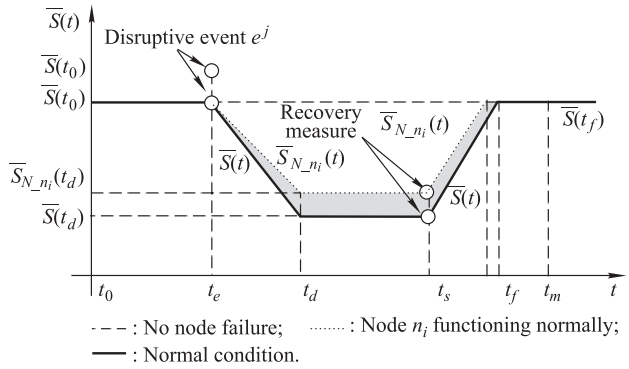

Fig. 4 Trends of SoS performance in middle-event importance measure

According to the definition of integral resilience, the dash area in Fig. 4 represents the accumulative effect of the SoS performance when node n_i does not fail. Given the ending time of recovery measure $t_f^{N\_n_i}$, the overall resilience of the SoS at time t_m can be calculated to measure the middle-event importance.

Therefore, middle-event RIM can be mathematically represented as

$$C_{N\_n_i} = \frac{R_{h\_N\_n_i} - R_h}{R_h} \tag{14}$$

where $R_{h\_N\_n_i}$ represents the overall resilience when the new node n_i does not fail; R_h represents the normal situation. Combining (11) and (14), we obtain

$$C_{N\_n_i} = \frac{R_{h\_N\_n_i} - R_h}{R_h} = \int_{t_0}^{t_m} \frac{\bar{S}_{N\_n_i}(t) - \bar{S}(t)}{\bar{S}(t)}\mathrm{d}(t). \tag{15}$$

3.3 Post-event importance measure

Post-event importance measure is to analyze the impact that a set of failure nodes are recovered after the disruptive event. As shown in Fig. 5, the three curves respectively represent the SoS performance after event e^j in three different situations of recovery: recover all nodes, recover node n_i only; and no recovery. The corresponding symbol of the performance under three situations is marked in the figure. Note that $t_f^{r\_n_i} < t_f$.

According to the definition of integral resilience, the dash area in Fig. 5 represents the accumulative effect of the SoS performance when node n_i is recovered.

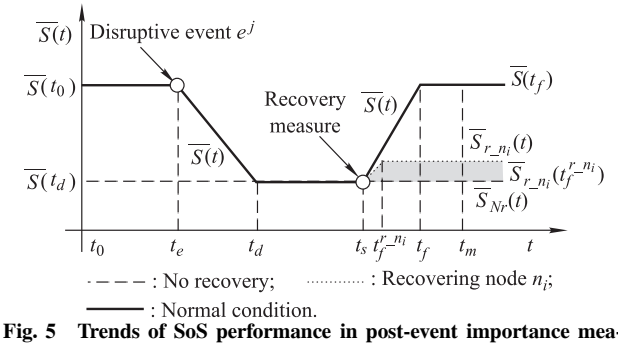

Fig. 5 Trends of SoS performance in post-event importance measure

Accordingly, after-event RIM can be mathematically represented as

$$C_{r\_n_i} = \frac{R_{h\_r\_n_i} - R_{h\_Nr}}{R_{h\_Nr}} \tag{16}$$

where $R_{h\_r\_n_i}$ represents the overall resilience when the failure node n_i is recovered; R_h represents the normal situation. Combining (11) and (16), we obtain

$$C_{r\_n_i} = \frac{R_{h\_r\_n_i} - R_{h\_Nr}}{R_{h\_Nr}} = \int_{t_0}^{t_m} \frac{\bar{S}_{r\_n_i}(t) - \bar{S}_{Nr}(t)}{\bar{S}_{Nr}(t)} \mathrm{d}(t). \tag{17}$$

4. Case study

4.1 Simple example

In this study, the process of resilience and importance measure analysis is examined by a simple but integrated case study, in which the sensors, decision points, influencers, and opponent targets are extracted from an operation SoS. Table 1 illustrates the types, numbers, and symbols of nodes in the network. Table 2 illustrates the probability that two nodes of different types are connected. For example, $P_{TS} = 0.4$ represents that the probability that a sensor node is connected to a target node is 0.4. Hence, the SoS network, which is generated with the model parameters in Table 1 and Table 2, is exhibited in Fig. 6. Note that different colors of nodes represent the node types.

Table 1 Nodes in the network

Type	Notation	Number
Sensor (S)	$S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8$	8
Decision point (D)	D_1, D_2, D_3	3
Influencer (I)	$I_1, I_2, I_3, I_4, I_5, I_6, I_7, I_8$	8
Target (T)	T_1, T_2, T_3, T_4	4

Table 2 Probabilities of connection between node types

Connection	Notation	Probability
Target→Sensor	P_{TS}	0.4
Sensor→Decision point	P_{SD}	0.6
Decision point→Decision point	P_{DD}	0.6
Decision point→Influencer	P_{DI}	0.6
Influencer→Target	P_{IT}	0.3

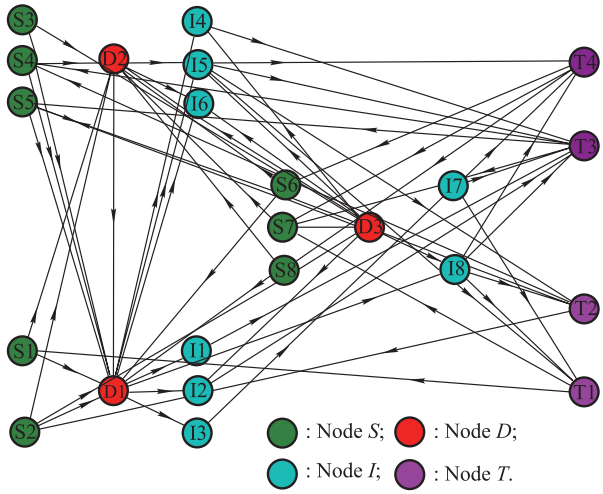

Fig. 6 SoS network in the case study

4.2 Resilience analysis

In this case study, without loss of generality, we assume there are two disruptive events: e^1, e^2. When e^1 occurs, nodes S_1, D_1, I_1 will fail, i.e., $N_f^{e^1} = 3$; when e^2 occurs, nodes S_8, S_4, and I_5 will fail, i.e., $N_f^{e^2} = 3$. Each node in the network has only two states: normal or malfunction, and the status of each node will change in the presence of attack or recovery.

Without loss of generality, we set the start time of the mission $t_0 = 0$, and the duration of the mission is 18 time units, therefore, $t_m = 18$. At time $t_e = 4$, the SoS is subject to attack until $t_d = 7$. When the attack begins, the abovementioned nodes will fail in sequence at random times in the attack duration. Meanwhile, the last failure occurs at the end of the attack duration. In the simulation, we generate $N_f - 1$ random numbers in time interval (t_e, t_d) to define the start times of each node failure: $t_{d1} = 4.8$, $t_{d2} = 6.1$, and $t_{d3} = 7$.

Before the recovery begins, we assume the preparation time is 3 time units, thus $t_s = 10$. During the recovery, the sequence of recovering each node depends on the types of the nodes. The priority of recovering different types of nodes follows $D > S > I$. When recovering nodes of the same type, nodes that possess higher degrees will be recovered first. Also, the recovery time, depicted as mean time to repair (MTTR), of each node varies with its type, as shown in Table 3.

Table 3 MTTR of network nodes

Node	S_1	D_1	I_1	S_8	S_4	I_5
Degree	5	15	2	6	3	2
MTTR	1.6	2	1.4	1.6	1.6	1.4

As mentioned above, the sequence of recovering each node in event e^1 follows $D_1 > S_1 > I_1$, and the recovery of each node finishes at time: $t_{r11} = 12$, $t_{r12} = 13.6$, and $t_{r13} = t_{f1} = 15$. Likewise, for event e^2, the recovery follows: $S_8 > S_4 > I_5$, $t_{r21} = 11.6$, $t_{r22} = 13.2$, and $t_{r23} = t_{f2} = 14.6$.

The above assumptions and settings are extracted from an imitative operational context and might not accord with the real operational situation, but they are applicable and feasible in the study of resilience. Substituting matrix $\boldsymbol{A}$ into (9) at any time during the resilience process, we can calculate the number of operation loops and plot the trend of the SoS performance, as shown in Fig. 7.

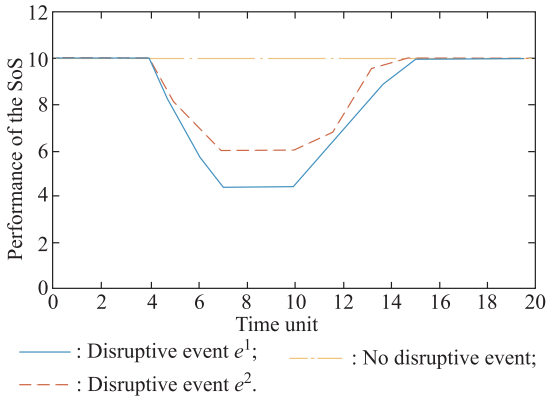

Fig. 7 Performance of the SoS during the disruptive events

According to (11), the overall resilience of the SoS during the disruptive events can be obtained in the following.

The overall resilience during e^1:

$$R_{h1} = \frac{\int_{t_0}^{t_m} \bar{S}_1(t)\mathrm{d}(t)}{\int_{t_0}^{t_m} \bar{S}_1(t_0)\mathrm{d}(t)} = \frac{140.58}{180} = 0.781\,0. \quad (18)$$

The overall resilience during e^2:

$$R_{h2} = \frac{\int_{t_0}^{t_m} \bar{S}_2(t)\mathrm{d}(t)}{\int_{t_0}^{t_m} \bar{S}_2(t_0)\mathrm{d}(t)} = \frac{152.08}{180} = 0.844\,9. \quad (19)$$

The above results show that R_{h2} is greater than R_{h1}, which indicates that the SoS is more resilient against event e^2. There are two reasons for the difference. In the attack process, event e^1 leads to the failure of decision point D_1, which is the key node in the SoS. Since there are only three decision points in the network, any component failure in decision points will result in large quantities of disconnected operation loops and sharp decrease of performance. On the other hand, in the recovery process, the recovery of decision points costs more time. Hence the SoS will remain in low performance for longer, and cannot perform the expected functions of command and control. From (13), (15) and (17), it is evident that if the SoS is in low performance for long, the SoS is less resilient.

4.3 Importance measure analysis

In this section, we conduct the RIM analysis on event e^1 in the network shown in Fig. 6. After the disruptive event, nodes S_1, D_1, and I_1 fail, by which we can measure the resilience importance of each node.

4.3.1 Pre-event RIM

In pre-event RIM, we add a node to the network and trace the performance of the SoS during event e^1. The new node can be a sensor (S), decision point (D), or an influencer (I), and the trends of performance in three conditions are respectively shown in Fig. 8.

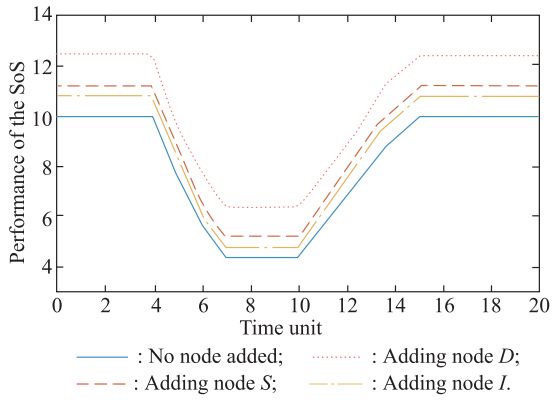

Fig. 8 Trends of SoS performance when different types of new nodes are added

The overall resilience of the SoS, and the pre-event resilience importance are illustrated in Table 4.

Table 4 Resilience and importance in pre-event analysis

Measure	Normal	Adding node S	Adding node D	Adding node I
R	0.641 6	0.741 5	0.851 1	0.701 5
RIM		0.155 6	0.3264	0.093 2

4.3.2 Middle-event RIM

Following the steps introduced in Section 3.2, we obtain the trends of SoS performance in different conditions in middle-event RIM, as shown in Fig. 9.

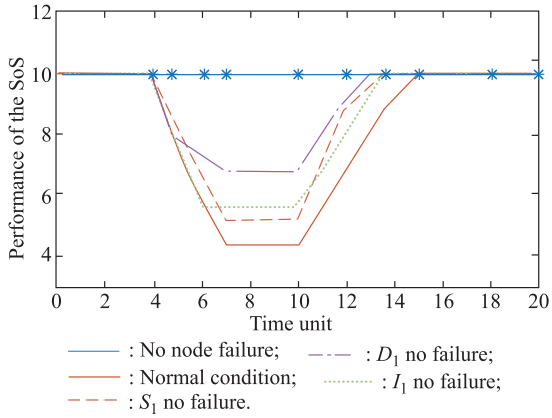

Fig. 9 Trends of SoS performance when encountering different types of failure

The overall resilience of the SoS, and the middle-event resilience importance are illustrated in Table 5.

Table 5 Resilience and importance in middle-event analysis

Measure	Normal	S_1 functioning normally	D_1 functioning normally	I_1 functioning normally
R	0.781 0	0.840 0	0.886 2	0.832 7
RIM		0.075 5	0.134 7	0.066 2

4.3.3 Post-event RIM

Following the steps introduced in Section 3.3, we obtain the trends of SoS performance in different conditions in post-event RIM, as shown in Fig. 10. The overall resilience of the SoS, and the middle-event resilience importance are illustrated in Table 6.

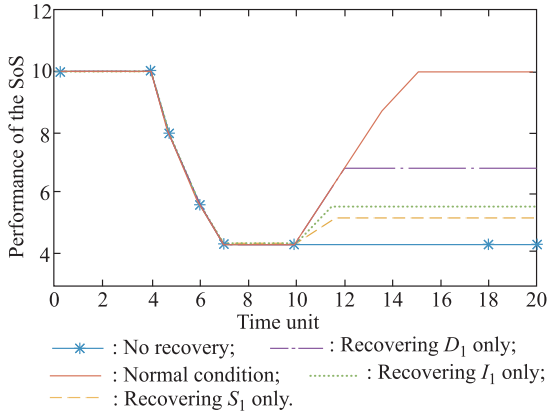

Fig. 10 Trends of SoS performance under different recovering measurements

Table 6 Resilience and importance in post-event analysis

Measure	No recovery	Recovering S_1 only	Recovering D_1 only	Recovering I_1 only
R	0.605 2	0.637 2	0.698 6	0.653 9
RIM		0.052 9	0.154 2	0.080 4

4.3.4 RIM of different nodes

In Fig. 11, the resilience importance of different types of nodes in the network is illustrated with a histogram. As shown in the histogram, the importance index of decision points D is high in pre-event, middle-event, and post-event. This is because the decision points possess high degrees and that all operation loops are subject to a small number of node Ds. Once more decision points are added to the network, the number of operation loops will considerably increase the number of operation loops. Hence, the performance of the operational network will increase and the SoS can maintain its performance during the disruptive events. If the decision points can maintain the expected functions during disruptive events, the SoS will lose only a small quantity of operation loops. Meanwhile, if the failed decision points are recovered in priority, the SoS will restore its performance rapidly. In summary, our results of importance measure analysis indicate that the decision points are vital for an SoS as well as for the improvement of resilience. In all the three types of RIM analysis, i.e., pre-event, middle-event, and post-event RIM, the decision points should be addressed more.

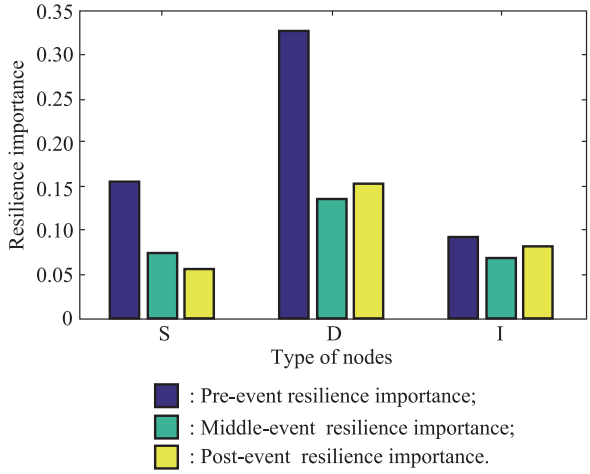

Fig. 11 Resilience importance of different types of nodes

5. Conclusions

Since the structure and quantity of member systems in an SoS are complex, it is important to design and optimize the SoS from the perspective of resilience importance, so that the SoS will be more resilient when confronted with uncertain disruptive events. In this study, we propose an NCW-based model to describe the components and connections of an SoS, in which the performance is measured by the number of operation loops. In the resilience analysis, we conduct RIM, focusing on the attack and recovery process of the SoS. From the perspective of resilience, we propose and examine the resilience indicator of SoS and the corresponding algorithms. Specifically, the resilience situations are classified into three types accord-

ing to the phases of performance change under disruptive events: pre-event, middle-event, and post-event. The difference of the three conditions is also the source of reasons for resilience: pre-event resilience depends on component redundancy, middle-event resilience depends on SoS reliability, and post-event resilience depends on the recovery of the SoS. Besides, other source of SoS resilience, e.g., SoS evolution, reconfiguration, task-reorganizing, are to be examined in the future research.

References

[1] GAMA DESSAVRE D, RAMIREZ-MARQUEZ J E, BARKER K. Multidimensional approach to complex system resilience analysis. Reliability Engineering and System Safety, 2016, 149: 34 – 43.

[2] OUYANG M, DUEÑAS-OSORIO L, MIN X. A three-stage resilience analysis framework for urban infrastructure systems. Structural Safety, 2012, 36/37: 23 – 31.

[3] HENRY D, RAMIREZ-MARQUEZ J E. Generic metrics and quantitative approaches for system resilience as a function of time. Reliability Engineering and System Safety, 2012, 99: 114 – 122.

[4] HOLLING C S. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 1973, 4(1): 1 – 23.

[5] WEBB C T. What is the role of ecology in understanding ecosystem resilience? BioScience, 2007, 57(6): 470 – 471.

[6] KECK M, SAKDAPOLRAK P. What is social resilience? Lessons learned and ways forward. Erdkunde, 2013, 67(1): 5 – 19.

[7] COHEN O, LEYKIN D, LAHAD M, et al. The conjoint community resiliency assessment measure as a baseline for profiling and predicting community resilience for emergencies. Technological Forecasting and Social Change, 2013, 80(9): 1732 – 1741.

[8] ROSE A, LIAO S Y. Modeling regional economic resilience to disasters: a computable general equilibrium analysis of water service disruptions. Journal of Regional Science, 2005, 45(1): 75 – 112.

[9] MARTIN R. Regional economic resilience, hysteresis and recessionary shocks. Journal of Economic Geography, 2012, 12(1): 1 – 32.

[10] YOUN B D, HU C, WANG P. Resilience-driven system design of complex engineered systems. Journal of Mechanical Design, 2011, 133(10): 101011.

[11] HOLLNAGEL E, WOODS D D, LEVESON N. Resilience engineering: concepts and precepts. Surrey: Ashgate Publishing Ltd., 2007.

[12] LAC C, STERBENZ J P G, PLATTNER B, et al. Network resilience: a systematic approach. IEEE Communications Magazine, 2011, 49(7): 88 – 97.

[13] CARES J R. Distributed networked operations: the foundations of network centric warfare. Bloomington: Iuniverse Inc, 2006.

[14] KRISHNAMURTHY V. Emission management for low probability intercept sensors in network centric warfare. IEEE Trans. on Aerospace and Electronic Systems, 2005, 41(1): 133 – 151.

[15] REN W, LI Y, LU J, et al. Operational demand optimization of defend special target under national air defense. Armament Automation, 2007, 26(9): 12 – 13.

[16] LI Y J, SONG Y L, CHEN X R, et al. The analysis for CEPR plant state restoration method after degrade mode test. Science and Technology Vision, 2018, 1(17): 1 – 3.

[17] ZHONG J L. GUO J L, WANG Z J, et al. Research on phased mission based efficient reliability evaluation algorithm for equipment system of systems. Systems Engineering and Electronics, 2016, 38(1): 232 – 238. (in Chinese)

[18] XU S L, ZHANG D, ZHAO H Y. Research on the multi-missile cooperative technology based on systemic confrontation. Tactical Missile Technology, 2019, 1(1): 79 – 86.

[19] WU Y, GE Y T, ZHANG D Q. Development of precision strike weapons and key technologies by reviewing DARPA research programs. Tactical Missile Technology, 2017, 1(6): 1 – 8.

[20] BARKER K, RAMIREZ-MARQUEZ J E, ROCCO C M. Resilience-based network component importance measures. Reliability Engineering and System Safety, 2013, 117: 89 – 97.

[21] MANUAL J. The long road to recovery: environmental health impacts of hurricane sandy. Environmental Health Perspectives, 2013, 121(5): A152 – 9.

[22] LIPTON E. Cost of storm-debris removal in city is at least twice the US average. New York: The New York Times, 2013.

[23] UDAY P, MARAIS K. Exploiting stand-in redundancy to improve resilience in a system-of-systems (SoS). Procedia Computer Science, 2013, 16: 532 – 541.

[24] PAN X, JIANG Z, YANG Y J. Resilience-based component importance and recovery strategy for system-of-systems. Journal of Beijing University of Aeronautics and Astronautics, 2017, 43(9): 1713 – 1720.

[25] DUTUIT Y, RAUZY A. Efficient algorithms to assess component and gate importance in fault tree analysis. Reliability Engineering and System Safety, 2001, 72: 213 – 222.

[26] LI J H, MOSLEH A, KANG R. Likelihood ratio gradient estimation for dynamic reliability applications. Reliability Engineering and System Safety, 2011, 96: 1667 – 1679.

[27] BORGONOVO E. A new uncertainty importance measure. Reliability Engineering and System Safety, 2007, 92: 771 – 784.

[28] BORGONOVO E, PLISCHKE E. Sensitivity analysis: a review of recent advances. European Journal of Operational Research, 2016, 248(3): 869 – 887.

[29] LIU Q, HOMMA T. A new computational method of a moment-independent uncertainty importance measure. Reliability Engineering and System Safety, 2009, 94: 1205 – 1211.

[30] PAN X, HU L H, XIN Z L, et al. Risk scenario generation based on importance measure analysis. Sustainability, 2018, 10(9): 3207.

[31] ZHANG L, LU Z, CHENG L, et al. A new method for evaluating Borgonovo moment-independent importance measure with its application in an aircraft structure. Reliability Engineering and System Safety, 2014, 132: 163 – 175.

[32] BORGONOVO E, ALIEE H, GLAß M, et al. A new time-independent reliability importance measure. European Journal of Operational Research, 2016, 254(2): 427 – 442.

[33] DUI H, SI S, YAM R C. A cost-based integrated importance measure of system components for preventive maintenance. Reliability Engineering and System Safety, 2017, 168: 98 – 104.

[34] SHI Y, LU Z, ZHOU Y. Global sensitivity analysis for fuzzy inputs based on the decomposition of fuzzy output entropy. Engineering Optimization, 2018, 50(6): 1078 – 1096.

[35] WU Y, PAN X, KANG R, et al. Multi-parameters uncertainty analysis of logistic support process based on GERT. Journal of Systems Engineering and Electronics, 2014, 25(16): 1011 – 1019.

[36] FANG Y P, PEDRONI N, ZIO E. Resilience-based component importance measures for critical infrastructure network

systems. IEEE Trans. on Reliability, 2016, 65(2): 502 – 512.
[37] DESSAVRE D G, RAMIREZ-MARQUEZ J E, BARKER K. Multidimensional approach to complex system resilience analysis. Reliability Engineering and System Safety, 2016, 149: 34 – 43.
[38] PAN X, WANG H. Resilience of and recovery strategies for weighted networks. PLoS ONE, 2018, 13(9): 1 – 15.
[39] VON LUBITZ D, BEAKLEY J E, PATRICELLI F. All hazards approach to disaster management: the role of information and information and knowledge management, Boyd's OODA loop, and network-centricity. Disasters, 2008, 32(4): 561 – 585.
[40] BRYANT D J. Rethinking OODA: toward a modern cognitive framework of command decision making. Military Psychology, 2006, 18(3): 183 – 206.
[41] ESTRADA E, RODRÍGUEZ- VELÁZQUEZ J A. Subgraph centrality in complex networks. Physical Review E, 2005, 71(5): 56103.
[42] TAN Y J, ZHANG X K, YANG K W. Research on networked description and modeling methods of armament system-of-systems. Journal of Systems and Management, 2016, 21(6): 781 – 786.

Biographies

PAN Xing was born in 1979. He received his B.S. degree in mechanical engineering, and Ph.D. degree in systems engineering from Beihang University (BUAA), Beijing, China, in 2000, and 2005, respectively. From 2005 to 2009, he was an assistant professor with the School of Reliability and Systems Engineering, Beihang University, Beijing, China. Since 2009, he has been an associate professor. From 2012 to 2013, he was a visiting scholar at the Department of Systems and Industrial Engineering, University of Arizona, Tucson, USA. His research interests include reliability engineering, systems engineering, and system risk analysis.
E-mail: panxing@buaa.edu.cn

WANG Huixiong was born in 1995. He received his B.S. degree in safety science from School of Reliability and Systems Engineering, Beihang University, in 2018. He is currently a master student in the same school. His interests of research include systems engineering and complex network.
E-mail: wanghuixiong@buaa.edu.cn

YANG Yanjing was born in 1991. He received his B.S. degree in material engineering from Yanshan University in 2015, and M.S. degree in industrial engineering from Beihang University in 2018. Since 2018, he has been an assistant engineer at China Railway Signal and Communication Corporation. His research interests include signal system engineering and system and systems engineering (SoSE).
E-mail: yangyanjing@crscu.com.cn

ZHANG Guozhong was born in 1979. He is a senior engineer with the Institute of Systems Engineering, China State Shipbuilding Corporation. His research interest is system of systems engineering (SoSE).
E-mail: 18911990023@189.cn