Journal of Systems Engineering and Electronics
Vol. 34, No. 3, June 2023, pp.543 – 573

Complex systems and network science: a survey

YANG Kewei *, LI Jichao †, LIU Maidi, LEI Tianyang, XU Xueming, WU Hongqian, CAO Jiaping, and QI Gaoxin

College of Systems Engineering, National University of Defense Technology, Changsha 410073, China

Abstract: Complex systems widely exist in nature and human society. There are complex interactions between system elements in a complex system, and systems show complex features at the macro level, such as emergence, self-organization, uncertainty, and dynamics. These complex features make it difficult to understand the internal operation mechanism of complex systems. Networked modeling of complex systems is a favorable means of understanding complex systems. It not only represents complex interactions but also reflects essential attributes of complex systems. This paper summarizes the research progress of complex systems modeling and analysis from the perspective of network science, including networked modeling, vital node analysis, network invulnerability analysis, network disintegration analysis, resilience analysis, complex network link prediction, and the attacker-defender game in complex networks. In addition, this paper presents some points of view on the trend and focus of future research on network analysis of complex systems.

Keywords: complex system, complex network, invulnerability and resilience, network disintegration, link prediction, attacker-defender game theory.

DOI: 10.23919/JSEE.2023.000080

1. Introduction

The complex system theory has experienced two breakthroughs, which provide strong theoretical support for people to understand complex systems. The achievement of the first theoretical breakthrough is usually called SCI theory, which specifically includes the systems theory [1], cybernetics [2], and information theory [3]. The theoretical achievement of the second breakthrough is usually called DSC theory, which specifically includes dissipative structure theory [4], synergetics [5], and catastrophe [6]. A system is an organism, which is not a mechanical combination of each component, and it possesses the overall features that elements do not have in their isolated state. Complex system [7] is an advanced academic concept in the field of system science. It was proposed in the 20th century and gained prominence in the 21st century. A complex system is composed of many components [8], and there are direct or indirect nonlinear interactions between the components. At present, there is no clear academic definition of complex systems, but complex systems share many unique features, such as emergence [9,10], self-organization, uncertainty, and dynamism. There are many complex systems in nature and human society [11]; for example, the global climate system, organisms, the human brain, the power grid, infrastructure systems, complex software and electronic systems, social and economic organizations, ecosystems, cells, and even the universe, can be regarded as complex systems [12,13].

Complexity means that the behavior of the system cannot be easily inferred from its attributes. Therefore, the best way to research the features and behavior of a complex system is to represent and analyze the complex system through system modeling [14]. However, accurately modeling a complex system is difficult because of the complex interaction between the system and the environment. Popular modeling methods for complex systems include the agent-based method [15], meta-model method [16], Petri network method [17], and system dynamics method [18]. The agent-based method considers that a system is composed of several independent agents, and these agents can interact with each other to promote the spontaneous behavior tendency of the system. These agents update their state according to internal micro-interactions and make the macro state of the system evolve. The meta-model method extracts the meta relationships of each subsystem by obtaining the interaction within the system, and it summarizes the meta elements with different attributes. The meta-model method is a basic method

Manuscript received November 23, 2022.
*Corresponding author.
†Co-first authors.
The work was supported by the State Key Program of National Natural Science Foundation of China (72231011), the National Natural Science Foundation of China (72071206; 72001209; 71971213), and the Science Foundation for Outstanding Youth Scholars of Hunan Province (2022JJ20047).

for researching complex systems. It is a representation of the interactions within the system, but it can only represent interactions between simple metadata. The Petri network is a theory concerning dynamic features of the system that mainly uses graphics to represent the system structure and is widely used in studies of system science. The system dynamics method introduces the dynamics theory into the complex system. The system dynamics method assumes that all kinds of systems have similar dynamics properties. It introduces the dynamics theory into the complex system and establishes the mathematical models. This method can not only effectively represent the composition of a complex system but also accurately depict the system structure. However, as this method is suitable for static modeling and cannot be dynamically adjusted according to external constraints, the method cannot accurately represent the complexity of the system.

The complex network theory [19,20] provides a new modeling method for complex systems. The complex network is a special kind of network structure that abstracts elements in a complex system as nodes and interactions between elements as edges. Compared with classic methods, the complex network method offers great advantages in not only allowing for directly depicting interactions between the elements of complex systems but also studying the features of complex systems, such as emergence, self-organization, and nonlinear dynamics of the network structure [21,22]. The complex network method can reveal the behavior and essential attributes of complex systems, and it has become a mainstream method of complex system modeling and analysis. In this paper, we summarize the research progress of complex systems modeling and analysis from the perspective of network science and prospects for a future research direction and focus.

The paper proceeds as follows. Section 2 reviews a few basic concepts of networked modeling of complex systems. Section 3 discusses vital node analysis of complex systems. Section 4 discusses network invulnerability analysis of complex systems. Section 5 provides a discussion of network disintegration analysis of complex systems. Section 6 introduces the resilience analysis of complex systems. Section 7 demonstrates the link prediction of complex systems. Section 8 discusses the attacker-defender game in complex networks. Section 9 concludes the paper with an outlook on future research.

2. Networked modeling of complex systems

The complex network provides an effective method to model and describe the internal components and relationship characteristics of complex systems. By abstracting the elements in complex systems as nodes, and relationships between nodes as edges, researchers construct interconnected complex network models to analyze the internal structure and explore the interactions between elements in complex systems [23]. The complex network theory has been widely used in research involving complex system modeling in many fields, including natural resource systems, Internet systems, transportation systems, energy systems, social systems, global climate systems, and brain neural systems, among others.

According to the practical characteristics of various fields of application, researchers have used different complex networks to model complex systems, including simple networks, heterogeneous networks, multilayer networks, and dynamic networks. In the following, the research on complex system modeling based on various networks is reviewed.

2.1 Complex system modeling based on simple networks

A simple complex network model can be seen as a mathematical graph, which is a set of nodes and edges, usually represented by $G=(V,E)$, where $V(G)=V$ represents the node set and $E(G)=E$ represents the edge set. If the network contains $N(N\neq 0)$ nodes, then the node set can be expressed as $V=\{v_1,v_2,\cdots,v_n\}$. Similarly, the set of edges $E=\{e_1,e_2,\cdots,e_W\}$ contains W edges, and each edge is a two-element subset $\{v_i,v_j\}$ of the set V, which is generally recorded as v_iv_j or v_jv_i, where $W\leqslant N(N-1)/2$. When the subset $v_iv_j\in E$, we consider that nodes v_i and v_j are adjacent; otherwise, they are considered not adjacent.

In the research involving complex system modeling based on simple networks, a complex system is generally regarded as a simple combination of many interrelated components. The definitions of nodes and edges in the network are diversified depending on the specific application background.

For example, Wu et al. [24] introduced the complex network theory into the modeling of river systems. They proposed that positions with significant hydraulic characteristics can be regarded as nodes and the routes of rivers as the edges between nodes. Moreover, they demonstrated through a case study that the complex network model is feasible for the modeling and analysis of river systems.

Another typical example is gene regulatory networks. Genes in organisms constitute a complex system, and the mechanism controlling gene expression is complicated. By taking genes as nodes and their interactions as edges, researchers construct the gene regulatory network, which entails powerful abstractions of biological systems with

widespread and increasing applications in biomedical research [25].

Simple network modeling has been applied in many fields, including transportation systems [26], communication systems [27], and ecosystems [28], among others. However, with the deepening of research, researchers found that many complex systems in reality have more complex characteristics, such as heterogeneity, hierarchy, and time variance. Apparently, these characteristics are difficult to model with simple networks. Therefore, researchers have carried out more diversified research on network modeling of complex systems, as discussed below.

2.2 Complex system modeling based on heterogeneous networks

In practical applications, the components and connections in complex systems may have different characteristics, while the simple network model will cause inevitable information loss under these circumstances. Compared with a simple and homogeneous network model, a heterogeneous network model involves specific information about the attributes of nodes and edges that are of great significance for the modeling, analysis, and optimization of complex systems.

As mentioned above, a complex network model can be abstracted as a graph $G=(V,E)$. Suppose there is an entity type mapping function $\varphi: V \to K$ and an edge type mapping function $\phi: E \to L$. Each entity $v \in V$ belongs to a specific entity type $\varphi(v) \in K$, and each edge $e \in E$ belongs to a specific relationship type $\phi(e) \in L$. If the number of entity types $|A|>1$ or the number of edge types $|L|>1$, the network is regarded as a heterogeneous network, as shown in Fig. 1.

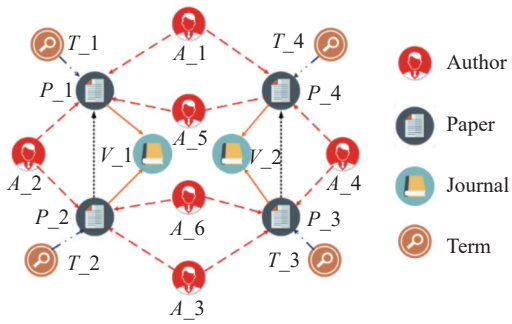


Fig. 1 Diagram of a heterogeneous network

Taking the academic information network as an illustration, there are four types of nodes in the network, namely, Author node, Paper node, Journal node, and Term node. The connections between different nodes have different meanings. There are four types of edges, namely, papers published by authors ($A \to P$), papers containing terms ($T \to P$), citations between papers ($P \to P$), and papers published in a journal ($P \to V$) [29].

Here, we give some examples of complex system modeling based on heterogeneous networks to illustrate.

The combat system is a typical heterogeneous complex system. Xing et al. [30] reviewed the research on joint operation system modeling based on complex networks. In the combat process, there are different types of equipment and pairwise operational relationships. The research on modeling combat systems regards the equipment in combat systems as nodes and the operational relationships between equipment as edges. On this basis, the combination of the OODA (Observe, Orient, Decide, Act) combat model and the complex network theory has become the main idea underpinning joint combat modeling research. The central idea is that the basic combat process is a loop composed of observe, orient, decide, and act operational entities.

Many other complex systems in reality also have typical heterogeneity, such as social systems, disease systems, and ecological systems. Heterogeneous network models are applied in many studies in these fields. For example, Li et al. [31] built a heterogeneous network model of social systems for discovering characteristics in social networks, including centrality and clustering. Letha et al. [32] provided a fractional-order Ebola virus epidemic model with delayed immune response in heterogeneous complex networks. Bancal et al. [33] studied the dynamical process of the forest fire model in heterogeneous networks by developing the corresponding heterogeneous mean-field theory and solving it in its steady state.

2.3 Complex system modeling based on multilayer networks

For complex systems with hierarchical characteristics, simple network models cannot describe these special properties. In comparison, the multilayer network model can describe the hierarchical characteristics of complex systems by separately modeling the internal structure and inter-layer relationships of each network layer.

The multilayer network model can be expressed as the set $M=(G,H)$, where G denotes different network layers, and H denotes the inter-layer edges between networks. Suppose G contains n single-layer networks, then $G=\{G_\alpha|\alpha \in \{1,2,\cdots,n\}\}$, where $G_\alpha=(N_\alpha,E_\alpha)$. Node set N_α denotes the nodes in network layer α. The intra-layer edge set E_α denotes the edges in network layer α:

$$E_\alpha=\left\{\left(N_\alpha^i,N_\alpha^j\right)\middle|N_\alpha^i,N_\alpha^j \in N_\alpha; i \neq j\right\}. \quad (1)$$

H denotes the inter-layer edges of nodes:

$$H = \{H_{\alpha\beta} \mid \alpha,\beta \in \{1,2,\cdots,n\}; \alpha \neq \beta\}. \tag{2}$$

$H_{\alpha\beta}$ denotes the inter-layer edge set between layers G_α and G_β:

$$H_{\alpha\beta} = \left\{\left(N_\alpha^i, N_\beta^j\right) \middle| \alpha,\beta = \{1,2,3,4\}; \alpha \neq \beta\right\}. \tag{3}$$

Multilayer network modeling has been widely used in the research on modeling and analysis of practical hierarchical complex systems, including the power system, financial system and transportation industry. To effectively detect the vulnerability of smart grids (electric power systems), Alonso et al. [34] modeled the smart grid system as a two-layer network model consisting of two interconnected networks, that is, the physical power network model and the information and communication technology (ICT) network model. The hidden interdependence of power and ICT networks is highlighted, including the interaction between the two systems. Chen et al. [35] built a three-layer weighted undirected network for Chinese stock markets, which characterizes different forms of dependencies among financial time series and considers the dependency types simultaneously. In addition, obvious clustering features are found in the network. Yang et al. [36] built the multilayer network model for the Chinese air transportation system and proposed a multilayer-based passenger rescheduling method and a multilayer cooperation approach to improve the efficiency of network traffic under random failures.

2.4 Complex system modeling based on temporal networks

The static network is the focus of traditional complex network research, but many complex systems are highly dynamic and time-varying in practical applications, and it is difficult for static models to effectively describe the formation and evolution of these networks. In addition, many practical applications pay special attention to the temporal and dynamic characteristics of complex systems, especially in sociology, infectious disease, and industrial production research, such as rumor spreading in social systems, disease spreading among people, and cascading failures of power systems. In these cases, it is of great significance to build the temporal network model with time series data and highlight the dynamic changes of the network, which can help in predicting the future trend of the complex system and provide theoretical support for decision-makers.

Previous research has proposed various temporal network models for studying the dynamic process of formation, generation, and development of network topology. Hanneke et al. [37] proposed the temporal exponential random graph model (TERGM), a family of statistical models, for studying social network evolution over time. Jiang et al. [38] proposed a temporal network model, the nodal attribute-based temporal exponential random graph model (NATERGM), for dynamic network analysis. The model is used to study the formation mechanisms of social media systems and comprehensively consider the impact of network temporal patterns and nodal attributes interaction on the dynamic development of networks. Zeno et al. [39] proposed a temporal graph generative model from a higher-order network perspective, using temporal motifs as building blocks, to study the temporal transfer between various motifs in time series data of different dynamic networks in reality.

There are also studies investigating the status transition of nodes to predict the dynamic evolution and dissolution process of networks. In a complex system with many interconnected units, the behavior of an entity is not limited to itself but will lead to a chain change among its neighbors in the network model. Therefore, it is impossible to infer the evolution of the whole system simply by the attributes and behaviors of a few elements. Complex network propagation dynamics can describe the propagation and diffusion between entities, and the system deduction can be effectively carried out to predict the development and evolution direction of the system. Specifically, according to the dynamic mechanism of network propagation, the evolution trend of the existing complex network structure can be analyzed, and then the deduction results of the complex system can be obtained. For example, researchers first set the state space and state transition probability of nodes and then infer the node state change process according to the network topology to infer the evolution process of the whole network.

Representative network propagation models are epidemic dynamics models, such as the susceptible-infected-susceptible (SIS) and susceptible-infected-recovered (SIR) models. The SIR model defines the state of individuals as the susceptible, the infected, and the recovered. Determining the transition probability of various states allows for deducing the network propagation and diffusion based on the network topology. At present, the epidemic dynamics models are still developing[40−42] and have huge application value in various fields, such as epidemic control [43], public opinion control [44,45], production safety control [46], and science of science research [47].

2.5 Future prospects of complex system modeling

In the future, higher-order networks will become one of the emerging and vital methods for complex system modeling. With the deepening of the research, complex sys-

tems in practical applications are developing in the direction of more individuals and more complex interactions. Researchers have found that there are complex interactions involving multiple individuals in the real system. Traditional pairwise edges are not suitable for describing these relationships, which will lead to the inapplicability and incompleteness of system modeling. Higher-order network theory takes the interaction of multiple individuals as the basic modeling unit and can get new insights into complex systems from a higher-order perspective, which is getting more research attention and will become an important research direction of complex system modeling in the future.

3. Vital nodes analysis of complex systems

Vital nodes of a complex network are a special kind of nodes that can greatly influence the structure and function of the network. The precise identification of vital nodes in a network can enable effective control of the network at minimal costs, such as facilitating information dissemination, discovering essential proteins in protein networks, identifying successful scientists, controlling the outbreak of epidemics, suppressing the spread of rumors, and preventing large-scale network disruptions. In the era of the information explosion and the consequent surge of information load of the system, how to obtain critical information at a lower cost has become an urgent problem to be solved. Therefore, it is of high theoretical and practical significance to study effective vital node identification algorithms.

According to incomplete statistics from the Centiserver platform (https://www.centiserver.org/) of Tehran University of Medical Sciences [48], 403 algorithms for vital node identification have been proposed by previous authors as of 2021; only articles published in English are counted. As the principles, advantages, and applicability of various algorithms are different, there is a need to differentiate various types of node identification algorithms.

This section will proceed with the following structure. First, classical single-layer network node identification algorithms are introduced and classified. Second, new methods based on classical algorithm improvements are introduced. Third, the current measures for evaluating the strengths and weaknesses of the algorithm are listed. Finally, future research directions of current vital node identification algorithms are proposed.

We will introduce the development and progress of node evaluation methods from simple to complex. This section will proceed with the following structure. First, classical single-layer network node identification algorithms are introduced and classified. Second, new methods based on classical algorithm improvements are introduced. Third, the current measures for evaluating the strengths and weaknesses of the algorithm are listed. Finally, future research directions of current vital node identification algorithms are proposed.

3.1 Classical vital nodes identification algorithm

The importance of nodes can be viewed from two perspectives: location in the network and network propagation dynamics [49]. Starting from the topology of the network, Lü et al. classified node importance ranking algorithms for single-layer networks into three categories according to the number of neighbors, paths, and eigenvectors of the adjacency matrix of nodes [50].

(i) Node-neighborhood-based ranking methods are the simplest and most intuitive methods: degree centrality examines the number of direct neighbors of a node [51]; semi-local centrality measure considers information about the node's 4-level neighbors [52]; and k-shell decomposition can be regarded as an extension of degree centrality, which defines the importance of a node according to its position in the network, considering that the closer the node is to the core, the more important it is[53]. This type of algorithm mainly examines local information and has low time complexity.

(ii) Path-based ranking methods simulate the flow of information in the network. Some portray the global information of the network from propagation, and the corresponding time complexity increases. For example, closeness centrality calculates the average distance between a node and all other nodes in the network as the average propagation time of information in the network [54]; betweenness centrality portrays the importance of a node by the number of shortest paths through the node [55]; and subgraph centrality [56] considers the path through a node as a closed loop, counting the number of closed loops with the node as the first and the last, and the smaller the path length of the closed loop, the more convenient the loop information exchange and the closer the connection between the nodes, the greater the contribution to the centrality of the node.

(iii) Algorithms that converge with the eigenvectors of the adjacency matrix due to the iterative process in calculating node centrality are summarized as eigenvector-based approaches. The classical PageRank algorithm [57] is used to identify the importance of webpages by simulating the process of users browsing webpages online so that the score of a node increases along the access path, but the random jump probability of a webpage needs to be defined. The LeaderRank algorithm [58] is an adaptive and parameter-free algorithm to improve PageRank to quantify the influence of users. The hyperlink-induced topic search (HITS) algorithm [59] and the stochastic

approach for link-structure analysis (SALSA) algorithm [60] consider the authority and hub of a node and that they influence each other. These algorithms consider not only the number of node neighbors but also the influence of their quality on the importance of nodes and are mainly applicable to directed networks.

There are other ways to determine the influence of a node from the network function by examining the effect of node contraction or removal on the network function and thus the influence of the node. For example, the node shrinkage method [61] entails shrinking a node and its neighboring nodes into a new node, and if the cohesiveness of the whole network changes significantly after the shrinkage, the node is determined to be important; residual closeness centrality [62] also evaluates the importance of nodes from the perspective of network functions, which considers a node as more important if its deletion makes the network more fragile.

3.2 Improved vital nodes identification algorithm

Local information-based methods represented by degree centrality are computationally simple but cannot take into account the global information of the network, while global metrics represented by intermediate centrality and proximity centrality can identify influential nodes but cannot be applied to large-scale networks due to their computational complexity. Therefore, a large number of researchers have focused on obtaining as much local or global information as possible and reducing the time complexity of the solution as much as possible.

Most of the scholarly research in recent years has been based on network topology improvement metrics. For example, global structure model (GSM) [63], global and local structure (GLS) [64], and local-and-global centrality (LGC) [65], from local information or global structure, are mostly couplings of local metrics (node degree value or kernel number) and global metrics (the shortest path between nodes) with similar paradigms, and the ranking results are affected by the parameter settings and network structure. Facing the problem that the k-shell decomposition method is not suitable for evaluating global information, Liu et al. proposed an improved k-shell method to evaluate the node propagation impact by considering the shortest distance between the target node and the set of nodes with the highest k-core value [66]. Lü et al. innovatively proposed the H-index and proved that the degree of a node, the H-index of a node, and the kernel degree can represent the initial state, intermediate state, and steady state of the operator function H during operation, respectively, and the H-index of all other stages can likewise represent the importance of a node in a complex network [67]. Chen et al. extracted and integrated the traditional centrality index and the propagation and proposed spreading influence-related centrality as a fusion metric to compensate for the shortcomings of a single algorithm by extracting and combining the traditional centrality metric and topological feature information of spreading influence [68]. Dong et al. proposed a localized strategy, considering that global information is usually only available for the static structure of the network, for identifying significant nodes without global knowledge of the network, which nominates the set of significant nodes by selecting a set of random nodes together with a set of nodes connected to these nodes through a joint nomination strategy [69]. After Tan et al. proposed the concept of network structural entropy (the ratio of the degree of a network node to the sum of the degree values of all nodes) [61], later generations improved it. For instance, Qiao et al. took into account the local influence and indirect influence of nodes and obtained local power by integrating structural entropy and interaction frequency entropy, followed by capturing the indirect influence with the help of a two-hop process of propagation [70].

For weighted or directed networks, the adjacency matrix or Laplace matrix of the network topology can be resorted to. Xu et al. defined an adjacency information entropy method by drawing on the concept of information entropy in information theory to identify important nodes in different networks by considering the weights and orientations of edges in the network, and the expansion operation of the adjacency matrix can identify important nodes in different network types (unweighted and undirected, unweighted and directed, weighted and undirected and weighted and directed) [71]. In a directional weighted network, Liu used the degree metric to characterize the importance of the node itself, indirectly reflect the importance of the node relative to its neighbors by defining the node attraction rate and node transfer rate, and calculate the degree, node attraction rate, and node transfer rate of the node using the entropy method to obtain a comprehensive evaluation of the node importance metric. The algorithm considers both the weight values of edges between a node and its neighbors and the incoming and outgoing strengths of its neighbors while taking into account its importance and relative importance to its neighbors [72]. Qi et al. defined Laplacian energy as the sum of squares of the eigenvalues of the Laplacian matrix of the weighted network G. The importance or centrality of vertex v is reflected by the decrease of the Laplacian energy of the network in response to the deactivation or deletion of vertices in the network [73].

Some scholars have also used physical laws for improving node importance identification algorithms. Fei

et al. proposed an influential node identification method based on the inverse-square law, which considers that the mutual attraction between different nodes is inversely proportional to the square of the distance between two nodes and then calculates the sum of the attraction between all node pairs in the network to determine the node importance [74]. Similarly, Ma et al. proposed a gravitational centrality metric to identify influential diffusers in complex networks, inspired by the gravity formula, using the k-shell value of each node as its mass and the shortest path distance between two nodes as its distance [75]. Qiu et al. realized that percolation clusters are dominated by local connections in the subcritical phase and by global connections in the supercritical phase. A competing percolation process based on the Achlioptas process was proposed to identify important nodes, which expands the possibility space of optimal solutions by exploiting the randomness of the percolation process and is of importance in practical applications [76].

In large-scale networks, vital node identification, also called vital node mining, is an NP-hard problem (NP, nondeterministic polynomial time). In some schools of thought, vital node identification is considered an optimization problem, and the core idea is to first establish the objective function as the spread of influence, then achieve optimization to maximize the influence, and then identify vital nodes. Some studies have focused on connectivity to determine the set of nodes whose removal minimizes the network connectivity according to some predefined connectivity metrics. Such optimization problems can be solved using exact solution algorithms, greedy algorithms, heuristic algorithms, reinforcement learning algorithms, etc [77].

The greedy algorithm is applied primarily to solve top-k vital nodes with the following idea. First, note that there are two sets of nodes: the set of vital nodes S, which must satisfy the constraint $|S| \leqslant k$, and the set of remaining nodes $V\backslash S$, which must have minimal pairwise connectivity. The two sets are initialized and then we iteratively remove a node from one set and add it to the other set until the number of removed nodes satisfies $|S| \leqslant k$ [78]. Ren et al. proposed a so-called reverse greedy method based on the greedy algorithm, where the preference is given to the least important nodes to make the size of the largest component in the corresponding induced subgraph as small as possible [79]. Regarding heuristic algorithms, previous authors have explored the application of simulated annealing and population-based incremental learning methods for vital node identification in large-scale networks [77]. Some scholars have also grounded the optimization problem in reducing the time complexity of global node ranking methods. Zhong et al. mapped the vital node identification problem to an optimization problem based on global information about the network structure and proposed an almost linear time complexity confidence propagation and node reinsertion method (via belief propagation and node reinsertion) that takes finding the minimum set of feedback vertices as the vital solution problem [80].

3.3 Methodology for evaluating ranking results

To date, most of the studies evaluating node identification algorithms have used network models to evaluate the effectiveness of various algorithms [63−65]. One approach is to use a network propagation dynamics model, such as the susceptible infective (SI)/SIS/SIR model, to calculate the propagation influence of nodes. The specific ideas of the evaluation are as follows. First, the vital node identification method that can best promote the transmission of the "disease" is better if the same number of the most important node group is the initial source of infection. Second, the vital node identification method that can best prevent the transmission of the disease is better if the same number of the most important node group is the immune group.

There is also an attack method to determine the change in network performance to establish the importance of the node size [50]. There are three implementation options. One way is to separately measure the network performance when the node is not deleted and the network performance after the node is deleted, and then compare the difference between the two. The greater the difference between the two, the greater the impact of the node on the network performance, but this also indicates that the more important the node is, the better the performance of the identification method is. The second way is to set the threshold value of the network performance and observe the proportion of nodes to be deleted to reach the threshold value. If the proportion of nodes required is smaller, it means that the nodes have a greater impact on the network performance and the performance of the identification method is better. The third way is to remove nodes in the network in order of importance until all nodes in the network have been removed, and the result measures the change in network performance after the individual nodes are removed in turn. If the change of network performance is large, it means that the nodes are more important and that the performance of the identification method is good.

For some special real networks, such as citation networks [81], established impact evaluation metrics can be used as reference values to verify the validity of the algorithm.

3.4 Perspectives on vital nodes identification algorithms

In the future, complex changes to systems and updates to network modeling approaches will not stop. Vital node identification algorithms for more complex network modeling approaches, such as supernetworks, multilayer networks, and temporal networks, have been partially studied, but there is still considerable room for progress. For some specific real systems, how to consider specific node properties or edge properties and then perform vital node identification is also a problem that must be considered. How to efficiently extend the recognition algorithms of static structures to dynamic systems is another real and urgent problem for rapidly changing complex systems that can no longer be satisfied with the acquisition of static local information only.

4. Network invulnerability analysis of complex systems

The network in which we live is becoming larger and more complex. However, accidents are also becoming increasingly frequent, which confronts us with a series of serious problems. At the end of 2015, the power grids in many regions of Ukraine were attacked by hackers, leading to large-scale power outages in the country. It was also the first large-scale power outage event triggered by information attacks in the world. How reliable are these networks? Will some insignificant potential accidents lead to the collapse of the entire network system? Can these networks function normally in the event of serious natural disasters or sabotage by hostile forces? These are the problems that the invulnerability research on complex networks must face. With the rise of complex network research as one of the most important research issues concerning complex networks, the invulnerability of complex networks has become an extremely important and challenging frontier topic in scientific research [82].

At present, invulnerability has different definitions in different research fields, but in general, network invulnerability considers the network's ability to continue to maintain functions after node or edge failures under certain destruction strategies. This kind of damage may originate from a random failure within the network or from a deliberate attack outside the network. To clarify the problem, we give the following definition of network invulnerability.

Definition 1 Network invulnerability broadly refers to the network's ability to maintain its functions when nodes or edges in the network experience natural failures or are subject to intentional attacks.

There may be many factors that affect network invulnerability, such as the reliability of network components, the number of backups, the number of tasks undertaken by the network, the routing strategy of the network, the maintenance and support capability of the network, and the efficiency of network operation and management. However, the most fundamental factor affecting network invulnerability is topology. We can then define it as narrow invulnerability.

Definition 2 Network invulnerability narrowly refers to the ability of network topology to maintain connectivity when nodes or edges in the network fail naturally or are attacked intentionally.

4.1 Measurement of network invulnerability

Network invulnerability research is mainly based on three theories: graph theory, statistical physics, and characteristic spectrum. Common metrics in different directions are shown in Table 1.

Table 1 Measurement of network invulnerability in three theories

Category	Indicator	Review
Graph theory	Connectivity Toughness Integrity Tenacity Scattering number Coefficient of expansion Algebraic connectivity	Graph theory-based network invulnerability usually has high computational complexity. It is unrealistic and unscientific to measure the invulnerability of complex networks with huge scales and uncertain connection relationships.
Statistical physics	Network invulnerability of different attack strategies Seepage problems in generalized stochastic networks Network invulnerability with the repair mechanism Network invulnerability considering degree correlation condition Network invulnerability of the local world evolution model	While adapting to the current situation of the huge scale of network complexity, it also greatly expands the vision of the research on the resistance of complex networks, and relevant achievements are concentrated in the research fields of network learning, network propagation, network synchronization, etc.
Characteristic spectrum	Natural connectivity Helmholtz free energy of network Physical implications of natural connectivity	It contains a lot of network topology information. Derivation and analysis of the network characteristic spectrum are helpful to deepen our understanding of some properties and behaviors of the network.

Graph theory is one of the most active branches of combinatorics, and there are many graph invariants used to depict the invulnerability of a graph. Among them, the node connectivity and edge connectivity of a graph is the first invulnerability parameters used to carve a graph. They are the minimum number of points and edges that need to be removed to make a graph disconnected or trivial. However, they only consider the difficulty of network destruction and not the degree of network destruction. To overcome this deficiency, many indicators have been put forward.

The toughness of graphs was first proposed by Chvátal [83] to study the Hamilton property of graphs. The integrity of graphs is inspired by communication interruption [84]. It not only considers the difficulty of network destruction but also the scale of the largest communication chip after destruction. Graph adhesiveness [85] not only considers the difficulty of network destruction but also the scale of the largest connected piece and the number of connected pieces after the network is destroyed, which is a more detailed invulnerability measure [86]. Scattering numbers were originally proposed by Jung to study maximum non-Hamilton graphs [87], which is a variation of toughness. Zhang et al. [88] proved that the calculation of scattering numbers is an NP-complete problem. The expansion graph was first proposed by Bassalygo and Pinsker [89] in 1973, and then Pinsker [90] proved the existence of the expansion graph. The initial motivation for proposing the expansion graph is to build a robust network (telephone network or computer network) with economy and no bottleneck. Fiedler found that the minor eigenvalue of the Laplace matrix can be used to measure the connectivity of the network, and thus it is called algebraic connectivity [91]. However, these indicators are NP-complete problems, which usually have high computational complexity [92].

In recent years, the focus of network research has gradually shifted from studying the precise properties of small-scale simple networks to studying the statistical properties of large-scale complex networks. Many methods of statistical physics have been widely used in the research on complex networks. Cohen et al. [93] transformed the network invulnerability problem into the seepage problem in the generalized random network [94] and studied the invulnerability of the complex network analytically [95] by using the seepage theory, that is, the node normally corresponds to the node occupied in the seepage problem, and the node failure corresponds to the node vacancy in the seepage problem. Chi [96] studied the critical removal ratio of the Barabasi-Albert (BA) scale-free network model, Watts-Strogatz (WS) small world network model, and Erdos-Renyi (ER) random network models under the repair mechanism and the topology changes of complex networks before and after repair. Vazquezl et al. [97] studied the invulnerability of complex networks considering degree correlation and proposed a new critical condition for network collapse considering degree correlation. Sun et al. [98] also studied the invulnerability of the local world evolution model. The method based on statistical physics has injected new vitality into the research on the destructibility measurement of complex networks, which not only adapts to the present situation of the huge complexity of networks but also greatly expands the vision of the research on the destructibility of complex networks.

In addition to the above two research methods, researchers began to focus on using the characteristic spectrum information of the network to describe the topology of the network and estimate some functions and behavioral attributes of the network, which also accumulates a certain number of research results. The characteristic spectrum information of the network is used to describe the topology of the network and estimate some functions and behavioral attributes of the network. The derivation and analysis of the network characteristic spectrum will help us deepen our understanding of some properties and behaviors of the network. Among them, natural connectivity proposed by Wu et al. [92] is a new network invulnerability measurement method based on the network adjacency characteristic spectrum, which has attracted wide attention due to its clear physical connotation, simple mathematical form, low computational complexity, and stable problem adaptability.

4.2 Cascading effect and its impact on invulnerability

Under the influence of various internal and external factors, huge networks are very prone to failure. Due to the complexity of network structure and function, these failures are likely to cause cascading effects that will lead to disastrous consequences. Some examples are the power outage in the United States on August 14, 2003, and the power network collapse in southern China in 2008. Similar catastrophic events occur frequently in infrastructure networks. With the rapid development of the economy and society, the loss resulting from such catastrophic accidents will become serious.

Cascading effect refers to the failure of some nodes due to the coupling between them and the initial failure node, which eventually leads to the collapse of a considerable number of nodes in the network, even the entire network. In the real world, most networks will bear a cer-

tain load, including material, energy, or information. This requires nodes (edges) to have a certain load processing capacity. If the load allocated to nodes (edges) exceeds their processing capacity, the nodes (edges) will fail due to overload. The load on the failed node (edge) will be reallocated to other good nodes (edges) according to a certain allocation strategy, which may lead to a new round of node (edge) overload failures. This process is called cascading failure, and it continues until the load on the network is stable. At present, the main models for studying network cascading failures, include the sandpile model, CASCADE model, ORNL-Pserc-Alaska (OPA) model, and load capacity models. In these models, at the initial time, each node (edge) will be given a certain load and maximum load handling capacity (also known as capacity), and the load of the failed node will be redistributed according to the corresponding theoretical principles. The preliminary analysis of the cascading failure model will reveal that there are three main factors affecting the cascading failure, namely, the initial load, capacity, and load-sharing strategy. Reasonable modeling of these three points is the key to studying cascading failures. The model of network cascading failure is shown in Table 2.

Table 2 Cascading failure model

Cascading failure model	Brief introduction
Load capacity model	When encountering some accidental failure or intentional damage, a node in the network will exceed the limit capacity and cause failure, which will then lead to the overload increase of other nodes or connections and cause failure until the entire network is restabilized [99].
Sandpile model	Assume that for sand in the sand pile, the sand surface gradually becomes steeper with the gradual increase of sand and the probability of a large area collapse of the sand pile increases [100].
OPA model	This model is based on the power grid with increasing energy demand. It can summarize the dynamic evolution process of the power grid, the engineering response process of system failures, and the continuous updating process of generation capacity. At the same time, it defines two types of cascading failure types, each with different dynamic characteristics [101].
CASCADE model	The model has two assumptions: for the nodes, the initial load is given randomly, and each node fails according to random probability; when the load of a node exceeds the limit capacity, it causes the node to redistribute its load so that other nodes in the network can obtain an equal amount of load [102].

Cascading effects in complex giant systems can affect the invulnerability of those systems. In recent years, with the robustness of these systems becoming increasingly important, the research related to the invulnerability and vulnerability of complex networks has developed vigorously [103−105]. Cascading effects play a more important role in the study of destructiveness measurements in dynamic processes. Albert [106] proposed the node importance evolution model under the overload mechanism. In this model, the node importance evolves gradually as the load redistribution caused by node failure in the network leads to a constant change in node load. The importance of the node is measured by the average vibration degree of the surrounding node load caused by the node failure within the load redistribution range.

4.3 Main methods for invulnerability optimization research

The ultimate goal of studying complex anti-destructive problems is to guide and assist the topological structure design of real-world networks and improve the anti-attack capability of network systems. Destructibility optimization of complex networks is used to solve this problem. Based on an effective evaluation of network destructiveness, to significantly improve the destructiveness of spatial information networks, many researchers have established a destructiveness optimization model based on new destructiveness measures, solved the model using intelligent algorithms, and obtained a more robust network structure. There are many ways to study invulnerability optimization, which can be divided into three categories: constructing the optimal network by analysis, optimizing invulnerability by edge augmentation, and optimizing invulnerability by edge reconnection. The relevant studies are shown in Table 3.

Table 3 Typical research on three kinds of optimization methods

Optimization method	Typical research
Constructing the optimal network by analytical method	Valente et al. [107] studied the optimal destructive network under random failure and intentional attack strategies. They analytically deduced the critical removal ratio and concluded that the optimal destructive network in the face of random failures or intentional attacks is a bimodal network with a fixed number of network edges (i.e., only two degrees for all nodes in the network).

Continued

Optimization method	Typical research	
	Paul et al. [108] also studied the robustness of networks with varying degrees of distribution. They analyzed and compared the critical removal ratios for scale-free, bi-power, and bimodal networks, and concluded that the best network with both random failures and intentional attack resistance is one with a bimodal distribution.	
	Tanizawa et al. [109] studied the robustness of networks when random failures and deliberate attacks work together. They stated that a network attack is usually an "attack wave" composed of random failures and intentional attacks, and controlled the proportion of random failures to deliberate attacks by adjusting parameters.	
Optimizing destruction by edge enhancement	Beygelzimer et al. [110] studied network invulnerability optimization results under different edge addition strategies. They found that moderate edge augmentation can effectively improve the vulnerability of scale-free networks to intentional attacks, especially when fewer nodes are attacked. When the number of attacked nodes is too large, the edge-increasing strategy has little impact on destructiveness.	
	Zhao et al. [111] determined whether new edges are added between nodes with a high or low degree of traffic by adjusting the size of parameters and compared the results of the corresponding network invulnerability optimization. They found that adding a new edge at a small degree node can effectively improve the network's ability to resist intentional attacks.	
	Cao et al. [112] studied an edge-increasing strategy for network invulnerability optimization considering cascade failures. They found that both high-median and low-polarization edge-increasing strategies can effectively improve the network against cascade-invalid network attacks.	
Optimizing destruction by edge reconnection	Non-guaranteed reconnection optimization	Liu et al. [113] studied the effect of network node degree value on network invulnerability in non-guaranteed reconnection optimization.
		Netotea et al. [114] used a genetic algorithm to optimize the robustness and efficiency of the network for heavy reconnection.
		Priester et al. [115] studied the trade-off optimization of network resilience against random failures and intentional attacks without guaranteed reconnection optimization.
	Guaranteed reconnection optimization	Peixoto et al. [116] optimized the seepage properties of a classical network based on a block model and found that the "core-periphery" structure of the network helps to improve the network's ability to resist random failures.
		Herrmann et al. [117] studied the topological structure of the optimal destructive network obtained by optimizing the measure with preserved reconnection.

An optimal network is constructed by using an analytic method. Due to its rigorous mathematical derivation process and clear theorem, the invulnerability of the optimized network obtained by this method is usually optimal. However, the disadvantage is that the analytic method often requires making numerous necessary simplification assumptions about the network, and the mathematical derivation is more difficult and unsuitable for application and popularization. Yet reconstructing a network is not suitable for the topological design of a real network because large-scale complex network systems, such as the Internet, have evolved over a long period and cannot be completely redesigned. It is also impossible to build a real network entirely on the principle of optimum destructibility while ignoring its other functional properties.

Optimization by adding edges is finding the optimal edge addition strategy based on given resources to maximize the destructibility of existing networks. However, in practical applications, adding edges often incurs a high cost. Furthermore, this optimization method does not help us find the topological characteristics of the optimal destructive network.

Structural adjustment using edge reconnection is also an important means of optimizing network destructibility. Edge reconnection optimizes network invulnerability. In short, it maximizes network invulnerability by adjusting network connectivity without changing network averages based on a given network. The average degree of a fixed network is essentially the number of edges in the network as a resource constraint. Destruction optimization is the only way to find the topological information that maximizes network destructibility.

The nodes and edges in a network can be considered cost resources for building the network, and considering the carrying capacity of nodes, changing the degree of nodes in a network often costs more than changing the network's connectivity. Analytic methods are not suitable for popularization and the results may not match the reality. Edge-adding methods often increase costs in real life. Therefore, it is of great theoretical and practical significance to study network structure optimization based

on edge-reconnection methods.

Network invulnerability analysis can help analyze the impact of various behaviors on the network from the perspective of network structure, or provide evaluation criteria for improving network robustness. In the next section, the network disintegration process and optimal strategy will be analyzed from the perspective of attackers, and the network invulnerability can be used as one of the indicators to evaluate the disintegration effect.

5. Network disintegration analysis of complex systems

Complex network theory has been continuously developed and refined and is widely used in complex systems, such as power, social, transportation, and biological systems. In general, networks, such as transportation, power, and logistics networks, are beneficial. For these beneficial networks, we hope to ensure the continuous, stable, and effective maintenance of their functions using planning and design, optimal control, defense, and protection.

However, networks can also be harmful. The most typical example is a terrorist organization network [118−120]. Since the 1960s, international terrorist activities have become increasingly rampant, and terrorist organizations have evolved from their traditional hierarchical structure to a network structure. How to effectively dismantle a terrorist network has become a common problem that all countries face. Another typical example is a disease transmission network [121]. In recent years, COVID-19, SARS, Ebola, avian influenza, and other infectious diseases have emerged one after another, causing huge loss to human society. How to effectively stop the propagation of infectious diseases is a difficult task for global public health. In the military context, enemy combat networks [122] are also harmful. System destruction warfare is the destruction of the enemy's entire combat network by focusing on the key nodes of the combat system network under the guidance of the system combat ideology. This causes the disordered structure of enemy forces and the disjointed structure of operational procedures. In addition, criminal networks [123,124], drug trafficking networks [125], nuclear material smuggling networks [126], cancer cell proliferation networks [127], rumor propagation networks [128], financial crisis networks [129], etc., are specific types of harmful networks. How to effectively disintegrate these harmful networks by means of blocking, jamming, immunization, blockade, and isolation has become an urgent problem to be solved.

5.1 Network disintegration problem

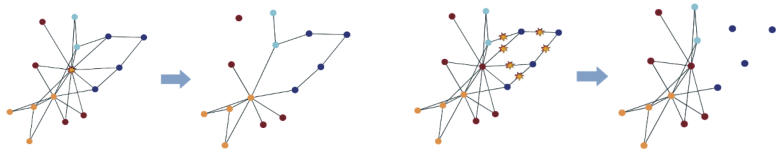
5.1.1 Types of network disintegration

The problem of network disintegration can be classified in different ways. Following the relevant research published so far, this paper classifies network disintegration from three perspectives: the target object of disintegration, the type of disintegration network, and the constraints of disintegration. The specific classification is shown in Table 4. It should be noted that the problem types corresponding to these three division perspectives are not independent of each other; that is, one network disintegration problem will belong to different problem types from different division perspectives.

Table 4 Classification of network disintegration problems

Perspective	Type	Related work
Target object of disintegration	Node-based	[130−134]
	Edge-based	[135−138]
Type of disintegration network	For homogeneous networks	[132−139]
	For heterogeneous networks	[130,140]
	For multilayer networks	[134,141,142]
Constraints of disintegration	Under the homogeneous cost constraint	[130,132,135,140]
	Under the heterogeneous cost constraint	[133,134,140]

The target object of disintegration can be divided into node-based and edge-based network disintegration. Node-based network disintegration takes a node as the object of attack disintegration, where it is generally believed that after a node is attacked, the node and the edges related to it will fail simultaneously, as shown in Fig. 2(a). Edge-based network disintegration considers the edge as the object of attack. When the edge between nodes is attacked, the nodes remain normal and only the edge fails, as shown in Fig. 2(b). Due to the difficulty and high cost of destroying nodes, edge-based attacks often occur in networks like transportation networks and power networks.



(a) Node-based disintegration (b) Edge-based disintegration

Fig. 2 Network disintegration problem with different objects

From the perspective of network types, network disintegration can be divided into three types: the disintegration of homogeneous networks, heterogeneous networks, and multilayer networks. From the previous review, research based on homogeneous networks is relatively mature from the perspectives of disintegration strategy and network robustness [143]. Yet there is relatively little research on heterogeneous network disintegration. Heterogeneous networks are usually regarded as homogeneous ones, ignoring the heterogeneous characteristics of nodes and links to facilitate the direct application of existing methods in the analysis and evaluation of networks, resulting in the loss of network information. The same situation has occurred in research on multilayer networks. A multilayer network can model complex systems with hierarchical structures. The existing research on multilayer networks has mainly focused on the structure characteristics, dynamics mechanism, cascading failure mechanism, and so on, and has been gradually applied to the social and economic systems. In general, both heterogeneous networks and multilayer networks have broadened research prospects.

Regarding the constraints of disintegration, network disintegration can be divided into homogeneous cost constrained and heterogeneous cost constrained network disintegration. Network disintegration with homogeneous cost constraints considers that the costs of destroying different nodes are the same to achieve the lowest cost and lowest network efficiency simultaneously. However, the difficulty of attacking nodes is often different, resulting in different costs. Besides, the resources that can be invested are limited. Therefore, it is more realistic to study the problem of network disintegration under resource constraints. This kind of network disintegration problem is the network disintegration problem with heterogeneous cost constraints.

In addition to the types of problems outlined above, there are a few other types of network disintegration problems. For example, Bellingeri et al. [144] has carried out attack disintegration of weighted networks, Yan et al. [145] proposed disintegration strategies for supernetworks, and Deng et al. [146] studied network disintegration strategies with spatial information.

5.1.2 Mathematical representation

The core of the network disintegration problem is how to determine the set of nodes (edges) to be removed under specific constraints and various disintegration objectives, that is, to find the key of the network system. Its mathematical essence is a combinatorial optimization problem.

$G=(V,E)$ denotes the target network, where $V=\{v_1,v_2,\cdots,v_N\}$ is the set of nodes, $E=\{e_1,e_2,\cdots,e_W\}\subseteq V\times V$ is the set of edges, $N=|V|$ is the number of nodes, and $W=|E|$ is the number of edges. The network disintegration entails node removal and edge removal. Let $\hat{V}\subseteq V$ be the set of nodes to be removed, $\hat{E}\subseteq E$ be the set of edges to be removed, and $\hat{G}=(V\backslash\hat{V},E\backslash\hat{E})$ be the network after disintegration. In general, we assume that all edges associated with a node are removed after the node is removed. The node disintegration strategy is denoted as $X=\{x_1,x_2,\cdots,x_N\}$, where $x_i=1$ when $v_i\in\hat{V}$, or $x_i=0$ otherwise. The edge disintegration strategy is denoted as $Y=\{y_1,y_2,\cdots,y_W\}$, where $y_j=1$ when $e_j\in\hat{E}$, or $y_j=0$ otherwise. The network disintegration solution is denoted as $I=(X,Y)\in\Omega$, where Ω presents the constraints. $\Phi(I)$ is the objective function of network disintegration. Therefore, the network disintegration problem can be described as the following general mathematical model:

$$\begin{aligned}&\max(\text{or}\min)\Phi(I)\\&\text{s.t. } I=(X,Y)\in\Omega.\end{aligned}\tag{4}$$

The optimal network disintegration strategy differs depending on the disintegration objectives [147,148]. In addition, the choice of objective function directly determines the computational complexity. After the network is disrupted, several subgraphs are usually formed. A subgraph can be called a component if it contains a link between any pair of nodes. Common network disintegration objective functions include the following measures:

(i) The number of connected pieces after network disintegration [149−151]:

$$\max\Phi(I)=L;\tag{5}$$

(ii) Size of the maximum connected slice after network disintegration [152−156]:

$$\min\Phi(I)=\max\{n_1,n_2,\cdots,n_L\};\tag{6}$$

(iii) Herfindahl-Hirschman index after network disintegration [149]:

$$\min\Phi(I)=\sum_{l=1}^{L}\left(\frac{n_l}{N}\right)^2;\tag{7}$$

(iv) Information entropy after network disintegration [157,158]:

$$\max \Phi(I) = -\sum_{l=1}^{L} \frac{n_l}{N} \ln \frac{n_l}{N}; \tag{8}$$

(v) The efficiency between node pairs after network disintegration [153]:

$$\min \Phi(I) = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \tag{9}$$

where d_{ij} presents the shortest path length between nodes v_i and v_j;

(vi) Natural connectivity degree after network disintegration [133]:

$$\min \Phi(I) = \ln\left(\frac{1}{N} \sum_{i=1}^{N} \mathrm{e}^{\lambda_i}\right) \tag{10}$$

where λ_i is the characteristic root of the adjacency matrix after network disintegration.

5.2 Network disintegration methods

Network disintegration has been proven to be an NP-complete problem. Due to its importance and challenges, it has been widely studied in operations research, network science, computer science, and other disciplines and has made important progress. Early studies on network disintegration mainly started from the perspective of solving mathematical programming models. Since the end of the last century, with the rise of complex network research, network disintegration methods based on the centrality index and heuristic algorithm emerged. In recent years, the latest achievements of evolutionary algorithms and reinforcement learning have been applied to the study of network disintegration. Next, this paper summarizes the research progress of complex network disintegration from the aspects of mathematical programming, centrality index, heuristic algorithm, reinforcement learning, and so on. The typical approaches at each stage, along with the pros and cons, are shown in Table 5.

Table 5 Classification of network disintegration methods and their typical methods

Classification	Typical method	Advantages and disadvantages
Methods based on mathematical programming	Branch and bound method Mixed iterative rounding method Univariate decomposition Dynamic programming ⋮	The optimal network disintegration scheme can be obtained. It has high requirements for the objective function and constraint conditions and is not applicable to large-scale networks.
Methods based on the centrality index	Degree centrality *k*-core centrality Intermediate centrality Proximity centrality ⋮	Simple and easy to implement, but the important node set under a single index is not necessarily the optimal node removal set.
Methods based on heuristic algorithms	Tabu search algorithm Genetic algorithm Simulated annealing algorithm Random greedy adaptive search algorithm ⋮	A good network disintegration scheme can be obtained that has high robustness and wide applicability. The time complexity is high.
Methods based on reinforcement learning	Q-learning Deep Q-network (DQN) ⋮	It has nothing to do with specific knowledge and rules and is applicable to all kinds of problems; it is not interpretable.

5.2.1 Network disintegration method based on mathematical programming

As the nature of the network disintegration problem is a combinatorial optimization problem, we can find the optimal network disintegration strategy by solving the mathematical programming model. Arulselvan et al. [159] proposed a linear integer programming model to solve the network disintegration problem, taking the number of connected node pairs as the objective function. On this basis, Di Summa et al. [160] used the branch-and-bound method to make the model solvable in polynomial time. It is worth noting that the complexity of the triangle inequality constraint in the integer programming model above is $O(n^3)$, restricting its use to small-scale networks. To overcome this limitation, Veremyev et al. [161] proposed a compact constraint form, which reduces the complexity to $O(n^2)$. Based on mathematical programming, the optimal network disintegration scheme can be obtained. However, it has high requirements for the objective function and constraint conditions and is not

applicable to large-scale networks.

5.2.2 Network disintegration method based on centrality index

Evaluating the importance of nodes is a key task in complex network research. According to the scale and research purpose of the network, an index can be defined to quantitatively measure the importance of each node in the network. Common indicators of the importance of nodes include the static indicators of a network, such as the degree of nodes, betweenness, and clustering coefficient. Holme et al. [162] handled network disintegration based on initial degree (ID) network disintegration based on initial betweenness (IB), a recalculated degree (RD) attack based on the current network node degree, and a recalculated betweenness (RB) attack based on the number of nodes in the current network. In addition, some scholars have proposed more targeted node importance indicators [163]. Node importance-based disintegration strategy ranks the importance of nodes and gives priority to attack-important nodes in the network. This kind of disintegration strategy has strong applicability, and can quickly identify the attack sequence of nodes, and the disintegration effect is significantly better than a random disintegration strategy.

5.2.3 Network disintegration method based on heuristic algorithm

The disintegration strategy based on the heuristic algorithm first numbers the nodes of the network and uses binary string to represent the current state of the network. Next, the network capability evaluation index is used as the objective function of algorithm optimization. Then the specific parameters and termination conditions of the algorithm are set. Finally, according to the optimal solution of the algorithm output, the network disintegration strategy is obtained. Common heuristic algorithms include the genetic algorithm, the tabu search algorithm, and the particle swarm optimization algorithm. These algorithms have good global optimization ability and universality and can be used to solve large-scale network disintegration problems. Yu et al. [164] proposed a directed network disintegration strategy based on a tabu search algorithm, which can effectively disrupt terrorists' social networks. Lozano et al. [165] proposed a network attack strategy based on an artificial bee colony algorithm, which showed obvious advantages compared with other methods. Faramondi et al. [166] used evolution algorithms to find key nodes in the network, providing decision support for the protection of network infrastructure. However, the heuristic algorithm-based disintegration method often consumes large computing resources and takes a long time to calculate, and the superiority of the algorithm is difficult to guarantee. In addition, the calculated disintegration strategy can only identify the node set that needs to be attacked and cannot obtain the disintegration order of nodes in the set.

5.2.4 Network disintegration method based on reinforcement learning

With the rapid development of artificial intelligence technology, a combinatorial optimization method based on reinforcement learning has been widely applied to all kinds of problems, showing such advantages as rapid solution speed and strong model generalization ability [167]. Some scholars have studied the network disintegration strategy through reinforcement learning. Yan et al. [145] described the disintegration problem of hypernetwork as a node sequence decision problem. The author first proposed a representation learning method of hypernetwork, where nodes and hypernetworks are represented by vectors as action and state space in deep reinforcement learning. Then a series of small-scale supernetworks are simulated and their disintegration strategies are explored in the deep reinforcement learning model. Finally, the optimized model is applied to hypernetwork disintegration in the real world. Fan et al. [168] effectively solved the disintegration problem of large-scale random networks by introducing a virtual node and using the vector representation of the virtual node as the state vector of the current network for training in the deep reinforcement learning model based on network representation learning. The key to this kind of disintegration strategy is to represent the current state of the network and the disintegration action of the network as the data type, which is convenient for the input model to learn, and then establish a deep reinforcement learning environment according to the evaluation index of the network disintegration. However, this approach lacks interpretability.

5.3 Directions for further research

Although complex network disintegration is not new for us, and considerable research has been accumulated, there are still many problems that need to be further studied and solved in the description and research of complex systems in reality. The future research direction will be discussed according to the network type and disintegration model.

5.3.1 Network type

In the future, the network of research will go from undirected to directed, from unweighted to weighted, from single-layer to multilayer, and it will include consideration of spatio-temporal properties.

First, the research on network disintegration has mainly focused on undirected networks and has seldom considered the influence of directed edges on the disintegration effect. In fact, many networks in the real world

are directed, such as one-way streets in the traffic network and accusatory relationships in the combat network. Within such research, how to effectively identify the key nodes (edges) in the directed network according to the distribution of directed edges in the network remains a noteworthy problem. Second, the research on network disintegration has also focused primarily on unweighted networks and thus assumed that all nodes or edges in the network are homogeneous. In fact, networks in the real world are usually weighted networks. For example, different nodes in a terrorist network have different degrees of harm, and the traffic flow of different roads varies in a traffic network. Third, complex relationships, such as coupling, dependence, and cascading, among multilayer networks are rarely considered. Multilayer network is a hot topic in complex network research. However, owing to the complex structural correlation between the layers of multilayer networks, the disintegration of multilayer networks will remain a challenging problem worth paying attention to in the future. Fourth, the research on network disintegration is assumed to be static and deterministic, and the geospatial location of nodes (edges) is rarely considered. However, many networks in the real world are geospatial networks, which are dynamic and time-varying. However, many networks in the real world are geospatial networks, which are dynamic and time-varying. For example, the failure of a power network is related to the shortest path change caused by geographical distribution, and the network structure of an unmanned aerial vehicle (UAV) cluster will evolve with the change of relative position over time.

5.3.2 Disintegration model

In the future, the network disintegration model will move from a single objective to multiple objectives, from simple constraints to complex constraints, from structure to function, and from a unilateral perspective to multiple perspectives.

First, it is a challenging problem to find an effective network disintegration strategy considering multiple objective functions simultaneously, such as topology indicators or performance indicators. Second, we must consider time, cost, information, or other specific constraints when formulating a network disruption plan. Third, in addition to damaging the network structure, the purpose of disrupting the network can also be achieved by interfering with the dynamic behavior of nodes or edges, for example, by inducing signal interference to destroy the synchronization of the enemy UAV cluster. Fourth, both sides participate in the network disintegration process, and its effect is not only related to the disintegration strategy but also to the defense strategy. In the game of attack and defense, the original optimal strategy may become suboptimal or completely unfeasible.

In this section, we focus on how to attack a malicious network from the perspective of an attacker. In the next section, we will evaluate the performance of the network from the overall process from destruction to recovery, that is, the resilience analysis of complex systems.

6. Resilience analysis of complex systems

The complex system is a kind of comprehensive, dynamic, and chaotic nonlinear system. However, internal failures and external events are inevitable during its operation, which has a strong negative impact on the normal operation of the complex system, causing occasional interruptions [169]. Hence, a natural question is how to reduce the impact of disturbances, ensuring that a complex system can continue operating when disturbances occur and restore the system to a normal and stable state in time.

A common property of many complex systems is resilience, that is, the ability of the system to react to internal failures and external events by resisting, absorbing, and/or reorganizing to maintain its functions [170]. According to existing research, the resilience concept can deal with these issues by providing a new indicator to analyze the ability of complex systems to provide reliable services, which includes the system performance before and after a disturbance. The word resilience can be traced back to the 17th century from the Latin term resiliere. In 1973, Holling introduced the concept of ecosystem resilience (trend to multiple balance) [171] to define the characteristics of the stable state of the ecosystem, indicating the ability of the ecosystem to withstand damage or maintain balance in the face of changes in the external environment. Subsequently, the concepts of engineering system resilience (trend to single balance) [172] and social-ecological resilience (trend to adaptive cycle) [173] were put forward. Currently, the fields of resilience include cities [174], infrastructure [175,176], disaster reconstruction [177], economics [178], management [179], and military [180]. Resilience has now become a tool for advanced development concepts and planning research regarding complex systems. In other words, it is an important indicator for measuring sustainable development in various fields.

As one of the most powerful tools for analyzing large-scale complex systems, the complex network is an effective method for describing complex systems. Complex networks originated from graph theory and topology, and then Erdos [181], Watts [182], Barabasi [183], and others further deepened this concept, resulting in a series of research achievements in different disciplines. The complex network theory and methods can describe the internal structure of complex systems and their interrelationships in detail, making them the most likely theory and methods, respectively, to break through the analysis of complex system resilience.

This section introduces the research hotspots in analyzing the resilience of complex systems with the help of complex networks. To better describe the resilience research of complex systems, this paper proposes a four-part (4E) framework within the concept of the complex network: establishing the dimension of complex system resilience, evaluating the resilience of complex systems, electing the key nodes or links for complex systems resilience, and enhancing the resilience of complex systems. The 4E framework is shown in Fig. 3.

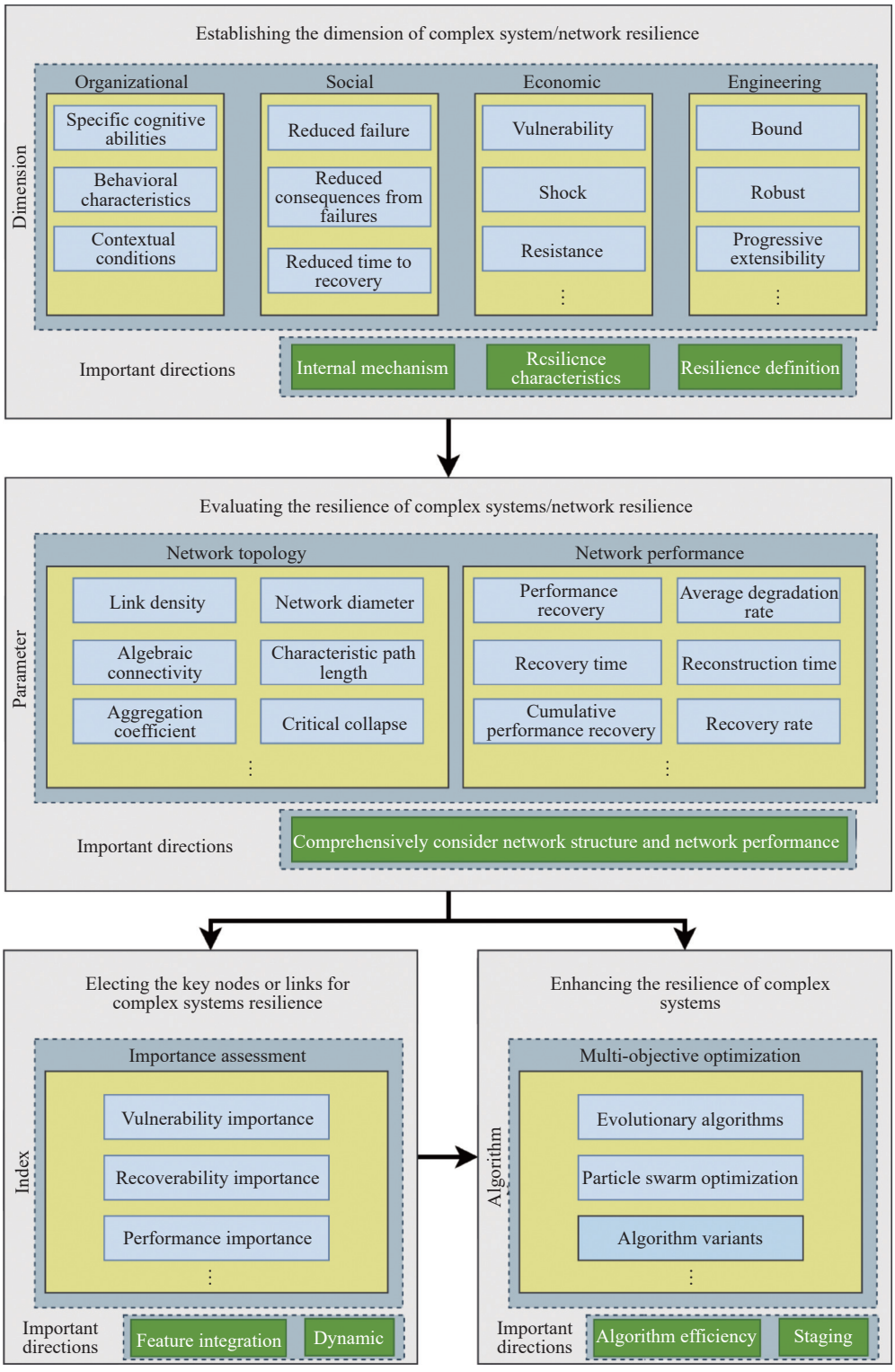


Fig. 3 4E framework for complex system/network resilience research

6.1 Establishing the dimension of complex system/network resilience

The first step of complex systems resilience research is to accurately analyze the resilience characteristics of complex systems and establish the dimension of complex system/network resilience. The main purpose of this step is to solve the problem of determining the resilience characteristics of complex systems. As different complex systems have different characteristics, the dimensions for evaluating their resilience are different. The following is an introduction to the dimensions of the resilience of complex systems from the organizational, social, economic, and engineering system domains [184]. The emergence of organizational resilience is mainly aimed at meeting the needs of companies, governments, and other institutions to respond to changes in the work environment. According to Lengnick-Hall [185], the three core elements for developing organizational resilience are specific cognitive abilities, behavioral characteristics, and contextual conditions. The emergence of social resilience mainly concerns changes in individuals, groups, and communities under extreme events. Bruneau [186] proposed a conceptual framework to define community resilience including three dimensions: reduced failure, reduced consequences of failure, and reduced time to recovery. The emergence of economic resilience mainly regards fully capturing the possible reactions of regional economies to major recessions [187]. Martin [188] believed that the study of regional economic resilience must consider the five dimensions of vulnerability, shock, resistance, robustness, and recoverability. The scope of engineering resilience is relatively extensive in comparison to other domains. Woods [189] explained and defined the resilience of systems around four basic concepts—bound, robust, progressive extensibility, and architectures for sustainable adaptability—to solve the problem of what resilience is and how to engineer it in complex adaptive systems.

To sum up, if a breakthrough is made in establishing the dimension of complex system/network resilience, it is necessary to have a deep understanding of the internal mechanism of the complex system. Specifically, researchers should explore its relationship with typical resilience characteristics, such as resistance, recovery, and adaptability, and give a clear definition of the resilience of the complex system.

6.2 Evaluating the resilience of complex systems/network resilience

The second step of complex system resilience research is to adopt appropriate methods to evaluate the resilience of complex systems based on the above resilience dimensions. The existing research has mainly evaluated the resilience of complex systems from two aspects: the network topology and the network performance within the concept of complex networks. Research concerning network topology has mainly been based on the statistical indicators or their variants in complex network theory and different network structures to evaluate the resilience of complex systems. Gao et al. [190] argued that the research on network resilience is mainly based on three factors: network structure, network dynamics, and the failure mechanism. Meng et al. [191] used link density, algebraic connectivity, and the aggregation coefficient to measure the number of links, fault tolerance, and redundancy of the network to evaluate the resilience of the power system. Based on the topological structure of an urban water distribution network, Pandit et al. [192] proposed a resilience metric that integrates six network attributes: the network diameter, characteristic path length, dominance, critical collapse, algebraic connectivity, and the network coefficient. Then he conducted a resilience evaluation of the urban water distribution network. Research concerning network performance has referred to dividing the process of assessing resilience into different stages and states according to changes in its performance. Omer et al. [193] defined the resilience of a submarine communication cable network by conducting a comparison of the flow of information transmission before and after the network is damaged or interfered with. Pan et al. [194] constructed a modeling framework based on the origin destination-grid network and provided a brand new performance metric for transportation network resilience analysis based on grid capacity and also developed two resilience assessment models based on performance recovery, recovery time, cumulative performance recovery, and cumulative performance without precise recovery time.

To sum up, existing research has often evaluated system resilience based on the network structure or the network performance, but topology parameters cannot fully reflect the actual quality of complex systems/networks. At the same time, performance parameters cannot comprehensively reflect the network's ability to withstand and recover from attacks or disturbances. In future work, both network topology parameters and performance parameters need to be considered to evaluate complex systems/networks comprehensively and effectively. Only in this way can we effectively provide an objective function for complex system/network resilience optimization and thus support the design of resilience of complex systems/networks.

6.3 Electing the key nodes or links for complex systems resilience

The third step of complex system resilience research is to allocate limited resources to nodes or links that have a significant impact on system resilience. Therefore, the impact of changes to the state of nodes or links on the system performance must be considered in complex system resilience design, that is, the key nodes or links must be selected. The concept of key nodes/links was first proposed by Birnbaum to define reliability importance, key importance, and structure importance [195]. This content has been extensively studied in the field of complex systems resilience. The following is an introduction to electing the key nodes or links for complex systems resilience from the organizational, social, economic, and engineering system domains. For the organizational system, Ruiz-Martin et al. [196] represented people as nodes in the network and their communication relations as links and then studied what happens in the communication structure of the organization if a person disappears or if only communications are broken, which provides a cost-effective way to analyze organizational resilience. For the social system, Blagojevic et al. [197] advanced a method based on Sobol's indices and a heuristic upper and lower bound search to measure the importance of vulnerability and recoverability of components for disaster resilience of communities. For the economic system, Ye et al. [198] applied the network analysis to evaluate the resilience of the economic network in Guanzhong Plain City Cluster and examine the impact of network structural properties on economic resilience. The results showed the difference between core and peripheral cities and suggested that strengthening the connection between the two can improve economic resilience. For engineering systems, considering the dynamic properties of road traffic and day-to-day disruptions, Gauthier et al. [199] proposed a methodological approach based on resilience stress testing and a dynamic mesoscopic simulator, the purpose of which is to identify and rank the links that are most critical to the overall performance of the road network.

To sum up, research on the selection of key nodes or links to achieve the resilience of complex systems is still at the preliminary stage. At present, it focuses on the performance loss and recoverability of single or combined factors. Hence, the next step is to consider the overall resilience measurement. In addition, the dynamics of complex systems/networks are a factor that cannot be ignored. In future research, key nodes/links should be selected in a dynamic context, because the importance of nodes/links may be different at different time points.

6.4 Enhancing the resilience of complex systems

When multiple nodes or links of a complex system/network are disturbed, the first problem to consider is how determining an appropriate recovery sequence to make the system performance recover quickly and effectively will enhance resilience [200]. As the optimization goal in the study of complex system/network resilience is often unknown, it is essentially a multi-objective optimization problem. At present, multi-objective optimization algorithms based on evolutionary algorithms [201,202], particle swarm optimization [203,204], and their variants have been successfully applied in various fields, and they are all committed to finding a more accurate and uniform Pareto optimal solution set. To reduce the cost of the algorithm, relevant scholars have tried to refine and reduce the Pareto optimal solution set, for example, by designing corresponding recovery strategies [205].

To sum up, the current idea of complex system/network resilience enhancement is to formulate optimization objectives, determine multi-objective optimization algorithms, reduce solution set space, and determine the recovery order. However, the process of complex system operation is extremely complex, and its resilience enhancement should be staged. In the next step of the work, we should not limit ourselves to the optimization goal of maximizing resilience. For example, in the emergency recovery phase of the equipment system-of-systems in the case of strong confrontation, priority should be given to enhanced robustness rather than performance. Only in this way can we meet the operational reality. In addition, developing efficient, fast, and low-cost multi-objective optimization algorithms is another important research direction.

7. Link prediction of complex systems

If the resilience of networks is an important way of defense, the offense is also essential in complex systems, in which link prediction is a typical method.

7.1 Introduction and background

Complex network is a common way to represent connections in a complex system. These connections can be represented graphically as a network where each node is a separate entity and each link denotes a partnership or association between relationships. Due to the difficulty in obtaining a large amount of information within the complex network, there are many hidden relationships among entities that must be uncovered in real applications, especially in many biological scenarios. In addition, complex networks are dynamic; many nodes can be added to the complex network, which usually applies in social net-

works. Complex networks consequently become incredibly sophisticated and dynamic. To deal with the aforementioned problems, we discuss a particular issue known as link prediction. Link prediction is a method to evaluate the probability of generating a link between two nodes by analyzing the known network structure.

We denote $G(V, E)$ as an undirected graph, where V represents a node set and E, a link set. A universal set U contains a total of $\frac{n(n-1)}{2}$ links (total node pairs), where $n = |V|$ denotes the number of total nodes in the graph. $(|U| - |E|)$ links are denoted as non-existing links, and some of these links may appear in the near future [206].

We propose a review of previous approaches for link prediction on complex network graphs based on the previous review [207]. We divide these approaches into various categories [208]. One of them calculates a similarity score between node pairs, where having higher scored pairs implies links between them. Another type of algorithm is based on probabilistic approaches, such as Bayesian and relational models. Dimensionality reduction approaches based on embedding and factorization have been grouped into one category, and several applications have also been researched.

7.2 Similarity-based models

Similarity-based metrics are the most basic metrics in link prediction, calculating a similarity score $S(x, y)$ for each pair x and y. The score $S(x, y)$ is determined by the structural or node properties of the node pair under consideration. Non-observed relationships are scored according to their similarity. The higher-scoring pair of nodes represents the predicted link between them. The similarity measures between each pair may be calculated using many network properties, one of which is structural property. Scores based on this property can be grouped into several categories, such as local or global.

In general, local indices are computed by using information about common neighbors and node degree. These indices take into account a node's immediate neighbors. Examples of such indices are common neighbor [207], preferential attachment [208], Adamic/Adar [209], and resource allocation [210]. Global indices are computed by using the complete topological information of a network. The computational complexities of such methods are higher and seem infeasible for large networks [211,212]. Quasi-local indices have been introduced as a trade-off between local and global approaches or performance and complexity. These metrics are as efficient to compute as local indices. Some of these indices extract the complete topological information of the network. The time complexities of these indices are still fewer than those of global approaches. Examples of such indices include local path index, local random walk index [213], and local directed path (LDP) [214].

7.3 Probabilistic and maximum likelihood models

For a given network $G(V, E)$, the probabilistic model optimizes an objective function to establish a model composed of several parameters. At that point, the likelihood of the presence of a non-existing link(i, j) is evaluated by using conditional probability $P(A_{ij} = 1|\theta)$. Several probabilistic models [215−217] and maximum likelihood models [218,219] have been proposed in the literature to infer missing links in the networks. In addition to structural information, the probabilistic models usually require further information, such as information about the node or edge attributes. It is difficult to extract this attribute information, and parameter tuning is important in these models, which restricts their applicability. Since maximum likelihood methods are complex and time-consuming, these models are not suitable for real large networks [206].

7.4 Link prediction using dimensionality reduction

The curse of dimensionality is a well-known issue in machine learning. To solve the aforementioned issue and use it in the link prediction scenario, several researchers [220,221] have used dimension reduction approaches. Network embedding and matrix decomposition approaches, which are frequently referred to as dimension decomposition methods, have attracted the attention of many authors.

Recently, some network embedding techniques [222−225] have been proposed and applied successfully to the link prediction problem. Perozzi et al. proposed the DeepWalk algorithm, where nodes and truncated random walks are treated as words and sentences [222]. Grover and Leskovec proposed the node2vec algorithm that learns low-dimensional representation by maximizing the likelihood of preserving neighborhoods of nodes [224]. In addition, the Laplacian eigenmaps [223], Isomap [226,227], and logically linear embedding (LLE) [228] are examples based on the simple notion of embedding. These embedding methods are highly sophisticated and have scalability problems. Numerous publications based on link prediction have employed matrix factorization [229−235] and recommendation systems [236]. Latent features that have been extracted have often been used to represent each node in latent space. Additional node/link or other attribute information may be utilized to further enhance the prediction results. In most of the works, non-negative matrix factorization has been used. Some

authors have also applied the singular value decomposition technique [237]. With the development of deep learning, such techniques have also been applied in link prediction and have achieved an excellent performance.

7.5 Applications

A recommendation system in a social network or e-commerce platform is a typical application of link prediction. On the basis of users' previous browsing behavior, such algorithms recommend new friends, accounts to follow on social platforms, and new products on online shopping portals (e.g., interests, preferences, ratings) [236,238−240].

Due to the huge size of a protein-protein network, it is difficult to obtain the relationship between proteins and diseases as it is not only time-consuming but also expensive to do experiments to ascertain those connections. Link prediction plays an important role in this field to predict relationships between proteins and diseases using existing information [241−243].

Collaborating author or reference recommendation is an essential task in bibliographic networks. The recommendation system will predict potential co-authors or references for a researcher according to previous citations, keywords, or other information, which can help the researcher find co-authorships [244−247].

With the transformation of the war system from network-centric warfare to decision-centric warfare, the concept of mosaic warfare has been widely studied and applied. Mosaic war causes originally isolated equipment to interact, which makes the network structure more complex. Owing to the use of high technology, which conceals equipment and causes confusion, comprehensive access to equipment relationships becomes more difficult. Thus, the observed network is biased, and we need to predict the potential links between pieces of equipment [130,247].

8. Attacker-defender game in complex networks

In reality, a defender will not allow an attacker to do damage, and the disintegration and protection of complex systems is interactive. At this point, it is necessary to model the offensive and defensive problems of complex systems in combination with game theory. Due to the dependence of residents on infrastructure, numerous scholars have conducted relevant studies on complex infrastructure systems.

In the following text, we will introduce static and dynamic game models under complete information and incomplete information.

8.1 Complete information static game model

The game model is complete information when players hold the full information of games, like strategies, sequence, and payoff. And when the players act simultaneously, the game can be called a static game.

There is substantial research based on the complete information static game model. Bier et al. studied how defensive resources are allocated in response to an attacker [248]. Feng et al. investigated the protection of multiple chemical facilities by integrating game theory with risk assessment [249]. Li et al. [250] developed a two-person static game model in a complex network, used the largest connected component as a metric function, and investigated the relationship between equilibrium strategies and node degree values as well as the effects of network structure, cost constraints, and cost sensitivity on equilibrium outcomes, and validated them with an airline network. Smart grid operation relies on communications infrastructure support to enable power management and reliable distribution [251,252]. Chen et al. [253] examined the offensive and defensive strategies for grid communication networks and evaluated the performance of the defense mechanism through a two-person zero-sum game model. Fu et al. [254] developed a two-person static game model and analyzed pure and mixed strategy equilibria. Bompard et al. [255] captured the strategic interactions between malicious agents who may be willing to attack power systems and the system operators. Research based on the complete information static game model has mainly focused on the problem of strategy selection or resource allocation in confrontation.

8.2 Complete information dynamic game model

The game model becomes dynamic when there is a sequence of player actions. Some research has been based on the complete information dynamic game model. Brown et al. applied game theory to military strikes and homeland defense and conducted extensive research [256,257]. By analyzing examples such as oil reserves and electric transportation networks, they found that the strategy choices of attackers and defenders under the game model differed from their intuition and emphasized the necessity of game theory for infrastructure protection [258]. They studied the dynamic game model through two-level and three-level programming models to study the dynamic game model. They also analyzed no-defense behavior, protection of critical nodes, and protection of three-quarters of nodes under three defense strategies to determine the optimal attack strategy. Li et al. [259] developed a dynamic game model based on the Stackelberg game where the defender moves first and the largest

connected component of the network is used as a metric function to investigate the effect of the first-mover advantage and network structure on the equilibrium solution. Fu et al. [260] first protected the network through protective or camouflaged behavior; then the attacker took action to destroy the network in a dynamic game model and studied the effect of defenders' intentions on the defenders using an evolutionary game approach.

8.3 Incomplete information static game model

A game model is called an incomplete information game when the participants do not have complete knowledge of the game. Some studies have also been based on the incomplete information static game model. Zhai et al. [261] developed an offense-defense game model considering the utility of different attackers, where the payoff function of the defender over the attacker is uncertain. On the basis of a static model with complete information, Feng et al. [262] considered chemical plant protection in the presence of multiple types of attackers. Powell [263] studied a game model when the attacker's preference for the target is uncertain. Zhang et al. [264] proposed a game model for plant security management.

8.4 Incomplete information dynamic game model

Lastly, some research has been based on the incomplete information dynamic game model. Li et al. [265] hid some of the node information to model a dynamic game in which the state moves first and the terrorists move second. Zeng et al. [266] established the concept of information gap for the first time using a Starkelberg game model between attackers and defenders with asymmetric information. Zhang et al. [267] studied the offense-defense game with deceptive targets that can be used to mislead attackers. Liu et al. [268] used uniform distribution to change the degree values of nodes and the degree values of nodes as asymmetric information to model the defender-first offense-defense game. Strictly speaking, the above two studies had complete information about the elements in the game model although the participants had incomplete information about the game. Tambe [269] studied the airport security problem via a Bayesian Stackelberg game model. Gu et al. [270] built a Bayesian Stackelberg game model in the face of attackers with different utility functions and analyzed the effect of type distribution on the equilibrium solution. Zeng et al. [271] developed a Bayesian dynamic game model with two types of attackers—global and local—where the global attacker is concerned with the connectivity of the whole network and the local attacker is concerned with the efficiency of node removal. Jiang et al. [272] developed a Bayesian Stackelberg game model to study the water supply network protection problem including four cases of private information.

In addition, there have been studies on the offensive and defensive problems of infrastructure based on multiple game perspectives. Baykal-Guersoy et al. [273] studied the strategy of infrastructure security under two game models, namely, static defense and dynamic patrol, by using the number of people affected or the occupancy level of critical infrastructure as a metric of attack. Guan et al. [274] developed static and dynamic game models for multiple targets, where the defender defends against attackers' attacks by allocating resources. In the static game model, the attacker and defender act simultaneously, and in the dynamic game model, the defender acts first. The results showed that an increase in defense resources can reduce the attacker's probability of attacking.

9. Summary and outlook

Complex network theory is an excellent system modeling method that can not only reveal the behavior of a complex system but also reflect the essential features of the complex system. There is considerable literature in this field and many interesting results have been obtained. In this paper, we provide a survey of the complex systems and network science focused on seven aspects—namely, networked modeling, vital node analysis, network invulnerability analysis, network disintegration analysis, resilience analysis, complex network link prediction, and the attacker-defender game in complex networks. For future work, there are many emerging topics worth studying in this field. Therefore, we summarize four topics for future research.

9.1 Temporal network analysis of complex systems

In practice, the structure of complex systems is not immutable, and the nodes or edges will change over time. Therefore, it is possible to model complex systems based on temporal networks. Temporal networks are generally divided into two forms. One is expressed by a multi-layer network in which each layer represents a timestamp; the other is based on the activity-driven model, which describes the interaction between nodes in the network through the activity potential function. Compared with a static network, a temporal network can capture temporal information, which includes the interaction order of nodes, enabling it to more accurately depict the dynamic process of a complex system. Modeling complex systems based on temporal networks, including the identification of vital nodes, measurement of node centrality, and measurement of topology, is an important future research topic.

9.2 Dynamic network analysis of complex systems

Network dynamics offer an important method for studying complex systems. Dynamic processes mainly include five categories: random walk, inert random walk, self-avoiding walk, tourist walk, and epidemic spread. By introducing the feedback mechanism, network dynamics can determine the cause of system complexity. In the future, the frontier of network dynamics can focus on multi-layer networks and metric graphs.

9.3 Adaptive network analysis of complex systems

Different from a classic complex network, adaptive networks focus on the coevolution of nodes. The attributes of nodes and interaction between nodes will change with the local network structure. Therefore, we can use adaptive network modeling to study the game and cooperation between nodes as well as the emergence of swarm intelligence.

9.4 Higher-order network analysis of complex systems

Classic network modeling only focuses on the interaction between node pairs, and it is difficult to describe the group interaction that commonly exists in social, biological, and technological systems. A higher-order network considers the interaction between multiple nodes. It is a frontier topic of network science that can describe interactions between multiple agents in an endogenous way and yield a more concise model. The typical representatives of higher-order networks are simplicial complex and hypergraph.

References

[1] BERTALANFFY L V. General system theory: foundations, development, applications. IEEE Trans. on Systems, Man, and Cybernetics, 1974, SMC-4(6): 592.

[2] ASHBY W R. An introduction to cybernetics. London: Chapman & Hall Ltd, 1964.

[3] THOMAS M. Elements of information theory. New Jersey: John Wiley & Sons, 1999.

[4] PRIGOGINE I, RENE L. Theory of dissipative structures. HAKEN H ed. Synergetics. Wiesbaden: Springer Fachmedien, 1973: 124−135.

[5] HAKEN H. Synergetics. Physics Bulletin, 2007, 28(9): 412.

[6] ZEEMAN E C. Catastrophe theory. Berlin: Springer, 1979.

[7] LADYMAN J, JAMES L, KAROLINE W. What is a complex system? European Journal for Philosophy of Science, 2013, 3(1): 33−67.

[8] SIEGENFELD A F, BAR-YAM Y. An introduction to complex systems science and its applications. Complexity, 2020, 2020: 1–16.

[9] YU M G, NIU Y J, LIU X D, et al. Adaptive dynamic reconfiguration mechanism of unmanned swarm topology based on an evolutionary game. Journal of Systems Engineering and Electronics, 2023. DOI: 10.23919/JSEE.2023.000041.

[10] CAVAGNA A, CIMARELLI A, GIARDINA I, et al. Scale-free correlations in starling flocks. Proceedings of the National Academy of Sciences, 2010, 107(26): 11865–11870.

[11] CHINELLATO D D, EPSTEIN I R, BRAHA D, et al. Dynamical response of networks under external perturbations: exact results. Journal of Statistical Physics, 2015, 159(2): 221–230.

[12] SHI S, ZHANG G S, MIN H F, et al. Exact uncertainty compensation of linear systems by continuous fixed-time output-feedback controller. Journal of Systems Engineering and Electronics, 2022, 33(3): 706–715.

[13] XU B, BAI G H, ZHANG Y A, et al. Failure analysis of unmanned autonomous swarm considering cascading effects. Journal of Systems Engineering and Electronics, 2022, 33(3): 759–770.

[14] LI R Q, DONG L, ZHANG J, et al. Simple spatial scaling rules behind complex cities. Nature Communications, 2017, 8(1): 1841.

[15] JACKSON J C, RAND D, LEWIS K, et al. Agent-based modeling: a guide for social psychologists. Social Psychological and Personality Science, 2017, 8(4): 387–395.

[16] AIT-AMIR B, PHILIPPE P, ABDELKHALAK E H. Metamodel development. Embedded Mechatronic Systems 2, 2020. DOI: 10.1016/B978-1-78548-014-0.50006-2.

[17] THONG W J, AMEEDEEN M A. A survey of Petri net tools. Advanced Computer and Communication Engineering Technology, 2015, 315: 537–551.

[18] WEISBUCH G. Complex systems dynamics. Boca Raton: CRC Press, 2018.

[19] BARABASI A. Network science. Cambridge: Cambridge University Press, 2013.

[20] WANG X F, LI X, CHEN G R. Theory and application of complex networks. Beijing: Tsinghua University Press, 2006. (in Chinese)

[21] LI L B, FAN Y, ZENG A, et al. Binary opinion dynamics on signed networks based on Ising model. Physica A: Statistical Mechanics and its Applications, 2019, 525: 433–442.

[22] PORTER M A. Nonlinearity+ networks: a 2020 vision. Emerging Frontiers in Nonlinear Science, 2020, 32: 131–159.

[23] BOCCALETTI S, LATORA V, MORENO Y, et al. Complex networks: structure and dynamics. Physics Reports, 2006, 424(4/5): 175–308.

[24] WU X W, LI L, QU Y G. Modelling and analysis of river networks based on complex networks theory. Advanced Materials Research, 2013, 756: 2728–2733.

[25] HUYNH-THU V A, SANGUINETTI G. Gene regulatory network inference: an introductory survey. https://doi.org/10.48550/arXiv.1801.04087.

[26] WANG L N, WANG K, SHEN J L. Weighted complex networks in urban public transportation: modeling and testing. Physica A: Statistical Mechanics and its Applications, 2020, 545: 123498.

[27] TAM W M, LAU F C M, TSE C K. Complex-network modeling of a call network. IEEE Trans. on Circuits and Systems I: Regular Papers, 2009, 56(2): 416–429.

[28] BORRETT S R, LAU M K. enaR: an R package for ecosystem network analysis. Methods in Ecology and Evolution, 2015, 5(11): 1206–1213.

[29] LI J C. Key technologies of heterogeneous information networks data mining. Changsha: National University of Defense Technology, 2019. (in Chinese)
[30] XING J C, CHEN C X, CHEN X R. Research progress on joint operation modeling based on complex networks. Proc. of the Chinese Control and Decision Conference, 2019: 2095−2099.
[31] LI C T, LIN S D. Centrality analysis, role-based clustering, and egocentric abstraction for heterogeneous social networks. Proc. of the International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing, 2013: 1−10.
[32] LATHA V P, RIHAN F A, RAKKIYAPPAN R, et al. A fractional-order model for Ebola virus infection with delayed immune response on heterogeneous complex networks. Journal of Computational & Applied Mathematics, 2017, 339: 134–146.
[33] BANCAL J D, PASTOR-SATORRAS R. Steady-state dynamics of the forest fire model on complex networks. The European Physical Journal B, 2010, 76: 109–121.
[34] ALONSO M, TURANZAS J, AMARIS H, et al. Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks. Sensors, 2021, 17: 5826.
[35] CHEN Y, MO D X. Community detection for multilayer weighted networks. Information Sciences, 2022, 595: 119–141.
[36] YANG Y, XU K J, HONG C. Network dynamics on the Chinese air transportation multilayer network. International Journal of Modern Physics C, 2021, 32(5): 2150070.
[37] HANNEKE S, FU W, XING E. Discrete temporal models of social networks. Proc. of the Conference on Statistical Network Analysis, 2006: 115–125.
[38] JIANG S, CHEN H C. NATERGM: a model for examining the role of nodal attributes in dynamic social media networks. IEEE Trans. on Knowledge and Data Engineering, 2016, 28(3): 729–740.
[39] ZENO G, FOND T L, NEVILLE J. Dynamic network modeling from motif-activity. Proc. of the Web Conference 2020, 2020: 390−397.
[40] TAGHVAEI A, GEORGIOU T T, NORTON L. Fractional SIR epidemiological models. Scientific Reports, 2020, 10: 20882.
[41] JARDON-KOJAKHMETOV H, KUEHN C, PUGLIESE A, et al. A geometric analysis of the SIR, SIRS and SIRWS epidemiological models. Nonlinear Analysis Real World Applications, 2021, 58: 103220.
[42] WU J Y, ZHANG X W, ZHU X B, et al. A variant SIRS virus spreading model. Proc. of the International Conference on Computer Systems, Electronics and Control, 2017: 121−124.
[43] YANG Y H, LI J H, SHEN D, et al. Evolutionary dynamics analysis of complex network with fusion nodes and overlap edges. Journal of Systems Engineering and Electronics, 2018, 29(3): 549–559.
[44] CUYPERE E D, TURCK K D, WITTEVRONGEL S, et al. Markovian SIR model for opinion propagation. Proc. of the 25th International Teletraffic Congress, 2013: 1−7.
[45] QIU L Q, JIA W, NIU W N, et al. Sir-im: sir rumor spreading model with influence mechanism in social networks. Soft Computing, 2020, 25: 13949–13958.
[46] CHEN T W, MA B C, WANG J N. SIRS contagion model of food safety risk. Journal of Food Safety, 2017, 38(1): e12410.
[47] REIA S M, FONTANARI J F. A SIR epidemic model for citation dynamics. European Physical Journal Plus, 2020, 136(2): 207.
[48] JALILI M, SALEHZADEH-YAZDI A, ASGARI Y, et al. CentiServer: a comprehensive resource, web-based application and R package for centrality analysis. PLoS One, 2015, 10: e0143111.
[49] LIU J G, REN Z M, GUO Q, et al. Node importance ranking of complex networks. Acta Physica Sinica, 2013, 62(17): 9–18.
[50] LÜ L Y, CHEN D B, REN X L, et al. Vital nodes identification in complex networks. Physics Reports, 2016, 650: 1–63.
[51] BONACICH P. Factoring and weighting approaches to status scores and clique identification. The Journal of Mathematical Sociology, 1972, 2: 113–120.
[52] CHEN D B, LÜ L Y, SHANG M S, et al. Identifying influential nodes in complex networks. Physica A: Statistical Mechanics and its Applications, 2012, 391: 1777–1787.
[53] KITSAK M, GALLOS L K, HAVLIN S, et al. Identification of influential spreaders in complex networks. Nature Physics, 2010, 6: 888–893.
[54] FREEMAN L C. Centrality in social networks: conceptual clarification. Social Networks, 1979, 1: 215–239.
[55] FREEMAN L C. A set of measures of centrality based on betweenness. Sociometry, 1977, 40: 35–41.
[56] ESTRADA E, RODRIGUEZ-VELAZQUEZ J A. Subgraph centrality and clustering in complex hyper-networks. Physica A: Statistical Mechanics and its Applications, 2006, 364: 581–594.
[57] BRIN S, PAGE L. Reprint of: the anatomy of a large-scale hypertextual web search engine. Computer Networks, 2012, 56: 3825–3833.
[58] LÜ L Y, ZHANG Y C, YEUNG C H, et al. Leaders in social networks, the delicious case. PLoS One, 2011, 6: e21202.
[59] KLEINBERG J M. Authoritative sources in a hyperlinked environment. Journal of the ACM, 1999, 46: 604–632.
[60] LEMPEL R, MORAN S. The stochastic approach for link-structure analysis (SALSA) and the TKC effect1Abridged version1. Computer Networks, 2000, 33: 387–401.
[61] TAN Y J, WU J, DENG H Z. Evaluation method for node importance based on node contraction in complex networks. Systems Engineering Theory and Practice, 2006, 26(11): 79–84. (in Chinese)
[62] DANGALCHEV C. Residual closeness in networks. Physica A: Statistical Mechanics and its Applications, 2006, 365(2): 556–564.
[63] ULLAH A, WANG B, SHENG J F, et al. Identification of nodes influence based on global structure model in complex networks. Scientific Reports, 2021, 11: 6173.
[64] SHENG J F, DAI J Y, WANG B, et al. Identifying influential nodes in complex networks based on global and local structure. Physica A: Statistical Mechanics and its Applications, 2020, 541: e123262.
[65] ULLAH A, WANG B, SHENG J F, et al. Identifying vital nodes from local and global perspectives in complex networks. Expert Systems with Applications, 2021, 186: e115778.
[66] LIU J G, REN Z M, GUO Q. Ranking the spreading influ-

ence in complex networks. Physica A: Statistical Mechanics and its Applications, 2013, 392: 4154–4159.
[67] LU L Y, ZHOU T, ZHANG Q M, et al. The H-index of a network node and its relation to degree and coreness. Nature Communications, 2016, 7: e10168.
[68] CHEN X, TAN M, ZHAO J, et al. Identifying influential nodes in complex networks based on a spreading influence related centrality. Physica A: Statistical Mechanics and its Applications, 2019, 536: e122481.
[69] DONG Z H, CHEN Y Z, TRICCO T S, et al. Hunting for vital nodes in complex networks using local information. Scientific Reports, 2021, 11: e9190.
[70] QIAO T, SHAN W, YU G J, et al. A novel entropy-based centrality approach for identifying vital nodes in weighted networks. Entropy, 2018, 20(4): e20040261.
[71] XU X, ZHU C, WANG Q Y, et al. Identifying vital nodes in complex networks by adjacency information entropy. Scientific Reports, 2020, 10: e2691.
[72] LIU X. Research on evaluation algorithms of node importance in directed-weighted networks. Lanzhou: Northwest Normal University, 2020. (in Chinese)
[73] QI X Q, FULLER E, WU Q, et al. Laplacian centrality: a new centrality measure for weighted networks. Information Sciences, 2012, 194: 240–253.
[74] FEI L G, ZHANG Q, DENG Y. Identifying influential nodes in complex networks based on the inverse-square law. Physica A: Statistical Mechanics and its Applications, 2018, 512: 1044–1059.
[75] MA L L, MA C, ZHANG H F, et al. Identifying influential spreaders in complex networks based on gravity formula. Physica A: Statistical Mechanics and its Applications, 2016, 451: 205–212.
[76] QIU Z H, FAN T L, LI M, et al. Identifying vital nodes by Achlioptas process. New Journal of Physics, 2021, 23(3): e033036.
[77] LALOU M, TAHRAOUI M A, KHEDDOUCI H. The vital node detection problem in networks: a survey. Computer Science Review, 2018, 28: 92–117.
[78] BIAN R, KOH Y S, DOBBIE G, et al. Identifying top-k nodes in social networks. ACM Computing Surveys, 2020, 52: 1–33.
[79] REN T, LI Z, QI Y, et al. Identifying vital nodes based on reverse greedy method. Scientific Reports, 2020, 10: 4826.
[80] ZHONG J L, ZHANG F M, LI Z X. Identification of vital nodes in complex network via belief propagation and node reinsertion. IEEE Access, 2018, 6: 29200–29210.
[81] HU Y L, LI J C, RUAN Y R. Finding influencers in complex networks: a novel method based on information theory. IEEE Systems Journal, 2022, 16(2): 3372–3380.
[82] TAN Y J, WU J, DENG H Z. Progress in invulnerability of complex networks. Journal of University of Shanghai for Science and Technology, 2011, 33(6): 653–668. (in Chinese)
[83] CHVATAL V. Tough graphs and Hamiltonian circuits. Discrete Mathematics, 1973, 5: 215–228.
[84] BAREFOOT C A, ENTRINGER R, SWART H. Vulnerability in graphs: a comparative survey. Journal of Combinatorial Mathematics and Combinatorial Computing, 1987, 1: 13–22.
[85] COZZEN M, MOAZZAMI D, STUECKLE S. The tenacity of a graph. Proc. of the 7th International Conference on the Theory and Applications of Graphs, 1995: 1111−1122.
[86] CHOUDUM S A, PRIYA N. Tenacity of complete graph products and grids. Networks, 1999, 34(3): 192–196.
[87] JUNG H A. Class of posets and corresponding comparability graphs. Journal of Combinatorial Theory Series B, 1978, 24(2): 125–133.
[88] ZHANG S G, LI X L, HAN X L. Computing the scattering number of graphs. International Journal of Computer Mathematics, 2002, 79(2): 179–187.
[89] BASSALYGO L A, PINSKER M S. The complexity of an optimal non-blocking commutation scheme without reorganization. Problems of Information Transmission, 1973, 9(1): 84–87.
[90] PINSKER M S. On the complexity of a concentrator. Proc. of the 7th International Teletraffic Conference, 1973: 1−4.
[91] FIEDLER M. Algebraic connectivity of graphs. Czechoslovak Mathematical Journal, 1973, 23(2): 298–305.
[92] WU J, BARAHONA M, TAN Y J, et al. Natural connectivity of complex networks. Chinese Physics Letters, 2010, 27(7): 078902.
[93] COHEN R, EREZ K, BEN-AVRAHAM D, et al. Resilience of the Internet to random breakdowns. Physical Review Letters, 2000, 85(21): 4626–4628.
[94] NEWMAN M E J, STROGATZ S H, WATTS D J. Random graphs with arbitrary degree distributions and their applications. Physical Review E, 2001, 64(2): 26118.
[95] BROADBENT S R, HAMMERSLEY J M. Percolation processes: I. crystals and mazes. Proceedings of the Cambridge Philological Society, 1957, 53: 629–641.
[96] CHI L P, YANG C B, CAI X. Stability of random networks under evolution of attack and repair. Chinese Physics Letters, 2006, 23(1): 263–266.
[97] VAZQUEZ A, MORENO Y. Resilience to damage of graphs with degree correlations. Physical Review E, 2003, 67(1): 015101.
[98] SUN S, LIU Z X, CHEN Z Q, et al. Error and attack tolerance of evolving networks with local preferential attachment. Physica A, 2007, 373: 851–860.
[99] WANG J W, RONG L L. Cascade-based attack vulnerability on the US power grid. Safety Sicence, 2009, 47: 1332–1336.
[100] CARRERAS B A, LYNCH V E. Complex dynamics of blackouts in power transmission systems. Chaos , 2004, 14(3): 643–652.
[101] DOBSON I, CHEN J, THROP J S, et al. Examining criticality of blackouts in power system models with cascading events. Proc. of the 35th Annual Hawaii International Conference on System Sciences, 2002. DOI: 10.1109/HICSS.2002.993975.
[102] WANG J W, RONG L L, ZHANG L, et al. Attack vulnerability of scale-free networks due to cascading failures. Physica A, 2008, 387: 6671–6678.
[103] MOTTER A E, LAI Y C. Cascade-based attacks on complex networks. Physical Review E: Statistical Nonlinear and Soft Matter Physics, 2002, 66(6): 1–4.
[104] WU J, TAN S Y, TAN Y J. Analysis of invulnerability in complex networks based on natural connectivity. Complex Systems and Complexity Science, 2014, 11(1): 77–86.
[105] SUN Y, YAO P Y, ZHANG J Y. Node attack strategy of complex networks based on optimization theory. Journal of Electronics & Information Technology, 2017, 39(3):

518524.
[106] ALBERT R, JEONG H, BARABSI A L. Diameter of the world-wide web. Nature, 1999, 401(6749): 130−131.
[107] VALENTE A X C N, SARKAR A, STONE H A. Two-peak and three-peak optimal complex networks. Physical Review Letters, 2004, 92(11): 118702.
[108] PAUL G, TANIZAWA T, HAVLIN S, et al. Optimization of robustness of complex networks. The European Physical Journal B-Condensed Matter and Complex Systems, 2004, 38(2): 187–191.
[109] TANIZAWA T, PAUL G, COHEN R, et al. Optimization of network robustness to waves of targeted and random attacks. Physical Review E, 2005, 71(4): 047101.
[110] BEYGELZIMER A, GRINSTEIN G, LINSKER R, et al. Improving network robustness by edge modification. Physica A: Statistical Mechanics and its Applications, 2005, 357(3): 593–612.
[111] ZHAO J C, XU K. Enhancing the robustness of scale-free networks. Physics A: Mathematical and Theoretical, 2009, 42(19): 195003.
[112] CAO X B, HONG C, DU W B, et al. Improving the network robustness against cascading failures by adding links. Chaos, Solitons & Fractals, 2013, 57: 35–40.
[113] LIU J G, WANG Z T, DANG Y Z. Optimization of robustness of scale-free network to random and targeted attacks. Modern Physics Letters B, 2005, 19(16): 785–792.
[114] NETOTEA S, PONGOR S. Evolution of robust and efficient system topologies. Cellular Immunology, 2006, 244(2): 80–83.
[115] PRIESTER C, SCHMITT S, PEIXOTO T P. Limits and trade-offs of topological network robustness. PLoS One, 2014, 9(9): e108215.
[116] PEIXOTO T P, BORNHOLDT S. Evolution of robust network topologies: emergence of central backbones. Physical Review Letters, 2012, 109(11): 118703.
[117] HERRMANN H J, SCHNEIDER C M, MOREIRA A A, et al. Onion-like network topology enhances robustness against malicious attacks. Journal of Statistical Mechanics: Theory and Experiment, 2011. DOI:10.1088/1742-5468/2011/01/P01027.
[118] FU J L, SUN D Y, XIAO J, et al. Review of the research on the terrorist networks based on social network analysis. Systems Engineering-Theory & Practice, 2013, 33(9): 2177–2186. (in Chinese)
[119] CARLEY K M, REMINGA J, KAMNEVA N. Destabilizing terrorist networks. Proc. of the 8th International Command and Control Research and Technology Symposium, 2003: 1−6.
[120] CHAURASIA N, TIWARI A. Efficient algorithm for destabilization of terrorist networks. International Journal of Information Technology and Computer Science, 2013, 12: 21–30.
[121] SUN H C, XU M D, XU X K. Infection and prevention of COVID-19 in schools based on real life interpersonal contact data. Journal of University Electronic Science and Technology of China, 2020, 49(3): 399–407. (in Chinese)
[122] JIN W X. SoS-Ops M&S based on the complex network. Beijing: Publishing House of Electronics Industry, 2010. (in Chinese)
[123] ANGGRAINI D, MADENDA S, WIBOWO E P, et al. Network disintegration in criminal network. Proc. of the 11th International Conference on Signal-Image Technology & Internet-Based Systems, 2015: 192−199.
[124] BRIGHT D, GREENHILL C, BRITZ T, et al. Criminal network vulnerabilities and adaptations. Global Crime, 2017, 18(4): 424–441.
[125] MALAVIYA A, RAINWATER C, SHARKEY T. Multi-period network interdiction problems with applications to city-level drug enforcement. IIE Transactions, 2012, 44(5): 368–380.
[126] MICHALOPOULOS D P, BARNES J W, MORTON D P. Prioritized interdiction of nuclear smuggling via tabu search. Optimization Letters, 2015, 9(8): 1477–1494.
[127] QUAYLE A P, SIDDIQUI A S, JONES S J M. Preferential network perturbation. Physica A, 2006, 371: 823–840.
[128] TRIPATHY R M, BAGCHI A, MEHTA S. A study of rumor control strategies on social networks. Proc. of the 19th ACM International Conference on Information and Knowledge Management, 2010: 1817−1820.
[129] KOBAYASHI T, HASUI K. Efficient immunization strategies to prevent financial contagion. Scientific Reports, 2014, 4(1): 1–7.
[130] LI J J, ZHAO D L, GE B F, et al. Disintegration of operational capability of heterogeneous combat networks under incomplete information. IEEE Trans. on Systems, Man, and Cybernetics: Systems, 2018, 50(12): 5172–5179.
[131] LI Q, LIU S Y, YANG X S. Neighborhood information based probabilistic algorithm for network disintegration. Expert Systems with Applications, 2020, 139: 112853.
[132] DENG Y, WU J, XIAO Y, et al. Optimal disintegration strategy with heterogeneous costs in complex networks. IEEE Trans. on Systems, Man, and Cybernetics: Systems, 2018, 50(8): 2905–2913.
[133] DENG Y, WU J, XIAO Y, et al. Efficient disintegration strategies with cost constraint in complex networks: the crucial role of nodes near average degree. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2018, 28(6): 061101.
[134] QI M Z, DENG Y, DENG H Z, et al. Optimal disintegration strategy in multiplex networks. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2018, 28(12): 121104.
[135] NIE S, WANG X W, ZHANG H F, et al. Robustness of controllability for networks based on edge attack. PLoS One, 2014, 9(2): e89066.
[136] WANG J W, RONG L L. Robustness of the western united states power gridunder edge attack strategies due to cascading failures. Safety Science, 2011, 49(6): 807–812.
[137] HAO Y C, JIA L M, WANG Y H. Edge attack strategies in interdependent scale free networks. Physica A: Statistical Mechanics and its Applications, 2020, 540: 122759.
[138] ZHANG X K, WU J, WANG H, et al. Optimization of disintegration strategy for multi edges complex networks. Proc. of the IEEE Congress on Evolutionary Computation, 2016: 522–528.
[139] REN X L, GLEINIG N, HELBING D, et al. Generalized network dismantling. Proceedings of the National Academy of Sciences, 2019, 116(14): 6554–6559.
[140] LI J J, JIANG J, YANG K W, et al. Research on functional robustness of heterogeneous combat networks. IEEE Systems Journal, 2018, 13(2): 1487–1495.
[141] QI M Z, BAI Y, LI X H, et al. Optimal disintegration strategy in multiplex networks under layer node-based attack. Applied Sciences, 2019, 9(19): 3968.

[142] HAN J H, TANG S Y, SHI Y F, et al. An efficient layer node attack strategy to dismantle large multiplex networks. The European Physical Journal B, 2021, 94: 1–8.
[143] MALIK H A M, ABID F, WAHIDDIN M R, et al. Robustness of dengue complex network under targeted versus random attack. Complexity, 2017, 2017: 2515928.
[144] BELLINGERI M, BEVACQUA D, SCOTOGNELLA F, et al. Efficacy of local attack strategies on the Beijing road complex weighted network. Physica A: Statistical Mechanics and its Applications, 2018, 510: 316–328.
[145] YAN D C, XIE W X, ZHANG Y W, et al. Hypernetwork dismantling via deep reinforcement learning. IEEE Trans. on Network Science and Engineering, 2022, 9(5): 3302–3315.
[146] DENG Y, WU J, QI M Z, et al. Optimal disintegration strategy in spatial networks with disintegration circle model. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2019, 29(6): 061102.
[147] SUN J B, LI J C, YOU Y Q, et al. Combat network link prediction based on embedding learning. Journal of Systems Engineering and Electronics, 2022, 33(2): 345–353.
[148] FARAMONDI L, OLIVA G, SETOLA R, et al. Performance analysis of single and multi-objective approaches for the critical node detection problem. Proc. of the International Conference on Optimization and Decision Science, 2017: 315−324.
[149] BORGATTI S P. Identifying sets of key players in a social network. Computational & Mathematical Organization Theory, 2006, 12: 21–34.
[150] VAN DER ZWAAN R, BERGER A, GRIGORIEV A. How to cut a graph into many pieces. Proc. of the International Conference on Theory and Applications of Models of Computation, 2011: 184−194.
[151] SHEN S Q, SMITH J C. Polynomial-time algorithms for solving a class of critical node problems on trees and series-parallel graphs. Networks, 2012, 60(2): 103–119.
[152] ALBERT R, JEONG H, BARABASI A L. Error and attack tolerance of complex networks. Nature , 2000, 406(6794): 378–382.
[153] ESTRADA E. The structure of complex networks: theory and applications. Oxford: Oxford University Press, 2012.
[154] COHEN R, HAVLIN S, BEN-AVRAHAM D. Efficient immunization strategies for computer networks and populations. Physical Review Letters, 2003, 91(24): 247901.
[155] HOLME P. Efficient local strategies for vaccination and network attack. Europhysics Letters, 2004, 68(6): 908.
[156] GALLOS L K, LILJEROS F, ARGYRAKIS P, et al. Improving immunization strategies. Physical Review E, 2007, 75(4): 045104.
[157] HEWETT R. Toward identification of key breakers in social cyber-physical networks. Proc. of the IEEE International Conference on Systems, Man, and Cybernetics, 2011: 2731−2736.
[158] ORTIZ-ARROYO D, HUSSAIN D M A. An information theory approach to identify sets of key players. Proc. of the European Conference on Intelligence and Security Informatics, 2008: 15−26.
[159] ARULSELVAN A, COMMANDER C W, ELEFTERIADOU L, et al. Detecting critical nodes in sparse graphs. Computers & Operations Research, 2009, 36(7): 2193–2200.
[160] DI SUMMA M, GROSSO A, LOCATELLI M. Branch and cut algorithms for detecting critical nodes in undirected graphs. Computational Optimization and Applications, 2012, 53: 649–680.
[161] VEREMYEV A, BOGINSKI V, PASILIAO E L. Exact identification of critical nodes in sparse networks via new compact formulations. Optimization Letters, 2014, 8: 1245–1259.
[162] HOLME P, KIM B J, YOON C N, et al. Attack vulnerability of complex networks. Physical Review E, 2002, 65(5): 056109.
[163] ZHOU J, YU X H, LU J A. Node importance in controlled complex networks. IEEE Trans. on Circuits and Systems II: Express Briefs, 2018, 66(3): 437–441.
[164] YU Y, DENG Y, TAN S Y, et al. Efficient disintegration strategy in directed networks based on tabu search. Physica A: Statistical Mechanics and its Applications, 2018, 507: 435–442.
[165] LOZANO M, GARCIA-MARTINEZ C, RODRIGUEZ F J, et al. Optimizing network attacks by artificial bee colony. Information Sciences, 2017, 377: 30–50.
[166] FARAMONDI L, SETOLA R, PANZIERI S, et al. Finding critical nodes in infrastructure networks. International Journal of Critical Infrastructure Protection, 2018, 20: 3–15.
[167] LI K W, ZHANG T, WANG R. Research reviews of combinatorial optimization methods based on deep reinforcement learning. Acta Automatica Sinica, 2020, 41: 1–17.
[168] FAN C J, ZENG L, SUN Y Z, et al. Finding key players in complex networks through deep reinforcement learning. Nature Machine Intelligence, 2020, 2(6): 317–324.
[169] YANG Q, ZHANG Y N, ZHOU Y Q, et al. A review of complex network theory and its application in the resilience of public transportation systems. China Journal of Highway and Transport, 2022, 35(4): 215–229. (in Chinese)
[170] FRACCASCIA L, GIANNOCCARO I, ALBINO V. Resilience of complex systems: state of the art and directions for future research. Complexity, 2018, 2018: 3421529.
[171] HOLLING C S. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 1973, 4(1): 1–23.
[172] HOLLING C S. Engineering resilience versus ecological resilience. Engineering within Ecological Constraints, 1996, 31: 32.
[173] HOLLING C S. Understanding the complexity of economic, ecological, and social systems. Ecosystems , 2001, 4: 390–405.
[174] ELMQVIST T, ANDERSSON E, FRANTZESKAKI N, et al. Sustainability and resilience for transformation in the urban century. Nature Sustainability, 2019, 2(4): 267–273.
[175] MIARA A, MACKNICK J E, VOROSMARTY C J, et al. Climate and water resource change impacts and adaptation potential for US power supply. Nature Climate Change, 2017, 7(11): 793–798.
[176] GANIN A A, KITSAK M, MARCHESE D, et al. Resilience and efficiency in transportation networks. Science Advances, 2017, 3(12): e1701079.
[177] WANG W P, YANG S N, STANLEY H E, et al. Local floods induce large-scale abrupt failures of road networks. Nature Communications, 2019, 10(1): 2114.
[178] HYNES W, TRUMP B D, KIRMAN A, et al. Systemic resilience in economics. Nature Physics, 2022, 18(4):

381–384.
[179] MAHONEY E, GOLAN M, KURTH M, et al. Resilience-by-design and resilience-by-intervention in supply chains for remote and indigenous communities. Nature Communications, 2022, 13(1): 1124.
[180] BUCHANAN R K, GOERGER S R, RINAUDO C H, et al. Resilience in engineered resilient systems. The Journal of Defense Modeling and Simulation, 2020, 17(4): 435–446.
[181] ERDOS P, RENYI A. On random graphs. Publication Mathematicae, 1959, 6: 290–297.
[182] WATTS D J, STROGATZ S H. Collective dynamics of 'small-world' networks. Nature, 1998, 393(6684): 440–442.
[183] BARABASI A L, ALBERT R. Emergence of scaling in random networks. Science, 1999, 286(5439): 509–512.
[184] HOSSEINI S, BARKER K, RAMIREZ-MARQUEZ J E. A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 2016, 145: 47–61.
[185] LENGNICK-HALL C A, BECK T E, LENGNICK-HALL M L. Developing a capacity for organizational resilience through strategic human resource management. Human Resource Management Review, 2011, 21(3): 243–255.
[186] BRUNEAU M, CHANG S E, EGUCHI R T, et al. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake Spectra, 2003, 19(4): 733–752.
[187] MARTIN R. Regional economic resilience, hysteresis and recessionary shocks. Journal of Economic Geography, 2012, 12(1): 1–32.
[188] MARTIN R, SUNLEY P. On the notion of regional economic resilience: conceptualization and explanation. Journal of Economic Geography, 2015, 15(1): 1–42.
[189] WOODS D D. Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety, 2015, 141: 5–9.
[190] GAO J X, LIU X M, LI D Q, et al. Recent progress on the resilience of complex networks. Energies , 2015, 8(10): 12187–12210.
[191] MENG F L, FU G T, FARMANI R, et al. Topological attributes of network resilience: a study in water distribution systems. Water Research, 2018, 143: 376–386.
[192] PANDIT A, CRITTENDEN J C. Index of network resilience (INR) for urban water distribution systems. Proc. of the Critical Infrastructure Symposium, 2012. DOI: 10.13140/2.1.2826.9442.
[193] OMER M, NILCHIANI R, MOSTASHARI A. Measuring the resilience of the trans-oceanic telecommunication cable system. IEEE Systems Journal, 2009, 3(3): 295–303.
[194] PAN X, DANG Y H, WANG H X, et al. Resilience model and recovery strategy of transportation network based on travel OD-grid analysis. Reliability Engineering & System Safety, 2022, 223: 108483.
[195] BIRNBAUM Z W. On the importance of different components in a multicomponent system. Seattle: University of Washington, 1968.
[196] RUIZ-MARTIN C, WAINER G, LOPEZ-PAREDES A. Exploration of network theory to evaluate organizational resilience. International Journal of Mathematical, Engineering and Management Sciences, 2022, 7(1): 28.
[197] BLAGOJEVIC N, DIDIER M, STOJADINOVIC B. Quantifying component importance for disaster resilience of communities with interdependent civil infrastructure systems. Reliability Engineering & System Safety, 2022, 228: 108747.
[198] YE S S, QIAN Z. The economic network resilience of the Guanzhong plain city cluster, China: a network analysis from the evolutionary perspective. Growth and Change, 2021, 52(4): 2391–2411.
[199] GAUTHIER P, FURNO A, EL FAOUZI N E. Road network resilience: how to identify critical links subject to day-to-day disruptions. Transportation Research Record, 2018, 2672(1): 54–65.
[200] XU R J, GONG L, XIE J, et al. Resilience-based link importance evaluation and recovery strategy for equipment system-of-systems. Systems Engineering and Electronics, 2023, 45(1): 139–147. (in Chinese)
[201] JIANG J Y, LI J C, YANG K W. Weapon system portfolio selection based on structural robustness. Journal of Systems Engineering and Electronics, 2020, 31(6): 1216–1229.
[202] AHMADIANFAR I, SHIRVANI-HOSSEINI S, HE J, et al. An improved adaptive neuro fuzzy inference system model using conjoined metaheuristic algorithms for electrical conductivity prediction. Scientific Reports, 2022, 12(1): 4934.
[203] WANG T L, WANG L, XIA G P. Combinatorial optimization method for shipping machinery based on hybrid PSO. Systems Engineering-Theory and Practice, 2012, 32(10): 2262–2269. (in Chinese)
[204] ALIAHMADI A, GHAHREMANI-NAHR J, NOZARI H. Pricing decisions in the closed-loop supply chain network, taking into account the queuing system in production centers. Expert Systems with Applications, 2023, 212: 118741.
[205] DIMAS D L F, VEGA-RODRIGUEZ MIGUEL A, PEREZ CARLOS J. Automatic selection of a single solution from the Pareto front to identify key players in social networks. Knowledge-Based Systems, 2018, 160: 228–236.
[206] KUMAR A, SINGH S S, SINGH K, et al. Link prediction techniques, applications, and performance: a survey. Physica A: Statistical Mechanics and its Applications, 2020, 553: 124289.
[207] NEWMAN M E J. Clustering and preferential attachment in growing networks. Physical Review E, 2001, 64(2): 025102.
[208] BARABASI A L, JEONG H, NEDA Z, et al. Evolution of the social network of scientific collaborations. Physica A: Statistical Mechanics and its Applications, 2002, 311(3/4): 590–614.
[209] ADAMIC L A, ADAR E. Friends and neighbors on the web. Social Networks, 2003, 25(3): 211–230.
[210] ZHOU T, LÜ L Y, ZHANG Y C. Predicting missing links via local information. The European Physical Journal B, 2009, 71: 623–630.
[211] KATZ L. A new status index derived from sociometric analysis. Psychometrika, 1953, 18(1): 39–43.
[212] TONG H, FALOUTSOS C, PAN J Y. Fast random walk with restart and its applications. Proc. of the 6th International Conference on Data Mining, 2006: 613−622.
[213] LIU W P, LÜ L Y. Link prediction based on local random walk. Europhysics Letters, 2010, 89(5): 58007.
[214] WANG X J, ZHANG X, ZHAO C L, et al. Predicting link directions using local directed path. Physica A: Statistical Mechanics and its Applications, 2015, 419: 260–267.
[215] WANG C, SATULURI V, PARTHASARATHY S. Local probabilistic models for link prediction. Proc. of the 7th IEEE International Conference on Data Mining, 2007: 322−331.

[216] NEVILLE J. Statistical models and analysis techniques for learning in relational data. Massachusetts: University of Massachusetts Amherst, 2006.
[217] YU K, CHU W, YU S P, et al. Stochastic relational models for discriminative link prediction. Proc. of the International Conference on Neural Information Processing Systems, 2006: 1553−1560.
[218] CLAUSET A, MOORE C, NEWMAN M E J. Hierarchical structure and the prediction of missing links in networks. Nature, 2008, 453(7191): 98–101.
[219] GUIMERA R, SALES-PARDO M. Missing and spurious interactions and the reconstruction of complex networks. Proceedings of the National Academy of Sciences, 2009, 106(52): 22073–22078.
[220] LAI Z H, CHEN Y D, MO D M, et al. Robust jointly sparse embedding for dimensionality reduction. Neurocomputing, 2018, 314: 30–38.
[221] BECHT E, MCINNES L, HEALY J, et al. Dimensionality reduction for visualizing single-cell data using UMAP. Nature Biotechnology, 2019, 37(1): 38–44.
[222] PEROZZI B, AL-RFOU R, SKIENA S. Deepwalk: online learning of social representations. Proc. of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2014: 701−710.
[223] BELKIN M, NIYOGI P. Laplacian eigenmaps and spectral techniques for embedding and clustering. Proc. of the 14th International Conference on Neural Information Processing Systems: Natural and Synthetic, 2001: 701–710.
[224] GROVER A, LESKOVEC J. node2vec: scalable feature learning for networks. Proc. of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016: 855−864.
[225] KAZEMI S M, POOLE D. Simple embedding for link prediction in knowledge graphs. Proc. of the 32nd International Conference on Neural Information Processing Systems, 2018: 4289–4300.
[226] TENENBAUM J B, SILVA V, LANGFORD J C. A global geometric framework for nonlinear dimensionality reduction. Science, 2000, 290(5500): 2319–2323.
[227] KUCHAIEV O, RASAJSKI M, HIGHAM D J, et al. Geometric de-noising of protein-protein interaction networks. PLoS Computational Biology, 2009, 5(8): e1000454.
[228] ROWEIS S T, SAUL L K. Nonlinear dimensionality reduction by locally linear embedding. Science, 2000, 290(5500): 2323–2326.
[229] ACAR E, DUNLAVY D M, KOLDA T G. Link prediction on evolving data using matrix and tensor factorizations. Proc. of the IEEE International Conference on Data Mining Workshops, 2009: 262−269.
[230] MA X K, SUN P G, QIN G M. Nonnegative matrix factorization algorithms for link prediction in temporal networks using graph communicability. Pattern Recognition, 2017, 71: 361–374.
[231] SHARAN U, NEVILLE J. Temporal-relational classifiers for prediction in evolving domains. Proc. of the 8th IEEE International Conference on Data Mining, 2008: 540−549.
[232] MENON A K, ELKAN C. Link prediction via matrix factorization. Proc. of the Joint European Conference on Machine Learning and Knowledge Discovery in Databases, 2011: 437−452.
[233] CHEN B L, LI F F, CHEN S B, et al. Link prediction based on non-negative matrix factorization. PLoS One, 2017, 12(8): e0182968.
[234] WANG W J, CAI F, JIAO P F, et al. A perturbation-based framework for link prediction via non-negative matrix factorization. Scientific Reports, 2016, 6(1): 1–11.
[235] AHMED N M, CHEN L, WANG Y, et al. DeepEye: link prediction in dynamic networks based on non-negative matrix factorization. Big Data Mining and Analytics, 2018, 1(1): 19–33.
[236] KOREN Y, BELL R, VOLINSKY C. Matrix factorization techniques for recommender systems. Computer , 2009, 42(8): 30–37.
[237] WU Z F, CHEN Y X. Link prediction using matrix factorization with bagging. Proc. of the IEEE/ACIS 15th International Conference on Computer and Information Science, 2016: 1−6.
[238] HUANG Z, LI X, CHEN H C. Link prediction approach to collaborative filtering. Proc. of the 5th ACM/IEEE-CS Joint Conference on Digital Libraries, 2005: 141−142.
[239] LU L Y, MEDO M, YEUNG C H, et al. Recommender systems. Physics Reports, 2012, 519(1): 1–49.
[240] ESSLIMANI I, BRUN A, BOYER A. Densifying a behavioral recommender system by social networks link prediction methods. Social Network Analysis and Mining, 2011, 1: 159–172.
[241] CHEN Z H, WANG X K, GAO P, et al. Predicting disease related microRNA based on similarity and topology. Cells, 2019, 8(11): 1405.
[242] LV H, LI J, ZHANG S, et al. Meta-path based MiRNA-disease association prediction. Proc. of the International Workshop on Big Data Management and Service, 2019: 34−48.
[243] ZENG X X, WANG W, DENG G S, et al. Prediction of potential disease-associated microRNAs by using neural networks. Molecular Therapy-Nucleic Acids, 2019, 16: 566–575.
[244] SUN Y Z, BARBER R, GUPTA M, et al. Co-author relationship prediction in heterogeneous bibliographic networks. Proc. of the International Conference on Advances in Social Networks Analysis and Mining, 2011: 121−128.
[245] ZHANG J. Uncovering mechanisms of co-authorship evolution by multirelations-based link prediction. Information Processing & Management, 2017, 53(1): 42–51.
[246] DO P, PHAM P, PHAN T, et al. T-MPP: a novel topic-driven meta-path-based approach for co-authorship prediction in large-scale content-based heterogeneous bibliographic network in distributed computing framework by spark. Proc. of the International Conference on Intelligent Computing & Optimization, 2019: 87−97.
[247] LI J C, GE B F, YANG K W, et al. Meta-path based heterogeneous combat network link prediction. Physica A: Statistical Mechanics and its Applications, 2017, 482: 507–523.
[248] BIER V, OLIVEROS S, SAMUELSON L. Choosing what to protect: strategic defensive allocation against an unknown attacker. Journal of Public Economic Theory, 2007, 9(4): 563–587.
[249] FENG Q L, CAI H, CHEN Z L, et al. Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. Journal of Loss Prevention in the Process Industries, 2016, 43: 614–628.
[250] LI Y P, TAN S Y, DENG Y, et al. Attacker-defender game

from a network science perspective. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2018, 28(5): 051102.
[251] LI Y P, DENG Y, XIAO Y, et al. Attack and defense strategies in complex networks based on game theory. Journal of Systems Science and Complexity, 2019, 32(6): 1630–1640.
[252] LI Y P, XIAO Y, LI Y, et al. Which targets to protect in critical infrastructures-a game-theoretic solution from a network science perspective. IEEE Access, 2018, 6: 56214–56221.
[253] CHEN P Y, CHENG S M, CHEN K C. Smart attacks in smart grid communication networks. IEEE Communications Magazine, 2012, 50(8): 24–29.
[254] FU C Q, GAO Y J, ZHONG J L, et al. Attack-defense game for critical infrastructure considering the cascade effect. Reliability Engineering & System Safety, 2021, 216: 107958.
[255] BOMPARD E, GAO C, NAPOLI R, et al. Risk assessment of malicious attacks against power systems. IEEE Trans. on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2009, 39(5): 1074–1085.
[256] BROWN G G, COX, JR L A. How probabilistic risk assessment can mislead terrorism risk analysts. Risk Analysis: An International Journal, 2011, 31(2): 196–204.
[257] YIN Z, JIANG A, JOHNSON M, et al. Trusts: scheduling randomized patrols for fare inspection in transit systems. Proc. of the AAAI Conference on Artificial Intelligence. 2012, 26(2): 2348−2355.
[258] BROWN G, CARLYLE M, SALMERON J, et al. Defending critical infrastructure. Interfaces, 2006, 36(6): 530–544.
[259] LI Y P, QIAO S, DENG Y, et al. Stackelberg game in critical infrastructures from a network science perspective. Physica A: Statistical Mechanics and its Applications, 2019, 521: 705–714.
[260] FU C Q, ZHANG P T, ZHOU L, et al. Camouflage strategy of a Stackelberg game based on evolution rules. Chaos, Solitons & Fractals, 2021, 153: 111603.
[261] ZHAI Q Q, PENG R, ZHUANG J. Defender-attacker games with asymmetric player utilities. Risk Analysis, 2020, 40(2): 408–420.
[262] FENG Q L, CAI H, CHEN Z L. Using game theory to optimize the allocation of defensive resources on a city scale to protect chemical facilities against multiple types of attackers. Reliability Engineering & System Safety, 2019, 191: 105900.
[263] POWELL R. Defending against terrorist attacks with limited resources. American Political Science Review, 2007, 101(3): 527–541.
[264] ZHANG L B, RENIERS G. A game-theoretical model to improve process plant protection from terrorist attacks. Risk Analysis, 2016, 36(12): 2285–2297.
[265] LI Q, LI M C, GAN J Y, et al. A game-theoretic approach for the location of terror response facilities with both disruption risk and hidden information. International Transactions in Operational Research, 2021, 28(4): 1864–1889.
[266] REN B A, LI M J, LIU H F, et al. Stackelberg game under asymmetric information in critical infrastructure system: from a complex network perspective. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2019, 29(8): 083129.
[267] ZHANG X X, DING S, GE B F, et al. Resource allocation among multiple targets for a defender-attacker game with false targets consideration. Reliability Engineering & System Safety, 2021, 211: 107617.
[268] LIU B H, SUN J T. Applying Stackelberg active deception game for network defense: from the perspective of imperfect network node information. Proc. of the 1st International Conference on Control and Intelligent Robotics, 2021: 28−32.
[269] TAMBE M. Security and game theory: algorithms, deployed systems, lessons learned. Cambridge: Cambridge University Press, 2011.
[270] GU X Q, ZENG C Y, XIANG F T. Applying a Bayesian Stackelberg game to secure infrastructure system: from a complex network perspective. Proc. of the 4th International Conference on Automation, Control and Robotics Engineering, 2019: 1−6.
[271] ZENG C Y, REN B A, LIU H F, et al. Applying the Bayesian Stackelberg active deception game for securing infrastructure networks. Entropy, 2019, 21(9): 909.
[272] JIANG J, LIU X. Bayesian Stackelberg game model for water supply networks against interdictions with mixed strategies. International Journal of Production Research, 2021, 59(8): 2537–2557.
[273] BAYKAL-GUERSOY M, DUAN Z, POOR H V, et al. Infrastructure security games. European Journal of Operational Research, 2014, 239(2): 469–478.
[274] GUAN P Q, HE M L, ZHUANG J, et al. Modeling a multi-target attacker-defender game with budget constraints. Decision Analysis, 2017, 14(2): 87–107.

Biographies

YANG Kewei was born in 1977. He is a professor with National University of Defense Technology. He serves as the director of Systems Engineering Society of China, and the vice president of Systems Engineering and Management Society of Hunan Province. He has been the head of Technology Innovation Group of Hunan Province named Big Data and System of Systems Engineering since 2020. His research interests focus on system-of-systems engineering, complex systems theory and complex equipment test and evaluation.
E-mail: kayyang27@nudt.edu.cn

LI Jichao was born in 1990. He received his B.E. degree in management science, M.E. and Ph.D. degrees in management science and engineering from National University of Defense Technology, Changsha, Hunan, China, in 2013, 2015, and 2019, respectively. He is currently an associate professor of management science and engineering at National University of Defense Technology. In 2017−2019, he was a visiting predoctoral fellow at the Northwestern Institute on Complex Systems (NICO) and Kellogg School of Management at Northwestern University, USA. His research interests focus on studying complex systems with a combination of theoretical tool and data analysis, including mathematical modeling of heterogeneous information networks, applying network methodologies to analyze the development of complex system-of-systems, and data-driven studying of the collective behavior of humans.
E-mail: ljcnudt@hotmail.com

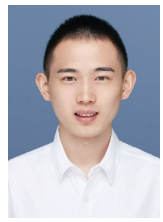
LIU Maidi was born in 1995. He received his B.E. degree in management engineering from National University of Defense Technology, Changsha, Hunan, China, in 2017. He is currently a Ph.D. student in management science and engineering at the College of Systems Engineering, National University of Defense Technology. His research interests focus on complex systems, complex network, and data mining.
E-mail: lmdnudt@hotmail.com

LEI Tianyang was born in 1994. He received his B.S. and M.S. degrees from Taiyuan University of Technology and University of Chinese Academy of Sciences in 2017 and 2020, respectively. He is currently a Ph.D. candidate at the College of Systems Engineering, National University of Defense Technology, Changsha, China. His research interests include Internet of Things, graph neural network, data mining, and complex networks.
E-mail: leitianyang20@163.com

XU Xueming was born in 1998. She received her B.E. degree in management science and engineering from Hefei University of Technology, Hefei, Anhui, China, in 2020. She is a master's student in management science and engineering from National University of Defense Technology. Her research interests include network disintegration and cascading effects.
E-mail: xueming_x2m@163.com

WU Hongqian was born in 1997. She received her M.E. degree in marine science from National University of Defense Technology, Changsha, Hunan, China, in 2021. She is a Ph.D. student in management science and engineering from National University of Defense Technology. Her research interests include higher-order systems and networks.
E-mail: wuhongqian19@nudt.edu.cn

CAO Jiaping was born in 1999. She received her B.E. degree in industrial engineering from Northeast Forestry University, Harbin, Heilongjiang, China, in 2021. She is an M.E. student in management science and engineering with National University of Defense Technology. Her research interests include complex system and complex network, and heterogeneous information network link prediction.
E-mail: jiapingcao@126.com



QI Gaoxin was born in 1998. He received his B.S. degree in mathematics and applied mathematics from Harbin Institute of Technology, Harbin, Heilongjiang, China, in 2020. He is a postgraduate student at National University of Defense Technology. His research interest focuses on evolutionary game theory of complex networks.
E-mail: qi198@foxmail.com