Hindawi
Security and Communication Networks
Volume 2022, Article ID 2036370, 17 pages
https://doi.org/10.1155/2022/2036370

Research Article

Research on the Identification of Internet Critical Nodes Based on Multilayer Network Modeling

Yongheng Zhang,[1,2] **Yuliang Lu**,[1,2] **Guozheng Yang**,[1,2] **and Zhihao Luo**[1,2]

[1]*Electronic Engineering Institute, National University of Defense Technology, Hefei 230037, China*
[2]*Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Anhui, China*

Correspondence should be addressed to Guozheng Yang; yangguoz0218@163.com

Received 4 July 2022; Accepted 29 August 2022; Published 10 October 2022

Academic Editor: Shudong Li

The research goal of cyberspace security situational awareness analysis is to predict the future security development of the target network by acquiring, understanding, and displaying the security elements in the large-scale network environment. Current cyberspace security situational awareness systems are mostly based on traditional single-layer network topology to analyze the security of the target network's operational posture. However, as the scale of the network continues to expand, the network structure becomes more complex, and the information fusion in multiple fields in practical applications deepens, the single-layer topology model can no longer meet the analysis requirements. In this paper, we construct a multilayer network topology model for cyberspace security situational awareness by integrating multidimensional information in the physical device layer network, business application layer network, and user role layer network. Meanwhile, to eliminate the limitations of traditional node importance indicators, a node importance assessment indicator that integrates topological centrality and node dependency factor is proposed in conjunction with model characteristics: multilayer dependency CRITIC indicator (MDCI). On the one hand, MDCI fits a variety of evaluation metrics through the CRITIC multi-attribute decision method to comprehensively assess the importance of nodes in network centrality, and on the other hand, MDCI better aggregates the important contributions of nodes in each network layer based on node dependency factor to coordinate multilayer network information. The experimental results show that MDCI has better ordering monotonicity and generates more stable metric sequences, and can effectively cause large-scale failures in multilayer network while destroying fewer physical device components, which can be better adapted to the critical node identification needs of multilayer network.

1. Introduction

In the field of cyberspace security situational awareness, to better portray the operation status of the user network, the network topology will be used as the background in related technology products to generate network security posture by aggregating information obtained from devices such as firewalls, intrusion detection, traffic monitoring, honeypots, vulnerability scanning [1–5], and the operation log information of terminal servers, to support the security operation and maintenance management of the network.

He [6] based on the double-feedback Elman model selected relevant indicators, established a security posture indicator system, and proposed a backpropagation neural network model to evaluate the situational values. Zhao [7] established multisource alarm data fusion rules based on improved D-S evidence theory to improve the accuracy of event detection. Tao [8] proposed a novel network security posture assessment method based on stacked self-coding networks and backpropagation neural networks, which can further reduce the complexity of model construction.

However, the current network topology information acquisition and analysis is mainly targeted at the interconnection level of network devices, and the configuration information table and routing information within routers and switches are obtained through authorization to portray the internal topology of the entire protection network. From the perspective of analyzing intradomain routing protocols,

most of the relevant studies are based on the OSPF protocol for topology discovery [9]. Due to the hierarchical design characteristics of the Internet itself and the different associations formed by various users when using the network, this topology based solely on the interconnection layer of that network device has significant limitations in characterizing the network security posture, which is mainly reflected in the following four aspects:

(i) The single-layer network topology model cannot characterize the business association relationships formed between network applications based on data traffic. The business systems in the network may differ greatly according to the business direction of the actual usage scenario. For example, for a campus network, it may include a student registration system, a student course selection system, a smart classroom system, a security management system, and various sites and forums for organizing student activities. In addition to interconnection at the network layer based on routing and switching equipment, these business systems and their client software will also establish logical link relationships based on the characteristics of their business systems themselves.

(ii) The single-layer network topology model cannot characterize the interpersonal relationships formed among network users based on business associations and communication interactions. People often have multiple virtual user roles in the process of using the network, which is reflected in the use of various business systems, mailboxes, forums, and instant messengers as various types of accounts or identity IDs, and these different individual virtual user roles will form an association relationship between each other through business access. In the current situation generation, there is a lack of such information acquisition and analysis, so there is still a large deficiency in analyzing abnormal user behavior and its associated user accounts.

(iii) After discovering anomalous network behavior, the simple device-level network topology is not sufficient for threat correlation analysis. Current cyberspace security threat incidents may be based on multiple business systems as a springboard, using multiple associated user accounts to participate together. Therefore, for the discovered network anomalous behavior, it is necessary not only to correlate device analysis at the physical device layer, but also to correlate business system analysis at the business application layer, and more importantly to correlate account analysis at the user role layer. Only by constructing multilayer network topology relationships across multiple dimensions from different levels for the whole network, it is possible to provide important support for comprehensive analysis when anomalies occur.

(iv) The single-layer network topology model has insufficient support information for critical node discovery, and the structural information of the network is monolithic. Most of the current methods for discovering important nodes in the network are based on the association relationship of physical devices, combined with topological centrality and subjective scaling for importance assessment. However, in terms of the overall operating posture of the multidimensional network, the access relationship between the physical devices and terminals that carry the business system, and the structural characteristics of the higher virtual user base all play a supporting role in determining the importance of a device in the network. Therefore, only by integrating multilayer network topology information can the set of critical nodes in the network security posture model be discovered more effectively.

To address the above-mentioned problems of the traditional topological model of cyberspace security situational awareness, we design an analysis framework that comprehensively characterizes the operation state of the entire network at three levels: physical device layer, business application layer, and user role layer. Meanwhile, based on this network topology model, this paper proposes a critical node identification method that can fuse multidomain network information and consider component dependencies to comprehensively evaluate the importance of nodes in a multilayer network topology model.

The structure of the study is organized as follows: Section 2 presents the theoretical sources and modeling ideas of the multilayer network topology model for cyberspace security situational awareness; Section 3 proposes a critical node identification metric that fuses topological centrality and network dependencies for multilayer network topology models: the multilayer dependency CRITIC indicator (MDCI); Section 4 evaluates the discovery results of MDCI evaluation metrics based on simulated experiments and network analysis in four dimensions: monotonicity, validity, similarity, and interlayer correlation; and Section 5 analyzes the reasonableness of the method and related deficiencies of this paper with the experimental results, and proposes relevant improvement ideas.

2. The Multilayer Network Topology Model for Cyberspace Security Situational Awareness

2.1. Network Model Research Foundation. Heterogeneous interdependent networks are complex networks with different elemental attributes and certain dependencies between heterogeneous nodes; i.e., when a node in a heterogeneous interdependent network changes its state, it usually has a certain impact on its neighborhood node group and transmits to the whole network, forming a Markov-like process of network state transfer. Therefore, this model is applied to the situational awareness system of the information-physical two-layer interdependent network [10]. When the power supply node fails, it will be able to monitor that the fault will propagate along the power supply path and affect other power supply nodes or load nodes, and then have

an impact on the upper information network [11, 12]. The definition has also been used to establish the relevant multilayer heterogeneous dependency framework in both the transportation and biological domains [13, 14]. The relevant definitions are as follows.

Definition 1. Heterogeneous networks (HN).

Let $G = (V, E; \phi, \psi; A, R)$ be a directed graph, where $V = \{v_1, v_2, \ldots, v_N,\}$ is the set of nodes, and $E = \{e_1, e_2, \ldots, e_N,\}$ is the set of edges. There exists a node-type mapping function $\phi: V \longrightarrow A$ satisfying $\phi(v) \in A(v \in V)$ and an edge-type mapping function $\psi: E \longrightarrow R$ satisfying $\Psi(e) \in R(e \in E)$. When the number of node types $|A| > 0$ or the number of edge types $|R| > 0$, then G is said to be a heterogeneous network.

Definition 2. Heterogeneous interdependent networks (HIN).

Let the directed graph $G = (V, E; \phi, \psi; A, R)$ be a heterogeneous network. The set of elements T_a and T_b are subsets of the set of nodes V or the set of edges E and satisfy $T_a \cap T_b = \varnothing, |T_a| > 0, |T_b| > 0$. If state $f(T_a)$ of set T_a becomes unstable (or fails), it will cause state $f(T_b)$ of set T_b to tend to be an unstable state or even fail.

However, combined with the practical application context of cyberspace security situational awareness, the classical heterogeneous interdependent network model cannot effectively characterize the existence of multiple heterogeneous links and multilayer network dependencies in real networks, so the research framework of situational awareness based on heterogeneous interdependent networks has the limitations as follows:

(i) *Homogenization of Link Dependencies*. In the current research, most of the studies on the association relationships of heterogeneous nodes in networks focus on the case where there are only two kinds of linkage relationships, "direct dependency" or "indirect dependency," which is useful for defining and discovering heterogeneous power grids, grid-information networks, and other network structures. However, for the interdependent network structure consisting of a physical resource network-computing resource network and other multidomain networks, the heterogeneous nodes not only have dependency relationships to characterize the coupling degree between networks, but also have interconnectivity relationships, i.e., undirected links to characterize the connectivity of networks (communication accessibility and business access relationship), so it is necessary to further introduce link heterogeneity.

(ii) *Single-Node Failure Mechanism*. The node failure in the current HIN is defined as a dependent node entering the failure state only when all the support nodes of a dependent node fail or reach a threshold value of the failure ratio. However, in communication backbone networks, for example, the links between device nodes represent network reachability and there is no interdependent relationship between certain heterogeneous nodes, but in fact, in communication-type networks, a node will be considered to enter a failure state when it is separated from the largest component of the network, so the node failure mechanism needs to be further extended.

(iii) *Distinguishment of the Importance of Network Layers*. The currently proposed critical node identification method based on heterogeneous interdependent networks uses the idea of network merging, which essentially adopts the idea of dependency conduction of single-layer networks, ignores the dependency weights between layers, and fails to address the situation that the endpoints of a link may come from different network layers.

In summary, based on the theory of heterogeneous interdependent networks, we design a multilayer network topology model for cyberspace security situational awareness, which is a three-layer network model capable of fusing multidomain network information with interdependent and interconnectivity network characteristics. It can provide important support for the identification of critical nodes in cyberspace security situational awareness. The model can help researchers assess the importance of nodes in the network from the perspective of the overall architecture of a multilayer network and enhance the security control of the underlying end nodes located at the edge of the network of physical devices.

2.2. Structure and Description Method of the Multilayer Network Topology Model for Cyberspace Security Situational Awareness. In our study, we propose a multilayer network model consisting of a combination of three network layers: physical device layer, business application layer, and user role layer:

(i) The physical device layer network (labeled as PD) consists of three types of components: router, server, and terminal. Among them, routers support routing functions in the communication process of the physical device network, servers provide deployment environments for important service systems, and user terminals are physical devices (e.g., mobile devices and PC) for ordinary users to access the network; in this layer of the network, each routing component forms an undirected association based on communication behavior, while servers and user terminals in a certain subnet depend on the gateway route based on the admission conditions, forming a directed dependence.

(ii) The business application layer network (labeled as BA) consists of business system nodes and access nodes. The business system node represents a network business system and carries related service functions, and the access node is a network node that has constituted access related to a business system, which is a mapping of user entity devices in

the business access relationship, and each business component is an undirected association relationship formed based on the access relationship.

(iii) The user role layer network (labeled as UR) is a social group formed by the virtual roles represented by user accounts or IDs identifiers in various business systems due to user behavior or business association, and there is an undirected association relationship between each user role based on user behavior.

Meanwhile, the following relationships exist for different network layers based on logical associations and component dependencies. First, the communication devices of the physical device layer network provide the physical support for the access associations of the various components within the business application layer. For example, since the servers in the physical device layer provide the deployment environment for the business systems in the business application layer, they form a directed dependency; i.e., if the server node fails, then the corresponding business system node will also fail. Similarly, a similar dependency relationship exists between user terminal nodes and access nodes. Between the business application layer network and the user role layer network, on the one hand, each user identity in the user role layer is based on user behavior habits, and the user is related to the access node; on the other hand, the user identity belongs to a specific business system; when the business system crashes, the account will no longer be able to request related services, which is regarded as a frozen state. Therefore, a user role node and its related access nodes may have an undirected association relationship (the account has no restrictions on logging in to the device)/directed dependency relationship (when the device is bound to the account). Moreover, there is a directed dependency relationship between the user role node and the business system node to which it belongs. The multilayer network model structure is shown in Figure 1.

To sum up, the network topology of the physical device layer is used to analyze the interconnection of the entire network device set as the basic support for daily operation and maintenance; the network topology of the business application layer is used to monitor the relationship between the running status of various business systems and business traffic at the application layer, so as to detect abnormal access conditions in time; the user role layer topology is used to construct the access relationship and social communication relationship between network user accounts, and to warn of possible abnormal behaviors of related accounts. The model can provide an important support role for network security situational analysis and auxiliary decision-making. Compared with the traditional single-layer network topology model, this multilayer network topology model for cyberspace security situational awareness has the following advantages:

(1) The business associations formed between network applications are successfully characterized in the multilayer network topology model, and this situational awareness framework can provide data support for security operations and maintenance in business systems in conjunction with traffic information.

(2) Based on the business association, the model includes the communication association between network users based on business access and social behavior, which complements the user-level analysis in situational awareness and refines the granularity of association analysis to the user level.

(3) The model establishes a multilayer network topology relationship across multiple dimensions, which enables the study and judgment of threat information from multiple perspectives when anomalies occur in the network and provides important support for comprehensive analysis of cyberspace security posture.

(4) Extracting link attributes between nodes from networks in different domains and integrating domain-wide situational information can effectively support the discovery of critical nodes.

3. Critical Node Identification Method

Analyzing the coupling structure in the multilayer network topology model proposed in this paper, we can find that the connection relationship between nodes in this multilayer network can be decomposed into two categories: interconnectivity relationship and interdependent relationship. Therefore, it can be seen that the importance of a node in a multilayer network depends on two aspects: on the one hand, in terms of interconnectedness, the topological centrality of a node in this network layer determines its importance in this network layer; on the other hand, in terms of interdependence, some nodes play a supporting role to the related dependent nodes, and the functionality of a dependent node is directly related to it, so the importance of its dependent node will also be used as a reference for the importance of that node. From this perspective, this paper proposes an integrated topological centrality and dependency relationship approach to identify critical nodes in multilayer networks.

3.1. Importance Analysis of Nodes in the Multilayer Network Model for Cyberspace Security Situational Awareness. The coupling decomposition of the multilayer network topology model reveals that the connection relationship between nodes in the model can be analyzed at two levels: interconnectivity relationship and interdependent relationship.

In the interconnectivity relationship, based on the existence of a three-layer topology, it is known that the network structure varies greatly in different network layers due to the specificity of the application area to which the network layer topology belongs, and the topological centrality of the node in the network will determine its network importance in this layer. At this point, the failure mechanism in the defined association network is similar to the general communication network, adding an initial perturbation to the

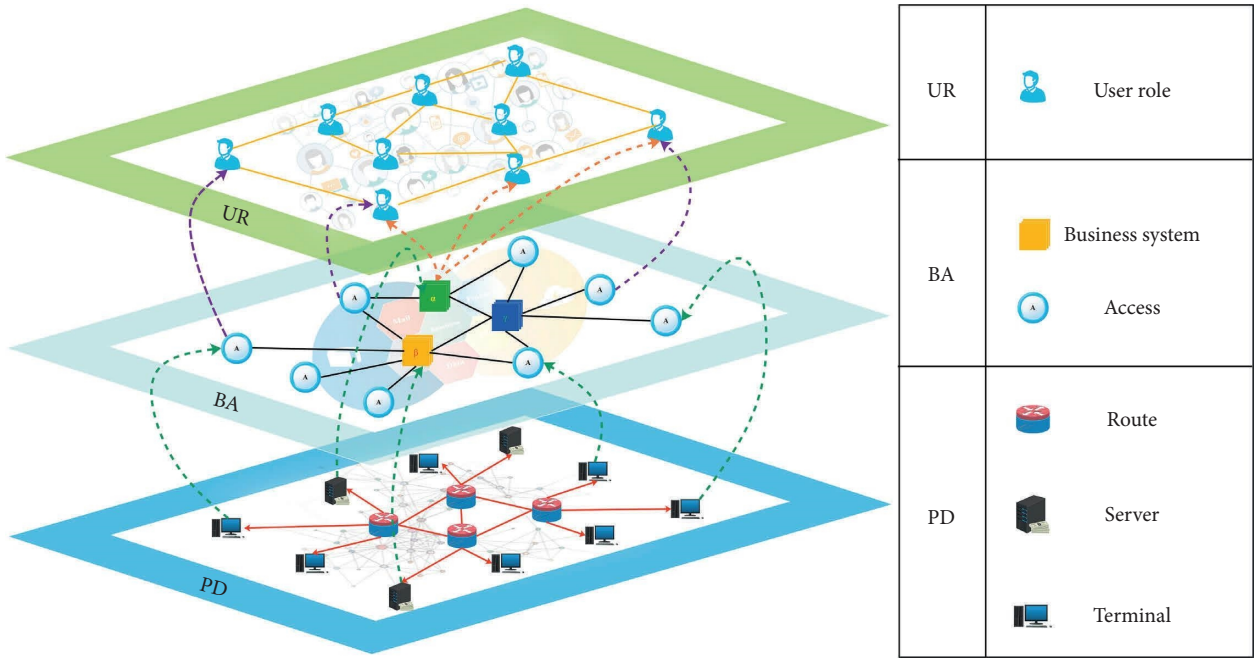


Figure 1: Structural diagram of the multilayer network topology model for cyberspace security situational awareness.

network, and the node and its associated connections fail when a node is affected by the initial disturbance resulting in the separation from the largest component of the network, as shown in Figure 2.

In the interdependent relationship, there are two kinds of dependencies: intralayer dependency relationship and interlayer dependency relationship. The intralayer dependency includes the dependency of servers and client terminals in the subnet on the incoming route, and when the incoming route fails, all devices in the subnet will not be able to access the Internet normally, which is defined as a failure state. The interlayer dependency is reflected in the support relationship between different network layers, including the operation and maintenance support capability of server nodes to business system nodes mentioned in the model, the direct mapping capability of client terminal hosts to access nodes, the dependency of virtual user roles to business system nodes, and the dependency of virtual users to access nodes that may exist when accounts are bound to devise IPs. In the interdependent network, an initial perturbation is added to the network, defining that a node and its associated connections fail when the set of support nodes for a node fails due to the initial disturbance, as shown in Figure 3.

Based on the coupling characteristics of this multilayer network topology model, this paper designs the critical node identification method from the following three requirements:

(i) The three-layer network topology often contains a large number of heterogeneous nodes, and the network scale is large, so the proposed node importance evaluation indicator needs good monotonicity, which can finely evaluate the node importance and try to avoid the decision ambiguity caused by a large number of nodes with the same importance ranking.

(ii) The structure of each network layer in the multilayer network topology model for cyberspace security situational awareness varies greatly, so the proposed node importance assessment index must consider all aspects of network structural information to avoid reducing the effectiveness of the assessment due to the singularity of the assessment perspective.

(iii) In the multilayer network topology model, there are different dependencies, so the proposed node importance assessment indicator must consider the degree of contribution of the existence of dependencies to the importance of each node, to avoid the unreasonable transmission of dependencies, resulting in weakened assessment rationality.

Based on the multilayer network topology, this paper proposes a critical node identification method that integrates node topological centrality and dependencies: multilayer dependency CRITIC indicator (labeled as MDCI), so it can lead to a better integrated assessment of node importance in multilayer networks, and the expression of MDCI is shown in the following equation:

$$\mathrm{MDCI}_i = TC_i + \sum_j k_{ij} \cdot s_j, \tag{1}$$

where i is the node to be evaluated, j is the dependent node that has a connection with i, TC_i characterizes the topological centrality importance of node i in the association relationship obtained based on the CRITIC multi-attribute evaluation method, s_j characterizes the importance of the dependent node j, and k_{ij} characterizes the network

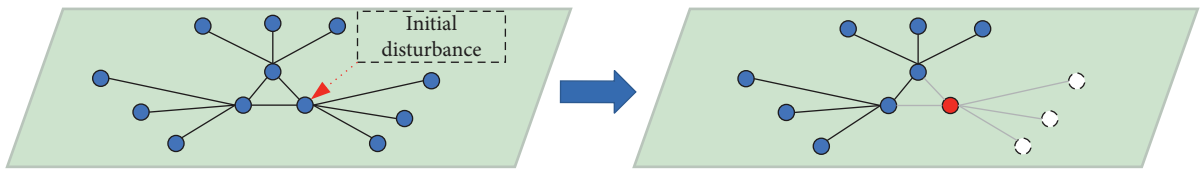


Figure 2: Node failure mechanisms in interconnectivity relationships.

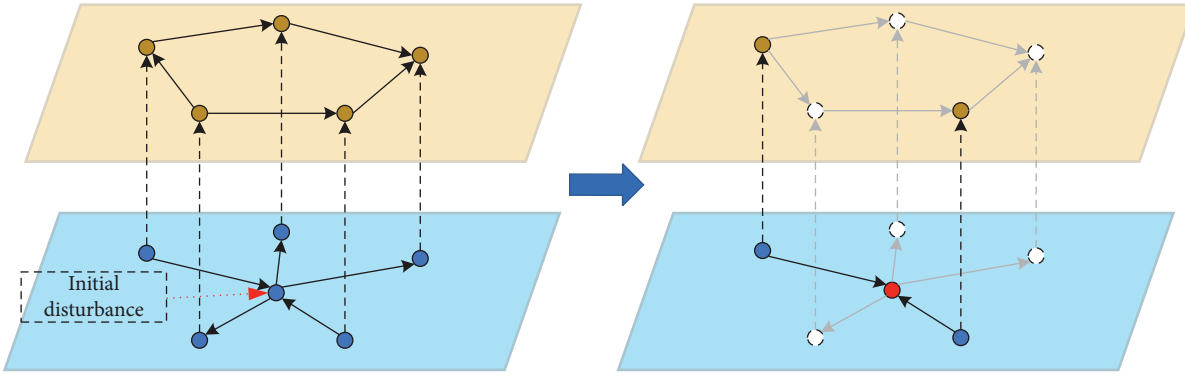


Figure 3: Node failure mechanisms in interdependent relationships.

dependency factor existing between the node i and the node j, and the discovery method for MDCI is described below in terms of node topological centrality evaluation and dependency evaluation, respectively.

3.2. Node Topology Centrality Evaluation. The multilayer network topology model is analyzed at the connectivity level, and at this time, there is only one decay mechanism in the network, which is the failure of nodes due to separation from the largest components of the network, so we can first rely on topological centrality assessment indicators for the study. Due to the ability of multi-attribute decision methods to construct metrics for comprehensive evaluation of target importance, they have been introduced in the field of complex networks as the main method for node importance assessment in recent years [13–17]. In our previous work, we [18] proposed a multi-attribute node importance assessment method for single-layer networks based on the CRITIC method, which can effectively overcome the problems of traditional centrality metrics with a single assessment perspective, lack of information about the analyzed network, and inability to comprehensively assess the importance of nodes. Therefore, in response to the metric design requirements of high monotonicity and comprehensive evaluation perspectives proposed in Subsection 3.1, this method will be used as the basis for the metric of node topological center in connectivity relationships and improved with the network characteristics, and the CRITIC method is described below.

3.2.1. Multiattribute Decision-Making Method—CRITIC. The CRITIC weight method is an objective weighting method based on data volatility that enables direct weight assignment based on ranking data without relying on subjective perceptions. The core idea of the CRITIC weight method is to assign weights to both the contrast strength and conflict degree information, where the contrast strength is expressed using the standard deviation of the assessment data under the same indicator; if the standard deviation is larger, it indicates that the assessment is more volatile and the weight will be higher. The conflict degree is expressed using the correlation coefficient value between different indicators' assessment data: if the larger the correlation coefficient value is, the weaker the conflict between different indicators is, and the lower the weight will be. The weights are calculated by multiplying the contrast intensity with the conflict degree indicator and are normalized to obtain the final weights.

The multi-attribute decision process based on the CRITIC method is as follows.

For pending evaluation set $A = \{a_1, a_2, a_3, \ldots, a_n\}$ with n selected objective and the indicator set $S = \{S_1, S_2, S_3, \ldots, S_m\}$ with m criteria, the decision matrix of the multicriteria problem can be defined as follows:

$$S = \begin{bmatrix} S_1(a_1) & S_2(a_1) & & S_m(a_1) \\ S_1(a_2) & S_2(a_2) & \cdots & S_m(a_2) \\ \vdots & \vdots & & \vdots \\ S_1(a_n) & S_2(a_n) & & S_m(a_n) \end{bmatrix}. \quad (2)$$

According to the concept of ideal point, for a certain assessment indicator S_j, the evaluated value of this indicator for set A to the interval [0, 1] is mapped to define the affiliation function Z_j. The definition of Z_{aj} is the degree to which alternative a is close to the ideal value S_j^+, in which S_j^+ indicates the best performance of criterion S_j. Meanwhile, Z_{aj} also indicates the extent to which alternative a is far from

the negative ideal S_j^-, and S_j^- indicates the worst performance of criterion S_j.

$$Z_{aj} = \frac{S_j(a) - S_j^-}{S_j^+ - S_j^-},$$
$$Z_j = \left(Z_j(1), Z_j(2), \ldots, Z_j(n)\right). \tag{3}$$

After that, the contrast strength and conflict degree of related indicators will be calculated separately.

$$\sigma_j = \sqrt{\frac{\sum_{i=1}^{n}\left(x_i^j - \overline{x}^j\right)}{n}}. \tag{4}$$

In the calculation of the contrast strength in (4), the standard deviation σ_j quantifies the contrast strength of vector Z_j, reflecting the variation of scores within the evaluation index, where x_i^j is the score of node i in the criterion S_j, and all object scores constitute the score vector x^j under this indicator system.

$$\text{Clash}_j = \sum_{k=1}^{m}\left(1 - \text{pearson}_{jk}\right). \tag{5}$$

In the conflict degree calculation of (5), next, combined with vector x^j , we can construct the $m \times m$ dimensional number score matrix. The conflict degree Clash_j between criterion S_j and other criteria is defined according to the Pearson coefficient (pearson_{jk}) between x^j and criterion x^k. The more inconsistent the distribution of x^j and x^k, the lower the value of the Pearson coefficient between them, which in turn leads to a stronger measure of conflicting differences between criterion S_j and the other criteria.

In summary, we can obtain the comprehensive information content Q_j emitted by the indicator by multiplicative aggregation of the contrast strength and the conflict degree.

$$Q_j = \sigma_j \times \text{Clash}_j. \tag{6}$$

The amount of information of the corresponding evaluation criterion increases with the value of Q_j: the greater the relative importance of the corresponding evaluation criterion in the decision-making process, the greater the weight of the corresponding indicator; normalizing the Q values of all indicators, we can obtain the decision weight ω_j.

$$\omega_j = \frac{Q_j}{\sum_{k=1}^{m} Q_k}. \tag{7}$$

Thus, the topological centrality of nodes at the level of connectivity relations can be characterized according to the CRITIC multi-attribute decision method as follows:

$$CRITIC_i = \sum_{j=1}^{m} \omega_j \cdot S_i^j. \tag{8}$$

3.2.2. Node Topology Centrality Indicator. Various centrality indicators have been proposed to measure the influence of nodes in complex networks: degree centrality (labeled as DC) [19], betweenness centrality (labeled as *BC*) [20], closeness centrality (labeled as *CC*) [21], network constraint coefficient (labeled as *NCC*) in structural hole theory [22], H-index (labeled as *H*) [23], K-core indicator (labeled as *KS*) [24], eigenvector centrality (labeled as *EC*) [25], etc.

The research idea of designing multi-attribute evaluation metrics is to synthesize multiple node importance information for critical node discovery, so the strategy of selecting subattributes must be based on application requirements. Since the structure of each layer in the multilayer network topology model oriented to cyberspace security situational awareness varies greatly and the submetrics are evaluated from similar perspectives, which will cause instability of evaluation effects in different networks, the selection of submetrics must be filtered under different evaluation perspectives. Classical topological centrality assessment metrics and classifications are shown in Table 1.

In this paper, four types of topological centrality indicators are summarized, and to ensure the effectiveness of the multi-attribute evaluation method, it should cover as much node centrality information as possible and reduce the input of homogeneous information, combined with the node deletion effect of the above metrics and monotonicity calculation in the experimental network in the pre-experiment (see in S1); a total of four centrality indicators of degree centrality, betweenness centrality, closeness centrality, and network constraint coefficient are selected in this paper to join the set of submetrics in the multi-attribute decision-making method, and the relevant metrics are defined as follows.

Definition 3. (*DC*). The degree centrality (*DC*) of node i is noted as DC_i and defined as follows:

$$DC_i = \sum_{j}^{N} x_{ij}. \tag{9}$$

In (9), i is the node to be evaluated, and j represents the other nodes in the network that represents the connection status between node i and node j, taking 1 (exists) or 0 (does not exist) depending on whether the link exists or not, respectively. N represents the total number of nodes in the network. The degree characterizes the total number of neighboring nodes around the target node that are connected to it, i.e., the degree of connectivity of the target node in the local network.

Definition 4. (*BC*). The betweenness centrality (*BC*) of node i is noted as BC_i and defined as follows:

$$BC_i = \sum_{k \in V} \frac{n_{jk}(i)}{n_{jk}}, (i \neq j \neq k). \tag{10}$$

In (10), n_{jk} is the number of shortest paths between any two nodes j and k in the network, and $n_{jk}(i)$ is the number of shortest paths that pass through a subset of node i in these shortest paths. The betweenness centrality measure characterizes the degree of contribution of the node in the network communication process.

Table 1: Topological centrality indicators and their classification.

Indicator type	Symbols	Description
Adjacency importance	*DC* *H*	The node importance is evaluated based on the number of neighbors in the neighborhood of the pair of nodes.
Network topology location	*CC* *KS*	Node importance is evaluated based on the location of the node in the network, i.e., how far it is from the center of the topology.
Path centrality	*BC*	The importance of nodes is evaluated based on the shortest path information in the network.
Mutual information volume	*NCC* *EC*	Node importance is evaluated based on the amount of information about the interactions between nodes.

Definition 5. (*CC*). The closeness centrality (*CC*) of node i is noted as CC_i and defined as follows:

$$CC_i = \frac{(N-1)}{\sum_{j=1}^{N} d_{ij}}. \tag{11}$$

In (11), d_{ij} represents the shortest path length between node i and node j. N represents the total number of nodes in the network. The closeness centrality measure is the distance between a node and other nodes in the network and characterizes the proximity between that node and the center of the network.

Definition 6. (*NCC*).The network constraint coefficient *NCC* of node i is denoted as NCC_i and defined as follows:

$$NCC_i = \sum_j \left(r_{ij} + \sum_q r_{iq} r_{qj} \right)^2, i \neq q \neq j, r_{ij} = \frac{Z_{ij}}{\sum_q Z_{iq}}. \tag{12}$$

In (12), r_{ij} is the ratio of resources allocated by i to j, node q lies in the first-order neighborhood of both node i and node j, as an indirect connection point between them represents the strength of the connection between node i and node j. It is known that r_{ij} is the direct connection strength and $\sum_q r_{iq} r_{qj}$ is the indirect connection strength, so NCC_i takes values between [0, 1]. The network constraint coefficient represents the information advantage and control advantage of the nodes in the network structure. The lower the network constraint coefficient is, the more obvious is the degree of structural holes in the evaluation nodes and the more important is the role they play in the network structure.

Therefore, in combination with the CRITIC multi-attribute decision method, the topological centrality (*TC*) of nodes at the level of connectivity relations can be characterized as follows:

$$TC_i = \omega_1 \cdot DC_i + \omega_2 \cdot BC_i + \omega_3 \cdot CC_i + \omega_4 \cdot NCC_i. \tag{13}$$

3.3. Node Dependency Importance Assessment. After the decomposition of the network coupling relationship, from the analysis of the interdependent relationship level, there is only one decay mechanism in the network, which is the failure of the interdependence between the supporting nodes and the dependent nodes; in this decay mechanism, the importance of the node depends on the degree of support to the directly dependent or indirectly dependent nodes: the more related dependent nodes the node has, the greater the importance of the dependent nodes is, the higher the importance of the corresponding nodes is, and the more the importance of the nodes can be transmitted between the nondirectly connected network layers through the intermediate layer.

When the importance of nodes is transferred across layers based on the degree of dependence, treating the importance between layers as equivalent will result in an uneven distribution of weight between intralayer and interlayer relationships and a significant focus on one aspect, thus losing the rationality of the assessment. Therefore, the index of dependency factor (labeled as *DF*) is proposed here to measure the degree of dependency between different network layers as a basis for weighting the importance of nodes for transmission. The dependence factor (*DF*) is characterized as follows:

$$DF_{\alpha\beta} = \frac{M_{\alpha\beta}^{\text{dependent}}}{N_{\beta}^{\text{dependent}}}. \tag{14}$$

In (14), α characterizes the support layer network in the adjacency network layer, i.e., the support network containing the support nodes; β characterizes the dependency network in the adjacency network layer, i.e., the dependency network containing the set of dependency nodes; $M_{\alpha\beta}^{\text{dependent}}$ characterizes the total number of dependent links between the neighboring layer networks; and $N_{\beta}^{\text{dependent}}$ indicates the number of dependent nodes within the dependent network layer. In the composition of the dependency factor, since the anomaly of the support node can directly lead to the functional failure of the dependent node, more dependent connections between network layers represent the stronger dependency of the dependent layer network on the support layer network and the stronger influence by the support network.

When the dependent nodes and the supporting nodes are located in the same network layer, the intralayer importance ratio is set to $DF = 1$ due to the internode dependency effect. The proposed dependency factor ensures that the node importance can be weighted according to the layer importance when intralayer and interlayer transfer is performed.

3.4. Critical Node Identification Process. In summary, the node importance indicator MDCI proposed in this paper can pass node importance scores based on the decomposition of network coupling relationships, and integrate node association importance and dependency importance for the discovery of critical nodes in multilayer networks.

The critical node identification process is shown in Figure 4.

The critical node discovery process for MDCI consists of five phases:

(S1) Network input phase: based on the target network data, the set of nodes and links are extracted and the network topology is constructed.

(S2) Topological centrality calculation phase: based on the CRITIC multi-attribute decision method, multiple node metric scores are fused to evaluate node topological centrality.

(S3) Dependency factor calculation stage: based on the node dependencies and interlayer connection characteristics, the dependency factor between nodes are calculated.

(S4) Comprehensive node importance assessment phase: based on the dependency factor, the topological centrality score of the fused nodes is used to calculate the node importance.

(S5) Sequence output stage: output critical node sequence is calculated according to node importance.

4. Simulation Experiments and Network Analysis

To further validate the effectiveness of the proposed critical node identification method MDCI in a multilayer network topology model for cyberspace security situational awareness, we use a three-layer network (physical device layer, business application layer, and user role layer) as a network example for validation experiments. The dataset used in this paper is the "regional business operations" three-tier network [26]. The network uses a heuristic algorithm to build a "one-to-one" dependency between physical devices and service application layers based on the collection of regional routing topology data: the failure of a server node leads to the immediate failure of its corresponding service system node, and the failure of a user terminal leads to the immediate failure of its corresponding access node; and "many-to-many" dependencies between the business application layer and the user role layer: i.e., the failure of a business system node or access node causes the immediate failure of its corresponding user node. The network contains three network layers, with 31957 nodes and 168277 links. It can be seen that in this paper, under the conditions of network security situational awareness context, the relevant datasets in the research process do not have weights and directions, and the link directions in the model characterize the control relationships between dependent node pairs rather than the data or information flow, and the importance measurement of the relevant nodes will be performed in such networks.

In addition to the critical node discovery metrics MDCI presented in this paper, seven centrality indicators (DC, BC, CC, NCC, H, KS, and EC) and the randomized strategy (RA) were used as the experimental reference group in this experiment.

From the structural analysis of the three-layer network, combined with the application context, we can clarify that the purpose of establishing a three-layer network topology is to use the business-level and user social-level information to support the importance evaluation score of the physical device components to ensure a more comprehensive assessment of the importance of the physical layer components, and because the support network layer in the multidomain network is the physical device layer, only when the failure of various components is within the physical device layer, the failure can be passed to the entire network topology through the dependent links to cause the decline in total network structure.

From the MDCI critical node discovery idea, the importance of the nodes in the upper two layers of the final three-layer network will be aggregated to the physical device layer through dependency conduction, which becomes the basis for judging the importance of various physical components, and theoretically, these final aggregation nodes in this layer will be at the top of the ranking.

Therefore, when generating node importance ranking sequences using various types of non-neighborhood centrality metrics (*BC*, *CC*, *KS*, and *EC*), we set their evaluation scope to the physical device layer to ensure consistency at the evaluation level.

The network node failure ratio θ of the three-layer network was used in the experiments to determine the degree of impact of node failure on the structural integrity of the network, θ, as defined below:

$$\theta = \frac{L_{P\,D}^{\text{loss}} + L_{BA}^{\text{loss}} + L_{UR}^{\text{loss}}}{L_{P\,D} + L_{BA} + L_{UR}}. \tag{15}$$

In (15), $L_{P\,D}, L_{BA}, L_{UR}$ denote the total number of nodes in the physical device layer, business application layer, and user role layer of the network topology, respectively. $L_{P\,D}^{\text{loss}}, L_{BA}^{\text{loss}}, L_{UR}^{\text{loss}}$ denote the number of network failure nodes at the physical device layer, business application layer, and user role layer, respectively, during the experiment.

Next, the experimental section will analyze the proposed critical node identification method from four perspectives: monotonicity, validity, similarity, and interlayer failure correlation.

4.1. Ranking Monotonicity Analysis. Ranking monotonicity is an important metric for the performance evaluation of critical node discovery methods. Higher ranking monotonicity means that the size of the set of moderate scores of the node output sequence is smaller, the ambiguity in making important decisions is weaker, and the granularity of importance evaluation is finer. The monotonicity index [27] is defined as follows:

$$M_i^p = \left(1 - \frac{\sum_{i \in i} N_i\left(N_i - 1\right)}{N^p\left(N^p - 1\right)}\right). \tag{16}$$

In (16), the set of nodes to be evaluated for monotonicity is often selected using sampling if the network size is large, P represents the proportion of the subset of nodes to be

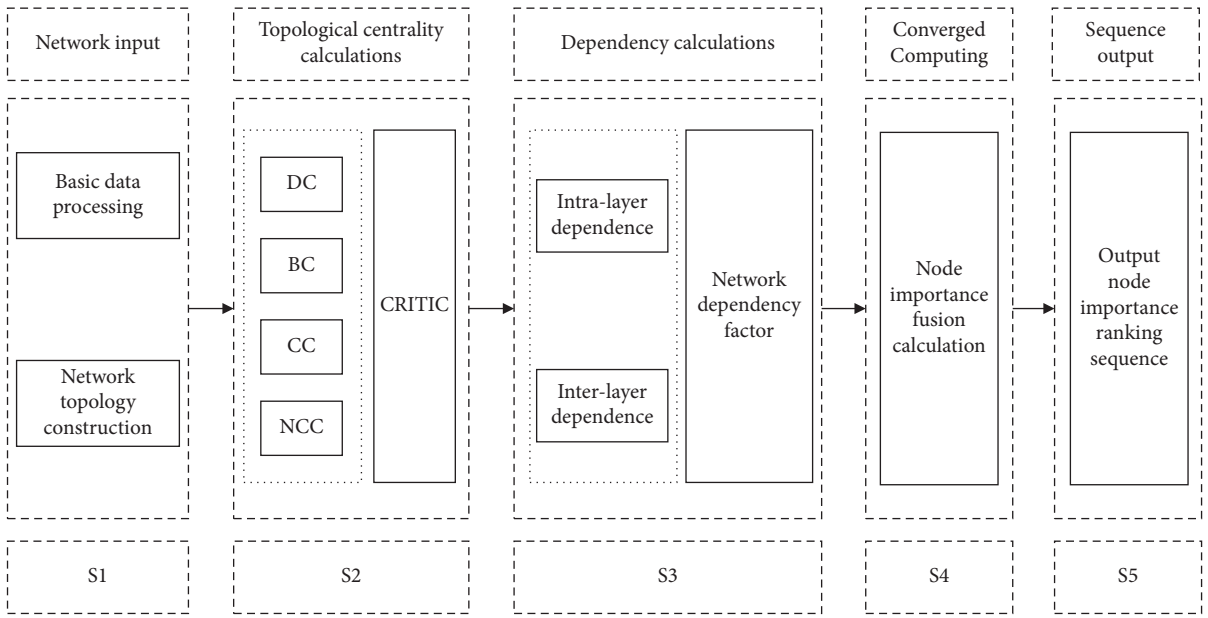


Figure 4: MDCI critical node identification process.

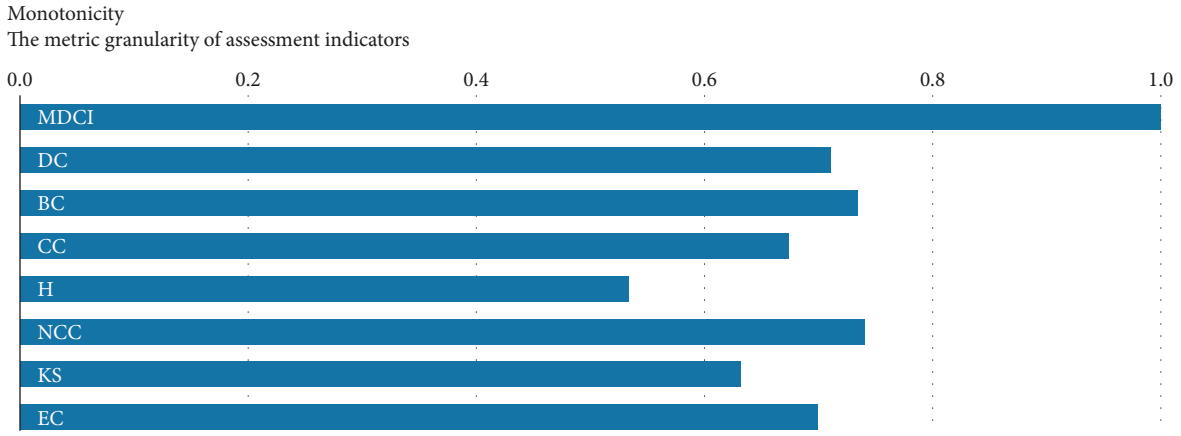
evaluated selected from the network nodes to the total number of nodes, N^p is the size of the set of nodes to be evaluated, and N_i is the number of nodes of each node group with the same score in the set of nodes to be evaluated. In this experiment, the top ten percent of nodes in the physical layer network layer in the ranking of MDCI and other indicators (DC, BC, CC, NCC, H, KS, and EC) are selected as nodes to be evaluated, and the monotonicity of each metric is shown in Figure 5. It can be observed that the monotonicity of the proposed node importance assessment indicator MDCI is close to 1.0 compared with other indicators, which means that the importance of each node in the framework of this index system is accurately classified. The reason is that MDCI integrates network topology information from multiple perspectives into the evaluation of node importance, avoiding the drawback of a large number of nodes with the same importance caused by a single evaluation perspective of a single indicator.

4.2. Method Validity Analysis. The node removal experiment is the main method to verify the effectiveness of the critical node discovery method. The experimental idea is to judge the effectiveness of the node importance assessment indicator by observing the change of node failure ratio in the network after removing a single node or a sequence of consecutive nodes. This section uses two types of removal strategies: one is to remove the target nodes individually in order of importance and calculate the node failure ratio; the other is to remove a set of sequences of consecutive nodes in order of importance.

In the individual node removal strategy, Figure 6 shows the correlation between the experimental network and the node importance ranking positions obtained according to the eight ranking methods and the percentage of node failures in the network when a single node is removed. The horizontal coordinates of the nodes in Figure 6 characterize the importance ranking of the nodes in each critical node discovery method, with higher rankings indicating higher importance scores of the nodes in that method; the vertical coordinates characterize the node failures after the corresponding nodes are removed. The experiment selects the top 100 node removal effects of each indicator for demonstration.

As shown in Figure 6, the MDCI importance ranking results of the node importance evaluation indicator proposed in this paper are the most reasonable, where the proportion of node failures caused by node removal in the network decreases as the node importance ranking decreases. The reason why some of the nodes in the top 50 have a smaller proportion of failures caused by node removal is that most of these nodes are important routing nodes that play the function of communication scheduling at the physical device layer or that gateway routes in the subnetwork they belong to are not deployed in important service systems and therefore score higher. For DC, BC, CC, and NCC, although the ranking of these four types of metrics can find the nodes with greater influence in a certain range, they cause unreasonable node ranking because they only combine the importance of node neighborhood and the amount of information in a single layer, and cannot be considered in a comprehensive three-layer topology. H and KS metrics, on the contrary, have coarse ranking results because a large number of nodes are located in the same score sequence during the importance assessment, and cannot effectively discover important nodes. EC focuses on the enrichment of important nodes in the process of node importance assessment and does not apply to the structure of the communication network where the components are distributed to perform functions, so the ranking results are scattered.

Removal strategy. In the sequential node sequence removal strategy, Figure 7 shows the variation in the percentage of



Sources: The top 10% nodes of the physical device layer under each evaluation index system are used as the monotonicity measurement set

Figure 5: Monotonicity performance of different critical node discovery methods on experimental networks.

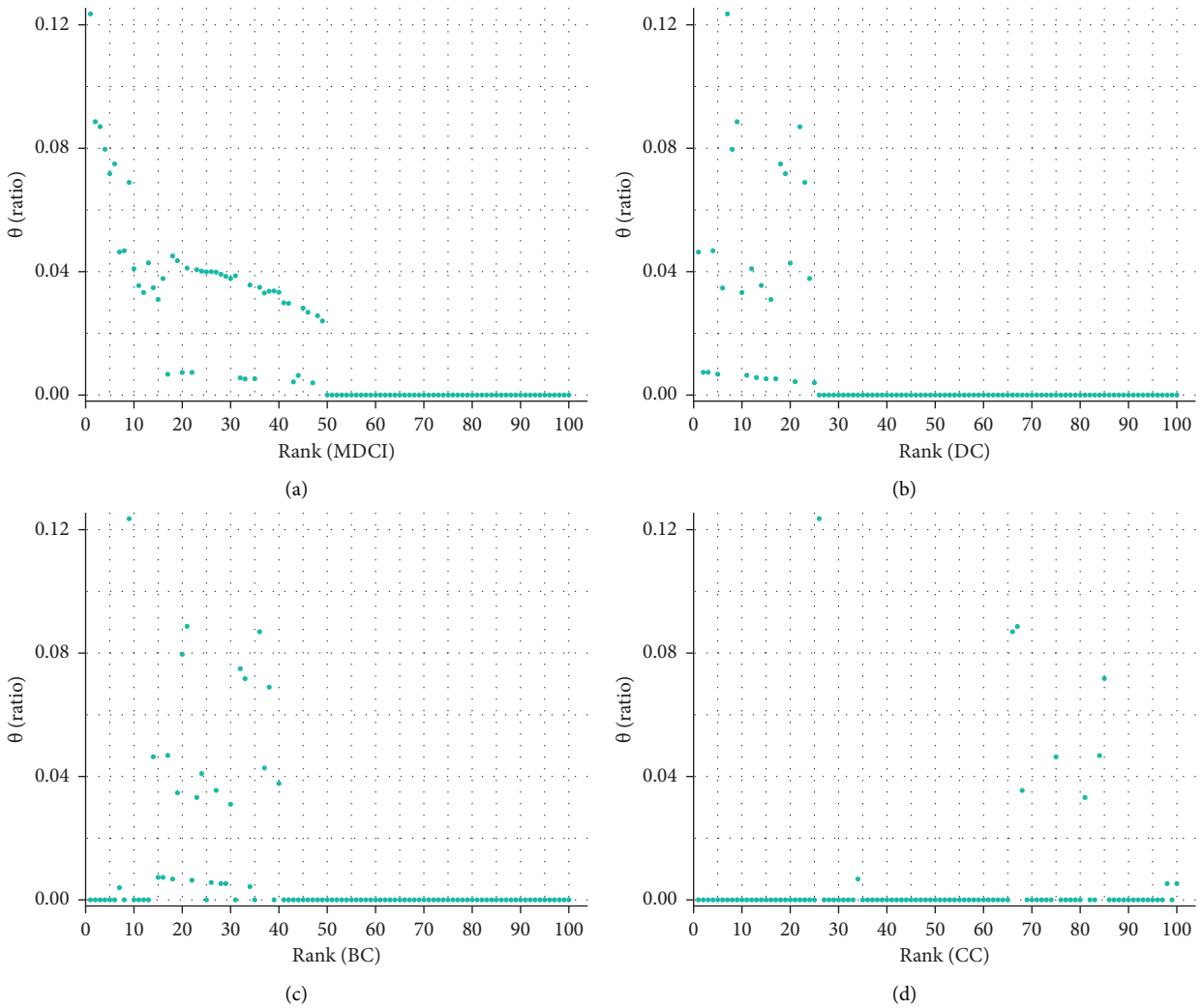


Figure 6: Continued.

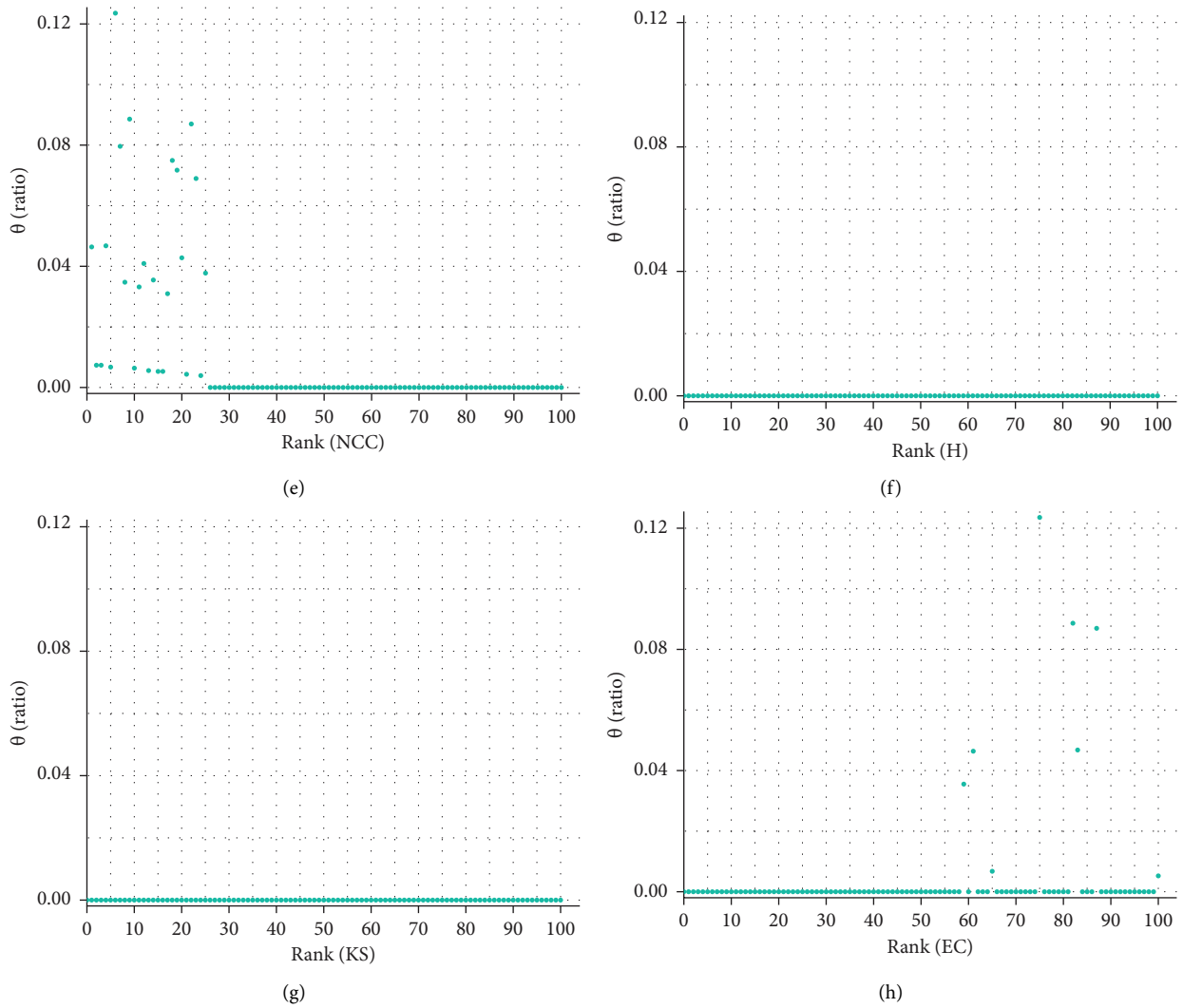


Figure 6: Relationship between node importance ranking and network failure ratio in a single node removal strategy.

network node failures when MDCI is compared to the eight sequential node removal methods based on the sequential node removal including the random strategy (*RA*). Figure 7(a) shows the comparison between MDCI and the four removal strategies *DC*, *BC*, *CC*, and *H*. Figure 7(b) shows the comparison between MDCI and the four removal strategies NCC, KS, EC, and RA. The horizontal coordinate in Figure 7 characterizes the importance ranking of the node in each critical node discovery method, and also indicates the order in which the nodes were removed at this point; the higher the ranking indicates, the higher the score of the node's importance in the method is, and the earlier it was removed in the experiment. The vertical coordinate characterizes the percentage of network failures after the corresponding node is removed. Compared with the node removal-alone strategy, the purpose of the continuous removal strategy is to verify the effectiveness of the critical node discovery method when the network structural changes with the removal of nodes. As shown in Figure 7 with the successive removal of node sequences, the proportion of network node failures increases, where the experimental results show that the proportion of node failures in the experimental network increases rapidly with the increase in the number of removed nodes when the node removal strategy is based on two types of indicators DC and NCC, while the growth rate of the proportion of node failures when the node removal is based on strategies such as BC and CC is slower at this time. Compared with DC and other 8 types of node removal strategies, the growth rate of the proportion of network failure maintains a constant advantage when node continuity removal is performed based on the node importance ranking sequence of MDCI, so this node importance assessment method is more effective in discovering critical nodes of multilayer network topology models.

4.3. Indicator Similarity Analysis. To further compare the similarities and differences between the critical node discovery method MDCI proposed in this paper and other

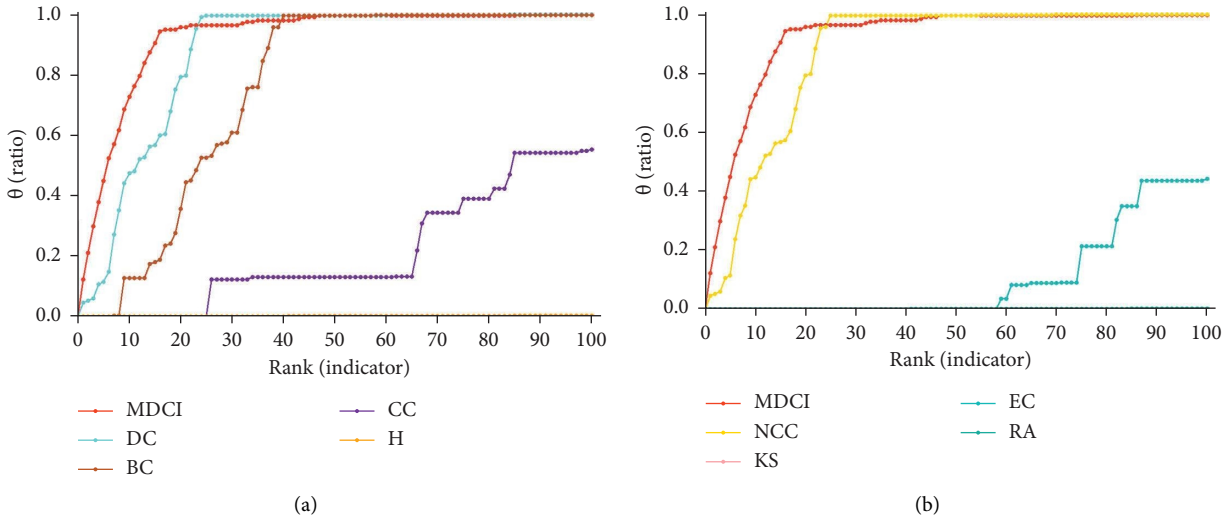


Figure 7: Relationship between node importance ranking and network failure ratio in continuous node sequence removal strategy.

methods in terms of node importance ranking, the Kendall coefficient [28] is used to calculate the metric correlation between MDCI and other methods. The Kendall coefficient τ is defined as follows:

$$\tau = \frac{2\left(N_p - N_q\right)}{N(N-1)}. \tag{17}$$

In (17), for the joint node pair $(A, B) = \{((a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n))\}$ of sequence A and sequence B, N_p characterizes the number of nodes to homogeneous sets, and N_q characterizes the number of nodes to heterogeneous sets. The Kendall coefficient, which takes values in the range [-1, 1], characterizes the association between the ranking of sequence A and sequence B from a perfectly negative to a perfectly positive correlation. In this experiment, the Kendall coefficient is calculated while plotting MDCI with each critical node discovery method in the node importance ranking distribution as shown in Figure 8; the horizontal coordinate in the figure is the importance ranking of the node under the current discovery method, the vertical coordinate in the figure indicates the importance ranking of the node in MDCI, and the color of the dot in the figure is the mapping of the importance ranking of the node in MDCI as marked in the legend on the right.

It can be seen from Figure 8 that since the MDCI method introduces the multi-attribute decision method CRITIC in the importance assessment process, DC, BC, CC, and NCC are used as subindicators in the topological centrality calculation process, MDCI maintains some consistency with the above four types of methods in the composition of the top-ranked important node set elements, and the Kendall coefficient is characterized as generally positive correlation. However, because MDCI is a node importance assessment indicator constructed by integrating two types of metrics, topological centrality and node dependency, it differs from subindicators in the ranking of specific nodes, and the removal experiment in Section 4.2 also finds that MDCI obtains a better destructive effect on the sequence of critical nodes. As for the H, KS, and EC methods, MDCI shows a weak correlation because the perspective of the importance of the evaluation nodes in MDCI is different from it. For example, in the KS evaluation indicator, the routing node located in the physical device layer is in the near-core layer in the network, but because of the multiselectivity of the routing function, when the node is removed, the near-neighbor route can complete the functional replacement, so the damage to the network structure is not obvious, and thus, the importance ranking in MDCI is low; on the contrary, a server node located in the lower core layer will have a higher importance ranking in MDCI because the upper layer carries important business systems and is enriched with a large-scale user community. At the same time, it is known that the RA strategy ranks the nodes based on the random principle, so the correlation with MDCI is weak.

4.4. Network Interlayer Failure Correlation. In this study, based on the node dependencies in the network, removing a certain amount of nodes in the physical device layer will lead to a secondary failure of the entire three-layer network topology. The variation in the proportion of network failures resulting from the removal of important node sequence output by different critical node discovery methods exhibits different traits in the local network and the three-layer network topology, respectively. In Figure 9, the correlation distribution of network failure ratio between physical device layer and three-layer network topology when successive node sequence removal is performed is depicted. The horizontal coordinates in the figure characterize the change of network failure ratio at the physical device layer, the vertical coordinates characterize the network failure ratio of the corresponding three-layer network topology in each type of discovery methods, and the black dashed line in the figure is the baseline when the failure ratio of physical device layer and three-layer network topology is the same. DC and BC,

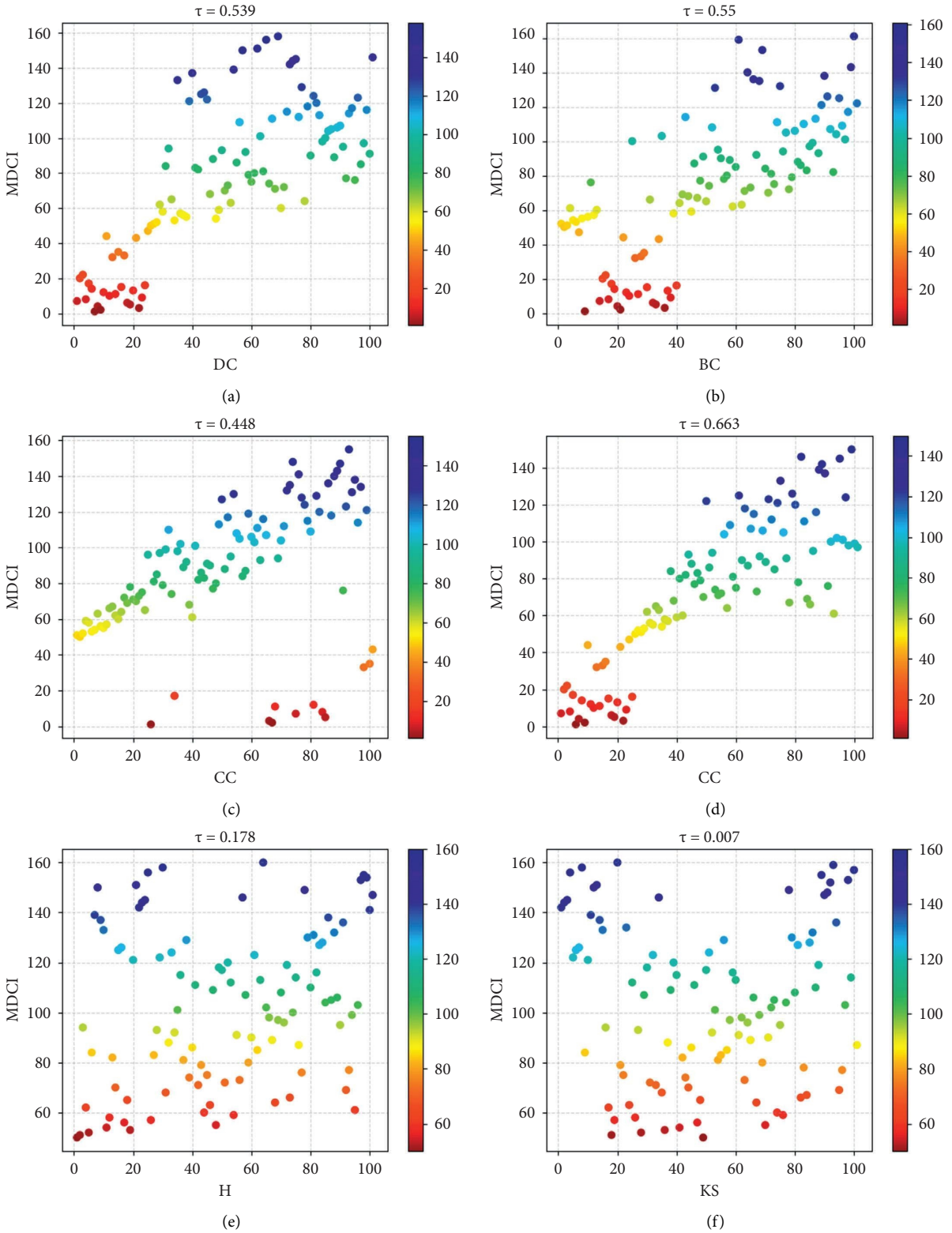


Figure 8: Continued.

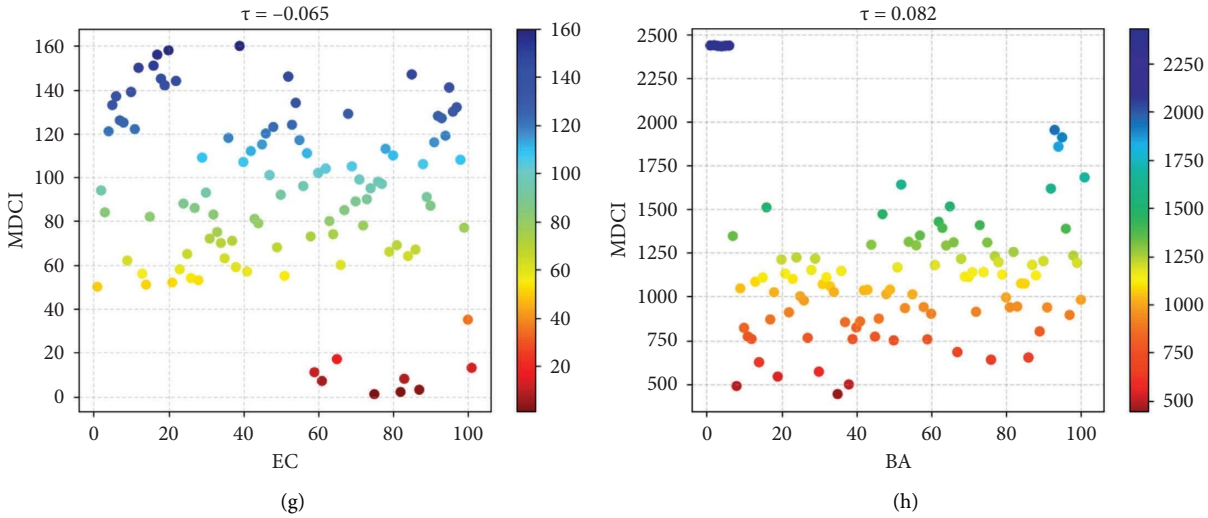


Figure 8: Correlation of MDCI with the ranking sequence of various node importance methods.

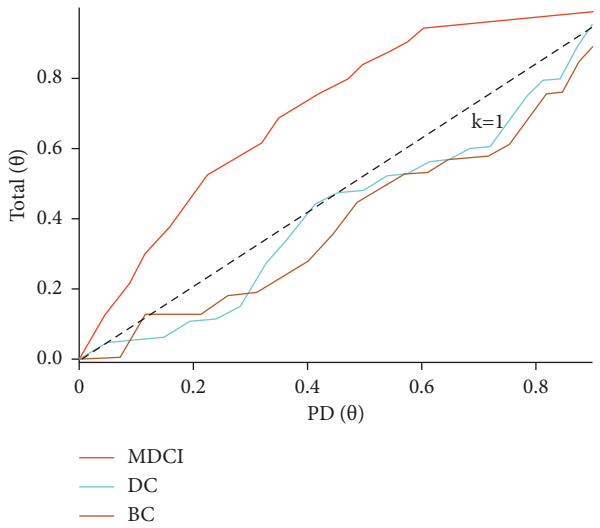


Figure 9: Physical device layer and three-layer network topology network failure ratio correlation distribution.

which have a faster growth of network failure ratio in the experiments in Section 4.3, are selected as the control methods in this experiment.

In Figure 9, it can be found that when node removal is performed based on two types of policies: DC and BC, the proportion of network failures at the physical device layer is often higher than that at the three-layer network topology under the same removal conditions, which indicates that the failure of some components in the physical device layer does not have an equivalent impact on the service operation of the whole network. Compared with DC and BC, node removal experiments are performed based on the node importance sequence output by MDCI, when it is found that the proportion of network failures within the physical device layer tends to be lower than the proportion of network failures in a three-layer network topology. This result indicates that the MDCI approach that integrates topology centrality and node dependency information can have a significant impact on the operational posture of the entire network while minimizing damage to the physical entity devices.

5. Conclusion

To better meet the application requirements of cyberspace security situational awareness, a multilayer network topology model is constructed in this paper based on physical device information, service traffic information, and user role information, which can characterize the situational information in the network in multiple dimensions. By decomposing the coupling relationships in the multilayer network model, this paper proposes a node importance assessment metric: multilayer dependency CRITIC indicator (MDCI), which is able to integrate the topological centrality and dependency relationships of nodes in the network for key node discovery, uses the CRITIC multi-attribute decision method to fuse degree centrality, betweenness centrality, closeness centrality, and network constraint coefficients to provide a stable measure of node topological centrality. At the same time, the setting of the dependency factor enables the node importance information to be smoothly transmitted between network layers, thus effectively supporting the discovery of network components that play a critical role in the overall dynamics of network operation. In the experimental part, this paper uses a variety of node importance assessment metrics, including the H-index, as the control sample set. The results of the ranking monotonicity experiments show that MDCI has a finer granularity of evaluation of the important measures of the nodes in the network; the results of the node removal experiments show that the node importance ranking of MDCI is more reasonable compared with that of the control group indicators, and there is a significant improvement in the convergence rate of the network failure ratio. Based on the Kendall coefficient analysis of index similarity, it can be found that MDCI can better synthesize the metric

information of mainstream importance indicators and comprehensively assess the importance of nodes. Finally, comparing between the trend of the proportion of network failures in the physical device layer and the overall network topology in the node removal experiment, it can be demonstrated that network destruction based on MDCI can achieve the ability to effectively cause large-scale failures in multilayer network topology with the destruction of fewer physical device components.

In terms of the next step of research, this paper focuses on the discovery of critical nodes from the perspective of network topology, but from the actual needs of the network security situational awareness system, the incorporation of service traffic dynamic information and user role information will further inspire the idea of critical node discovery. For example, the aggregation of malicious traffic monitoring information within the business application layer will help target anomalous access nodes, and the social association traces of suspicious accounts will be mapped to the information of their logged-in devices, thus helping to build monitoring lists. Therefore, in future research, with the support of multilayer network information, based on network topology combined with knowledge graph [29], evidence theory [30], and other related methods, the collection of critical nodes at each level can be discovered from a multidimensional perspective to finally achieve a comprehensive perception and control of the cyberspace security posture. Meanwhile, the migration application of relevant AI technologies [31, 32] in the direction of cyberspace security situational awareness will be an important pivot point for the field to eventually mature.

Data Availability

The Network Topology data used to support the findings of this study have been deposited in the Multilayer Network Repository (https://github.com/multilayer-go/muti-layer-network).

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Supplementary Materials

The pre-experimental content within Section 3.2.2 of this paper includes supplementary materials. (*Supplementary Materials*)

References

[1] C. Togay, A. Kasif, C. Catal, and B. Tekinerdogan, "A firewall policy anomaly detection framework for reliable network security," *IEEE Transactions on Reliability, Reliability, IEEE Transactions on, IEEE Trans Rel*, vol. 71, no. 1, pp. 339–347, 2022.

[2] J. E. Varghese and B. Muniyal, "An efficient IDS framework for DDoS attacks in SDN environment," *IEEE Access, Access, IEEE*, vol. 9, Article ID 69680, 2021.

[3] H. Mostafaei and S. Afridi, "P4Flow: monitoring traffic flows with programmable networks," *IEEE Communications Letters, Communications Letters, IEEE, IEEE Commun Lett*, vol. 25, no. 11, pp. 3546–3550, 2021.

[4] W. Zhang, B. Zhang, Y. Zhou, H. He, and Z. Ding, "An IoT honeynet based on multiport honeypots for capturing IoT attacks," *IEEE Internet of Things Journal, Internet of Things Journal, IEEE, IEEE Internet Things J*, vol. 7, no. 5, pp. 3991–3999, 2020.

[5] K. I. M. Hwankuk and K. I. M. Taeeun, "A design of automated vulnerability information management system for secure use of internet-connected devices based on internet-wide scanning methods," *IEICE - Transactions on Info and Systems*, vol. 11, p. E104, 2021.

[6] J. He and J. Yang, "Network security situational level prediction based on a double-feedback elman model," *Informatica*, vol. 46, no. 1, pp. 87–93, Article ID 03505596, 2022.

[7] Z. Zhao, Y. Peng, J. Huang, T. Zhou, and H. Wang, "An evaluation method of network security situation using data fusion theory," *International Journal of Performability Engineering*, vol. 16, no. 7, pp. 1046–1057, 2020.

[8] X. Tao, K. Kong, F. Zhao, S. Cheng, and S. Wang, "An efficient method for network security situation assessment," *International Journal of Distributed Sensor Networks*, vol. 16, no. 11, pp. 1–13, 2020.

[9] Y. Wang, N. Pan, and X. Tao, "Network Topology Discovery Algorithm Based on OSPF," in *Proceedings of the 2010 International Conference on Intelligent Computing and Integrated Systems, Intelligent Computing and Integrated Systems (ICISS)*, pp. 136–139, Guilin, China, October 2010.

[10] H. Zhang, M. Peng, J. M. Guerrero, X. Gao, and Y. Liu, "Modelling and vulnerability analysis of cyber-physical power systems based on interdependent networks," *Energies*, vol. 12, no. 18, p. 3439, Article ID 19961073, 2019.

[11] S.-Yu Wu and G. Xu, "Degeneration characters of heterogeneous-interdependent network and key node identification," *Acta Automatica Sinica*, vol. 44, no. 5, pp. 953–960, 2018.

[12] Y. Zhang, X. Song, L. Xie, H. Liu, and Y. Li, "Vulnerable point identification using heterogeneous interdependent node theory for distribution systems," *CSEE JOURNAL OF POWER AND ENERGY SYSTEMS*, vol. 8, no. 2, pp. 591–598, 2022.

[13] R. Gallotti and M. Barthelemy, *The multilayer temporal network of public transport in Great Britain Scientific Data*, vol. 2, 2015.

[14] X. Liu, E. Maiorino, and A. Halu, "Robustness and lethality in multilayer biological molecular networks," *Nature Communications*, vol. 11, 2020.

[15] S. Wang and J. Zhao, "Multi-attribute integrated measurement of node importanc40e in complex networks," *Chaos*, vol. 25, no. 11, Article ID 113105, 2015.

[16] H. Sotoodeh and M. Falahrad, "Relative degree structural hole centrality, CRD–SH: a new centrality measure in complex networks," *Journal of Systems Science and Complexity*, vol. 32, no. 5, pp. 1306–1323, 2019.

[17] C. Liu, H. Yin, Y. Sun, L. Wang, and X. Guo, "A grade identification method of critical node in urban road network based on multi-attribute evaluation correction," *Applied Sciences*, vol. 12, no. 2, p. 813, Article ID 2076-3417, 2022.

[18] Y. Zhang, Y. Lu, G. Yang, and Z. Hang, "Multi-attribute decision making method for node importance metric in complex network," *Applied Sciences*, vol. 12, no. 4, p. 1944, Article ID 2076-3417, 2022.

[19] C. Linton and Freeman, "Centrality in Social Networks Conceptual Clarification," *Social Networks*, vol. 1, 1978.
[20] Y.-jin Tan, J. Wu, and H.-zhong Deng, "Evaluation method for node importance based on node contraction in complex networks," *SYSTEMS ENGINEERING —THEORY & PRACTICE*, vol. 26, no. 11, pp. 79–102, 2006.
[21] G. Sabidussi, "The centrality index of a graph," *Psychometrika*, vol. 31, no. 4, pp. 581–603, 1966.
[22] Z. Lin, Y. Zhang, Q. Gong, Y. Chen, A. Oksanen, and A. Y. Ding, "Structural hole theory in social network analysis: a review," *IEEE Transactions on Computational Social Systems, Computational Social Systems, IEEE Transactions on, IEEE Trans Comput Soc Syst*, vol. 9, no. 3, pp. 724–739, 2022.
[23] R. Wang, M. Lewis, R. Zheng-Pywell, J. Julson, M. Smithson, and H. Chen, "Using the H-index as a factor in the promotion of surgical faculty," *Heliyon*, vol. 8, no. 4, 2022.
[24] B. Fu, J. Zhang, and R. Xiong, "A heuristic algorithm of social influence based on K-shell value diversity," in *Proceedings of the 2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST), Science and Technology Innovation (IAECST)*, pp. 664–670, Guangzhou, China, December 2021.
[25] H. R. Frost, "Eigenvector centrality for multilayer networks with dependent node importance," 2022, https://arxiv.org/abs/2205.01478.
[26] github.com, "github.com," 2021, https://github.com/multilayer-go/muti-layer-network/.
[27] J. Bae and S. Kim, "Identifying and ranking influential spreaders in complex networks by neighborhood coreness," *Physica A: Statistical Mechanics and Its Applications*, vol. 395, pp. 549–559, 2014.
[28] D.-B. Chen, H. Gao, L. Lü, and T. Zhou, "Identifying influential nodes in large-scale directed networks: the role of clustering," *PLoS One*, vol. 8, no. 10, pp. 1–10, 2013.
[29] K. Liang, B. Zhou, Y. Zhang, Y. Li, B. Zhang, and X. Zhang, "PF2RM: a power fault retrieval and recommendation model based on knowledge graph," *Energies*, vol. 15, no. 5, p. 1810, Article ID 19961073, 2022.
[30] J. Zhao and Y. Deng, "Complex network modeling of evidence theory," *IEEE Transactions on Fuzzy Systems, Fuzzy Systems, IEEE Transactions on, IEEE Trans Fuzzy Syst*, vol. 29, no. 11, pp. 3470–3480, 2021.
[31] B. Thuraisingham, "The role of artificial intelligence and cyber security for social media," in *Proceedings of the 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, IEEE, New Orleans, LA, USA, May, 2020.
[32] A. Bhardwaj and V. Sapra, *Security incidents & response against cyber attacks*, Springer Nature, London, UK, 2021.