Reliability Engineering and System Safety 196 (2020) 106782

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

The vulnerability of communities in complex networks: An entropy approach

Tao Wen, Yong Deng*

Institute of Fundamental and Frontier Science, University of Electronic Science and Technology of China, Chengdu, 610054, China

ARTICLE INFO

Keywords:
Complex network
Community vulnerability
Entropy

ABSTRACT

Measuring the vulnerability of communities in complex networks has become an important topic in the research of complex systems. Numerous existing vulnerability measures have been proposed to solve such a problem, however, most of these methods have their own shortcomings and limitations. Therefore, a new entropy-based approach is proposed in this paper to address such a problem. This measure combines the internal factors and external factors for each community which can give the quantitative description of the community vulnerability. The internal factors contain the complexity degree of the community and the number of edges inside the community, and the external factors contain the similarity degree between the chosen community and other communities and the number of edges outside the community. Considering the community vulnerability from the perspective of entropy provides a new solution to such a problem. Due to the sufficient consideration of community information, more reasonable vulnerability result can be obtained. In order to show the performance and effectiveness of this proposed method, one example network and four real-world complex networks are used to compare with some exiting methods, and the sensitivity of weight factors is analyzed by Sobol' indices. The experiment results demonstrate the reasonableness and superiority of this proposed method.

1. Introduction

Recently, cyber-physical system (CPS) has attracted wide attention in numerous fields, such as microgrid [1], smart city [2], internet of things [3,4], and so on. Meanwhile, how to model CPS into specific physical models to analyze their performance and property has become the focus of researches [5]. Therefore, complex networks have been applied in this field to better understand the performance of CPS [6,7], where nodes in the network represent individuals in the system, and edges would show the relationship between these individuals. Most previous researches focus on the structure and topological property, which can quantify the characteristics and performances of networks. Particularly, the community structure has received increasing attention, because it can reveal human dynamics [8,9], inference reliable links [10], and identify influential nodes [11–13]. The community structure in the network demonstrates a higher density of nodes and edges, which can cause critical influence on the function and structure of subnetwork, improve the system reliability [14,15], and counteract the aging effect [16,17].

There are several different problems with the research of community structure, which can be divided into two issues. The first one is how to detect the community structure, such as dividing network community structure [18–20], detecting overlapping community [21], and dynamic changing of community in evolving networks [22]. Another one is exploring the community property [23], including measuring the community reliance [24–26], reconfiguring networks [27], and measuring the community vulnerability [28,29]. For nodes, identifying the influential spreaders in the networks by community structure caught the attention of researchers [30–32]; for network, the reliability [33,34] and immunization [35] of the whole network have broad application prospects. Researches on the whole network and individual nodes have become important recently, and the community vulnerability in the network gradually aroused researchers' interest [36]. For example, Rocco et al. [37] defined a vulnerability set and value for different communities, and proposed the relative vulnerability value to compare with remaining communities. Wei et al. [38] proposed a measure which considers more information about the community itself, and used a non-linear weighted function to combine these factors. Aniko et al. [39] proposed a topological index (distance-based fragmentation) to quantify the structural vulnerability in the plant-visitation network. Alim et al. [40] assessed the community vulnerability through social-based forwarding and routing method in opportunistic networks, which shows significant contribution about some devices on the performance of the entire network. Che et al. [41]

* Corresponding author.
E-mail address: dengentropy@uestc.edu.cn (Y. Deng).

https://doi.org/10.1016/j.ress.2019.106782
Received 6 July 2019; Received in revised form 9 December 2019; Accepted 27 December 2019
Available online 30 December 2019
0951-8320/

modified the original evolution method, and proposed a non-dimensionalized scoring standard to form a complete assessment system to measure the vulnerability of the urban power grid. Chen et al. [42] explored the relationship between the vulnerability of complex network and the fractal dimension. These methods have their own limitations, like computational complexity, inaccurate measure, and not suitable for certain scenarios.

Since entropy is an useful tool to measure the uncertain of information [43,44], it has been wildly used in the network theory, like dimension presentation [45,46], evidence theory [47,48], influential nodes identification [49,50], and time series prediction [51–53]. In addition, the structure and property of communities can be expressed by probability sets, the entropy-based method has gradually been a reasonable and effective method to quantify the property of network [54]. Therefore, an entropy-based approach is applied in this paper to measure the community vulnerability which can overcome the shortcomings and limitations of previous methods.

In this paper, an entropy-based measure is proposed to quantify the vulnerability degree of community structure. This proposed method can combine two parts of information, i.e., internal factors and external factors, which can consider more information about communities and give a reasonable vulnerability result of each community. The internal factors contain the number of edges inside the community and the complexity degree of the community which is measured by Tsallis structure entropy [55], and the external factors contain the number of edges outside the community and the similarity degree between the chosen community and other communities which is measured by relative entropy. These two kinds of entropy can quantify the property of communities in a more reasonable and effective way. Finally, the vulnerability and relative vulnerability result can be obtained by this proposed method to quantitatively describe the vulnerability of different communities. In order to show the performance and effectiveness of this proposed method, one example network and four real-world complex networks are applied in this paper. In addition, the sensitivity of four weight factors are analyzed by Sobol' indices in Manzi network, the vulnerability of large community is analyzed by random attack in Email network, and the vulnerability orders obtained by different methods are compared in Italian 380KV power grid network. The experiment results show the superiority and reasonableness of this proposed method. Meanwhile, this proposed method can overcome the shortcomings and limitations of previous methods.

The organization of the rest of this paper is as follows. Section 2 presents some basic properties about the node and the community detecting method. This novel entropy-based method is proposed in Section 3 to measure the community vulnerability. Meanwhile, numerical experiments are performed to illustrate the reasonableness and effectiveness of this proposed method in Section 4. The conclusions are discussed in Section 5.

2. Preliminaries

In order to facilitate the study of this problem, the following notations are introduced in Table 1. In this section, some basic concepts about complex networks are introduced. In addition, a community detection algorithm and classical community vulnerability measure are described in this section.

2.1. Node properties in the network

A given complex network can be denoted as $G(N, E)$, where $N = \{1, 2, \cdots, n\}$ and $E = \{1, 2, \cdots, m\}$ are the set of nodes and edges respectively, and n and m are the number of nodes and edges in the complex network respectively. A is the adjacency matrix of complex network whose size is $n \times n$, where $a_{ij} = 1$ represents there is an edge between node i and node j, and $a_{ij} = 0$ is the opposite.

Table 1
The notation in this method.

Notation	Introduction
$\alpha, \beta, \lambda, \eta$	Weight factors of different parameters.
a_{ij}	Element of adjacency matrix A.
d_i	Degree of node i.
$\langle d \rangle$, d_{max}	Average and maximum value of degree.
dis_{ij}	Shortest distance between node i and node j.
$\langle dis \rangle$, dis_{max}	Average and maximum value of shortest distance.
D_x^{in}, D_x^{out}	Number of edges inside and outside the community x.
Deg_x	Total degree of nodes in community x.
e_x	Number of edges in community x.
E_{PL}	Path length efficiency index.
g_{se}	Number of shortest paths between two nodes.
$g_{se}(i)$	Number of shortest paths between two nodes which passes through node i.
L_x	Average path length of community x.
m	Number of edges in the network.
n	Number of nodes in the network.
n_x	Number of nodes in community x.
p_i	Degree distribution of node i.
p_i'	Betweenness distribution of node i.
$P(i)$	Probability set of community x_i.
$p(i, t)$	The tth element of probability set $P(i)$.
$P'(i)$, $p'(i, t)$	Decreasing order of $P(i)$ and $p(i, t)$.
q_i	Modified betweenness distribution.
Q	Modularity of community structure.
r_{ij}	Symmetrical relative entropy R_{ij}.
R_{ij}	Relative entropy between two communities.
s_{ij}	Similarity index between two communities.
s'	Minimum value of size of two communities.
S_x	Similarity degree of community x.
$SI(X_i)$	First-order Sobol' index.
$ST(X_i)$	Total effect index.
T_x	Complexity degree of the community x.
v_x, R_x	Classical vulnerability and relative vulnerability of community x.
v	Minimum value of classical vulnerability among all communities.
$\lvert V_x \rvert$	Number of edges connecting community x and all other communities.
Vul_x, RV_x	Proposed vulnerability and relative vulnerability of community x.
Vul	Minimum value of proposed vulnerability among all communities.

Definition 2.1. (Node Degree). The degree of node i in the complex network is denoted as d_i and defined as follows,

$$d_i = \sum_{j=1}^{n} a_{ij} \tag{1}$$

where a_{ij} is one element of adjacency matrix A. The degree distribution of node i is defined as follows,

$$p_i = \frac{d_i}{\sum_{i \in N} d_i} \tag{2}$$

Definition 2.2. (Node Betweenness)[56]. The betweenness distribution of node i in the complex network is denoted as p_i' and defined as follows,

$$p_i' = \sum_{s,e \neq i} \frac{g_{se}(i)}{g_{se}} \tag{3}$$

where g_{se} is the total number of shortest paths between node s and node e, and $g_{se}(i)$ is the number of shortest paths between node s and node e which passes through node i.

2.2. Community detection algorithm

Lots of measures have been proposed to detect the community structure in complex networks. In order to find the community structure in the network, Newman's modularity method [57] is applied in this paper.

Definition 2.3. (Newman's modularity). For a given complex network G with k communities, the modularity is denoted as Q and defined as follows,

$$Q = \sum_{x=1}^{k} \left(\frac{e_x}{m} - \left(\frac{Deg_x}{2m} \right)^2 \right) \tag{4}$$

where k is the number of communities, m is the total number of edges in the complex network, e_x is the number of edges in community x, and Deg_x is the total degree of nodes in community x.

The value of Q can show the presence of community structure in the complex network. Different values of Q represent different situations. $Q = 0$ means all nodes in the network are in one single community and there is no community structure in the network. $Q > 0$ represents there are some kinds of community structure, and high value of Q means more edges would stay within the community than expected. $Q = 1$ means the community structure is strong in the network which is a good sign of community characteristics but not happen often in practice [58]. The value of Q indicates the apparent degree of community structure in the network. The high value of Q means more nodes are relatively densely connected with the nodes in the same community but sparsely connected with the nodes in other communities. Meanwhile, Newman and Girvan [58] suggested the value of Q should fall in the range $0.2 \sim 0.7$, and this value of Q would show the existence of community structures. The main idea of this method is to find the changes in Q, and more detail can refer to [57].

2.3. Classical community vulnerability measure

To measure the community vulnerability, lots of measures have been proposed. One classical measure is introduced in this subsection.

Definition 2.4. (Community vulnerability measure). The vulnerability of community x is denoted as v_x and defined as follows,

$$v_x = \frac{1}{|V_x|} \tag{5}$$

where V_x is the set of communities which are connected with community x, and $|V_x|$ is the number of edges connecting community x and all other communities, i.e. the connection of selected community to other communities.

Then, the relative vulnerability of community x is denoted as R_x and defined as follows,

$$R_x = \frac{v_x}{v},\ v = \min\{v_1, v_2, \cdots, v_k\} \tag{6}$$

where v_x is the vulnerability of community x, v is the minimum value of vulnerability among all communities, and k is the number of communities in the network.

3. The proposed method

3.1. Basic method

In this section, a novel method is proposed to measure the community vulnerability via the entropy approach. This proposed method focuses two parts of information which can consider more details in the community, including internal factors and external factors. The internal factors contain the complexity degree of the community and the number of edges within the community, and the external factors contain the similarity degree and number of edges between the chosen community and other communities. The complexity and similarity would be obtained by entropy method which would overcome the shortcomings and limitations of previous methods. The flow chart of this proposed method is shown in Fig. 1.

3.1.1. Complexity measure

Entropy plays an important role in many applications [59–62]. Firstly, the complexity degree of the community is measured by Tsallis structure entropy which combines the degree distribution and betweenness distribution. Because the degree distribution focuses on the local topological information of central node and the betweenness distribution considers the global topological information, Tsallis structure entropy which combines these two topological information can give a reasonable measure for community complexity.

Definition 3.1. (Complexity measure based on Tsallis structure entropy). The complexity degree of community x is denoted as T_x and defined as follows,

$$T_x = \sum_{i=1}^{n_x} \frac{p_i^{q_i} - p_i}{1 - q_i} \tag{7}$$

where n_x is the number of nodes in community x, p_i is the degree distribution of node i which can be obtained by Eq. (2), q_i is the ith entropic index which can be obtained from the betweenness distribution of node i, and the relationship between q_i and p_i' is shown as follows,

$$q_i = 1 + (p_{\max}{}' - p_i') \tag{8}$$

where p_i' can be obtained from Eq. (3), $p_{\max}{}'$ is the maximum value of p_i'. The purpose of Eq. (8) is to make the index q_i bigger than 1 which can show the subadditivity influence of subsystem to community x. In the information theory, different values of q mean different additivity among subsystems for Tsallis entropy, i.e., $q < 1$, $q = 1$, $q > 1$ represent superadditivity, addiitivity, and subadditivity respectively. Extended to the network theory, one node and corresponding connnected edges are regarded as one subsystem when the community is regarded as the system. Because the betweenness distribution is the global property to describe the characteristics of networks, it can represent the relationship between each node and corresponding community and the relationship among different nodes. The betweenness distribution is reasonable to be chosen as the entropic index of each subsystem to describe the nonextensive additivity between the subsystem and corresponding community. In addition, each subsystems' index q_i has a unique value which can represent different relationships.

When each node's q_i equals 1, Tsallis entropy would degenerate to Shannon entropy. More details can refer to [63], and the transformation is shown as follows,

$$\begin{aligned} T_x &= \textstyle\sum_{i=1}^{n_x} \frac{p_i^{q_i} - p_i}{1 - q_i} = \frac{1 - \sum_{i=1}^{n_x} p_i^{q_i}}{q_i - 1} \\ &= \lim_{q_i \to 1} \frac{1 - \sum_{i=1}^{n_x} p_i \exp[(q_i - 1)\ln p_i]}{q_i - 1} \\ &= -\textstyle\sum_{i=1}^{n_x} p_i \log p_i \end{aligned} \tag{9}$$

This form of entropy would only focus on the local topological structure information.

The degree distribution is based on the local topological structure around central node i. The betweenness distribution focuses on the whole topological structure which can describe the global property of community. Most time, q_i would be bigger than 1 which can show the influence of subsystem. When each node q_i equals 1, Tsallis entropy would degenerate to Shannon entropy based on the degree distribution which only focuses on the local structure. Using betweenness distribution to replace the constant parameter q can describe the information about the network itself which is more reasonable for measuring the community complexity. This method's property also obeys the classical Tsallis entropy.

3.1.2. Similarity measure

Then, relative entropy is used in this section to obtain the similarity degree between the chosen community and other communities. The

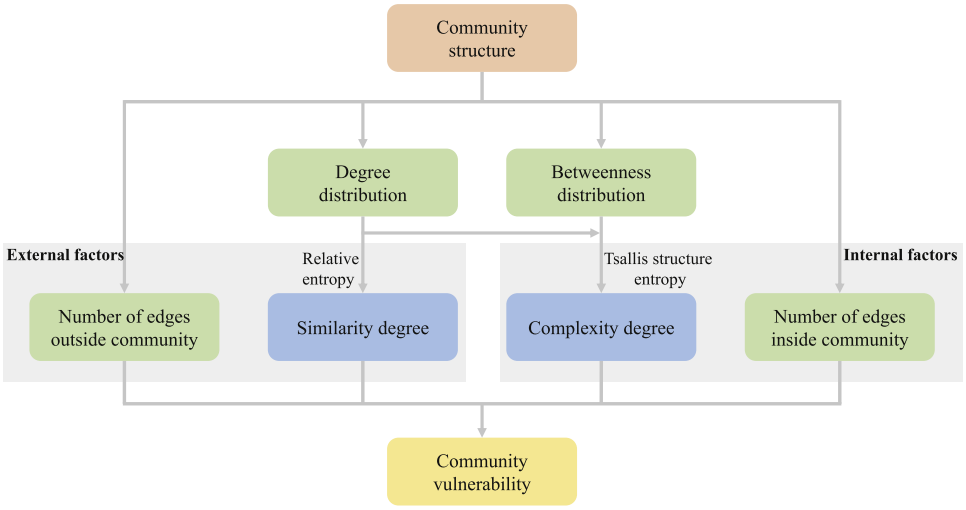

Fig. 1. The flow chart of this proposed method.

relative entropy (Kullback − Leibler divergence) was wildly used in information theory and probability theory which is proposed by Kullback and Leibler et al. [64]. In general, the relative entropy is used to measure the difference between two probability sets. In this section, the relative entropy based on Shannon entropy and degree distribution can measure the similarity between two community structures.

For two community x_i and x_j, the community structures are denoted as $L_{x_i}(N_i, D_i)$ and $L_{x_j}(N_j, D_j)$ respectively, where N_i and D_i are the set of nodes and the set of degree of nodes in community x_i. n_{x_i} is the number of nodes in community x_i and $\max n_{x_i}$ is the maximum size of community in the network. The probability set of community x_i is denoted as $P(i)$ and obtained by degree distribution. The scale of every probability set s would be the same and equals $\max n_{x_i}$. So the probability set of community x_i can be shown as follows,

$$P(i) = [p(i, 1), p(i, 2), \cdots, p(i, s)] \tag{10}$$

The element in probability set is based on the degree distribution. When the size n_{x_i} of community x_i equals $\max n_{x_i}$, all of the elements would be obtained by nodes' degree, but when $n_{x_i} < \max n_{x_i}$, some elements would equal zero to make the probability set complete. The detail of $p(i, t)$ is defined as follows,

$$p(i, t) = \begin{cases} \frac{d_t}{\sum_{t=1}^{n_{x_i}} d_t} & t \le n_{x_i} \\ 0 & t > n_{x_i} \end{cases} \tag{11}$$

where d_t is the degree of node t, n_{x_i} is the number of nodes in community x_i.

To measure the similarity between community x_i and x_j, the relative entropy is used in this section and it is defined as follows,

Definition 3.2. (Similarity measure based on relative entropy). The difference between two communities is obtained by relative entropy R_{ij} and defined as follows,

$$R_{ij}(P'(i)\|P'(j)) = \sum_{t=1}^{s'} p'(i, t)\log\frac{p'(i, t)}{p'(j, t)} \tag{12}$$

Because the order of element would affect the relative entropy and the similarity result, $p'(i, t)$ and $p'(j, t)$ are the decreasing order of $p(i, t)$ and $p(j, t)$ in Eq. (10). s' can be obtained as follows,

$$s' = \min(n_{x_i}, n_{x_j}) \tag{13}$$

The adjustment of s' is to avoid $\frac{p'(i,t)}{p'(j,t)}$ being 0 or positive infinity, which would be beneficial for calculation. The relative entropy' property is not symmetry, so the following changes are needed to make it symmetrical,

$$r_{ij} = R_{ij}(P'(i)\|P'(j)) + R_{ji}(P'(j)\|P'(i)) \tag{14}$$

Thus, $r_{ij} = r_{ji}$ holds, and the relative entropy between two communities is symmetry. Because the relative entropy can measure the difference between two probability sets, the difference between two communities are obtained in this situation. The bigger r_{ij}, the greater the difference between two communities' structure is. So the similarity index is obtained based on the relative entropy and is defined as follows,

$$s_{ij} = 1 - \frac{r_{ij}}{\max(r_{ij})} \tag{15}$$

where s_{ij} is also symmetry, and shows the similarity between two communities' structure. The more similar the two communities, the less the difference between them is, the closer r_{ij} is to max (r_{ij}) and the closer s_{ij} is to zero.

So the similarity between two communities can be measured by the relative entropy, which can give a novel approach to this problem. The relative entropy focuses on the local structure topological information in the community structure, which is more reasonable.

3.1.3. Edges in the network

The number of edges inside and outside the community are also important for community vulnerability measuring. In this section, the number of edges is considered.

Definition 3.3. (Number of edges inside the community). The number of edges inside community x is donated as D_x^{in} and defined as follows,

$$D_x^{in} = \frac{\sum_{i\in x}\sum_{j\in x} a_{ij}}{2} \tag{16}$$

where node i and node j are within community x, a_{ij} is the element of adjacency matrix A. Thus, a_{ij} is entirely inside the community.

Definition 3.4. (Number of edges outside the community). The number of edges outside community x is donated as D_x^{out} and defined as follows,

$$D_x^{out} = \sum_{i\in x}\sum_{j\notin x} a_{ij} \tag{17}$$

where node i is within community x, and node j is outside community x, a_{ij} is the element of adjacency matrix A. Thus, a_{ij} connects the chosen community and other communities which can show the relationship between them.

3.1.4. Community vulnerability measure

Lastly, all factors defined in Definition 3.1 to 3.4 are considered in

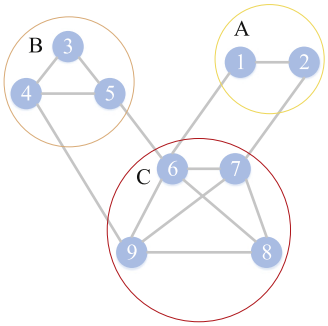

Fig. 2. An example network with 9 nodes.

the vulnerability measuring model. This proposed method would consider the internal factors and external factors which considers more details of community, and it is defined as follows,

Definition 3.5. (Proposed community vulnerability measure). The vulnerability of community x is donated as Vul_x and defined as follows,

$$Vul_x = \frac{1}{(D_x^{out})^{\beta}(D_x^{in})^{\lambda}} \frac{(S_x)^{\alpha}}{(T_x)^{\eta}} \tag{18}$$

where $\alpha, \beta, \lambda, \eta$ are the weight factors of different parameters, and they are bigger than zero. D_x^{in} and D_x^{out} are the number of edges inside and outside community x respectively, T_x is the complexity degree of community x, and S_x represents the similarity degree between community x and other communities (exclude community x itself) which can be shown as follows,

$$S_x = \sum_{j=1}^{k} s_{xj}, j \neq x \tag{19}$$

where s_{xj} can be obtained by Eq. (15)

The relative vulnerability of community x is denoted as RV_x and defined as follows,

$$RV_x = \frac{Vul_x}{Vul}, Vul = \min\{Vul_1, Vul_2, \cdots, Vul_k\} \tag{20}$$

where Vul_x is the vulnerability of community x, vul is the minimum value of vulnerability among all communities, and k is the number of communities in the network.

In order for these parameters to be considered on the same scale, all of these four parameters s_{xj}, D_x^{out}, D_x^{in}, T_x are normalized firstly. The weight factors $\alpha, \beta, \lambda, \eta$ can give different considerations to different parameters, which can be adjusted in different situation. This setting of weight factor makes this proposed method more reasonable. Some special cases of this proposed method Vul_x are shown as follows,

1) When $\alpha = \beta = \lambda = \eta$, these four parameters are considered equally.
2) When $\beta = 1$, and $\alpha = \lambda = \eta = 0$, this proposed method Vul_x would degenerate to the classical vulnerability measure v_x in Eq. (5).
3) When $\alpha = \beta$=0, this proposed method Vul_x would consider the external factors, which is the communities connected with the chosen community.
4) When $\lambda = \eta = 0$, this proposed method Vul_x would only consider the internal factors, i.e., the chosen community.

3.2. Sensitivity analysis

Because these four weight factors ($\alpha, \beta, \lambda, \eta$) are important for community vulnerability measuring, and the vulnerability result would have related changes as weight factors change. Thus, how to determine weight factors has been a problem in this model. In this section, the sensitivity of these weight factors are analyzed. In general, the global sensitivity analysis is a useful tool to obtain the influence of inputs on the output variability in the mathematical and physical model, and the Sobol' index based on variance decomposition is applied in this paper. The first-order Sobol' index $SI(X_i)$ and total effect index $ST(X_i)$ are defined as follows respectively,

$$SI(X_i) = \frac{Var_{X_i}(E_{X_{\sim i}}(Y|X_i))}{Var(Y)} \tag{21}$$

$$ST(X_i) = \frac{E_{X_{\sim i}}(Var_{X_i}(Y|X_{\sim i}))}{Var(Y)} \tag{22}$$

where Y represents the output of system, X_i is the ith independent input X, $X_{\sim i}$ is all inputs exclude X_i, $Var(Y)$ is the variance which change with these inputs. The first-order Sobol' index $SI(X_i)$ can get the contribution of X_i to Y, and total effect index $ST(X_i)$ can get the contribution to the variance of Y by the variability of each input X_i, which considers its individual effect and the interaction with other variables.

Each weight factor is randomly generated 10000 times by Monte Carlo method, and the range falls into [1/5, 5]. The reason for setting these weight factors in this interval is that these factors are exponentially present in the vulnerability measure model. In the exponential index, 1/5 and 5 are symmetric. Therefore, the setting of this interval can show the influence of factors on vulnerability results more reasonable. The vulnerability result would be obtained by these random factor combinations, and the contribution of different weight factors can be obtained by the first-order Sobol' index and total effect index.

3.3. An illustrative example

In this section, an example network is given to show the difference between this proposed method Vul_x and classical measure v_x. The network structure is shown in Fig. 2. Observed from Fig. 2, this network has 9 nodes and 14 edges, and the community structure of the network is detected by Newman's modularity in Eq. (4). The network is divided into three communities ($Q = 0.2857$) and each of the weight factors $\alpha, \beta, \lambda, \eta$ equal one which makes four parameters equally important. According to this proposed method in Eq. (18), (20) and classical measure in Eq. (5), (6), four parameters and the vulnerability of three communities are shown in Table 2.

From Table 2 when $\alpha = \beta = \lambda = \eta$=1, it can be found that the vulnerability of community C is the lowest, which is the same as the classical measure, but the vulnerability of community A and B is different with classical measure. It can be found from Table 2 that v_x of community A and B is the same and it is 2 because of the same number of edges outside the chosen community. However, this classical method is not reasonable, because the vulnerability of one chosen community is determined not only by external factors but also by internal factors. From Fig. 2, community A is a fully-connected network with only two nodes, but community B is a fully-connected network with three nodes. When the network' structure is similar, i.e., fully-connected, the

Table 2
The vulnerability of three communities in example network in Fig. 2.

Community	S_x	T_x	D_x^{in}	D_x^{out}	$\|V_x\|$	Vul_x	RV_x	v_x	R_x
Community A	1	0.5	0.1667	0.5	0.5	24	27.6264	2	2
Community B	0.4298	0.7924	0.5	0.5	0.5	2.1696	2.4975	2	2
Community C	0.8687	1	1	1	1	0.8687	1	1	1

Table 3
The topological properties of real-world complex networks.

Network	n	m	$\langle d \rangle$	$d_{\max}$	$\langle dis \rangle$	$dis_{\max}$
Karate	34	78	4.5882	17	2.4082	5
Manzi	52	76	2.8077	5	5.5000	13
Italian	127	171	2.6929	7	8.5682	25
Email	1133	5451	9.6222	71	3.6060	8

network with more nodes would be more robust, so community B is more robust than community A. The similar vulnerability result can be obtained by this proposed method ($Vul_B = 2.1696 < Vul_C = 24$), which means this proposed method is more reasonable for real-world application. The relative vulnerability RV_x can be more obvious to show the vulnerability difference between different communities. From the comparison result of the example network, this proposed vulnerability method Vul_x outperforms the classical method, and can distinguish the vulnerability level of community that the classical method cannot distinguish.

4. Experimental study

In this section, four real-world complex networks are applied to show the performance and effectiveness of this proposed method. These four networks are namely as Manzi network [65], Karate network [66], Email network [67], and Italian power network [68] respectively. The basic topological properties of these four networks are shown in Table 3. Observed from Table 3, n and m are the number of nodes and edges respectively. $\langle d \rangle$ and $d_{\max}$ are the average and maximum value of degree respectively, and $\langle dis \rangle$ and $dis_{\max}$ are the average and maximum value of the shortest distance respectively in the network.

4.1. Manzi network

Firstly, the telephone network in Belgium [65] which is usually analyzed for reliability purposes is used in this section. The topological structure of this network and the community structure obtained by Newman's modularity [57] are shown in Fig. 3. Observed from Fig. 3, Manzi network is divided into seven communities ($Q = 0.6316$), and the detail nodes in each community are shown in Table 4.

Table 4
The community details of Manzi network.

community k	Nodes in community k
1	3,6,7,8,9,10,13
2	1,2,4,5,11,12,14
3	15,16,17,18,20,21,24,25,29,31
4	19,22,26
5	23,38,30,32,36,37,41,43
6	27,33,34,35,38,39,40,42,45,46,47,49,50
7	44,48,51,52

The vulnerability of communities can guide the identification of critical community in the network. The vulnerability Vul_x and relative vulnerability RV_x of each community are given in Table 5, the classical comparing vulnerability method v_x and R_x are also shown in Table 5. Observed from R_x in Table 5, community 7 is the most vulnerable community, and community 3 is the most robust community in the network. The vulnerability of the rest of communities (community 1, 2, 4, 5, 6) cannot be identified by the classical measure because of the same value of R_x. Thus, this novel method is proposed based on two parts of information, including internal factors and external factors. The results of this proposed method (Vul_x, RV_x) are shown in Table 5. It can be found that community 3 is also considered to be the most robust community in the network which is the same as the classical method. The values of RV_x in community 4 and community 7 are close, and they are far greater than other communities' vulnerability. This result means that these two communities are far vulnerable than other communities which can be also seen from the topological structure in Fig. 3. In addition, the vulnerabilities of community 4 and community 7 identified by this proposed method and classical method are opposite. Observed from Fig. 3, community 4 and 7 have 3 and 4 nodes respectively, and the degree of each node equals 2. When anyone node in communities is

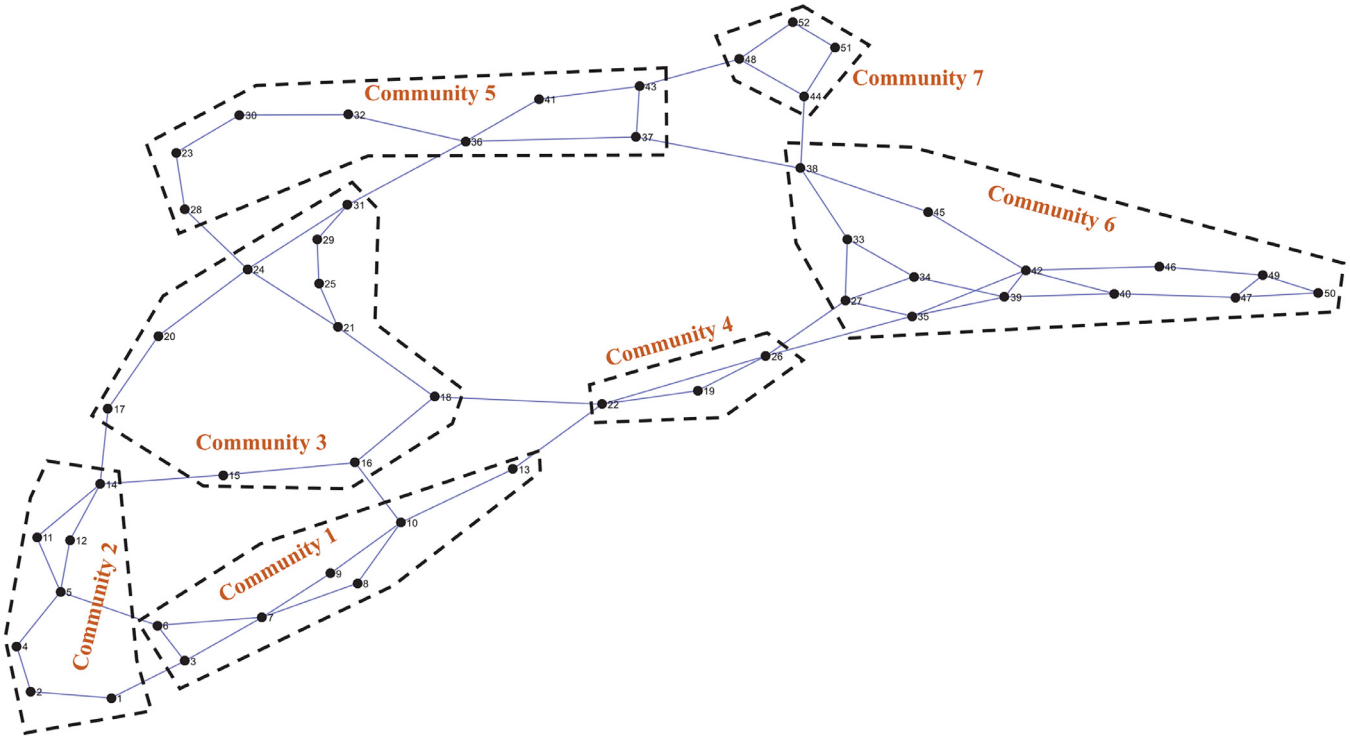

Fig. 3. Manzi et al. network.

Table 5
The vulnerability of communities in Manzi network.

Community	S_x	T_x	D_x^{in}	D_x^{out}	$\|V_x\|$	Vul_x	RV_x	v_x	R_x
1	0.3518	0.6864	0.4210	0.6667	0.6667	1.8260	1.8775	1.5	1.5
2	0.3529	0.7909	0.3684	0.6667	0.6667	1.8170	1.8682	1.5	1.5
3	0.4783	0.9344	0.5263	1	1	0.9725	1	1	1
4	1	0.5447	0.1578	0.6667	0.6667	17.4406	17.9322	1.5	1.5
5	0.4139	0.8814	0.4210	0.6667	0.6667	1.6730	1.7202	1.5	1.5
6	0.7654	1	1	0.6667	0.6667	1.1482	1.1805	1.5	1.5
7	0.6429	0.5915	0.2105	0.3333	0.3333	15.4872	15.9238	3	3

damaged and removed, the remaining nodes in community 4 and 7 would form a chain network, and the number of remaining nodes in community 7 (3 nodes) is larger than the number in community 4 (2 nodes). In addition, each community have two outer edges. Community 4 (2/3) will be more easily disconnected from the network than community 7 (2/4) when attacked. In these cases, the community left behind by the damage shows the vulnerability of the original community, and community 4 is more vulnerable than community 7 which is consistent with the result obtained by this proposed method. The rest of communities can get close but different RV_x, which can give a determined vulnerable order of these communities (community 6 > community 5 > community 2 > community 1). However, these communities' vulnerability differences cannot be identified by classical method because of the same R_x. The vulnerable order of community obtained by RV_x is community 4 > community 7 > community 6 > community 5 > community 2 > community 1 > community 3. So RV_x can consider more information in the network and give a determined vulnerable order for these communities which can overcome some limitations of classical method.

Then, Sobol' indices introduced in Section 3.2 are used in this section to analyze the global sensitivity of four weight factor α, β, λ, η. These weight factors can adjust the consideration of different parameters which can give a different vulnerability result. The sensitivity analysis resultswith different weight factors are shown in Table 6. Some conclusions can be obtained as follows,

1) The value of first-order Sobol' index can show the sensitivity of different wight factors. For instance, the vulnerability of community 1 is most sensitive to weight factor α, followed by λ, the other two factors β and η are less sensitive.
2) When the parameters of community equal 1, the first-order Sobol' index and total effect index would equal 1. That is because no matter how weight factor changes, the influence parameter would remain the same, i.e., equals 1. For example, T_x and D_x^{in} equal 1 in community 6, so $SI(\eta)$, $ST(\eta)$, $SI(\lambda)$ and $ST(\lambda)$ equal 0. Thus, the variability of these two weight factors would not affect the vulnerability of community 6. The same situation can occur in S_x of community 4 and D_x^{out} of community 3.
3) In most communities, the first-order Sobol' index $SI(\beta)$ and $SI(\eta)$ are smaller than $SI(\alpha)$ and $SI(\lambda)$, which means the vulnerability is more sensitive with α and λ. The similarity degree and the number of edges within the community are more influential to the vulnerability results.
4) The first-order Sobol' index $SI(\beta)$, $SI(\lambda)$, $SI(\eta)$ would be smaller when the values of T_x, D_x^{in}, and D_x^{out} are bigger, but $SI(\alpha)$ is a different situation which is bigger with bigger parameters S_x. This situation occurs because Vul_x is positively correlated with S_x, but negatively correlated with T_x, D_x^{in}, and D_x^{out}. Hence the value trend of these parameters have different impacts on the vulnerability of communities. These patterns can be observed from the communities vulnerability sensitivity analysis in Table 6.
5) The sum of the first-order Sobol' index over these four weight factors in different communities is less than 1, which means there is an interaction between these four parameters. But this situation does not occur in the total effect index.
6) Because of the interaction between these parameters, there would be a huge difference between first-order Sobol' index and total effect index. But it is interesting to find that the order of total effect index would be the same as first-order Sobol' index. For instance, the order of first-order Sobol' index in community 1 is $SI(\eta) < SI(\beta) < SI(\lambda) < SI(\alpha)$, and the order of total effect index is $ST(\eta) < ST(\beta) < ST(\lambda) < ST(\alpha)$, which is the same as previous order.

Because Sobol' indices are convenient to be obtained, and similar results can be obtained in different networks, we only analyze the sensitivity of weight factors in Manzi network and don't analyze the subsequent network.

4.2. Karate network

Next, a social network is used in this section to show the performance of this proposed method. This social network is named as Karate club network, which describes the relationship between 34 members of one club in US university [66]. After a conflict between the club administrator (node 34) and the instructor (node 1), the instructor left with half of the members, leaving the club divided into two separate communities. The topological structure and community structure divided by Newman's modularity are shown in Fig. 4. Every node in the network denotes a member in the karate club, including the instructors and administrators, and the edges in the network represent the relationship between two members beyond their normal activities in the club. The network is divided into two communities ($Q = 0.38$), and it is the same as the well-known community structure result because there

Table 6
The sensitivity analysis results of the vulnerability of communities in Manzi network with different weight factors.

Community	$SI(\alpha)$	$ST(\alpha)$	$SI(\beta)$	$ST(\beta)$	$SI(\lambda)$	$ST(\lambda)$	$SI(\eta)$	$ST(\eta)$
1	0.2055	0.7504	0.0529	0.2604	0.1570	0.5644	0.0294	0.2394
2	0.1983	0.7288	0.0509	0.2655	0.1941	0.6308	0.0114	0.1070
3	0.3969	0.6861	0	0	0.3116	0.5945	0.0044	0.0124
4	0	0	0.0253	0.2524	0.4246	0.8596	0.0883	0.4478
5	0.2229	0.6721	0.0650	0.2812	0.2247	0.6074	0.0048	0.0345
6	0.2895	0.3756	0.6343	0.7163	0	0	0	0
7	0.0275	0.3536	0.0966	0.6666	0.1579	0.7105	0.0374	0.3531

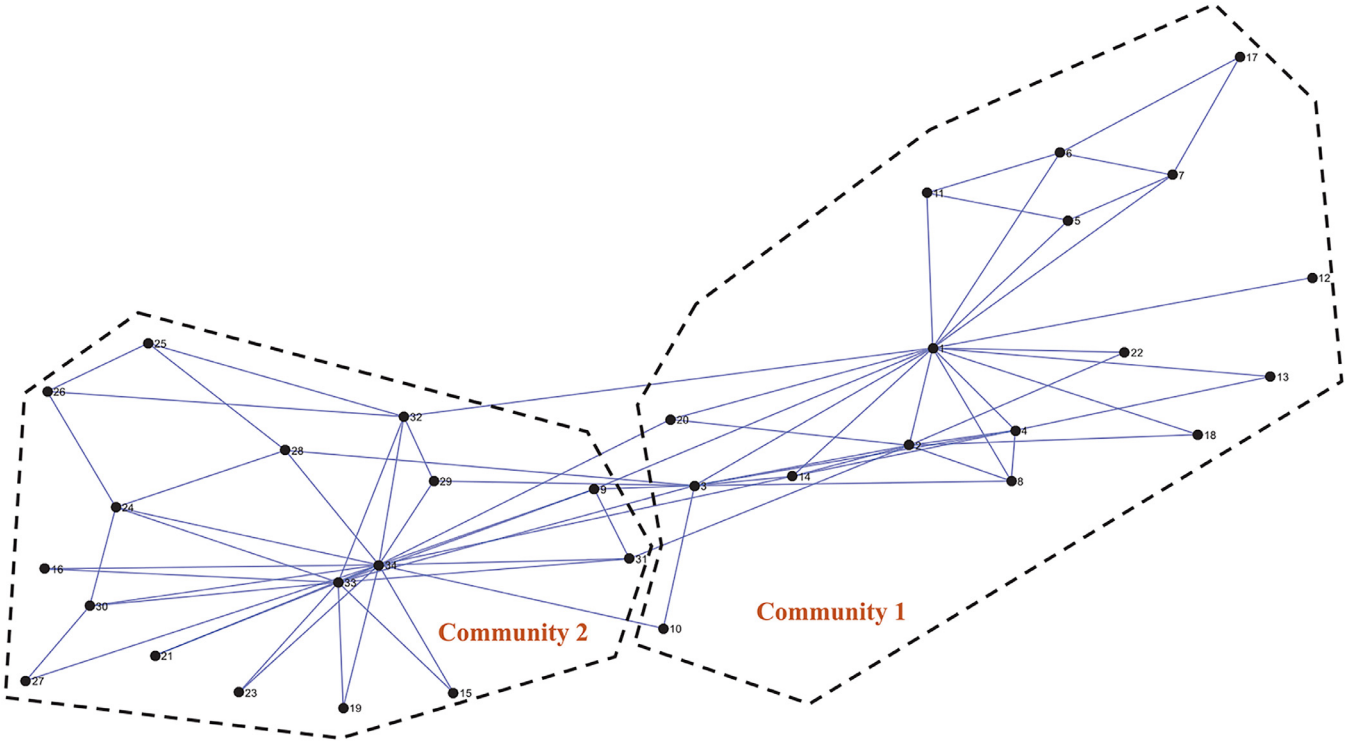

Fig. 4. Karate club network.

Table 7
The community details of Karate network.

community k	Nodes in community k
1	1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 17, 18, 20, 22
2	9, 15, 16, 19, 21, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34

has been a disagreement between the administrator and the instructor [66]. The detail members in each community are shown in Table 7, and it can be found that the members are divided equally and each community has 17 members. The leader in each community is node 1 and node 34 respectively because of their largest degree.

The vulnerability result of Karate network is shown in Table 8. Because there are only two communities, it can be found that the external factors (S_x, D_x^{out}) are the same which are determined by each other. Thus, the classical measure R_x would obtain the same vulnerability result and cannot identify the vulnerability degree of each community. But the internal factors are determined by community itself, these parameters can give a different vulnerability result. It is interesting to find that the number of edges inside the community D_x^{in} is also the same and it is 34, but the edges between nodes are different which results in a different complexity degree. The complexity degree T_x of two communities are 0.7060 and 1 respectively, which would get a different vulnerability measure for different communities. This means that the original administrator-led community is more complex than the new separated instructor-led community. The difference of T_x leads to the difference of vulnerability, and RV_x of two communities are 1.4162 and 1 respectively, which can get a conclusion that community 1 is more vulnerable than community 2. The main reason for their different vulnerability results is the complexity degree of each community, and the initial reason is the topological structure of each community. Observed from Fig. 4, all nodes in community 2 have at least two edges, which makes these marginal nodes more closely connected to the two center nodes (node 33 and 34), resulting in community 2 being more robust. For community 1, most marginal nodes only have one edge connected to center node 1, and the connection capacity of the second center (node 2) is not strong, resulting in community 1 being more vulnerable. Thus, the topological structure also supports the results of this proposed method. Judging from the actual situation, the newly established community (community 1) is more vulnerable than the existing community (community 2). From this case, we can find that the vulnerability cannot be distinguished when the number of communities is too small. The topological structure inside the community is also important for the vulnerability, and more factors should be considered to make an accurate identification for their vulnerability. So this proposed method can get a reasonable vulnerability result in Karate club network, whereas, the classical method R_x can only get the same vulnerability for two communities.

Table 8
The vulnerability of communities in Karate network.

Community	S_x	T_x	D_x^{in}	D_x^{out}	$\|V_x\|$	Vul_x	RV_x	v_x	R_x
1	1	0.7060	1	1	1	1.4162	1.4162	1	1
2	1	1	1	1	1	1	1	1	1

4.3. Email network

Then, the email network which describes the email interchanges between different members in the University Rovira i Virgili is used to analyze the vulnerability result between two methods. This network totally contains 1133 nodes and 5451 edges which is hard to represent the topological structure through figure. Thus, Newman's modularity method is directly used to detect the community structure in this network. The Email network is divided into 10 communities ($Q = 0.5037$), and the number of nodes n_x in each community is shown in the last column of Table 9.

The corresponding parameters and vulnerability results of each community in Email network are shown in Table 9. Because this network is far greater than other networks, the number of edges outside the community is different, resulting in the classical method measuring

Table 9
The vulnerability of communities in Email network.

Community	S_x	T_x	D_x^{in}	D_x^{out}	$\|V_x\|$	Vul_x	RV_x	v_x	R_x	n_x
1	0.6553	1	1	1	1	0.6553	1	1	1	319
2	0.5724	0.9056	0.7431	0.5687	0.5687	1.4957	2.2826	1.7584	1.7584	207
3	0.3993	0.7277	0.1783	0.2475	0.2475	12.4325	18.9732	4.0408	4.0408	114
4	0.4508	0.7761	0.5750	0.5020	0.5020	2.0122	3.0708	1.9920	1.9920	186
5	0.5509	0.8973	0.5436	0.5313	0.5313	2.1257	3.2441	1.8821	1.8821	238
6	0.4741	0.3537	0.0165	0.0525	0.0525	1546.9122	2360.7374	19.0385	19.0385	14
7	0.3575	0.3895	0.0299	0.0606	0.0606	507.2816	774.1607	16.5	16.5	26
8	1	0.1463	0.0016	0.0020	0.0020	2153638	3286660	495	495	3
9	0.3989	0.4182	0.0196	0.0323	0.0323	1502.5261	2293	30.9375	30.9375	20
10	0.7219	0.2715	0.0055	0.0091	0.0091	53198	81186	110	110	6

the vulnerability of communities differently. Observed from the result of RV_x and R_x, community 1 and community 8 is the most robust and most vulnerable community measured by two methods at the same time, which shows the effectiveness of these two methods. In addition, the vulnerability gap between two communities in RV_x is bigger than the gap in R_x, which means this proposed method would magnify the vulnerability gap between two communities to facilitate comparison of vulnerability. When comparing other communities, there are only two pair of communities with different orders, and they are community 4 and community 5; community 6 and community 9.

The number of nodes in community 4 and 5 is too large and about 200 nodes, which is difficult to analyze the vulnerability from their topological structure. Therefore, a network-based metric is considered to measure the vulnerability of communities. More detail, a certain percentage of edges are randomly removed from the community in order, and the percentage is set as $P_{Remove} = 30\%$ in this paper. Then, the path length efficiency E_{PL} which is used as the indicator to describe the vulnerability is defined as follows,

$$E_{PL} = \frac{L_x - L_x'}{L_x} \tag{23}$$

where E_{PL} is the path length efficiency index, L_x and L_x' are the average path length of community x and x', x is the original community and x' is the community which has been attacked and some edges have been removed. The average path length of community is defined as follows,

$$L_x = \frac{1}{n_x(n_x - 1)} \sum_{i \neq j \in x} \frac{1}{dis_{ij}} \tag{24}$$

where n_x is the number of nodes in community x, dis_{ij} is the shortest distance from node i to node j in community x.

E_{PL} is the average value of 200 experiment results, and the results in different removed ratios are shown in Fig. 5. Observed from Fig. 5, it can be found that E_{PL} of community 5 grows faster as more edges in the community are removed. When E_{PL} increases faster, the faster L_x' decreases when a certain percentage of edges are removed, and the more vulnerable the community is. This is because when the same proportion of edges are removed, the faster the average path length changes, the greater the loss of network performance, resulting in lower vulnerability. The experiment results verify the results of RV_x, that is, community 5 is more vulnerable than community 4. Thus, this proposed method is more effective to measure the community vulnerability.

Then, we analyze the vulnerability of community 6 and community 9. The structure of community 6 and community 9 includes internal nodes and directly connected external nodes are shown in Fig. 6. The internal nodes and directly connected external nodes are represented by different signs. Observed from the topological structure, the smallest closed shape of community 9 has 3 polygons and 4 triangles, while the smallest closed shape of community 6 has 1 polygon and 6 triangles. There is the same number of smallest closed shapes but more polygons in community 9, and the number of nodes in polygon of community 9 is larger. This structure property shows that community 6 is more vulnerable than community 9 which is the same as the results of RV_x.

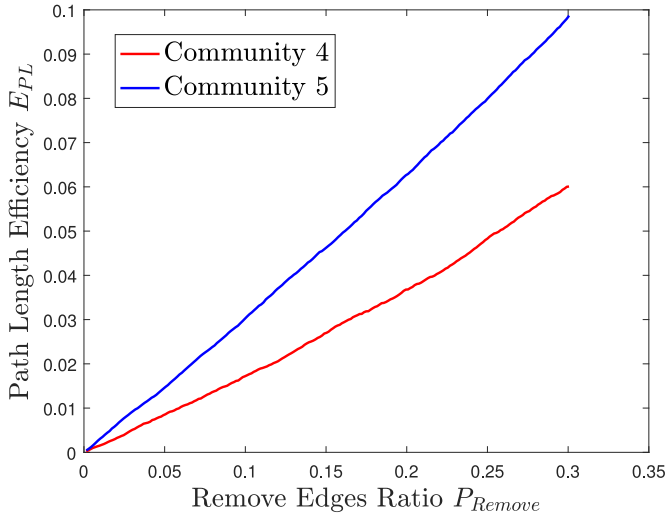

Fig. 5. The path length efficiency index E_{PL} with different ratios of removed edges P_{Remove}.

In conclusion, this proposed method considers more information of community than just external connectivity. Through this experiment, the vulnerability results obtained by this proposed method would be more reasonable, which has been verified by random attacks and structure property.

4.4. Italian 380KV power grid

Lastly, the Italian 380KV power transmission grid network [68] is used in this section. This network has been frequently used to analyze network vulnerability performance. The topological structure and community structure are shown in Fig. 7. Observed from Fig. 7, this network is divided into 10 communities ($Q = 0.7596$), and different communities have different number of components and the detail is shown in Table 10. It can be found that community 9 and community 7 have the maximum and minimum number of components respectively.

The vulnerability results are shown in Table 11. In this network, a novel method which is proposed by Wei et al. [38] is used as a comparing method, and this method is also modified from Ref [37]. Wei method considers five different properties as parameters to measure the vulnerability of each community, and all parameters are based on the topological structure. Different with Wei method, this proposed method considers the properties of community from the entropy aspect which focus on two parts of information and four parameters.

The detail results of each community are shown in Table 11. Observed from Table 11, community 5 is considered as the most robust community from RV_x and R_x, but R'_x give a different result that community 7 is the most robust. Observed from the topological structure in

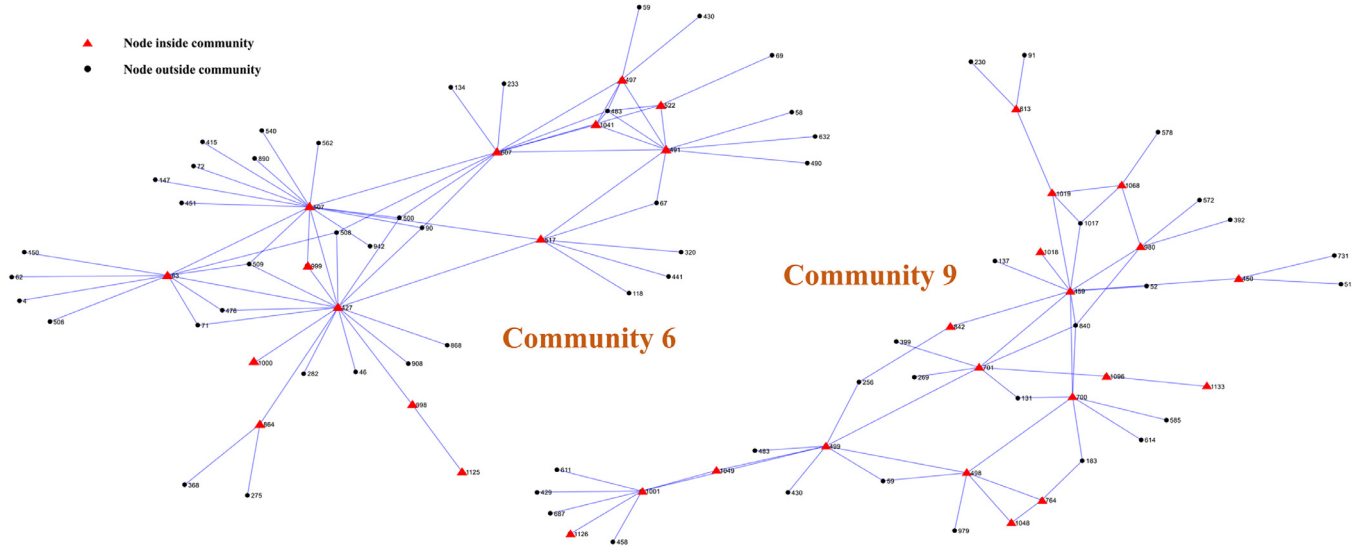

Fig. 6. The topological structure of community 6 and community 9 in Email network.

Fig. 7, community 7 contains two intersecting triangle structures, and the number of nodes in community 7 is only 6 which is the minimum value in the whole network. In contrast, community 5 has more nodes (15 nodes) in the network which locates in the middle of the network, and the topological structure is obviously more complex and robust which contains one polygon and three triangles. In addition, community 5 has more critical nodes, like node 61 (the only one node connecting community 6 and community 4), node 40 (the only one node connecting community 2 and community 3 indirectly), node 63 and 64 (the shortest path connecting community 6 and community 2). These critical nodes make community 5 more robust and critical. The judgement of the most robust community shows the reasonableness of this proposed method and classical method. Then, Community 10 is considered to be the most vulnerable from three methods at the same time.

The classical method cannot measure some communities' vulnerability changes in Italian power network, like the community 1, 3, 7, 8, and community 2, 4, 6. Because the classical method only consider one parameter ($|V_x|$), the vulnerability changes of these two group communities cannot be identified correctly. However, due to the sufficient consideration of information, RV_x and R'_x can show all vulnerability changes and give a certain vulnerability order (shown in

Table 10
The community details of Italian 380KV power network.

community k	Nodes in community k
1	1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 20, 19
2	37, 38, 36, 39, 35, 32, 60, 33, 31, 30, 34, 42
3	57, 56, 52, 49, 50, 47, 46, 45, 43, 44, 51, 54, 55
4	10, 16, 15, 17, 18, 21, 22, 24, 26, 25, 28, 29, 27, 23, 59, 58
5	61, 62, 63, 64, 65, 67, 71, 40, 41, 66, 68, 70, 53, 48, 69
6	77, 78, 81, 74, 75, 79, 82, 76, 72, 14, 73
7	83, 84, 85, 86, 101, 100
8	102, 110, 111, 115, 120, 113, 117, 118, 116, 114, 112
9	119, 109, 107, 108, 106, 104, 103, 105, 97, 99, 98, 88, 87, 96, 91, 95, 80, 92, 90, 93, 94, 89
10	122, 123, 121, 126, 125, 124, 127

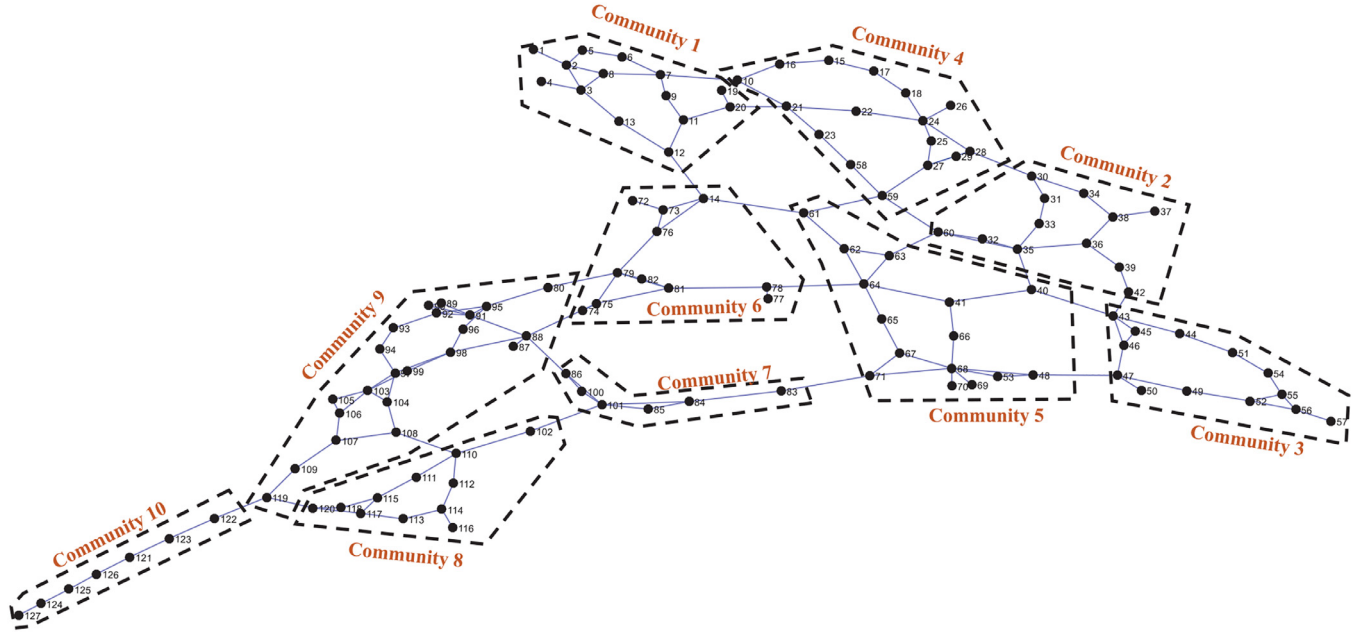

Fig. 7. Italian 380KV power grid network.

Table 11
The vulnerability of communities in Italian 380KV power network.

Community	S_x	T_x	D_x^{in}	D_x^{out}	$\|V_x\|$	Vul_x	RV_x	v_x	R_x	v'_x [38]	R'_x [38]
1	0.3469	0.9205	0.5161	0.3750	0.3750	1.9470	1.9444	2.6667	2.6667	9.1020	2.6547
2	0.4055	0.7882	0.4193	0.6250	0.6250	1.9629	1.9603	1.6000	1.6000	5.0539	1.4741
3	0.4675	0.8954	0.4838	0.3750	0.3750	2.8773	2.8734	2.6667	2.6667	6.9333	2.0222
4	0.5951	0.8733	0.6129	0.6250	0.6250	1.7789	1.7765	1.6000	1.6000	5.6606	1.651
5	0.4661	0.8017	0.5806	1	1	1.0013	1	1	1	4.0843	1.1912
6	0.4017	0.7588	0.4193	0.6250	0.6250	2.0198	2.0171	1.6000	1.6000	3.4459	1.005
7	1	0.4891	0.2258	0.3750	0.3750	24.1426	24.1102	2.6667	2.6667	3.4286	1
8	0.4114	0.8543	0.3870	0.3750	0.3750	3.3173	3.3128	2.6667	2.6667	8.5554	2.4953
9	0.7848	1	1	0.7500	0.7500	1.0465	1.0451	1.3333	1.3333	9.5387	2.7821
10	0.7305	0.6875	0.1935	0.1250	0.1250	43.9213	43.8623	8	8	39.2052	11.4347

Table 12
The vulnerability order of Italian 380KV power network obtained by different methods.

Method	Vulnerability order
Classical [37]	Community 5 < 9 < 2 = 4 = 6 < 1 = 3 = 7 = 8 < 10
Proposed	Community 5 < 9 < 4 < 1 < 2 < 6 < 3 < 8 < 7 < 10
Wei et al. [38]	Community 7 < 6 < 5 < 2 < 4 < 3 < 8 < 1 < 9 < 10

Table 12). For instance, the result of these two methods represents community 8 is more vulnerable than community 3. From the topological structure in Fig. 7, community 3 has more polygons and connection nodes connecting different communities (node 43) than community 8. The topological structure confirms that the vulnerability between communities is different, which is contrary to the classical method.

In addition, the result of this proposed method is more similar to the classical method, but Wei method is significantly different. Some detail differences are analysed below. Community 9 is considered as the second to last vulnerable community in R_x and RV_x, but it is considered as the second vulnerable community by R'_x. Observed from Fig. 7, it can be found that the structure of community 9 is very complex, there are lots of polygons in the community which make it more robust, and there are many connection nodes connecting different communities (node 88 and 119). The structure shows that the vulnerability of community 9 must be very low in the entire network compared with other communities which agrees with this proposed method. Community 3, 7, 8 are considered as the second vulnerable community by R_x at the same time, and RV_x gives a conclusion that community 7, 8, 3 are the second, third, forth vulnerable community respectively which is similar with classical method, but Wei method gives a dissimilar order (The vulnerabilities of community 3, 7, 8 have been discussed before). The vulnerability of directly connected community 2 and 4 is also analyzed below. Community 4 has more nodes than community 2, and community 4 is closer to the middle of network than community 2. There are three polygons in community 4, but only one polygon and one triangle in community 2. All these characteristics show that community 2 is more vulnerable than community 4 which agrees with RV_x. Other more detail information about the vulnerability order can be obtained from Table 12.

Eventually, this proposed method would magnify the vulnerability of communities, like the maximum value of the relative vulnerability of propose method $RV_8 = 43.8623$ and other methods $R_8 = 8$, $R'_8 = 11.4347$. The RV_x of the most vulnerable community would be much bigger than other methods, which is convenient to find the vulnerability of communities.

Therefore, through the analysis of the above experimental results, this proposed method would consider more information of community and give a determined vulnerability order, which is more reasonable than other methods.

5. Discussion and Conclusion

Quantitative vulnerability measure gradually became the focus of community research in the network theory. In general, a model which considers more kinds of information is more credible. In this paper, a new entropy-based approach is proposed to measure the vulnerability of communities which can overcome the shortcomings and limitations of previous methods. Different from previous methods, this proposed method combines the internal factors and external factors of community which can give sufficient considerations of community information. The internal factors contain the number of edges inside the community and the complexity degree of the community measured by Tsallis structure entropy, and the external factors contain the number of edges outside the community and the similarity degree between the chosen community and other communities measured by relative entropy. The vulnerability and the relative vulnerability of communities are obtained to give the quantitative description of the community vulnerability eventually.

Different from two comparison methods in this paper, this proposed method considers four important parameters which belong to internal and external factors through entropy. The complexity and similarity degree of each community are measured by entropy rather than the apparent community topological structure. The entropy can deal with the uncertain information in each community and give a reasonable measure result to the community property. The result obtained by this proposed method is more similar to classical method than the method in Ref. [38], which is more supportive of vulnerability results of actual phenomena in the community. The classical method only considers the external connectivity, and only uses a single criterion to determine the community vulnerability. In the judgment of communities with different topological structures, it is easy to give the same vulnerability results, and the lower recognition cannot be used in a wide range of applications. The method in Ref. [38] takes into account 5 parameters, which are more considered than this proposed method consider. These parameters are the direct reflection of the community topological properties, and these topological properties are not processed and extracted. Application in some real-world networks is inconsistent with the actual vulnerability results. Therefore, this proposed method considers less community information through entropy and gives relatively reasonable vulnerability results. Communities with different structure topological are given different vulnerability assessments which means this proposed method is high resolution. In addition, the result obtained by this proposed method is also consistent with reality topology. These

advantages make this proposed method applicable to most networks in the real world.

In order to show the performance and effectiveness of this proposed method, one example network and four real-world complex networks are applied. Through the vulnerability order obtained by different methods, the rationality of this method is demonstrated. In addition, the sensitivity of weight factors is analyzed by Sobol' indices, and the important parameters considered in this model can be obtained. In large and complex communities, random attacks are used to show the effectiveness of the proposed method. All experiment results show the superiority and reasonableness of this proposed method in real-world network applications.

CRediT authorship contribution statement

Tao Wen: . **Yong Deng:** Writing - original draft, Validation, Writing - review & editing.

Declaration of Competing Interest

None.

Acknowledgment

The authors greatly appreciate the reviewers' suggestions and editor's encouragement. The authors thank Prof. Claudio Rocco for providing us with some network data. This work is partially supported by the National Natural Science Foundation of China (Grant Nos. 61973332, 61573290, and 61503237).

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.ress.2019.106782.

References

[1] Guan X, Xu Z, Jia QS. Energy-efficient buildings facilitated by microgrid. IEEE Trans Smart Grid 2010;1(3):243–52. https://doi.org/10.1109/tsg.2010.2083705.
[2] Bruneo D, Distefano S, Giacobbe M, Minnolo AL, Longo F, Merlino G, et al. An IoT service ecosystem for smart cities: The smartme project. Internet Things 2019;5:12–33. https://doi.org/10.1016/j.iot.2018.11.004.
[3] Dautov R, Distefano S, Buyya R. Hierarchical data fusion for smart healthcare. J Big Data 2019;6(1):19. https://doi.org/10.1186/s40537-019-0183-6.
[4] Dautov R, Distefano S, Bruneo D, Longo F, Merlino G, Puliafito A, et al. Metropolitan intelligent surveillance systems for urban areas by harnessing IoT and edge computing paradigms. Software 2018;48(8):1475–92. https://doi.org/10.1002/spe.2586.
[5] Lee L, Hu P. Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks. Int J Electr Power Energy Syst 2019;111:182–90. https://doi.org/10.1016/j.ijepes.2019.03.062.
[6] Cheng LF, Yu T. Smart dispatching for energy internet with complex cyber-physical-social systems: a parallel dispatch perspective. Int J Energy Res 2019;43(8):3080–133. https://doi.org/10.1002/er.4384.
[7] Guo H, Yu SS, Iu HHC, Fernando T, Zheng C. A complex network theory analytical approach to power system cascading failure-from a cyber-physical perspective. Chaos 2019;29(5):53111. https://doi.org/10.1063/1.5092629.
[8] Wang Z, Jusup M, Shi L, Lee JH, Iwasa Y, Boccaletti S. Exploiting a cognitive bias promotes cooperation in social dilemma experiments. Nat Commun 2018;9(1):2954.
[9] Wang Z, Jusup M, Wang RW, Shi L, Iwasa Y, Moreno Y, et al. Onymity promotes cooperation in social dilemma experiments. Sci Adv 2017;3(3):e1601444.
[10] Ma L, Li J, Lin Q, Gong M, Coello Coello CA, Ming Z. Reliable link inference for network data with community structures. IEEE Trans Cybern 2019;49(9):3347–61. https://doi.org/10.1109/TCYB.2018.2860284.
[11] Zhang W, Yang J, yu Ding X, mei Zou X, yu Han H, chao Zhao Q. Groups make nodes powerful: identifying influential nodes in social networks based on social conformity theory and community features. Expert Syst Appl 2019;125:249–58. https://doi.org/10.1016/j.eswa.2019.02.007.
[12] Ghalmane Z, Hassouni ME, Cherifi H. Betweenness centrality for networks with non-overlapping community structure. 2018 IEEE Workshop on complexity in engineering (COMPENG). 2018. p. 1–5. https://doi.org/10.1109/CompEng.2018.8536229.
[13] Wen T, Deng Y. Identification of influencers in complex networks by local information dimensionality. Inf Sci 2020;512:549–62. https://doi.org/10.1016/j.ins.2019.10.003.
[14] Dui H, Li S, Xing L, Liu H. System performance-based joint importance analysis guided maintenance for repairable systems. Reliab Eng Syst Saf 2019;186:162–75. https://doi.org/10.1016/j.ress.2019.02.021.
[15] Levitin G, Xing L, Huang HZ. Optimization of partial software rejuvenation policy. Reliab Eng Syst Saf 2019;188:289–96. https://doi.org/10.1016/j.ress.2019.03.011.
[16] Levitin G, Xing L, Haim HB, Huang HZ. Dynamic demand satisfaction probability of consecutive sliding window systems with warm standby components. Reliab Eng Syst Saf 2019;189:397–405. https://doi.org/10.1016/j.ress.2019.05.002.
[17] Levitin G, Xing L, Luo L. Joint optimal checkpointing and rejuvenation policy for real-time computing tasks. Reliab Eng Syst Saf 2019;182:63–72. https://doi.org/10.1016/j.ress.2018.10.006.
[18] Orman GK, Labatut V, Plantevit M, Boulicaut JF. Interpreting communities based on the evolution of a dynamic attributed network. Soc Netw Anal Min 2015;5(1):20. https://doi.org/10.1007/s13278-015-0262-4.
[19] Yang H, Deng Y. A bio-inspired optimal network division method. Phys A 2019;527:210–9.
[20] Rocco CM, Moronta J, Ramirez-Marquez JE, Barker K. Effects of multi-state links in network community detection. Reliab Eng Syst Saf 2017;163:46–56. https://doi.org/10.1016/j.ress.2017.02.004.
[21] Orman GK, Karadeli O, ÇaliŞr E. Overlapping communities via k-connected ego centered groups. Proceedings of the 2015 IEEE/ACM international conference on advances in social networks analysis and mining 2015. New York, NY, USA: ACM978-1-4503-3854-7; 2015. p. 1598–9. https://doi.org/10.1145/2808797.2809351.
[22] Orman GK, Labatut V, Naskali AT. Exploring the evolution of node neighborhoods in dynamic networks. Physica A: Statistical Mechanics and its Applications 2017;482:375–91. https://doi.org/10.1016/j.physa.2017.04.084. http://www.sciencedirect.com/science/article/pii/S0378437117304053
[23] Cherifi H, Palla G, Szymanski BK, Lu X. On community structure in complex networks: challenges and opportunities. Appl Network Sci 2019;4(117):1–35. https://doi.org/10.1007/s41109-019-0238-9.
[24] Ramirez-Marquez JE, Rocco CM, Barker K, Moronta J. Quantifying the resilience of community structures in networks. Reliab Eng Syst Saf 2018;169:466–74. https://doi.org/10.1016/j.ress.2017.09.019.
[25] Zhang X, Mahadevan S, Sankararaman S, Goebel K. Resilience-based network design under uncertainty. Reliab Eng Syst Saf 2018;169:364–79. https://doi.org/10.1016/j.ress.2017.09.009.
[26] Cerqueti R, Ferraro G, Iovanella A. Measuring network resilience through connection patterns. Reliab Eng Syst Saf 2019;188:320–9. https://doi.org/10.1016/j.ress.2019.03.030.
[27] Zhang X, Mahadevan S, Goebel K. Network reconfiguration for increasing transportation system resilience under extreme events. Risk Anal 2019. https://doi.org/10.1111/risa.13320.
[28] Zhou J, Huang N, Coit DW, Felder FA. Combined effects of load dynamics and dependence clusters on cascading failures in network systems. Reliab Eng Syst Saf 2018;170:116–26. https://doi.org/10.1016/j.ress.2017.10.008.
[29] Lu LQ, Wang X, Ouyang YF, Roningen J, Myers N, Calfas G. Vulnerability of interdependent urban infrastructure networks: Equilibrium after failure propagation and cascading impacts. Comput-Aided Civ InfrastructEng 2018;33(4):300–15. https://doi.org/10.1111/mice.12347.
[30] Ghalmane Z, Cherifi C, Cherifi H, El Hassouni M. Centrality in complex networks with overlapping community structure. Sci Rep 2019;9:29. https://doi.org/10.1038/s41598-019-46507-y.
[31] Ghalmane Z, El Hassouni M, Cherifi C, Cherifi H. Centrality in modular networks. Epj Data Sci 2019;8:27. https://doi.org/10.1140/epjds/s13688-019-0195-7.
[32] Ghalmane Z, El Hassouni M, Cherifi C, Cherifi H. k-truss decomposition for modular centrality. 2018 9th International symposium on signal, image, video and communications (ISIVC). 2018. p. 241–8. https://doi.org/10.1109/ISIVC.2018.8709196.
[33] Ramirez-Marquez JE, Rocco CM, Moronta J, Gama Dessavre D. Robustness in network community detection under links weights uncertainties. Reliab Eng Syst Saf 2016;153:88–95. https://doi.org/10.1016/j.ress.2016.04.009.
[34] Zhang X, Mahadevan S, Deng X. Reliability analysis with linguistic data: an evidential network approach. Reliab Eng Syst Saf 2017;162:111–21. https://doi.org/10.1016/j.ress.2017.01.009.
[35] Ghalmane Z, Hassouni ME, Cherifi H. Immunization of networks with non-overlapping community structure. Soc Netw Anal Min 2019;9(45). https://doi.org/10.1007/s13278-019-0591-9.
[36] Wang SL, Stanley HE, Gao YC. A methodological framework for vulnerability analysis of interdependent infrastructure systems under deliberate attacks. Chaos Solitons Fractals 2018;117:21–9. https://doi.org/10.1016/j.chaos.2018.10.011.
[37] Rocco S CM, Ramirez-Marquez JE. Vulnerability metrics and analysis for communities in complex networks. Reliab Eng Syst Saf 2011;96(10):1360–6. https://doi.org/10.1016/j.ress.2011.03.001.
[38] Wei D, Zhang X, Mahadevan S. Measuring the vulnerability of community structure in complex networks. Reliab Eng Syst Saf 2018;174:41–52. https://doi.org/10.1016/j.ress.2018.02.001.
[39] Kovacs-Hostyanszki A, Foldesi R, Baldi A, Endredi A, Jordan F. The vulnerability of plant-pollinator communities to honeybee decline: a comparative network analysis in different habitat types. Ecol Indic 2019;97:35–50. https://doi.org/10.1016/j.ecolind.2018.09.047.
[40] Alim MA, Li X, Nguyen NP, Thai MT, Helal A. Structural vulnerability assessment of community-based routing in opportunistic networks. IEEE Trans Mob Comput 2016;15(12):3156–70. https://doi.org/10.1109/tmc.2016.2524571.

[41] Che Y, Jia J, Zhao Y, He D, Cao T. Vulnerability assessment of urban power grid based on combination evaluation. Saf Sci 2019;113:144–53. https://doi.org/10.1016/j.ssci.2018.11.015.
[42] Wu Y., Chen Z., Yao K., Zhao X., Chen Y.. On the correlation between fractal dimension and robustness of complex networks. Fractals195006710.1142/S0218348X19500671.
[43] Deng W, Deng Y. Entropic methodology for entanglement measures. Phys A 2018;512:693–7.
[44] Wang Z, Bauch CT, Bhattacharyya S, d'Onofrio A, Manfredi P, Perc M, et al. Statistical physics of vaccination. Phys Rep 2016;664:1–113.
[45] Wei B, Deng Y. A cluster-growing dimension of complex networks: from the view of node closeness centrality. Phys A 2019;522:80–7. https://doi.org/10.1016/j.physa.2019.01.125.
[46] Wu Y, Yao K, Zhang X. The Hadamard fractional calculus of a fractal function. Fractals 2018;26(03):1850025. https://doi.org/10.1142/S0218348X18500251.
[47] Kang B, Deng Y. The maximum Deng entropy. IEEE Access 2019;7(1):120758–65.
[48] Gao X, Liu F, Pan L, Deng Y, Tsai S-B. Uncertainty measure based on Tsallis entropy in evidence theory. Int J Intell Syst 2019;34(11):3105–20.
[49] Tulu MM, Hou RH, Younas T. Identifying influential nodes based on community structure to speed up the dissemination of information in complex network. IEEE Access 2018;6:7390–401. https://doi.org/10.1109/access.2018.2794324.
[50] Salavati C, Abdollahpouri A, Manbari Z. Ranking nodes in complex networks based on local structure and improving closeness centrality. Neurocomputing 2019;336:36–45. https://doi.org/10.1016/j.neucom.2018.04.086.
[51] Xu P, Zhang R, Deng Y. A novel visibility graph transformation of time series into weighted networks. Chaos Solitons Fractals 2018;117:201–8.
[52] Wei B, Xiao F, Shi Y. Synchronization in Kuramoto oscillator networks with sampled-data updating law. IEEE Trans Cybern 2019:1–9. https://doi.org/10.1109/TCYB.2019.2940987.
[53] Liu F, Deng Y. A fast algorithm for network forecasting time series. IEEE Access 2019;7:102554–60. https://doi.org/10.1109/ACCESS.2019.2926986.
[54] Wen T, Duan S, Jiang W. Node similarity measuring in complex networks with relative entropy. Commun Nonlinear Sci NumerSimul 2019;78:104867. https://doi.org/10.1016/j.cnsns.2019.104867.
[55] Wen T, Jiang W. Measuring the complexity of complex network by Tsallis entropy. Phys A 2019;526:121054. https://doi.org/10.1016/j.physa.2019.121054.
[56] Newman MEJ. A measure of betweenness centrality based on random walks. Soc Netw 2005;27(1):39–54.
[57] Newman MEJ. Fast algorithm for detecting community structure in networks. Phys Rev E 2004;69(6):5. https://doi.org/10.1103/PhysRevE.69.066133.
[58] Newman MEJ, Girvan M. Finding and evaluating community structure in networks. Phys Rev E 2004;69(2). https://doi.org/10.1103/PhysRevE.69.026113.
[59] Liu F, Gao X, Zhao J, Deng Y. Generalized belief entropy and its application in identifying conflict evidence. IEEE Access 2019;7(1):126625–33.
[60] Song Y, Deng Y. Divergence measure of belief function and its application in data fusion. IEEE Access 2019;7(1):107465–72.
[61] Cao X, Deng Y. A new geometric mean FMEA method based on information quality. IEEE Access 2019;7(1):95547–54.
[62] Li M, Xu H, Deng Y. Evidential Decision Tree Based on Belief Entropy. Entropy 2019;21(9):897. https://doi.org/10.3390/e21090897.
[63] Tsallis C. Possible generalization of Boltzmann-Gibbs statistics. J Stat Phys 1988;52(1):479–87. https://doi.org/10.1007/BF01016429.
[64] Kullback S, Leibler RA. On information and sufficiency. Ann Math Stat 1951;22(1):79–86. https://doi.org/10.1214/aoms/1177729694.
[65] Manzi E, Labbe M, Latouche G, Maffioli F. Fishman's sampling plan for computing network reliability. IEEE Trans Reliab 2001;50(1):41–6. https://doi.org/10.1109/24.935016.
[66] Zachary WW. An information flow model for conflict and fission in small groups. J Anthropol Res 1977;33(4):452–73. https://doi.org/10.1086/jar.33.4.3629752.
[67] Guimerá R, Danon L, Díaz-Guilera A, Giralt F, Arenas A. Self-similar community structure in a network of human interactions. Phys Rev E 2003;68:65103. https://doi.org/10.1103/PhysRevE.68.065103.
[68] Crucitti P, Latora V, Marchiori M. Locating critical lines in high-voltage electrical power grids. Fluctuation Noise Lett 2005;5(2):201–8. https://doi.org/10.1142/s0219477505002562.