Int. J. Fuzzy Syst. (2018) 20(6):1956–1967
https://doi.org/10.1007/s40815-018-0457-8

Evaluating Topological Vulnerability Based on Fuzzy Fractal Dimension

Tao Wen[1] · Moxian Song[1] · Wen Jiang[1]

Received: 25 July 2017 / Revised: 13 December 2017 / Accepted: 31 January 2018 / Published online: 6 March 2018

Abstract Complex networks have been widely applied in many complex systems existed in nature and society because of its rapid development. Many methods have been proposed to evaluate the vulnerability of the complex networks because of the high security requirements of the network. In this paper, a novel method is proposed to evaluate network's vulnerability, which is based on fuzzy fractal dimension and average edge betweenness. Fuzzy fractal dimension can reflect the dynamic structure and topological structure of complex network, which is important to the vulnerability of complex network. So this proposed method can overcome the shortcomings of previous works by replacing the key coefficient p by fuzzy fractal dimension. In order to show this proposed method's accuracy and effectiveness, six USAir networks in different years are applied in this paper. Three common methods are used to compare the results with this proposed method, and the RB attack strategy is used to analyze the vulnerability of dynamic characteristic. The fuzzy fractal dimension of randomly selecting largest connected subset which is close to the initial fuzzy fractal dimension shows the reliability and stability of this proposed method. The vulnerability order obtained by this proposed method is more realistic, because the Pearson correlation coefficient r about this method equals to 0.9805, which shows a extremely strong correlation with the reality.

Keywords Fuzzy sets · Fractal dimension · Complex networks · Vulnerability evaluation · Average edge betweenness

1 Introduction

Recently, complex network [48] develops very quickly and becomes an important research field because it can model the complex system existed in the real world, such as protein network [33, 68], citation network [18], and so on. The previous researches pay more attention to the importance of nodes [28], the efficient spreading strategies [27, 38, 47, 67], the progress of society [54, 61], emergency management [19, 42]. Based on these existed research results, complex network can be used to predict the development of an unknown system [31]. Then, many practical models have been proposed, and these have been used in the real productions, like analyzing traffic congestion [24, 25, 63], recognizing the edges of the image [49].

Different methods to evaluate the vulnerability of networks have been proposed, which can be divided into two types. The first type is the topological property of network [2, 3], such as the average inverse geodesic length [35], the size of largest component [36], normalized average edge betweenness [6], and so on. These methods pay more attention to the structure of the network itself. The second type focuses on dynamical robustness [20, 59, 60]. Deleting some nodes or edges would increase other nodes' burden and change the network's structure, which can affect the vulnerability of networks. The most common method is proposed by Boccaletti et al. [6]. He evaluated vulnerability by multiscale evaluation model. This method combines the average edge betweenness and a key

✉ Wen Jiang
jiangwen@nwpu.edu.cn; jiangwenpaper@hotmail.com

[1] School of Electronics and Information, Northwestern Polytechnical University, Xi'an, Shaanxi 710072, China

coefficient p, and p would change with different networks. Because it is effective, it is widely studied by many researches [46]. One of the most serious problems is how to determine the key coefficient p because p does not have any physical meaning. Then, Li et al. [32] used the fractal dimension to evaluate the vulnerability, and it has a great progress.

Zadeh [65] first proposed fuzzy theory in 1965. This method regards the object to be investigated and the fuzzy concept as a certain fuzzy set. Then, he establishes the appropriate membership function and analyzes the fuzzy object through the operation and transformation of the fuzzy set. Because fuzzy set can describe the uncertain information more accurately, it has been used in many fields [17, 50] like supporting vector machine [26, 41, 58], D-S theory [21, 39, 62, 69, 70], ant colony optimization [8, 13], fuzzy regression [4, 14, 15, 66], information granules [51, 53], designing type 2 fuzzy systems [11, 12], data mining [16, 37, 43], and multiobjective evolutionary algorithm [7, 22, 23, 40, 44]. Pedryca [52] has already calculated the fractal dimension by fuzzy sets in time series. Fuzzy fractal dimension has been used in many fields by Castillo et al. such as measuring the complexity of the sound signal [45], time series prediction [10], simulation of robotic dynamic systems [9]. Fractal dimension can show the self-similarity and fractal properties of complex networks [29, 30, 56], which can reveal the dynamic structure and topological structure of complex network. Based on these excellent features, Tsallis information dimension [64] and generalized volume dimension [55] of complex networks have been proposed later. Meanwhile, the box-covering algorithm has been used to get the number of boxes in complex networks by Song et al. [56, 57]. Zhang et al. [5] proposed the fuzzy fractal dimension of complex networks, which can depict the covering ability of each boxes and spend less time. It can describe the self-similarity and fractal properties of complex networks too.

In this paper, a novel method to evaluate the vulnerability is proposed, which is based on fuzzy fractal dimension. The fuzzy sets make the influence between different nodes more accurate through a interval continuous function between 0 and 1. Fuzzy fractal dimension can reflect the dynamic structure and topological structure of complex network, which is important to the vulnerability of complex network. Based on this, fuzzy fractal dimension replaces the key coefficient p to evaluate the vulnerability of complex network. Three methods which are the average inverse geodesic length, the size of largest component, normalized average edge betweenness are used to compare the results with this proposed method. The RB attack strategy [35] is used to analyze the vulnerability of dynamic characteristic. In order to show this method's accuracy, six US airline networks in different years are applied in this paper, and the Pearson correlation coefficient r is used to analyze the correlation between the results and the reality. The results show that this method is more accurate and consistent with the actual situation. The result of randomly selecting largest connected subset is close to the initial fuzzy fractal dimension, and it shows the reliability and stability of this method.

The remainder of this paper is organized as follows. Some brief overview of vulnerability evaluation, fuzzy sets, and fractal dimension is given in Sect. 2. In Sect. 3, the method which is based on the fuzzy fractal dimension to evaluate the vulnerability of network is proposed. Six US airline networks in different years are used to compare this proposed method and other already existing methods in Sect. 4. Some conclusions are given in Sect. 5.

2 Preliminaries

2.1 Multiscale Vulnerability

Boccaletti et al. [6] proposed a vulnerability evaluation model by the average edge betweenness, which is shown as follows:

$$b_l(G) = \frac{1}{|E|}\sum_{l\in E} b_l, \tag{1}$$

where $|E|$ is the number of the edges, b_l is the betweenness of edge l, which is defined as follows:

$$b_l = \sum_{j,k\in V} \frac{n_{jk}(l)}{n_{jk}}, \tag{2}$$

where n_{jk} is the number of geodesics (the shortest distance) from node j to node k, $n_{jk}(l)$ is the number of geodesics from node j to node k, which contain the edge l.

This evaluation method b_l cannot give relevant new information about the vulnerability of some special networks. For instance, two networks are shown in Fig. 1,

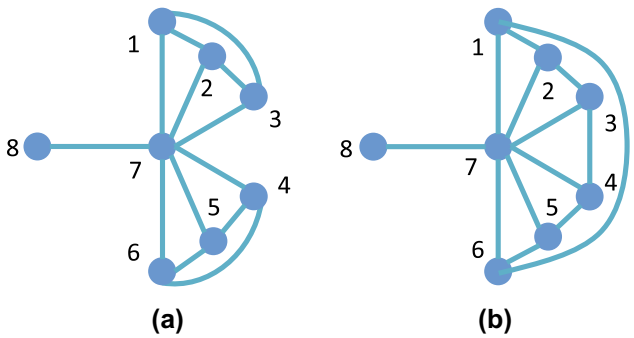

Fig. 1 The "bat" network and the "umbrella" network

which is called "bat" network G and "umbrella" network G' separately. When evaluating these two networks' vulnerability by Eq. (1), the result is that $b_l(G) = b_l(G') = 43/13$. But the "umbrella" network G' is more robust than the "bat" network G, so this method is not accurate.

Then, Boccaletti et al. [6] improved this method to overcome this limitation by a key coefficient p. This improved work is called multiscale vulnerability and shown as follows:

$$\mathrm{b_p}(G) = \left(\frac{1}{|E|}\sum_{l\in E} b_l^p\right)^{\frac{1}{|p|}} \tag{3}$$

When we use this improved method to compare two networks G and G', first compute b_1. If $b_1(G) < b_1(G')$, network G is more robust than network G', and $b_1(G) > b_1(G')$ is an opposite case. When $b_1(G) = b_1(G')$, then increase p and compute b_p until $b_p(G) \neq b_p(G')$.

Boccaletti et al. proposed a relative function of p to ensure the coefficient p which is shown as follows:

$$f(p) = \frac{\left|\mathrm{b_p}(G) - \mathrm{b_p}(G')\right|}{\max(\mathrm{b_p}(G), \mathrm{b_p}(G'))} \tag{4}$$

The key coefficient p is obtained when the relative function has a maximal value. For more detailed information about coefficient p, please refer [6].

2.2 Fuzzy Sets

In the traditional case of things divided into two categories, when there is a class C which is a subset of the universal set X, any case of an input variable $\mathrm{x} \in \mathrm{X}$ whether belongs to the given subset C or not. There is a characteristic function $I_C(x) \rightarrow \{0, 1\}$, which is defined as follows:

$$I_C(x) = \begin{cases} 0, & x \in C \\ 1, & x \notin C \end{cases} \tag{5}$$

where there is a premise $\mathrm{x} \in \mathrm{X}$.

Facing real-world situations, there is no clear boundary between two categories or the boundary may be overlapping. So it is uncertain that the input variable x belongs to

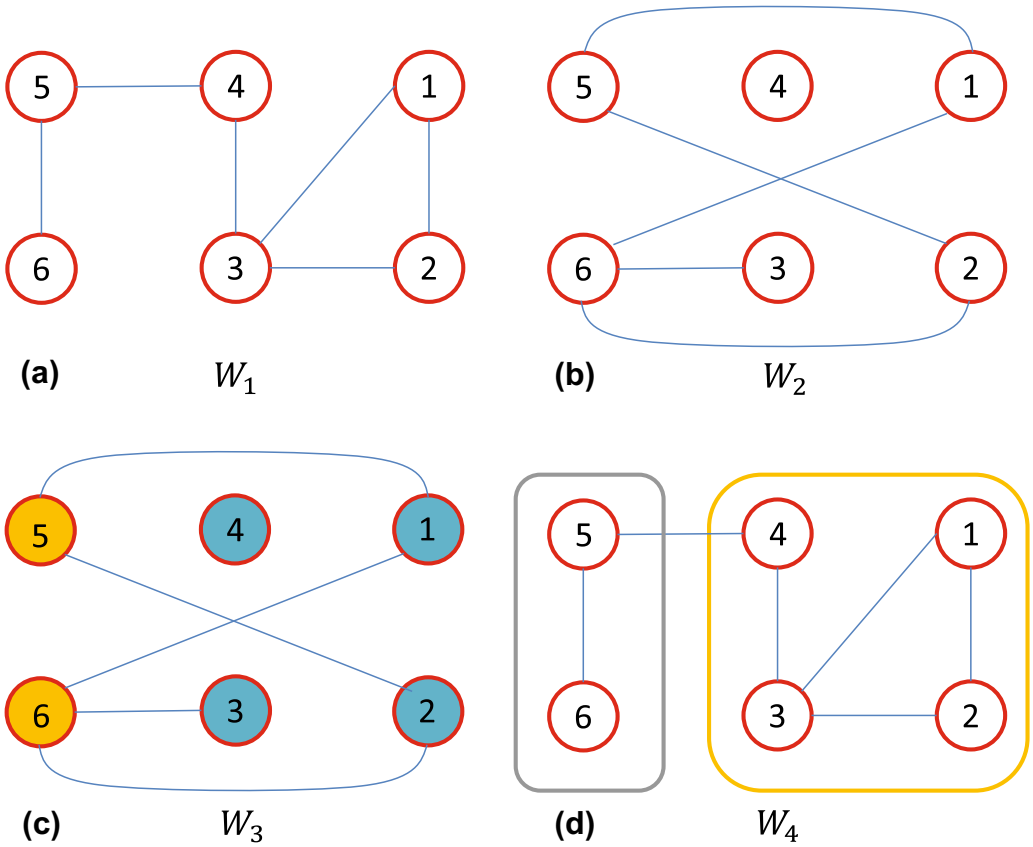

Fig. 2 Detail about the box-covering algorithm. **a** There is a random weighted network called W_1, which has six nodes and six weighted edges. Observing from the figure, the path between any two nodes can be easily obtained. **b** Node i can be connected to node j when $d_{ij} \geq 3$. A new weighted network is established, and it is called W_2. **c** These nodes connected directly have different colors, and the rest of the nodes have the same color with node 3 because node 3 has the maximum value of node strength. **d** Finally, as one color for one box, the minimum number of box of W_1 can be obtained, and it is two, as shown in W_4

the subset C totally. To deal with this problem, this characteristic function must be improved to describe the intermediate value between 0 and 1. Zadeh [65] proposed the fuzzy sets to modify the characteristic function $I_C(x)$ to the membership function $\mu_C(x)$, which can describe the interval continuous function between 0 and 1.

2.3 Fuzzy Fractal Dimension

A complex network is shown as $G(N, E)$, where N is the set of node and E is the set of edge. The box-covering dimension is originally proposed by Hausdorff [34]. The number of boxes and the box size have a relationship as follows:

$$N(\varepsilon) \approx \varepsilon^{-d_B}, \tag{6}$$

where $N(\varepsilon)$ is the minimum number of boxes to cover the whole network when the box size is equal to ε, and d_B is the fractal dimension. The distance between any two nodes in one box is less than the box size ε. Then, the fractal dimension d_B can be obtained as follows:

$$d_B \approx -\frac{\ln(N(\varepsilon))}{\ln(\varepsilon)} \tag{7}$$

The detail about box-covering algorithm is shown in Fig. 2

Equation (7) can be rewritten as follows:

$$d_B \approx \frac{\ln(N(\varepsilon)^{-1})}{\ln(\varepsilon)} \tag{8}$$

where $N(\varepsilon)^{-1}$ is the reciprocal of $N(\varepsilon)$ and it can be seen as the covering ability (CA) of each boxes. When more boxes are needed, the covering ability of each box is smaller. Then, the covering ability $N(\varepsilon)^{-1}$ of the box size ε is obtained as follows:

$$N^{-1}(\varepsilon) = \frac{1}{N(N-1)} \sum_{i=1}^{N} \sum_{j=1(j\neq i)}^{N} A_{ij}(\varepsilon) \tag{9}$$

where ε is the size of box, $A_{ij}(\varepsilon)$ is a membership function when the shortest distance between node i and node j is close to the box size ε, and Gaussian membership is used in this method, which is shown as follows:

$$A_{ij}(\varepsilon) = \exp\left(-\frac{d_{ij}^2}{\varepsilon^2}\right), \tag{10}$$

where d_{ij} is the shortest distance between node i and node j, and ε is the box size. $A_{ij}(\varepsilon)$ is a membership function which can give the degree how close other nodes from the center node. The membership function $A_{ij}(\varepsilon)$ can give a different weight between 0 and 1 to the neighbor node j based on the shortest distance, and it would be larger when the neighbor node j is closer to the center node i. The larger of the $A_{ij}(\varepsilon)$ represents the greater the contribution of neighbor node j to the center node i.

2.4 Comparison Methods

To compare this method, three methods which are frequently used to evaluate the networks' vulnerability are shown as follows. First, the average inverse geodesic length l^{-1} is shown as follows:

$$l^{-1} = \left\langle \frac{1}{d(v,w)} \right\rangle = \frac{1}{N(N-1)} \sum \sum \frac{1}{d(v,w)} \tag{11}$$

where $d(v, w)$ is the length of geodesic (the shortest distance) between node v and node w which are both contained in network node set N, and $N(N-1)$ is the number of node pairs. When l^{-1} is larger, the network is more robust.

Secondly, the size of largest component $LGS(0 < LGS < 1)$ can obtain the number of nodes in the largest connected subgraph, which is shown as follows:

$$LGS = \frac{N_s}{N}, \tag{12}$$

where N_s is the size of the largest connected subgraph. So when LGS is larger, the network is more robust.

Thirdly, this method is called normalized average edge betweenness $b_{\text{nor}}\langle G\rangle$ which is based on Eq. (3) while $p = 1$. This method is shown as follows:

$$b_{\text{nor}}\langle G\rangle = \frac{b_1(G) - b_1(G_{\text{complete}})}{b_1(G_{\text{path}}) - b_1(G_{\text{complete}})} = \frac{b_1(G) - 1}{\frac{N(N+1)}{6} - 1} \tag{13}$$

where G_{complete} is a complete graph and G_{path} is a path graph. When $b_{\text{nor}}\langle G\rangle$ is smaller, the network is more robust.

3 Evaluating Topological Vulnerability Based on Fuzzy Fractal Dimension

3.1 Basic Method

In this section, because the average edge betweenness cannot distinguish special networks like the "bat" and "umbrella" network, a novel method is proposed to evaluate the vulnerability of complex networks. Because the key coefficient p is a constant which does not have any physical meaning, it should be changed into special coefficient which can reveal the topological structure of the whole complex network. In this method, the fuzzy fractal dimension is considered as a advantageous alternative to define the key coefficient p. It is universally known that fractal dimension can reveal the dynamic structure and topological structure of complex network, and it can

illustrate self-similarity and fractal properties of networks. Fuzzy sets can describe the interval continuous function between 0 and 1, which is more accurate. For a complex network $G(N, E)$, where N and E, respectively, represent the sets of nodes and edges in the whole complex networks, when there are more edges in this network, the diameter of network would be smaller, less boxes are needed to cover the whole network, and the space-filling capacity would be higher. These would cause the decrease in the fuzzy fractal dimension, and it is well known that a network with more edges is more robust. Based on these, fuzzy fractal dimension is more likely to reveal the networks' vulnerability. So using fuzzy fractal dimension to replace the key coefficient p is more logical.

The fuzzy fractal dimension of complex networks can be obtained as follows:

$$d_B \approx \frac{\ln(N(\varepsilon)^{-1})}{\ln(\varepsilon)}, \tag{14}$$

where $N(\varepsilon)^{-1}$ is the covering ability (CA) of each boxes, which can be obtained as follows:

$$N^{-1}(\varepsilon) = \frac{1}{N(N-1)} \sum_{i=1}^{N} \sum_{j=1(j\neq i)}^{N} A_{ij}(\varepsilon) \tag{15}$$

where $A_{ij}(\varepsilon)$ is Gaussian membership function which can be obtained from Eq. (10). Using membership function can reveal the covering ability more accurately because it can describe the interval continuous function between 0 and 1.

After replacing the key coefficient p by fuzzy fractal dimension to evaluate the networks' vulnerability, the novel method is shown as follows:

$$V_{d_B}(G) = \left(\frac{1}{|E|} \sum_{l \in E} b_l^{d_B} \right)^{\frac{1}{|d_B|}}, \tag{16}$$

where b_l is the set of edge closeness and $|E|$ is the number of edges.

When V_{d_B} is smaller, the network is more robust. This method can be widely used in many complex networks with fractal property to evaluate vulnerability. This proposed method could be more effective and realistic because of the use of fuzzy fractal dimension.

3.2 Example Explanation

Because the previous works cannot compare the "bat" network G and "umbrella" network G' well, this novel method can be used to compare the vulnerability. These two networks are shown in Fig. 1.

Step 1 Firstly, "bat" network is selected to be an example. When the box size is equal to 1, the covering ability of a box whose center node is node 1 can be obtained as follows:

$$\begin{aligned} N_1(1)^{-1} &= \frac{\exp\left(-\frac{d_{12}^2}{1^2}\right) + \exp\left(-\frac{d_{13}^2}{1^2}\right) + \exp\left(-\frac{d_{14}^2}{1^2}\right)}{(N-1)} \\ &\quad \frac{+\exp\left(-\frac{d_{15}^2}{1^2}\right) + \exp\left(-\frac{d_{16}^2}{1^2}\right) + \exp\left(-\frac{d_{17}^2}{1^2}\right) + \exp\left(-\frac{d_{18}^2}{1^2}\right)}{(N-1)} \\ &= \frac{\exp\left(-\frac{1^2}{1^2}\right) + \exp\left(-\frac{1^2}{1^2}\right) + \exp\left(-\frac{1^2}{1^2}\right)}{7} \\ &= 0.1577 \end{aligned} \tag{17}$$

The covering ability of other center node can be obtained in the same way,

$$\begin{aligned} N_2(1)^{-1} &= 0.1577 \\ N_3(1)^{-1} &= 0.1577 \\ N_4(1)^{-1} &= 0.1577 \\ N_5(1)^{-1} &= 0.1577 \\ N_6(1)^{-1} &= 0.1577 \\ N_7(1)^{-1} &= 0.3680 \\ N_8(1)^{-1} &= 0.0526 \end{aligned} \tag{18}$$

So when the box size is equal to 1, the covering ability is $N(1)^{-1} = 0.1708$, which means that each box covers 17.08% nodes of the whole network.

Step 2 The box size would increase from 1 until it is greater than the box diameter. The covering ability can be obtained from Eq. (9),

$$N(2)^{-1} = 0.5587 \tag{19}$$

Step 3 The relationship between covering ability and box size is shown in Fig. 3. The slope of red straight line is obtained in the log–log plot by means of the least squares fit, and the fuzzy fractal dimension can be obtained from the slope of the line.

Step 4 Then, the vulnerability of "bat" network can be evaluated based on fuzzy fractal dimension by Eq. (16), and it is $V_{d_B}(G) = 0.0835$.

Step 5 Using the same way to get "umbrella" network's fuzzy fractal dimension and vulnerability, the fuzzy fractal dimension is shown in Fig. 4, and the vulnerability is $V_{d_B}(G') = 0.0810$.

When V_{d_B} is smaller, the network is more robust. Because $V_{d_B}(G) > V_{d_B}(G')$, a conclusion can be obtained that "umbrella" network is more robust than "bat" network, and this conclusion is same as vision. When node 7 is attacked, "bat" network would be separated into three parts, but "umbrella" network only be separated into two parts. The edge of "umbrella" network is more uniform, and the edges of "bat" network are centered near node 7.

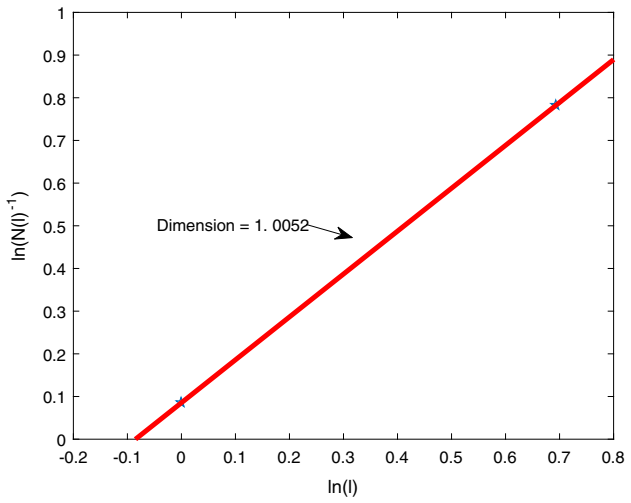

Fig. 3 The fuzzy fractal dimension of "bat" network

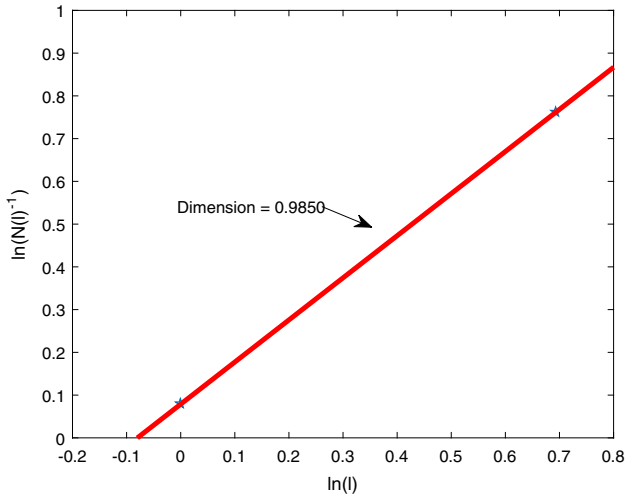

Fig. 4 The fuzzy fractal dimension of "umbrella" network

4 Experimental Study

In order to test the effectiveness and accuracy of this proposed method, six unweighted undirected US airline networks are used, that is, US airline network in 2005, 2007, 2009, 2010, 2011, 2013. These networks can be downloaded from Bureau of Transportation Statistics (BTS) [1]. The node represents the airport, and the edge represents there is airline between these two airports. The small subgraph and self-loops are removed to form unweighted undirected complex networks, so only the largest connected subset of the original network is retained.

4.1 Comparison with Other Three Methods

Three methods which are introduced in Sect. 2 are used as a comparison, that is, the average inverse geodesic length l^{-1}, the size of largest component LGS, and the normalized average edge betweenness $b_{\text{nor}}\langle G\rangle$. The RB attack strategy [35] is used to analyze the vulnerability of dynamic characteristic, and it is more trusted. RB attack strategy is deleting the node with highest betweenness value and calculating the betweenness of this new network. Then, the node with highest betweenness value in the new network is also deleted until required number of nodes is deleted. Lastly, the vulnerability of the network can be obtained from the remaining network. In this paper, the top 1% nodes should be deleted from the original network to obtain l^{-1}, LGS, and $b_{\text{nor}}\langle G\rangle$.

The fuzzy fractal dimension is shown in Fig. 5. The dot sign represents the relationship between the covering ability $N(\varepsilon)^{-1}$ and the size of box ε, and the slope of the red line is obtained in the log–log by means of the least squares fit. The fuzzy fractal dimension is 2.1682, 2.5095, 2.3630, 2.3756, 2.4013, 2.0883, respectively, in different years. With the development of time, the fuzzy fractal dimension V_{d_B} does not have the monotony but the irregular change, and it keeps between 2 and 3, which agrees the law of this network.

The results obtained by these methods are shown in Table 1. From Table 1, it can be found that with the development of USAir network, the number of nodes and edges are slightly increased. The fuzzy fractal dimension is irregularly changed, but it keeps between 2 and 3. For all of these four methods, only this proposed method V_{d_B} is monotonically decreasing (0.0018, 0.0015, 0.0014, 0.0012, 0.0011, 0.0010). The network would be more vulnerable with the larger value of V_{d_B}, so this proposed method would give a realistic vulnerability order about USAir network ($USAir2003 > USAir\quad 2005 > USAir2007 > USAir2009 > USAir2011 > USAir2013$). The rest of methods ($l^{-1}$, LGS, $b_{\text{nor}}\langle G\rangle$) cannot give a monotonous changed result, so realistic vulnerability orders cannot be obtained according to their own nature. A conclusion can be obtained that this proposed method V_{d_B} shows better performance than other methods and has a realistic result.

Based on the results shown in Table 1, each method can get a order of vulnerability, and it is shown in Table 2. Three conclusions can be obtained as follows:

1. The average edge betweenness b_1 of six US airline networks is very small, and it is not suitable for ranking the vulnerability. The results obtained by this proposed method are an order of magnitude larger than the average edge betweenness, and it shows that this proposed method is more suitable to rank the vulnerability of networks.
2. The order of vulnerability obtained by other methods is not exactly right. For example, the average inverse geodesic length l^{-1} and the size of largest component

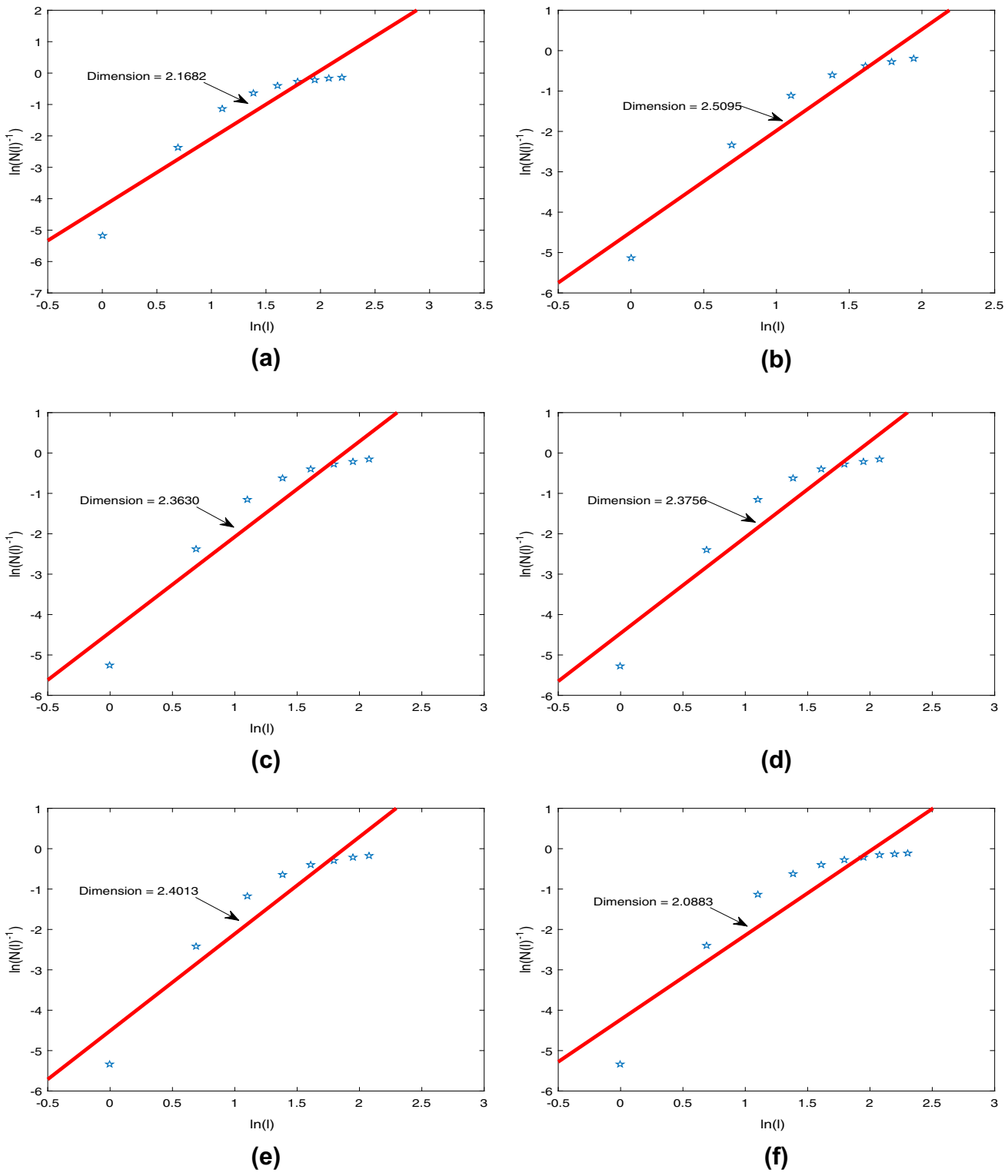

Fig. 5 The fuzzy fractal dimension of different networks. **a** US airline network in 2003. **b** US airline network in 2005. **c** US airline network in 2007. **d** US airline network in 2009. **e** US airline network in 2011. **f** US airline network in 2013

LGS show that USAir 2007 is the most robust network and USAir 2013 is the most vulnerable network, and the normalized average edge betweenness $b_{\text{nor}}\langle G\rangle$ shows that USAir 2005 is the most robust network and USAir 2007 is the most vulnerable network. All of these are not realistic like this proposed method.

Table 1 The results of six USAir networks in different years

Network	N	E	d_B	V_{d_B}	b_1	$l^{-1'}$	LGS'	$b_{\mathrm{nor}}(G)'$	$\mathrm{d}_{\mathrm{B_{M\pm SD}}}$
USAir 2003	1387	15618	2.1682	0.0018	0.00017	0.1221	0.3223	0.0096	2.1071 ± 0.1290
USAir 2005	1447	17453	2.5095	0.0015	0.00018	0.1312	0.3034	0.0984	2.2374 ± 0.1642
USAir 2007	1605	19166	2.3630	0.0014	0.00018	0.1389	0.3352	0.1051	2.2841 ± 0.1165
USAir 2009	1548	17415	2.3756	0.0012	0.00020	0.1211	0.3204	0.0487	2.2510 ± 0.1178
USAir 2011	1587	17969	2.4013	0.0011	0.00019	0.0916	0.2823	0.0961	2.2263 ± 0.1412
USAir 2013	1635	16215	2.0883	0.0010	0.00021	0.0899	0.2557	0.042	2.1847 ± 0.1309

d_B is the fuzzy fractal dimension, and V_{d_B} is the proposed method in this paper, which is based on d_B. The average inverse geodesic length $l^{-1'}$, the size of largest component LGS', and the normalized average edge betweenness $b_{\mathrm{nor}}(G)'$ are obtained after deleting 1% nodes. $\mathrm{d}_{\mathrm{B_{M\pm SD}}}$ is the mean value and standard deviation after randomly deleting 500 nodes

Table 2 The vulnerability orders obtained by different methods

Methods	Vulnerability order
$l^{-1'}$	$USAir2013 > USAir2011 > USAir2009 > USAir2003 > USAir2005 > USAir2007$
LGS'	$USAir2013 > USAir2011 > USAir2005 > USAir2009 > USAir2003 > USAir2007$
$b_{\mathrm{nor}}(G)'$	$USAir2007 > USAir2011 > USAir2009 > USAir2013 > USAir2003 > USAir2005$
V_{d_B}	$USAir2003 > USAir2005 > USAir2007 > USAir2009 > USAir2011 > USAir2013$

3. Although the fuzzy fractal dimension is similar, but the order of vulnerability is completely correct. It is $USAir2003 > USAir2005 > USAir2007 > USAir2009 > USAir2011 > USAir2013$, and this order is consistent with the actual situation.

After randomly deleting 500 nodes from the original network, the new network would be smaller. Then, the same method is used, that is, to find the largest connected subset of the deleted network. Based on the largest connected subset, the fuzzy fractal dimension can be obtained easily by Eq. (14). Because randomly 500 nodes are deleted in this method, a large number of experiments are needed to reduce error. In this literature, 500 same experiments are repeated for this purpose. The mean value and standard deviation $\mathrm{d}_{\mathrm{B_{M\pm SD}}}$ of 500 repeated experiments are shown in the last column of Table 1. From the results in Table 1, it can be found that the mean of fuzzy fractal dimension $\mathrm{d}_{\mathrm{B_M}}$ is close to the initial fuzzy fractal dimension d_B, and the difference between them is close to the standard deviation. It demonstrates the robustness, reliability, and stability of this proposed method.

To explore the correlation degree between all of these results and the reality, Pearson product-moment moment correlation coefficient r which is a common correlation coefficient is used in this paper. r is defined as follows:

$$\mathrm{r_{xy}} = \frac{\sum (X-\bar{X})(Y-\bar{Y})}{\left(\sqrt{\sum_{i=1}^{n}(X_i-\bar{X})^2}\right)\left(\sqrt{\sum_{i=1}^{n}(Y_i-\bar{Y})^2}\right)}, \tag{20}$$

Table 3 r between different results and the reality

Methods	r	Correlation degree
$l^{-1'}$	0.7771	Strong correlation
LGS'	0.7426	Strong correlation
$b_{\mathrm{nor}}(G)'$	0.4983	Moderate degree correlation
V_{d_B}	0.9805	Extremely strong correlation

where n is the sample capacity, X and Y are two samples which need to explore their correlation, and $\bar{X}$ and $\bar{Y}$ are the mean of X and Y respectively. r should be a value between -1 and 1, where $r = 1$ represents perfect positive correlation, $r = -1$ represents perfect negative correlation, and $r = 0$ represents two irrelevant samples. The reality is the later the network is more robust ($X = \{6, 5, 4, 3, 2, 1\}$), Y is the result about l^{-1}, LGS, $b_{\mathrm{nor}}\langle G\rangle$, V_{d_B} which can be obtained in Table 1. The correlation degree between X and different Y is shown in Table 3.

From Table 3, it can be easily found that only this proposed method V_{d_B} gives a more realistic vulnerability order whose r is close to 1, and other methods cannot give accurate results because their r are only between 0.4 and 0.8. So this proposed method can evaluate the vulnerability of complex networks more correctly than other methods.

From these results, the fuzzy fractal dimension replaces the key coefficient p that can evaluate the vulnerability of complex networks more correctly. The rest of the methods have their own shortcomings, and their results cannot give

Table 4 The fuzzy fractal dimension and vulnerability based on different MF

Network	d_{B-Gau}	$V_{d_{B-Gau}}$	d_{B-Tri}	$V_{d_{B-Tri}}$	d_{B-Tra}	$V_{d_{B-Tra}}$
USAir 2003	2.1682	0.0018	2.7441	0.0019	2.6748	0.0017
USAir 2005	2.5095	0.0015	3.3242	0.0049	3.2865	0.0047
USAir 2007	2.3630	0.0014	2.9361	0.0027	2.8442	0.0025
USAir 2009	2.3756	0.0012	2.9636	0.0026	2.8877	0.0025
USAir 2011	2.4013	0.0011	3.1101	0.0032	3.9294	0.0030
USAir 2013	2.0883	0.0010	2.6083	0.0015	2.5231	0.0013

the exactly right orders. So this proposed method is accurate and effective.

4.2 Comparison With Other Two Membership Functions

In order to show the superiority of Gaussian Membership Function (MF) to this proposed method, two other MFs (Triangular MF, Trapezoidal MF) are introduced as contrast experiments in this section. Triangular MF and Trapezoidal MF are used as common MFs in the fuzzy sets, so they have certain representativeness.

Triangular membership function is shown as follows:

$$A_{\mathrm{ij\_tri}}(\varepsilon) = \begin{cases} \dfrac{\varepsilon - d_{ij}}{\varepsilon}, & d_{ij} \le \varepsilon \\ 0, & d_{ij} > \varepsilon \end{cases} \tag{21}$$

where ε is the size of box, and d_{ij} is the shortest distance between node i and node j. This MF gives the weight of a single function form to other node j whose shortest distance from node i is less than ε, and the node whose shortest distance from node i is larger than ε has no weight.

Trapezoidal membership function is shown as follows:

$$A_{\mathrm{ij\_tra}}(\varepsilon) = \begin{cases} 1, & d_{ij} \le 0.4\varepsilon \\ \dfrac{\varepsilon - d_{ij}}{\varepsilon - 0.4\varepsilon}, & 0.4\varepsilon < d_{ij} \le \varepsilon \\ 0, & d_{ij} > \varepsilon \end{cases} \tag{22}$$

where ε is the size of box, and d_{ij} is the shortest distance between node i and node j. This MF gives a weight of 1 for the node whose shortest distance is less than 0.4ε, the node whose shortest distance from node i is between 0.4ε and ε has a weight of a single function form, and other nodes would have no weight.

The fuzzy fractal dimension based on these three MFs is shown in Table 4. From Table 4, it can be found that the fuzzy fractal dimension based on different MFs is irregularly changed. The fuzzy fractal dimension based on triangular MF and trapezoidal MF is closer to 3, which is bigger than the fuzzy fractal dimension based on Gaussian MF. Based on the different fuzzy fractal dimensions, the vulnerability of USA complex networks can be obtained by Eq. (16). With the larger value of V_{d_B}, the network would be more vulnerable, so the vulnerability order can be easily obtained and they are different from each other. The vulnerability order based on Gaussian MF is realistic, which was discussed in detail in Sect. 4.1, but the vulnerability orders based on triangular MF and trapezoidal MF are not regular like Gaussian MF. The details are shown in Table 5.

It can be found that only the vulnerability order based on Gaussian MF is consistent with the development of USAir network, and the rest of the methods cannot obtain correct orders. The vulnerability of USAir 2007 and USAir 2009 based on trapezoidal MF is even equal, so this method cannot judge similar networks. The correlation coefficients r in triangular MF and trapezoidal MF are between 0.2 and 0.4, which show the weak correlation about these methods.

When contribution is affected by multiple factors, and each factor cannot give a dominant influence, the contribution would be subject to the Gaussian MF. Because Gaussian MF is the most common distribution in nature, and the information entropy of it is largest, so it can reveal the covering ability more accurately.

5 Conclusion

Fractal dimension can reveal the dynamic structure and topological structure of complex network, and it can illustrate self-similarity and fractal properties of networks. When fractal dimension is smaller, the space-filling capacity is higher and less number of boxes is needed to cover the whole network, which would lead to more robust

Table 5 The vulnerability orders based on different MFs

MFs	Vulnerability order	r	Correlation degree
$V_{d_{B-Gau}}$	$USAir2003 > USAir2005 > USAir2007 > USAir2009 > USAir2011 > USAir2013$	0.9805	Extremely strong correlation
$V_{d_{B-Tri}}$	$USAir2005 > USAir2011 > USAir2007 > USAir2009 > USAir2003 > USAir2013$	0.3225	Weak correlation
$V_{d_{B-Tra}}$	$USAir2005 > USAir2011 > USAir2007 = USAir2009 > USAir2003 > USAir2013$	0.3187	Weak correlation

structure. So it is a unique parameter for each network, which is closely related to the vulnerability of the network. Fuzzy sets can describe the relationship between any two nodes more accurately through a interval continuous function between 0 and 1. So fuzzy fractal dimension can reveal the structure more effectively. The combination of fuzzy fractal dimension and average edge betweenness can improve the flaws of the previous work, and it is more concerned about the structure of the network itself. In this paper, "bat" network and "umbrella" network are used to show how this method works, and several real-world complex networks are used to show the effectiveness and accuracy of this proposed method. The result of randomly selecting largest connected subset is close to the initial fuzzy fractal dimension, and it shows the reliability and stability of this method. The order of vulnerability obtained by this proposed is consistent with the actual situation, and the r about this proposed method is 0.9805, which shows this proposed method gives a more realistic vulnerability order. The comparison with other already existing methods shows this proposed method is more accurate because r of the proposed method is only between 0.4 and 0.8. So this proposed method is accurate and the result is realistic.

Acknowledgements The authors greatly appreciate the reviewer's suggestions and the editor's encouragement. The work is partially supported by National Natural Science Foundation of China (Program No. 61671384, 61703338), Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2016JM6018), Project of Science and Technology Foundation, and Fundamental Research Funds for the Central Universities (Program No. 3102017OQD020).

References

1. Albert, R., Albert, I., Nakarado, G.L.: Structural vulnerability of the north american power grid. Phys. Rev. E **69**(2) (2004). https://doi.org/10.1103/PhysRevE.69.025103
2. Albert, R., Barabasi, A.L.: Statistical mechanics of complex networks. Rev. Mod. Phys. **74**(1), 47–97 (2002). https://doi.org/10.1103/RevModPhys.74.47
3. Ayhan, M.B., Aydin, M.E., Oztemel, E.: A multi-agent based approach for change management in manufacturing enterprises. J. Intell. Manuf. **26**(5), 975–988 (2015). https://doi.org/10.1007/s10845-013-0794-2
4. Bian, T., Zheng, H., Yin, L., Deng, Y.: Failure mode and effects analysis based on Dnumbers and topsis. Qual. Reliab. Eng. Int. Article ID: QRE2268 (2018). https://doi.org/10.1002/qre.2268
5. Boccaletti, S., Buldu, J., Criado, R., Flores, J., Latora, V., Pello, J., Romance, M.: Multiscale vulnerability of complex networks. Chaos **17**(4) (2007). https://doi.org/10.1063/1.2801687
6. Bureau of transportation statistics. http://www.transtats.bts.gov/DL_SelectFields.asp?Table_ID=292
7. Carmona, C.J., Chrysostomou, C., Seker, H., del Jesus, M.J.: Fuzzy rules for describing subgroups from influenza a virus using a multi-objective evolutionary algorithm. Appl. Soft Comput. **13**(8), 3439–3448 (2013). https://doi.org/10.1016/j.asoc.2013.04.011
8. Castillo, O., Lizarraga, E., Soria, J., Melin, P., Valdez, F.: New approach using ant colony optimization with ant set partition for fuzzy control design applied to the ball and beam system. Inf. Sci. **294**, 203–215 (2015). https://doi.org/10.1016/j.ins.2014.09.040
9. Castillo, O., Melin, P.: Automated mathematical modelling, simulation and behavior identification of robotic dynamic systems using a new fuzzy-fractal-genetic approach. Robot. Auton. Syst. **28**(1), 19–30 (1999). https://doi.org/10.1016/s0921-8890(99)00026-3
10. Castillo, O., Melin, P.: Hybrid intelligent systems for time series prediction using neural networks, fuzzy logic, and fractal theory. IEEE Trans. Neural Netw. **13**(6), 1395–1408 (2002). https://doi.org/10.1109/tnn.2002.804316
11. Castillo, O., Melin, P.: Optimization of type-2 fuzzy systems based on bio-inspired methods: a concise review. Inf. Sci. **205**, 1–19 (2012). https://doi.org/10.1016/j.ins.2012.04.003
12. Castillo, O., Melin, P., Pedrycz, W.: Design of interval type-2 fuzzy models through optimal granularity allocation. Appl. Soft Comput. **11**(8), 5590–5601 (2011). https://doi.org/10.1016/j.asoc.2011.04.005
13. Castillo, O., Neyoy, H., Soria, J., Melin, P., Valdez, F.: A new approach for dynamic fuzzy logic parameter tuning in ant colony optimization and its application in fuzzy control of a mobile robot. Appl. Soft Comput. **28**, 150–159 (2015). https://doi.org/10.1016/j.asoc.2014.12.002
14. Chan, K.Y., Engelke, U.: Varying spread fuzzy regression for affective quality estimation. IEEE Trans. Fuzzy Syst. **25**(3), 594–613 (2017). https://doi.org/10.1109/tfuzz.2016.2566812
15. Chan, K.Y., Lam, H.K., Dillon, T.S., Ling, S.H.: A stepwise-based fuzzy regression procedure for developing customer preference models in new product development. IEEE Trans. Fuzzy Syst. **23**(5), 1728–1745 (2015). https://doi.org/10.1109/tfuzz.2014.2375911
16. Chen, C.H., Lan, G.C., Hong, T.P., Lin, S.B.: Mining fuzzy temporal association rules by item lifespans. Appl. Soft Comput. **41**, 265–274 (2016). https://doi.org/10.1016/j.asoc.2015.01.008
17. Chou, C.C.: A generalized similarity measure for fuzzy numbers. J. Intell. Fuzzy Syst. **30**(2), 1147–1155 (2016)
18. Clough, J.R., Evans, T.S.: What is the dimension of citation space? Phys. Stat. Mech. Appl. **448**, 235–247 (2016). https://doi.org/10.1016/j.physa.2015.12.053
19. Crisan, G.C., Pintea, C.M., Palade, V.: Emergency management using geographic information systems: application to the first romanian traveling salesman problem instance. Knowl. Inf. Syst. **50**(1), 265–285 (2017). https://doi.org/10.1007/s10115-016-0938-8
20. Crucitti, P., Latora, V., Marchiori, M.: Model for cascading failures in complex networks. Phys. Rev. E **69**(4) (2004). https://doi.org/10.1103/PhysRevE.69.045104
21. Deng, X., Deng, Y.: D-AHP method with different credibility of information. Soft Comput. pp. Published online, https://doi.org/10.1007/s00,500–017–2993–9(2018)
22. Deng, X., Han, D., Dezert, J., Deng, Y., Shyr, Y.: Evidence combination from an evolutionary game theory perspective. IEEE Trans. Cybern. **46**(9), 2070–2082 (2016)
23. Deng, X., Jiang, W.: An evidential axiomatic design approach for decision making using the evaluation of belief structure satisfaction to uncertain target values. Int. J. Intell. Syst. **33**(1), 15–32 (2018). https://doi.org/10.1002/int.21929
24. Du, W.J., Zhang, J.G., An, X.L., Qin, S., Yu, J.N.: Outer synchronization between two coupled complex networks and its application in public traffic supernetwork. Discrete Dyn. Nat. Soc. p. 8 (2016). https://doi.org/10.1155/2016/8920764
25. Du, W.J., Zhang, J.G., Li, Y.Z., Qin, S.: Synchronization between different networks with time-varying delay and its application in

bilayer coupled public traffic network. Math. Probl. Eng. p. 11 (2016). https://doi.org/10.1155/2016/6498316
26. Ekong, U., Lam, H.K., Xiao, B., Ouyang, G.X., Liu, H.B., Chan, K.Y., Ling, S.H.: Classification of epilepsy seizure phase using interval type-2 fuzzy support vector machines. Neurocomputing **199**, 66–76 (2016). https://doi.org/10.1016/j.neucom.2016.03.033
27. Gallos, L.K., Fefferman, N.H.: The effect of disease-induced mortality on structural network properties. Plos One **10**(8), 17 (2015). https://doi.org/10.1371/journal.pone.0136704
28. Gallos, L.K., Fefferman, N.H.: Simple and efficient self-healing strategy for damaged complex networks. Phys. Rev. E **92**(5) (2015). https://doi.org/10.1103/PhysRevE.92.052806
29. Gallos, L.K., Makse, H.A., Sigman, M.: A small world of weak ties provides optimal global integration of self-similar modules in functional brain networks. Proc. Natl. Acad. Sci. U. S. A. **109**(8), 2825–2830 (2012). https://doi.org/10.1073/pnas.1106612109
30. Gallos, L.K., Potiguar, F.Q., Andrade, J.S., Makse, H.A.: Imdb network revisited: Unveiling fractal and modular properties from a typical small-world network. Plos One **8**(6), 8 (2013). https://doi.org/10.1371/journal.pone.0066443
31. Gao, J.X., Barzel, B., Barabasi, A.L.: Universal resilience patterns in complex networks. Nature **530**(7590), 307–312 (2016). https://doi.org/10.1038/nature16948
32. Gou, L., Wei, B., Sadiq, R., Sadiq, Y., Deng, Y.: Topological vulnerability evaluation model based on fractal dimension of complex networks. Plos One **11**(1) (2016). https://doi.org/10.1371/journal.pone.0146896
33. Hahn, K., Massopust, P.R., Prigarin, S.: A new method to measure complexity in binary or weighted networks and applications to functional connectivity in the human brain. Bmc Bioinform. **17**, 18 (2016). https://doi.org/10.1186/s12859-016-0933-9
34. Hausdorff, F.: Dimension and outer dimension. Mathematische Annalen **79**, 157–179 (1919)
35. Holme, P., Kim, B.J., Yoon, C.N., Han, S.K.: Attack vulnerability of complex networks. Phys. Rev. E **65**(5) (2002). https://doi.org/10.1103/PhysRevE.65.056109
36. Holmgren, A.J.: Using graph models to analyze the vulnerability of electric power networks. Risk Anal. **26**(4), 955–969 (2006). https://doi.org/10.1111/j.1539-6924.2006.00791.x
37. Hong, T.P., Lee, Y.C., Wu, M.T.: An effective parallel approach for genetic-fuzzy data mining. Expert Syst. Appl. **41**(2), 655–662 (2014). https://doi.org/10.1016/j.eswa.2013.07.090
38. Huang, D.W., Yu, Z.G.: Dynamic-sensitive centrality of nodes in temporal networks. Sci. Rep. **7**, 11 (2017). https://doi.org/10.1038/srep41454
39. Jiang, W., Wang, S.: An uncertainty measure for interval-valued evidences. Int. J. Comput. Commun. Control **12**(5), 631–644 (2017)
40. Jiang, W., Wei, B., Liu, X., Li, X., Zheng, H.: Intuitionistic fuzzy evidential power aggregation operator and its application in multiple criteria decision-making. Int. J. Syst. Sci. Published on line. https://doi.org/10.1002/int.21939(2018)
41. Jiang, W., Wei, B., Liu, X., Li, X., Zheng, H.: Intuitionistic fuzzy power aggregation operator based on entropy and its application in decision making. Int. J. Intell. Syst. **33**(1), 49–67 (2018). https://doi.org/10.1002/int.21939
42. Kang, B., Chhipi-Shrestha, G., Deng, Y., Hewage, K., Sadiq, R.: Stable strategies analysis based on the utility of z-number in the evolutionary games. Appl. Mathe. Comput. (2017). https://doi.org/10.1016/j.amc.2017.12.006
43. Lan, G.C., Hong, T.P., Lin, Y.H., Wang, S.L.: Fuzzy utility mining with upper-bound measure. Appl. Soft Comput. **30**, 767–777 (2015). https://doi.org/10.1016/j.asoc.2015.01.055
44. Liu, T., Deng, Y., Chan, F.: Evidential supplier selection based on DEMATEL and game theory. Int. J. Fuzzy Syst. https://doi.org/10.1007/s40815-017-0400-4(2017)
45. Melin, P., Castillo, O.: An intelligent hybrid approach for industrial quality control combining neural networks, fuzzy logic and fractal theory. Inf. Sci. **177**(7), 1543–1557 (2007). https://doi.org/10.1016/j.ins.2006.07.022
46. Mishkovski, I., Biey, M., Kocarev, L.: Vulnerability of complex networks. Commun. Nonlinear Sci. Numer. Simul. **16**(1), 341–349 (2011). https://doi.org/10.1016/j.cnsns.2010.03.018
47. Morone, F., Makse, H.A.: Influence maximization in complex networks through optimal percolation. Nature **524**(7563), 65–U122 (2015). https://doi.org/10.1038/nature14604
48. Newman, M.E.J.: The structure and function of complex networks. Siam Rev. **45**(2), 167–256 (2003). https://doi.org/10.1137/s003614450342480
49. Paun, V.A., Paun, V.P.: Fracture surface evaluation of zircaloy-4. Mater. Plast. **53**(2), 326–331 (2016)
50. Pedrycz, W.: From fuzzy data analysis and fuzzy regression to granular fuzzy data analysis. Fuzzy Sets Syst. **274**, 12–17 (2015). https://doi.org/10.1016/j.fss.2014.04.017
51. Pedrycz, W.: From fuzzy models to granular fuzzy models. Int. J. Comput. Intell. Syst. **9**, 35–42 (2016). https://doi.org/10.1080/18756891.2016.1180818
52. Pedrycz, W., Bargiela, A.: Fuzzy fractal dimensions and fuzzy modeling. Inf. Sci. **153**, 199–216 (2003). https://doi.org/10.1016/s0020-0255(03)00075-6
53. Pedrycz, W., Jastrzebska, A., Homenda, W.: Design of fuzzy cognitive maps for modeling time series. IEEE Trans. Fuzzy Syst. **24**(1), 120–130 (2016). https://doi.org/10.1109/tfuzz.2015.2428717
54. Schich, M., Song, C.M., Ahn, Y.Y., Mirsky, A., Martino, M., Barabasi, A.L., Helbing, D.: A network framework of cultural history. Science **345**(6196), 558–562 (2014). https://doi.org/10.1126/science.1240064
55. Shanker, O.: Defining dimension of a complex network. Mod. Phys. Lett. B **21**(6), 321–326 (2007). https://doi.org/10.1142/s0217984907012773
56. Song, C.M., Gallos, L.K., Havlin, S., Makse, H.A.: How to calculate the fractal dimension of a complex network: the box covering algorithm. J. Stat. Mech-Theory Exp. p. 16 (2007). https://doi.org/10.1088/1742-5468/2007/03/p03006
57. Song, C.M., Havlin, S., Makse, H.A.: Origins of fractality in the growth of complex networks. Nat. Phys. **2**(4), 275–281 (2006). https://doi.org/10.1038/nphys266
58. Uslan, V., Seker, H.: Quantitative prediction of peptide binding affinity by using hybrid fuzzy support vector regression. Appl. Comput. **43**, 210–221 (2016). https://doi.org/10.1016/j.asoc.2016.01.024
59. Wang, J.: Robustness of complex networks with the local protection strategy against cascading failures. Saf. Sci. **53**, 219–225 (2013). https://doi.org/10.1016/j.ssci.2012.09.011
60. Wang, J.W., Rong, L.L.: Cascade-based attack vulnerability on the us power grid. Saf. Sci. **47**(10), 1332–1336 (2009). https://doi.org/10.1016/j.ssci.2009.02.002
61. Wang, Z., Xia, C.Y., Meloni, S., Zhou, C.S., Moreno, Y.: Impact of social punishment on cooperative behavior in complex networks. Sci. Rep. **3**, 7 (2013). https://doi.org/10.1038/srep03055
62. Xu, H., Deng, Y.: Dependent evidence combination based on shearman coefficient and pearson coefficient. IEEE Access https://doi.org/10.1109/ACCESS.2017.2783320 (2018)
63. Xu, S., Jiang, W., Deng, X., Shou, Y.: A modified physarum-inspired model for the user equilibrium traffic assignment problem. Appl. Math. Model. **55**, 340–353 (2018). https://doi.org/10.1016/j.apm.2017.07.032
64. Yin, L., Deng, Y.: Measuring transferring similarity via local information. Phys. A: Stat. Mech. Appl. (2018). https://doi.org/10.1016/j.physa.2017.12.144

65. Zadeh, L.: Fuzzy sets. Inf. Control evaluation Method Based **8**(3), 338–353 (1965). https://doi.org/10.1016/S0019-9958(65)90241-X
66. Zhang, R., Ashuri, B., Deng, Y.: A novel method for forecasting time series based on fuzzy logic and visibility graph. Adv. Data Anal. Classif. **11**(4), 759–783 (2018). https://doi.org/10.1007/s11634-017-0300-3
67. Zhang, X., Feng, L., Berman, Y., Hu, N., Stanley, H.E.: Exacerbated vulnerability of coupled socio-economic risk in complex networks. Epl **116**(1), 6 (2016). https://doi.org/10.1209/0295-5075/116/18001
68. Zhao, Z.Q., Yu, Z.G., Anh, V., Wu, J.Y., Han, G.S.: Protein folding kinetic order prediction from amino acid sequence based on horizontal visibility network. Curr. Bioinf. **11**(2), 173–185 (2016). https://doi.org/10.2174/1574893611666160125221326
69. Zheng, H., Deng, Y.: Evaluation method based on fuzzy relations between Dempster-Shafer belief structure. Int. J. Intell. Syst. (2017). https://doi.org/10.1002/int.21956
70. Zheng, X., Deng, Y.: Dependence assessment in human reliability analysis based on evidence credibility decay model and iowa operator. Ann. Nucl. Energy **112**, 673–684 (2018)

Tao Wen was born in Shaanxi, P. R. China, in 1998. He is currently an undergraduate student in School of Electronics and Information, Northwestern Polytechnical University. His research interests are in the areas of complex network and vital node identifying.

Moxian Song was born in Jiangsu, P. R. China, in 1997. He is currently an undergraduate student in School of Electronics and Information, Northwestern Polytechnical University. His research interests are in the areas of information fusion, fault diagnosis and multiple attribute decision-making.

Wen Jiang was born in Hunan, P. R. China. She received the Bachelor degree in signal and system from Information Engineering University, Zhengzhou, China, in 1994, the Master degree in Image processing from Information Engineering University, Zhengzhou, China, in 1997, the Ph. D. degree in systems engineering from Northwestern Polytechnical University, Xi'an, China, in 2009. She is currently a professor in school of electronics and information, Northwestern Polytechnical University. Her research interests are in the areas of information fusion and Intelligent Information Processing.chool of Electronics and Information, Northwestern Polytechnical University. His research interests are in the areas of complex network and vital node identifying.