RESEARCH ARTICLE

Topological Vulnerability Evaluation Model Based on Fractal Dimension of Complex Networks

Li Gou[1,2], Bo Wei[1], Rehan Sadiq[3], Yong Sadiq[3], Yong Deng[1,4]*

1 School of Computer and Information Science, Southwest University, Chongqing 400715, China,
2 Department of Computer Science, Michigan Technological University, Houghton, MI 49931, United States of America, **3** School of Engineering, University of British Columbia Okanagan, 3333 University Way, Kelowna, BC, Canada V1V 1V7, **4** School of Engineering, Vanderbilt University, Nashville, TN 37235, United States of America

* ydeng@swu.edu.cn; prof.deng@hotmail.com

OPEN ACCESS

Citation: Gou L, Wei B, Sadiq R, Sadiq Y, Deng Y (2016) Topological Vulnerability Evaluation Model Based on Fractal Dimension of Complex Networks. PLoS ONE 11(1): e0146896. doi:10.1371/journal.pone.0146896

Editor: Zhen Wang, Kyushu University, JAPAN

Received: December 6, 2014

Accepted: December 24, 2015

Published: January 11, 2016

Data Availability Statement: All airline network datas are available from the RITA database through website http://www.transtats.bts.gov/dl_selectfields.asp?table_id=292.

Funding: The work is partially supported by National High Technology Research and Development Program of China (863 Program) (grant no. 2013AA013801), National Natural Science Foundation of China (grant nos. 61174022, 61573290, 61503237), China State Key Laboratory of Virtual Reality Technology and Systems, Beihang University (grant no.BUAA-VR-14KF-02). The funders had no role in study design, data collection

Abstract

With an increasing emphasis on network security, much more attentions have been attracted to the vulnerability of complex networks. In this paper, the fractal dimension, which can reflect space-filling capacity of networks, is redefined as the origin moment of the edge betweenness to obtain a more reasonable evaluation of vulnerability. The proposed model combining multiple evaluation indexes not only overcomes the shortage of average edge betweenness's failing to evaluate vulnerability of some special networks, but also characterizes the topological structure and highlights the space-filling capacity of networks. The applications to six US airline networks illustrate the practicality and effectiveness of our proposed method, and the comparisons with three other commonly used methods further validate the superiority of our proposed method.

1 Introduction

Complex network is widely used to model the structure of many complex systems in nature and society [1, 2]. Some network models are used to solve natural problems, such as climate issues [3]. While some are used to analyze social and practical problems, such as supply chain management [4], transportation networks [5], power grid networks [6–9], water distribution networks [10], network optimization [11–13], as well as game theory in operation research [14, 15] and etc. An open issue is how to assess the vulnerability of complex networks [16–18], whose main objective is to understand, predict, and even control the behavior of a networked system under vicious attacks or any types of dysfunctions [19].

Different approaches to characterize network vulnerability and robustness have recently been proposed, which can be grouped into two types broadly [9, 20, 21]. The first type of the

and analysis, decision to publish, or preparation of the manuscript.

Competing Interests: The authors have declared that no competing interests exist.

approaches is structural robustness—topological properties of networks [22, 23]. Such as, the average edge betweenness [19], the network connectivity level, the size of largest component [16] and the average geodesic length [6] and etc., are directly used to define network vulnerability. The second one concerns dynamical robustness [24–26]. The dysfunctions of a node or link will cause the redistribution on the the load of other nodes or links, with the risk that some other nodes or links may be overloaded, which will further cause a sequence of failures and even threaten the global stability [6, 20, 27]. Such behavior is called cascading failures [28–30]. In addition, the evaluation of network vulnerability is of uncertainty, and many methods have promising aspect to address such problem. For example, fuzzy set theory is efficient to model linguistic information [31] wihle Dempster-Shafer evidence theory can combine different information in an efficient manner [32–34]. The vulnerability analysis of complex systems, such as physic protect systems, is modelled by these mathematical tools [35].

One of the mostly used methods is proposed by Boccaletti *et.al* [19]. They construct a multi-scale evaluation model of vulnerability, which makes use of the average edge betweenness and introduces a key coefficient p. Due to its effectiveness, this method has been heavily studied [20]. One limitation of the original average edge betweenness model is that it cannot differentiate two different networks in some situations. To solve this problem, a key coefficient p is introduced to improve the original model in their work. However, a straight problem is how to determine the coefficient p. The way used in Boccaletti *et.al*'s work is lack of physical significance.

The main motivation of our work is that we believe this coefficient p should be determined by the network itself but not just geometrically. To address this issue, we take the fractal dimension of complex network into consideration.

Dimension is one of the fundamental properties of complex networks characterizing not only its topological properties but also dynamic characteristics [36–38], which are two key aspects to determine network vulnerability. Analyses of a variety of real complex networks show that self-similar characteristic exists on all length scales, that is, many complex networks exhibit fractal properties [23, 39, 40]. Then researchers found that this self-similar characteristic can used to characterize dimension, i.e., fractal dimension, which gives a good definition to dimension of many geometric images and the network with fractal properties, such as Koch curve, Sierpinski triangle, the Coast of Britain, social networks, power grid networks, airline networks and so on [41–43]. In addition, fractal dimension has also been confirmed to be able to measure the space-filling capacity of a pattern reflecting the complexity of network directly [44], which has relationships with network vulnerability. Based on this idea, we propose that fractal dimension is a promising alternative to be the key coefficient in determining network vulnerability in this paper.

This paper is organized as follows. Section 2 introduces the preliminaries. Section 3 presents details of the proposed method and the steps about its application. Section 4 compares the proposed method with the existing methods listed in other papers by calculating the vulnerability of them. Finally, we summarize our results in Section 5.

2 Preliminaries

In this section, we introduce Boccaletti *et.al*'s vulnerability model[19] and three other commonly used methods of vulnerability evaluation [6, 16, 20]. In general, the complex networks can be represented by an undirected and unweighted graph $G = (V, E)$, where V is the set of nodes and E is the set of edges. Each edge connects exactly one pair of nodes, and a vertex-pair can be connected by maximally one edge, i.e. loop is not allowed.

2.1 Multi-scale Evaluation of Vulnerability

In Boccaletti *et.al*'s work [19], the original method to evaluate the vulnerability is represented by the average edge betweenness, which is defined as:

$$b_1(G) = \frac{1}{|E|}\sum_{l\in E} b_l, \tag{1}$$

Where $|E|$ is the number of the edges, and b_l is the edge betweenness of the edge l, define as:

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

Where n_{jk} is the total number of geodesics (shortest path) from node j to k, and $n_{jk}(l)$ is the number of geodesics from j to k that contain the link l.

However, this evaluation method of $b_1(G)$ gives no relevant new information about the vulnerability of some special networks. For example, two networks referred in [19] shown in Fig 1 can't be distinguished using this method. By evaluating the vulnerability according to Eq 1, one gets $b_1(G) = b_1(G') = 43/13$. It's absolute that the "bat" graph G is more vulnerable than the "umbrella" graph G', but Eq 1 gives the same evaluation results about them.

In order to overcome the original method's limitation of failing to distinguish some networks, a key coefficient p was introduced by Boccaletti *et.al* in the improved model, which is called multi-scale evaluation of vulnerability [19] and shown as below:

$$b_p(G) = \left(\frac{1}{|E|}\sum_{l\in E} b_l^p\right)^{\frac{1}{|p|}} \qquad (p > 0). \tag{3}$$

If we want to compare two networks G and G', first computes b_1. If $b_1(G) < b_1(G')$, then G is more robust than G'. On the other hand, if $b_1(G) = b_1(G')$ then one takes $p > 1$ and computes b_p until $b_p(G) \neq b_p(G')$.

To get the coefficient p, Boccaletti *et.al* define a relative function of p like:

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

The coefficient p is obtained when the function has a maximal value. For more detailed information to determine the coefficient p, refer [19]. It's clear that, the definition of coefficient p is based on geometrical definition and lack of physical significance. In our opinion, the coefficient p should be defined by the complex network itself, we take the fractal dimension as consideration.

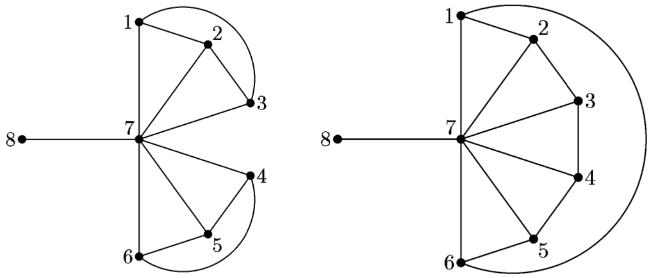

Fig 1. The "bat" graph *G* and the "umbrella" graph *G'* [19].

doi:10.1371/journal.pone.0146896.g001

2.2 Fractal Dimension

One of the most typical ways to calculate the fractal dimension is Box covering algorithm, a power-law relation between the number of boxes needed to cover the network and the size of the box [45–47]. For a given network G and box size l_B, a box is a set of nodes where all distances l_{ij} between any two nodes i and j in the box are smaller than l_B. The minimum number of boxes required to cover the entire network is denoted by N_B. The detailed illustration of the calculation of the fractal dimension referred in [46] is given in Fig 2. The fractal dimension or box dimension d_B calculated with the box covering algorithm is given as follows [40, 46]:

$$N_B \approx l_B^{-d_B}. \tag{5}$$

2.3 Comparison Preparation

For the sake of comparison, three other commonly used methods to calculate vulnerability are described as follows. The first method is the average inverse geodesic length l^{-1} [6]:

$$l^{-1} = \langle \frac{1}{d(v,w)} \rangle \equiv \frac{1}{N(N-1)} \sum \sum \frac{1}{d(v,w)}. \tag{6}$$

Where $d(v, w)$ is the length of the geodesic between v and w ($v, w \in V$), and the factor $N(N-1)$ is the number of pairs of nodes. The larger l^{-1} is, the better the network functions.

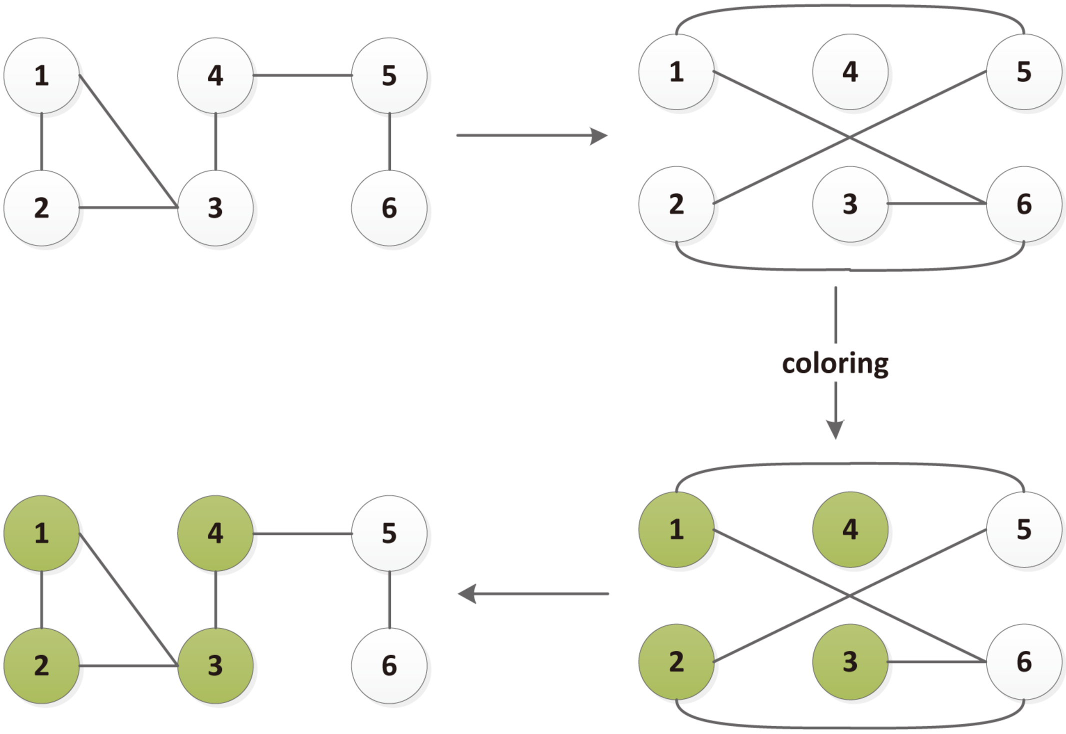

Fig 2. Illustration of the box-covering algorithms. Starting from G (upper left panel), a dual network G' (upper right panel) was constructed for a given box size (here $l_B = 3$), where two nodes are connected if they are at a distance of $l \geq l_B$. A greedy algorithm was used for node colouring in G', which is then used to determine the box covering in G, as shown in the plot [46].

doi:10.1371/journal.pone.0146896.g002

The second method is the size of largest component LCS $(0 < LCS < 1)$ [16], which quantifies the number of nodes in the largest connected subgraph and is defined as follows:

$$LCS = \frac{N_s}{N}. \tag{7}$$

Where N_s is the size of the largest connected subgraph. The larger LCS is, the more robust the network is.

And the third method is the normalized average edge betweenness $b_{nor}(G)$ [20], which is on the base of the Eq 3 while $p = 1$ and is defined as:

$$b_{nor}(G) = \frac{b_1(G) - b_1(G_{complete})}{b_1(G_{path}) - b_1(G_{complete})} = \frac{b_1(G) - 1}{\frac{N(N+1)}{6} - 1}. \tag{8}$$

Where $G_{complete}$ is a complete graph and G_{path} is a path graph. The larger LCS is, the more vulnerable the network is.

3 Methods

In this section, the proposed method is detailed. As mentioned in introduction section, average edge betweenness can't highlight difference between some special networks, which is caused by the average process. Because for a network whose geodesic distribution concentrates strongly around a single link or node, the potential risk of the failure in this critical link/node will be hidden by the average process with the rest of minor links. For example, edge betweenness of some edges in "bat" graph are much higher than "umbrella" graph, which represents the "bat" graph is more vulnerable than "umbrella" graph, but the average process hides their differences and gives the same vulnerability of them. The improved multi-scale evaluation model is equivalent to the p origin moment of edge betweenness. Since p origin moment can highlight the difference between data to eliminate the effect of average process. But the problem is how to determine the key coefficient p to make effective and reasonable evaluation, which is the motivation of our work.

In our opinion, the fractal dimension of the complex network is a promising alternative to redefine the coefficient p. It is well-known that the fractal dimension can characterize the network structure and basic physical properties including space-filling capacity. For a given network with fixed number of nodes, the higher the space-filling capacity is, the more edges connecting the nodes in this network, and then the smaller of the diameter of the network, thus the less boxes will be required to cover the whole network, i.e., the smaller the fractal dimension is. So the fractal dimension decreases with the space-filling capacity of network. We also know that given fixed number of nodes of a network, the more edges, the more connected and robust of this network. That is, the fractal dimension has direct relationships with network vulnerability. So using the fractal dimension to redefine p can not only highlight difference between networks properly, but also ensure practical significance of p, which is more reasonable than geometric coefficient p in multi-scale model. Therefore, we use the fractal dimension to redefine p.

Definition. Given a set of edge betweenness $B = \{b_{l_1}, b_{l_2}, \ldots, b_{l_n}\}$ and fractal dimension d_B of network G, the proposed network vulnerability model is defined as:

$$V_{d_B}(G) = \left(\frac{1}{|E|}\sum_{l \in E} b_l^{d_B}\right)^{\frac{1}{|d_B|}}. \tag{9}$$

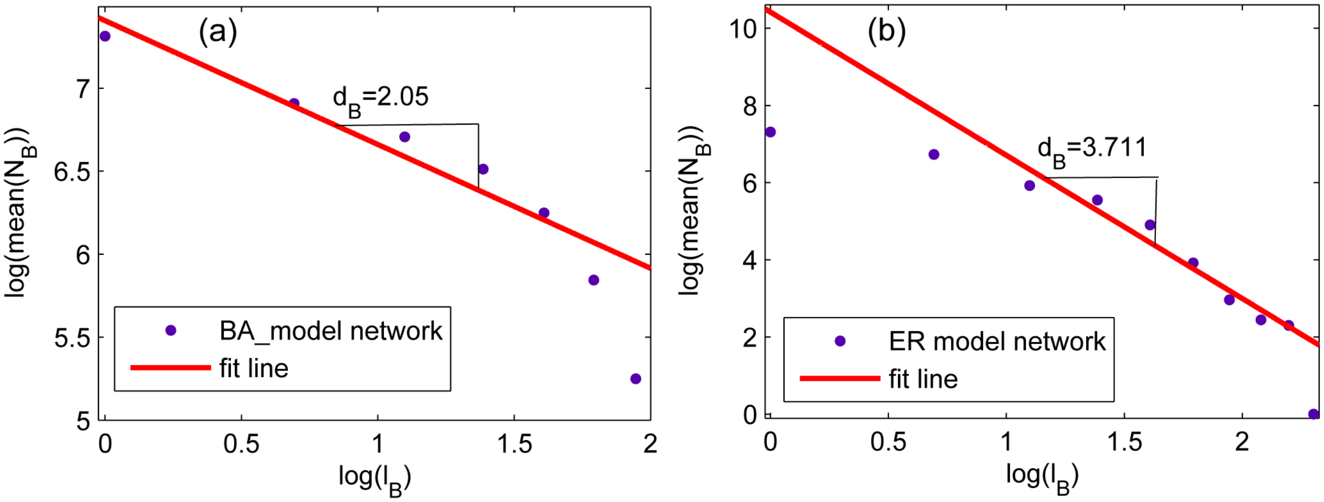

Fig 3. The N_B versus l_B of complex networks obtained in a log-log scale. (a) the ER network with the size N = 1500 and the average degree <k> = 6. (b) the BA network with N = 1500 and the average degree <k > = 4.8. The vertical ordinate of every subplot is the mean value of N_B for 100 times, and the horizonal ordinate represents the box size l_B. The absolute value of the slope is the fractal dimension.

doi:10.1371/journal.pone.0146896.g003

The larger the V_{d_B}, the more vulnerable the network. Any network that exhibits fractal properties can be applied to this proposed method to evaluate its vulnerability.

To demonstrate the usage of the proposed method, we apply it to two synthetic networks: Erdős-Rényi(ER) random networks [48] and Barabási-Albert(BA) model of scale-free networks [49]. The vulnerability of a network should be calculated as follow steps:

Step 1 calculate the fractal dimension d_B of the network using box-covering algorithm [40, 46], i.e. Eq 5. The results of the two networks are illustrated in Fig 3.

Step 2 Calculate the average edge betweenness according to Eq 2, and normalized by $\frac{N(N-1)}{2}$.

Step 3 Calculate the vulnerability V_{d_B} in accordance with Eq 9.

Table 1 shows the results: $V_{d_B}(BA) > V_{d_B}(ER)$, which mean that the ER network is more robust than the BA network. One point should be noted is that, the two networks are synthesized randomly, the results will vary with different network structure.

4 Comparison and Discussion

In this section, to testify the correctness and effectiveness of the proposed method, three commonly used methods presented in section 2, that is, the average inverse geodesic length l^{-1}, the largest component size LCS and the normalized average edge betweenness $b_{nor}(G)$, are applied to some real situations to compare with the proposed method. In order to get vulnerability embodying dynamic characteristics of networks to make a more reasonable comparison, we apply the RB attack strategy [6] to networks when using the three methods reflecting just static

Table 1. General characteristics of the two networks: the number of nodes N, the average degree <k>, the fractal dimension d_B, and the vulnerability V_{d_B} obtained by the proposed method.

network	N	<k>	d_B	V_{d_B}
ER	1500	6	3.711	0.0011
BA	1500	4.8	2.05	0.0014

doi:10.1371/journal.pone.0146896.t001

topological properties. RB attack strategy means that one should remove the node with highest betweenness value and recalculate the betweenness of the network. Similarly, removing other nodes until all required number of nodes have been removed. Finally, we can get the vulnerability of the network based on the remaining network. In this paper, l^{-1}, LCS and $b_{nor}(G)$ are computed on attack strategy of removing 1% nodes from the original networks.

In this paper, six unweighed US airline networks, categorized by year, are used to do analysis. That is, US airline network in 2005, 2007, 2009, 2010, 2011, 2013 (UAN2005, UAN2007 and etc.). These data are downloaded from the Bureau of Transportation Statistics (BTS) Transtats site with the following filters [50]: Geography = all; Year = 2011; Months = all; and columns: Passengers, Origin, Dest. Based on this table, the airport codes are converted into id numbers; if there are flights between two airports, an edge between two nodes will be connected correspondingly. Also ties with a weight of 0 are removed (only cargo), self-loops and small subgraph are removed, constructing connected and unweighed networks.

Firstly, l^{-1}, LCS and $b_{nor}(G)$ are applied to these six airline network to calculate vulnerability, and the results are illustrated in Table 2. Then the fractal dimension of these networks are calculated and illustrated in Fig 4. It's absolute that all these networks exhibit fractal properties, which reaches the prerequisite of the proposed method to use fractal dimension to characterize network vulnerability. Table 2 and Table 3 show the evaluation results of all these method, which are concluded as follows:

1. The average edge betweenness of these networks are very small, while the evaluation results of our method is larger than b_1 at magnitude level, which indicates that the fractal dimension is appropriate to be the p origin moment of edge betweenness to highlight the difference between networks effectively.
2. The vulnerability order given by other three commonly used methods are unreasonable to some extent. l^{-1} and LCS show that UAN2013 is the most vulnerable network and $b_{nor}(G)$ illustrates a high robustness of UAN2003 and UAN2005.
3. Our method give the most reasonable results among these methods, and the vulnerability order obtained by it is: $UAN2003 > UAN2005 > UAN2007 > UAN2009 > UAN2011 > UAN2013$. The robustness of these airline networks increases over years, which is consistent with the real situations in the country.

The obvious advantage of the proposed method is due to its multiple evaluation index, that is, edge betweenness, p origin moment and fractal dimension, which are all crucial to the vulnerability evaluation as described in section 3. While the evaluation index of other three methods is obvious inferior to ours, in detail, $\widetilde{l^{-1}}$ just utilizes the geodesic length of network, $\widetilde{LCS}$

Table 2. General characteristics of these networks and results illustrations. The proposed vulnerability evaluation method V_{d_B} is calculated based on fractal dimension d_B. The normalized average inverse geodesic length $\widetilde{l^{-1}}$, normalized largest component size $\widetilde{LCS}$ and the normalized average edge betweenness $b_{nor}(G)$ are computed after 1% of vertices are removed and are normalized by the corresponding values of the initial networks.

network	N	E	d_B	V_{d_B}	b_1	$\widetilde{l^{-1}}$	$\widetilde{LCS}$	$b_{nor}(G)$
UAN2003	1387	15618	3.742	**0.0023**	0.00017	0.1221	0.3223	0.0096
UAN2005	1447	17453	3.783	**0.0021**	0.00018	0.1312	0.3034	-0.0984
UAN2007	1605	19166	3.784	**0.002**	0.00018	0.1389	0.3352	0.1051
UAN2009	1548	17415	3.715	**0.0019**	0.00020	0.1211	0.3204	0.0487
UAN2011	1587	17969	3.103	**0.0014**	0.00019	0.0916	0.2823	0.0961
UAN2013	1635	16215	3.134	**0.0013**	0.00021	0.0899	0.2557	0.042

doi:10.1371/journal.pone.0146896.t002

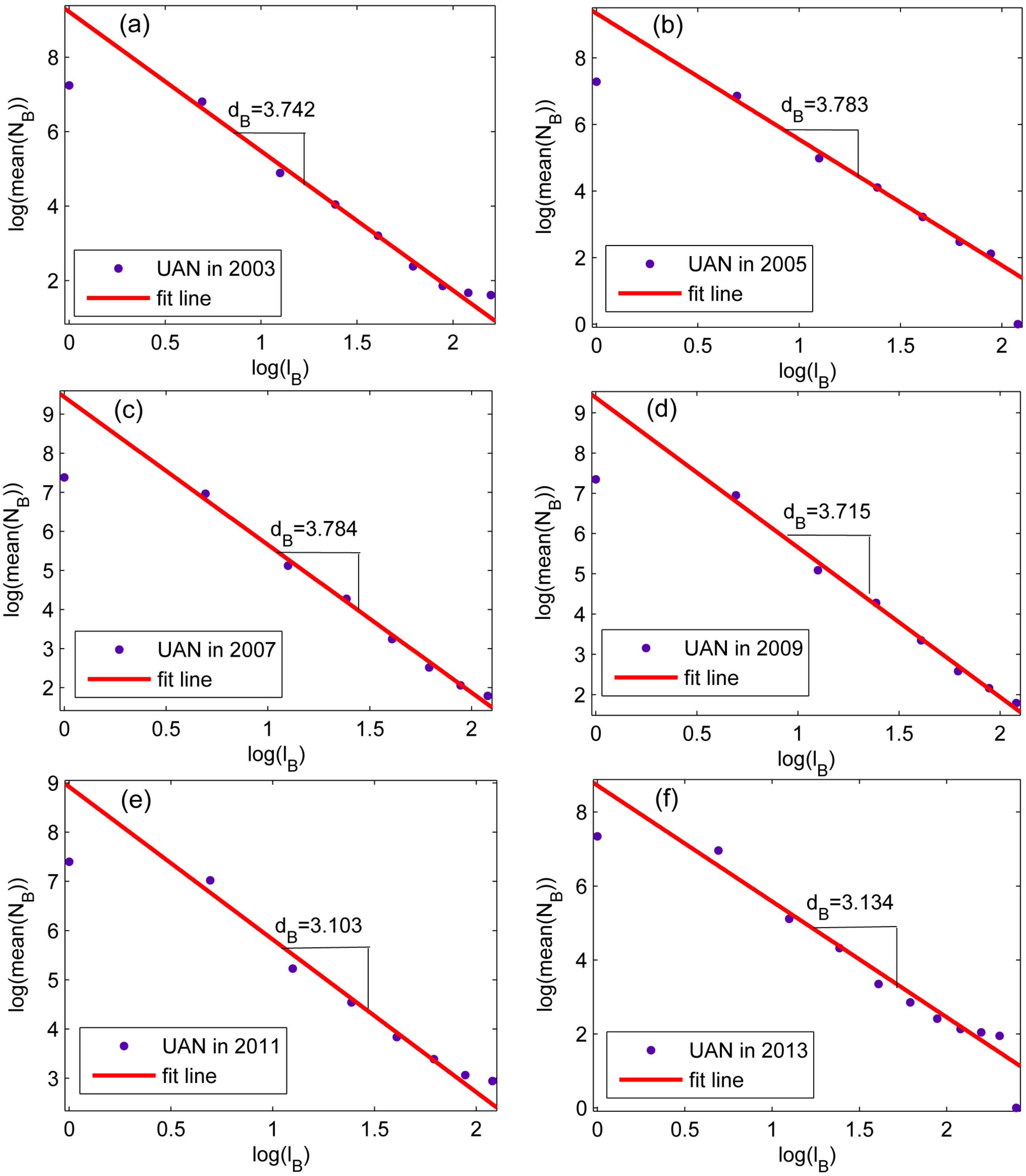

Fig 4. The N_B versus l_B of six real complex networks obtained in a log-log scale. the US airline network in 2003, 2005, 2007, 2009, 2011, 2013. The vertical ordinate of every subplot is the mean value of N_B (number of box required) for 100 times, and the horizonal ordinate represents the box size l_B. The absolute value of the slope is the fractal dimension.

doi:10.1371/journal.pone.0146896.g004

Table 3. The vulnerability evaluation rank of all these methods.

Methods	vulnerability order
V_{d_B}	*UAN*2003 > *UAN*2005 > *UAN*2007 > *UAN*2009 > *UAN*2011 > *UAN*2013
$\widetilde{I^{-1}}$	*UAN*2013 > *UAN*2011 > *UAN*2009 > *UAN*2003 > *UAN*2005 > *UAN*2007
$\widetilde{LCS}$	*UAN*2013 > *UAN*2011 > *UAN*2005 > *UAN*2009 > *UAN*2003 > *UAN*2007
$b_{nor}(G)$	*UAN*2007 > *UAN*2011 > *UAN*2009 > *UAN*2013 > *UAN*2003 > *UAN*2005

doi:10.1371/journal.pone.0146896.t003

just considers the simple structure properties–connectivity, and $b_{nor}(G)$ only involves the average betweeness.

In conclusion, p origin moment is an effective approach to improve the average process of edge betweenness and the application of fractal dimension can highlight the difference between networks efficiently. So the proposed method has its geometrical and physical significance, and the reasonable application results also illustrate its effectiveness and practicality.

5 Conclusions

In this paper, the fractal dimension is redefined as p origin moment of edge betweenness to improve the vulnerability evaluation of multi-scale model. The experiments indicate that the fractal dimension indeed has relationships with network vulnerability, because a higher space-filling capacity means that less boxes will be required to cover the whole network, thus with smaller fractal dimension; while a network with higher space-filling capacity will contribute to more connected and robust structure. The applications to several real airline networks and comparison with other commonly used methods also illustrate the effectiveness and practicability of using the fractal dimension to evaluate network vulnerability. One of our ongoing works is to explore the specific relationship between vulnerability and topological properties, such as connectivity, cluster degrees and so on.

Acknowledgments

The authors greatly appreciate the reviews' suggestions and the editor's encouragement. The work is partially supported by National High Technology Research and Development Program of China (863 Program) (Grant No. 2013AA013801), National Natural Science Foundation of China (Grant Nos. 61174022,61573290,61503237), China State Key Laboratory of Virtual Reality Technology and Systems, Beihang University (Grant No.BUAA-VR-14KF-02).

Author Contributions

Conceived and designed the experiments: LG BW RS YD. Performed the experiments: LG BW YD. Analyzed the data: LG BW RS YD. Contributed reagents/materials/analysis tools: LG BW RS YD. Wrote the paper: LG YD.

References

1. Tang Q, Zhao J, Hu T. Detecting Chaos Time Series via Complex Network Feature. Modern Physics Letters B. 2011; 25(23):1889–1896. doi: 10.1142/S0217984911027133
2. Boccaletti S, Bianconi G, Criado R, del Genio CI, Gómez-Gardeñes J, Romance M, et al. The structure and dynamics of multilayer networks. Physics Reports. 2014; 544(1):1–122. doi: 10.1016/j.physrep.2014.07.001
3. Wang J, Yang H. Complex network-based analysis of air temperature data in China. Modern Physics Letters B. 2009; 23(14):1781–1789. doi: 10.1142/S0217984909019946

4. Deng X, Hu Y, Deng Y, Mahadevan S. Supplier selection using AHP methodology extended by D numbers. Expert Systems with Applications. 2014; 41(1):156–167. doi: 10.1016/j.eswa.2013.07.018

5. Du WB, Wu ZX, Cai KQ. Effective usage of shortest paths promotes transportation efficiency on scale-free networks. Physica A Statistical Mechanics & Its Applications. 2013; 392(17):3505–3512.

6. Holme P, Kim BJ, Yoon CN, Han SK. Attack vulnerability of complex networks. Physical Review E. 2002; 65(5):056109. doi: 10.1103/PhysRevE.65.056109

7. Qi X, Shao ZG, Qi J, Yang L. Efficiency Dynamics on Scale-Free Networks with Communities. Modern Physics Letters B. 2010; 24(14):1549–1557. doi: 10.1142/S0217984910023347

8. Saniee Monfared MA, Jalili M, Alipour Z. Topology and vulnerability of the Iranian power grid. Physica A: Statistical Mechanics and its Applications. 2014; 406:24–33. doi: 10.1016/j.physa.2014.03.031

9. Deng Y. A Threat Assessment Model under Uncertain Environment. Mathematical Problems in Engineering. 2015; 2015:878024,http://dx.doi.org/10.1155/2015/878024. doi: 10.1155/2015/878024

10. Deng Y, Jiang W, Sadiq R. Modeling contaminant intrusion in water distribution networks: A new similarity-based DST method. Expert Systems with Applications. 2011; 38(1):571–578. doi: 10.1016/j.eswa.2010.07.004

11. Liu C, Du WB, Wang WX. Particle Swarm Optimization with Scale-Free Interactions. Plos One. 2014; 9 (5):57–57.

12. Gao Y, Du W, Yan G. Selectively-informed particle swarm optimization. Scientific Reports. 2015; 5.

13. Deng Y, Liu Y, Zhou D. An Improved Genetic Algorithm with Initial Population Strategy for Symmetric TSP. Mathematical Problems in Engineering. 2015; 2015:212794. doi: 10.1155/2015/212794

14. Wang Z, Wang L, Perc M. Degree mixing in multilayer networks impedes the evolution of cooperation. Physical Review E. 2014; 89(5):052813. doi: 10.1103/PhysRevE.89.052813

15. Wang Z, Zhu X, Arenzon JJ. Cooperation and age structure in spatial games. Physical Review E. 2012; 85(1):011149. doi: 10.1103/PhysRevE.85.011149

16. Holmgren ÅJ. Using graph models to analyze the vulnerability of electric power networks. Risk analysis. 2006; 26(4):955–969. doi: 10.1111/j.1539-6924.2006.00791.x PMID: 16948688

17. Zhang J, Xu X, Hong L, Wang S, Fei Q. Attack vulnerability of self-organizing networks. Safety science. 2012; 50(3):443–447. doi: 10.1016/j.ssci.2011.10.005

18. Wang S, Hong L, Ouyang M, Zhang J, Chen X. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. Safety science. 2013; 51(1):328–337. doi: 10.1016/j.ssci.2012.07.003

19. Boccaletti S, Buldú J, Criado R, Flores J, Latora V, Pello J, et al. Multiscale vulnerability of complex networks. Chaos: An Interdisciplinary Journal of Nonlinear Science. 2007; 17(4):043110–043110. doi: 10.1063/1.2801687

20. Mishkovski I, Biey M, Kocarev L. Vulnerability of complex networks. Communications in Nonlinear Science and Numerical Simulation. 2011; 16(1):341–349. doi: 10.1016/j.cnsns.2010.03.018

21. Ouyang M, Pan Z, Hong L, Zhao L. Correlation analysis of different vulnerability metrics on power grids. Physica A: Statistical Mechanics and its Applications. 2014; 396:204–211. doi: 10.1016/j.physa.2013.10.041

22. Albert R, Albert I, Nakarado GL. Structural vulnerability of the North American power grid. Physical review E. 2004; 69(2):025103. doi: 10.1103/PhysRevE.69.025103

23. Albert R, Barabási AL. Statistical mechanics of complex networks. Reviews of modern physics. 2002; 74(1):47. doi: 10.1103/RevModPhys.74.47

24. Crucitti P, Latora V, Marchiori M. Model for cascading failures in complex networks. Physical Review E. 2004; 69(4):045104. doi: 10.1103/PhysRevE.69.045104

25. Wang JW, Rong LL. Cascade-based attack vulnerability on the US power grid. Safety Science. 2009; 47(10):1332–1336. doi: 10.1016/j.ssci.2009.02.002

26. Wang J. Robustness of complex networks with the local protection strategy against cascading failures. Safety Science. 2013; 53:219–225. doi: 10.1016/j.ssci.2012.09.011

27. Motter AE, Lai YC. Cascade-based attacks on complex networks. Physical Review E. 2002; 66 (6):065102.

28. Wang JW, Rong LL. Vulnerability of effective attack on edges in scale-free networks due to cascading failures. International Journal of Modern Physics C. 2009; 20(08):1291–1298. doi: 10.1142/S0129183109014357

29. Wang J, Jiang C, Qian J. Improving robustness of coupled networks against cascading failures. International Journal of Modern Physics C. 2013; 24(11):1350076. doi: 10.1142/S0129183113500769

30. Wang JW, Rong LL. Robustness of the western United States power grid under edge attack strategies due to cascading failures. Safety science. 2011; 49(6):807–812. doi: 10.1016/j.ssci.2010.10.003

31. Jiang W, Luo Y, Qin X, Zhan J. An improved method to rank generalized fuzzy numbers with different left heights and right heights. Journal of Intelligent & Fuzzy Systems. 2015; 28:2343–2355. doi: 10.3233/IFS-151639

32. Deng Y. Generalized evidence theory. Applied Intelligence. 2015; 43(3):530–543. doi: 10.1007/s10489-015-0661-2

33. Jiang W, Yang Y, Luo Y, Qin X. Determining Basic Probability Assignment Based on the Improved Similarity Measures of Generalized Fuzzy Numbers. International Journal of Computers Communications & Control. 2015; 10(3):333–347. doi: 10.15837/ijccc.2015.3.1656

34. Su X, Mahadevan S, Xu P, Deng Y. Dependence assessment in Human Reliability Analysis using evidence theory and AHP. Risk Analysis. 2015; 35:1296–1316. doi: 10.1111/risa.12347 PMID: 25847228

35. Deng Y, Mahadevan S, Zhou D. Vulnerability assessment of physical protection systems: a bio-inspired approach. International Journal of Unconventional Computing. 2015; 11:accepted.

36. Daqing L, Kosmidis K, Bunde A, Havlin S. Dimension of spatially embedded networks. Nature Physics. 2011; 7(6):481–484. doi: 10.1038/nphys1932

37. Shanker O. Graph zeta function and dimension of complex network. Modern Physics Letters B. 2007; 21(11):639–644. doi: 10.1142/S0217984907013146

38. Wei D, Wei B, Hu Y, Zhang H, Deng Y. A new information dimension of complex networks. Physics Letters A. 2014; 378(16):1091–1094. doi: 10.1016/j.physleta.2014.02.010

39. Newman M. The Structure and Function of Complex Networks. SIAM Review. 2003; 45(2):167–256. doi: 10.1137/S003614450342480

40. Song C, Havlin S, Makse HA. Self-similarity of complex networks. Nature. 2005; 433(7024):392–395. doi: 10.1038/nature03248 PMID: 15674285

41. Mandelbrot B. The fractal geometry of nature. vol. 173. Macmillan; 1983.

42. Mandelbrot B. How Long Is the Coast of Britain? Statistical Self-Similarity and Fractional Dimension. Science. 1967; 156(3775):636–638. doi: 10.1126/science.156.3775.636 PMID: 17837158

43. Goh KI, Salvi G, Kahng B, Kim D. Skeleton and Fractal Scaling in Complex Networks. Phys Rev Lett. 2006; 96:018701. doi: 10.1103/PhysRevLett.96.018701 PMID: 16486532

44. Mokbel MF, Aref WG. Space-Filling Curves. In: Encyclopedia of GIS. Springer US; 2008. p.1068–1072.

45. Shanker O. Algorithms for fractal dimension calculation. Modern Physics Letters B. 2008; 22(07):459–466. doi: 10.1142/S0217984908015048

46. Song C, Gallos LK, Havlin S, Makse HA. How to calculate the fractal dimension of a complex network: the box covering algorithm. Journal of Statistical Mechanics: Theory and Experiment. 2007; 2007(03): P03006. doi: 10.1088/1742-5468/2007/03/P03006

47. Wei D, Liu Q, Zhang H, Hu Y, Deng Y, Mahadevan S. Box-covering algorithm for fractal dimension of weighted networks. Scientific reports. 2013; 3. doi: 10.1038/srep03049

48. Erdos P, Rényi A. ON THE EVOLUTION OF RANDOM GRAPHS. Bulletin of the International Statistical Institute. 1960; 38(4):343–347.

49. Barabási AL, Albert R. Emergence of scaling in random networks. science. 1999; 286(5439):509–512. doi: 10.1126/science.286.5439.509 PMID: 10521342

50. http://www.transtats.bts.gov/DL_SelectFields.asp?Table_ID=292;.