Computers and Mathematics with Applications 64 (2012) 840–848

Contents lists available at SciVerse ScienceDirect

Computers and Mathematics with Applications

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

Differentiating complex network models: An engineering perspective

Zhengping Fan [a], Guanrong Chen [b,*], Yunong Zhang [a]

[a] Department of Automation, Sun Yat-sen University, Guangzhou 510275, PR China

[b] Department of Electronic Engineering, City University of Hong Kong, Hong Kong Special Administrative Region

ARTICLE INFO

Keywords:
Internet
Complex network model
Model evaluation

ABSTRACT

Network models that can capture the underlying network's topologies and functionalities are crucial for the development of complex network algorithms and protocols. In the engineering community, the performances of network algorithms and protocols are usually evaluated by running them on a network model. In most if not all reported work, the criteria used to determine such a network model rely on how close it matches the network data in terms of some basic topological characteristics. However, the intrinsic relations between a network topology and its functionalities are still unclear. A question arises naturally: For a network model which can reproduce some topological characteristics of the underlying network, is it reasonable and valid to use this model to be a test-bed for evaluating the network's performances? To answer this question, we take a close look at several typical complex network models of the AS-level Internet as examples of study. We find that although a model can represent the Internet in terms of topological metrics, it cannot be used to evaluate the Internet performances. Our findings reveal that the approaches using topological metrics to discriminate network models, which have been widely used in the engineering community, may lead to confusing or even incorrect conclusions.

1. Introduction

The topological properties of a complex network are typically very complicated due to its large size and intrinsic interconnection patterns. To better understand the structure of a network and to analyze its dynamical behavior, it is important and even necessary to construct a simplified abstract model that can well preserve the most fundamental topological characteristics of the network.

Graphs, consisting of nodes with links connecting them in some topologies, have been widely used to model and analyze the structural features of various complex networks [1]. Representative examples include those discussed in the following. For social networks, Saban et al. [2] proposed a growth network model to represent the bilateral investment treaties network; Kitsak et al. [3] proposed a scale-free model to describe the business firm network; Vieira et al. [4] investigated the sexual transmission of HIV within a population based on a small-world network model; Yang et al. [5] studied a spreading scheme of viral marketing based on a complex network model. For biological networks, Nicolau and Schoenauer [6] introduced a network model to reproduce some statistical measurements of the gene regulatory network; Nacher and Araki [7] suggested an evolutionary model to rebuild the degree distribution of the ncRNA–protein interaction network; Sneppen et al. [8] presented a simplified model to understand the large-scale regulatory networks; Ponten et al. [9] examined the relationship between structural and functional connectivity on the basis of the EEG neural mass

* Corresponding author. Tel.: +852 3442 7922; fax: +852 3442 0562.
E-mail address: eegchen@cityu.edu.hk (G. Chen).

0898-1221/$ – see front matter
doi:10.1016/j.camwa.2011.12.063

model. For communication and transportation networks, Boas et al. [10] developed a modified geographical model to discuss worldwide highway networks; Wang and Loguinov [11] derived a wealth-based Internet model to study the AS-level Internet topology. In fact, along the same line of research on network modeling, many other examples can be easily given.

Once a model is constructed to describe a network, it needs to be evaluated to see if it is "good" to represent that network and, moreover, if it is "better" than other existing models designated for the same network.

At present, most if not all reported network models rely only on topological characteristics of the underlying network, and these criteria are used to evaluate and differentiate comparable models. From this perspective, a model is considered to be "good" if it can reproduce basic topological features of the underlying network from its measured data; furthermore, this model is considered to be "better" than other models if it can match the network data-set more closely, also in terms of the same topological characteristics. In a word, topological characteristics are used as litmus for testing and judging network models today.

Specifically, some well-studied topological characteristics such as node degree distribution, clustering coefficient, distance distribution, and spectrum of the adjacency matrix, are commonly used to validate a model for a network or to evaluate and differentiate different models. For instance, Nacher and Araki [7] used degree distribution to evaluate their proposed model for an ncRNA–protein interaction network; Wang and Loguinov [11] asserted that their proposed wealth-based Internet model is better than other existing models because it can better capture the clustering coefficient and the distance distribution of the AS-level Internet network according to a set of real data; Toivonen et al. [12] utilized degree distribution, clustering coefficient and community structure to compare different models of friendship and email networks.

The main concern in the engineering community, however, is typically the network performances instead of the network topological features, the main reason being that a network (e.g., the Internet) is designed and built for certain intended tasks and functionalities. In such cases, it is important for a network model to behave as the underlying network in terms of some concerned performance indexes, yet not necessarily being able to capture the network topological characteristics as many as possible. Lacking profound knowledge about the intrinsic relations between the network topology and its dynamics and functionalities, the existing criteria using topological characteristics to evaluate and differentiate network models remains in place for most scientific and engineering applications today-one example in point is a new design of Internet routing protocols from the complex network approach [13].

To identify to what extent a network model obtained by the criteria using topological characteristics to evaluate models is useful for engineering applications, by taking models of the AS-level Internet topology as the underlying test-bed, we show that the current approaches using the topological characteristics to evaluate different models may be misleading for engineering applications. Specifically, we show that different Internet models may have very little difference in resisting random removals although they are very different in major topological metrics, namely the clustering coefficient, the distance distribution, the largest eigenvalue of the adjacency matrix, and the gap between the first and the second largest eigenvalues.

We also show that some network models that closely match the Internet data-sets in terms of the aforementioned topological metrics can be very different from the real Internet in their performances of resisting intentional attacks and traffic load distribution. We thereby conclude that it is misleading if the network performances are evaluated based on the model which is obtained by the commonly-adopted criteria using topological characteristics to evaluate and differentiate Internet models.

The rest of the paper is organized as follows. Section 2 provides some background and preliminaries on network models and their topological metrics. Section 3 compares some basic topological characteristics and Section 4 compares the robustness against random failures and intentional attacks, as well as data traffic performance of the Internet, all supported by extensive data-based simulations. Section 5 briefly concludes the investigation.

2. Network models and their topological metrics

For the AS-level Internet, since the first observation by Faloutsos et al. [14], several power-law models such as the Barabási–Albert (BA) model [15], Extended BA (EBA) model [16], Fitness model [17], Generalized Linear Preference (GLP) model [18], Highly Optimized Tolerance (HOT) model [19], Positive-Feedback Preference (PFP) model [20], Multi-Local-World (MLW) model [21], and Wealth-based Internet Topology (WIT) [11] model, have been proposed to describe the Internet topology, despite the fact that most of them were not intended for the Internet.

In order to evaluate and differentiate the above-listed models against the real Internet, basic topological characteristics have been examined and discussed in the literature, particularly the following:

Clustering coefficient—it is defined to measure how closely the neighbors of a node are interconnected, popularly known as the probability of two friends of a person being friends themselves in a social network. It is an important characteristic used to describe the robustness performance in resisting removals of nodes–links, and even to evaluate routing algorithms in computer networks, because a node with a higher clustering coefficient generally has higher path diversity.

Distance distribution—it is to measure the probability that a randomly selected pair of nodes are separated by a pre-designated distance. As a global topological characteristic, it plays a vital role in many Internet applications such as data routing and virus spreading prevention.

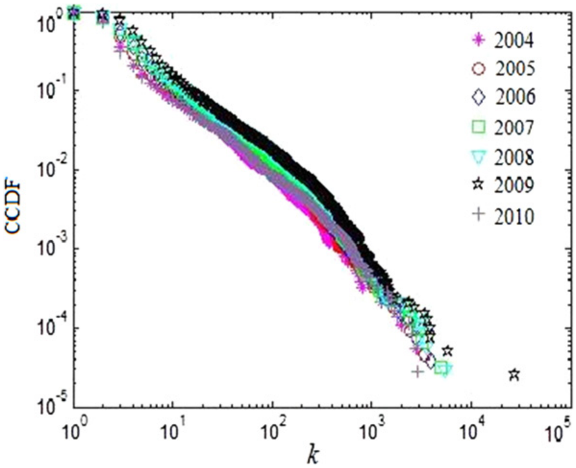

Fig. 1. Cumulative degree distribution of the AS-level Internet on May 15 from 2004 to 2010.

The first largest eigenvalue and the gap between the first and the second largest eigenvalues of the adjacency matrix—eigenvalues of the adjacency matrix of a network represent another global characteristic of the network. Particularly, the first largest eigenvalue of the network adjacency matrix and the gap between the first and the second largest eigenvalues of this matrix are very important because the former is key to the network robustness against node–link removals and the latter is closely related to the maximum traffic throughput of the network. Here, the adjacency matrix, $\{a_{i,j}\}_{N\times N}$, is defined by setting $a_{i,j} = 1$ if nodes *i* and *j* are connected, or $= 0$ otherwise.

The above three basic topological characteristics have been frequently used to evaluate newly proposed models for the Internet. For example, Wang and Loguinov [22] compared the wealth-based evolution model with the BA model, the generalized linear preferential model [23], and the HOT model [19], by examining whether or not they can reproduce the average clustering coefficient and the average distance characteristics of the real Internet topology. They also used the dynamical behaviors of the average clustering coefficient, the average distance, and the second smallest eigenvalue of the normalized Laplacian matrix (the negativity of the adjacency matrix), so as to differentiate different models [11]. As another example, Bu and Towsley [18] argued that their proposed model is better than the others by evaluating the degree of resemblance to the Internet in terms of the power-law exponent, average clustering coefficient and average distance.

On the other hand, in the engineering community, two usually concerned and widely studied issues are the following:

Robustness in resisting random failures and intentional attacks—On the Internet, events such as equipment failures, power lost, traffic overloading, and distributed DoS attacks, frequently occur. Such incidents are expected to have little effect on the effective operation of the entire network, namely the Internet should be robust against them.

Traffic load distribution—In Internet data traffic engineering, the traffic load distribution pattern of the Internet is very important because it can be used to measure the potential traffic on nodes–links and potential congestion points in the network.

By taking all the above-referred network metrics and concerned issues into consideration, the objective of this paper is to answer the following question:

If an Internet model "closely matches" the real Internet data-set in terms of the three key topological characteristics listed above, can it be used to evaluate the Internet performances of resisting random failures and intentional attacks and to uncover the pattern of the Internet traffic load distribution?

To address this question, the familiar BA, EBA, Fitness, and MLW models are used for evaluation and comparison, because they can be precisely formulated and programmed to match therefore investigate the AS-level Internet topology constructed based on the daily data collected by UCLA [24], for example on 15 May 2005 which will be examined below.

Noticing the argument [25] that the degree distribution of the AS-level Internet might not be a power-law but a Weibull or perhaps something else, we plot Fig. 1 here for verification, to show the cumulative degree distributions of the data-set collected on every 15th of May from year 2004 to 2010. During this period of a total of six years, although the Internet had grown and changed dramatically, these cumulative degree distributions turned out to be very similar to each other and they all look like in power-law (albeit not perfectly). For this reason, some traditional Internet models, such as random graph [26] and Tiers and Transit-Stub models [23], are excluded from our comparisons below. On the other hand, previous observations have shown [27] that the three basic topological characteristics, namely the average degree, degree distribution and joint degree distribution, are key to reproduce an Internet-like topology. Therefore, the models considered here, namely the BA, EBA, Fitness, and MLW models, will apply the same set of values of these three characteristics (see [21] for more details in performing such simulations).

Table 1
Values of topological parameters for the Internet and the network models. N is the number of nodes, γ is the power-law exponent, r is the assortativity coefficient, $\bar{C}$ is the average clustering coefficient, $\bar{d}$ is the average distance between nodes, and λ is the largest eigenvalue of the adjacency matrix.

	Internet	BA	EBA	Fitness	MLW
N	21 999	21 999	21 999	21 999	21 999
γ	2.18	3.0	2.69	2.45	2.36
r	−0.18	−0.02	0.02	−0.11	0.03
$\bar{C}$	0.46	0.003	0.01	0.01	0.24
$\bar{d}$	3.49	4.14	3.49	3.71	3.45
λ	141.12	27.82	62.83	39.16	111.87

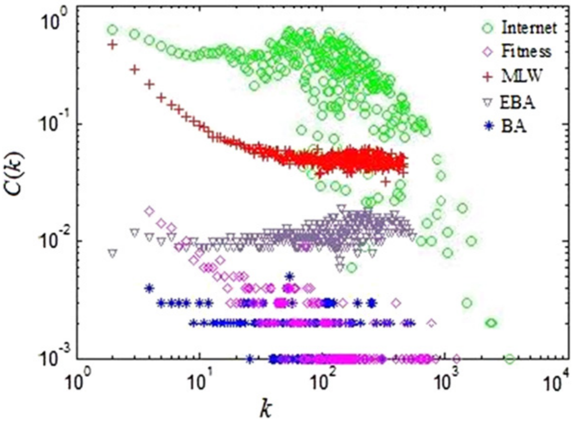

Fig. 2. Comparison of clustering coefficient.

At this point, it should be remarked that our emphasis here is not to claim which model is the best one to represent the Internet, nor to optimize a model to best fit the Internet topology. Instead, our intention is to demonstrate that the current approaches using topological metrics to evaluate and differentiate complex network (e.g., the Internet) models may lead to confusing or even incorrect conclusions in the field of engineering applications. Therefore, it is often not necessary to tune the model parameters to best fit the snapshots of the Internet topology data-set in simulations. This will become clearer as our presentation develops.

3. Comparison of basic topological characteristics

The parameter values of some basic topological metrics obtained from our extensive simulations, such as the network size (number of nodes), power-law exponent, assortativity coefficient, average clustering coefficient, average distance, and largest eigenvalue of the adjacency matrix, are summarized in Table 1.

It can be observed from Table 1 that the MLW and EBA models are closer to the Internet in terms of the average clustering coefficient, average distance and largest eigenvalue. Clearly, the MLW and EBA models are better than the BA and Fitness models if they are compared based on these topological characteristics.

Fig. 2 shows the relationship between the clustering coefficient and the node degree k for the Internet and the models in question. It can be seen that high-degree nodes of the Internet have lower clustering coefficients while low-degree nodes have higher clustering coefficients, which is consistent with the observations reported earlier in [28] that the core is loosely connected and the structure is clearly hierarchical in the Internet. It can also be observed from Fig. 2 that the clustering coefficient of the MLW model is closer to that of the Internet as compared to the other models.

Fig. 3 displays the distance distributions of the Internet and the models. It can be seen that the BA and Fitness models have a Poisson-like distance distribution, with a peak around a certain distance d_0 and exponentially delaying when distance d is far from d_0. Clearly, the MLW and EBA models are better than the BA and Fitness models in capturing the characteristic of distance distribution of the Internet.

Fig. 4 depicts the first and second largest eigenvalues of the adjacency matrix of the Internet and the models. For the Internet, the first largest eigenvalue is quite large and there is a big gap between the first and the second largest eigenvalues. It can be observed that the first largest eigenvalue and the gap between the first and the second largest eigenvalues are both bigger in the MLW and EBA models, but they are smaller in the BA and Fitness models. Clearly, if only the first largest eigenvalue is concerned, the MLW and EBA models are better than the BA and Fitness models. Furthermore, in evaluating both the first largest eigenvalue and the gap between the first and the second largest eigenvalues, the same can be concluded.

In summary, the MLW is the best choice among the studied models to fit the Internet topology, on the basis of the above-referred real AS-level Internet data-set, if the models are evaluated by their topological characteristics such as the average

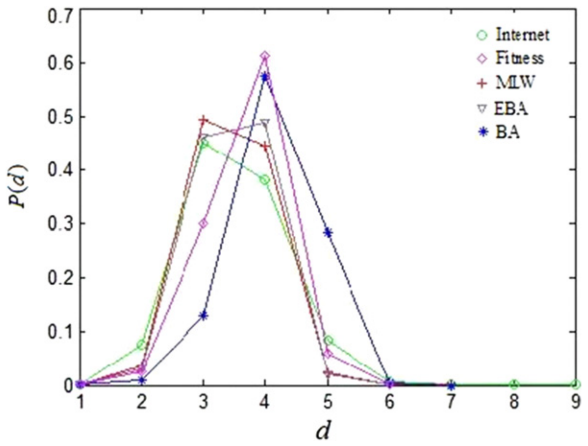

Fig. 3. Comparison of distance distribution.

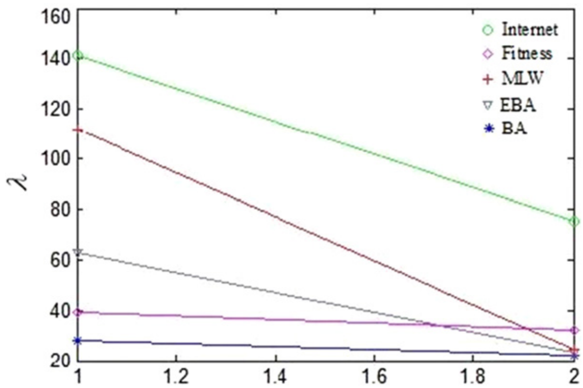

Fig. 4. Comparison of the first and second largest eigenvalues of adjacent matrix.

clustering coefficient, average distance, clustering coefficient distribution, distance distribution, the first largest eigenvalue, and the gap between the first and the second largest eigenvalues.

4. Comparison of performances in robustness and data traffic

The robustness of a network against attacks and failures can be studied by using S_f, the size of the largest connected component after a fraction of nodes, f, in the network were randomly or intentionally removed from the original network S_0. Clearly, the ratio S_f/S_0 measures the capability of the network regarding how many nodes remain functioning in communicating with each other after the f portion of nodes had been removed.

Fig. 5 shows a comparison of robustness in resisting random removals of nodes. It can be observed that all models have only little differences. However, as discussed above, all these models are very different in their topological characteristics, namely the clustering coefficient, distance distribution, the first largest eigenvalue, and the gap between the first and the second largest eigenvalues. We therefore conclude that the model obtained by the approach using topological metrics to evaluate models provides quite limited information on the resistance ability of the Internet against random removals.

It can also be observed that the BA and Fitness models have different power-law exponents but they behave similarly in resisting random removals. Therefore, concerning the robustness of the Internet against random removals, it is not necessary to require a model to be able to exactly reproduce the value of the power-law exponent of the real Internet. Even the simplest BA model can roughly reflect the Internet's robustness against random removals. This also shows that the so-called ''robust yet fragile'' property of the Internet [29], or of its BA model, does not essentially depend on the power-law distribution of its topology.

Fig. 6 compares the robustness in resisting intentional attacks. Here, as usual, intentional attack means that nodes are removed one after another following the decreasing order of the node degrees. It can be observed from the figure that the MLW model is the best while, surprisingly, the EBA model is the worst in reflecting the Internet's robustness in resisting intentional attacks. However, both the MLW and EBA models are better than the BA and Fitness models in

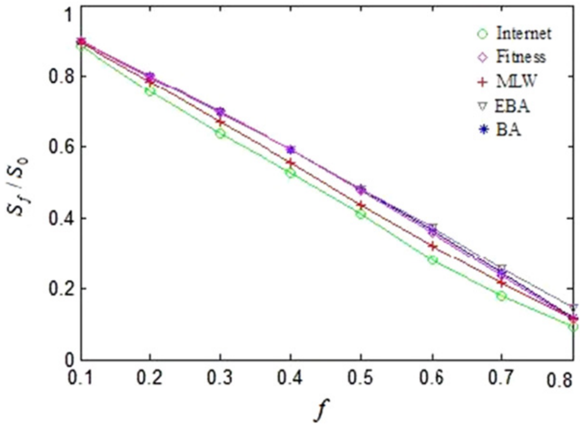

Fig. 5. Comparison of robustness in resisting random removals.

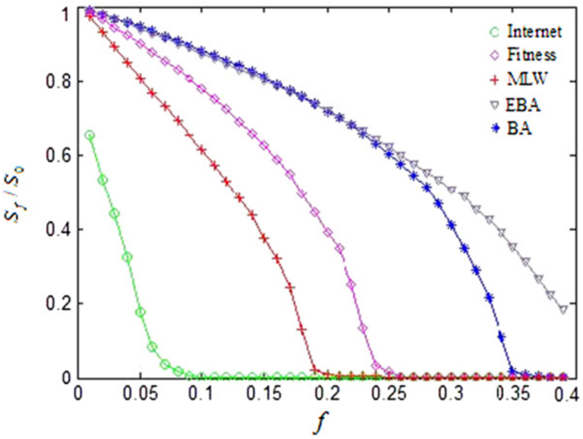

Fig. 6. Comparison of robustness in resisting intentional attacks.

terms of reproducing the average clustering coefficient and the average distance. Therefore, the model obtained on the basis of the average clustering coefficient and the average distance, as did in [18], provides an incorrect information on the resistance ability of the Internet against intentional attacks. Note also that the EBA model is better than the Fitness model in reproducing the Internet's topological characteristics, including the clustering coefficient, distance distribution, the first largest eigenvalue, and the gap between the first and the second largest eigenvalues. However, the Fitness models is closer to the Internet than the EBA model in matching the robustness against intentional attacks. Thus, the approach using topological metrics to evaluate and differentiate models leads to an incorrect conclusion on the resistance ability of the Internet against intentional attacks.

Next, to investigate the traffic load distribution, it is natural to study $T(r)$, the ratio of the traffic load of the first r largest nodes over the total traffic load of the whole network. Here, it is assumed that a data packet is sent from node i to j, for every possible pair of nodes (i, j). For simplicity, it takes into account the time delays of data transmission at nodes and links, and it adopts the Open-Shortest-Path-First (OSPF) routing protocol to transmit data packets. Thus, the traffic load of a node is defined as the total number of packets passing through it, after all pairs of nodes have sent and received one packet between them.

Fig. 7 shows the traffic load distribution of the Internet and the concerned models. It can be seen that the traffic load distribution of the Internet is quite heterogeneous: a small fraction of the first largest nodes occupy most traffic load of the network, while a large number of low-degree nodes occupy only a small portion of the total traffic. Compared to the BA and Fitness models, the MLW and EBA models significantly underestimate the heterogeneity of the traffic load distribution of the Internet. Again, for the traffic load distribution concerned by the engineering community, the approach using topological metrics to evaluate and differentiate models leads to an incorrect conclusion.

5. Conclusions and discussions

Topological characteristics of the Internet can highly influence the dynamics of the processes running on it. The state of the art is that every existing Internet model can only present one subset of the real Internet topological features.

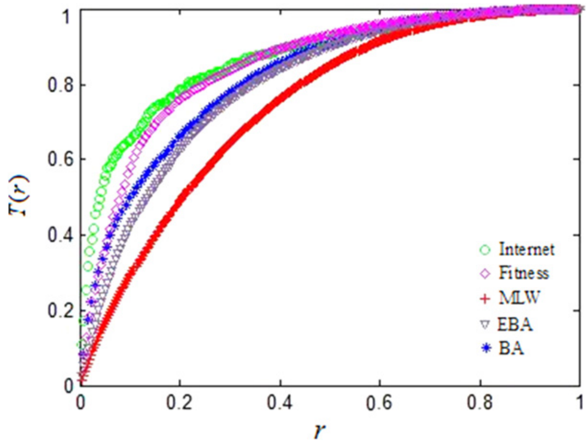

Fig. 7. Comparison of traffic load distribution.

The evaluation and differentiation of the Internet models, therefore, rely on the use of trustworthy measures of fundamental topological characteristics. Yet, this paper has revealed that the commonly-adopted criteria that use basic topological characteristics to evaluate and compare Internet models can be confusing and they are, *de facto*, questionable.

Observe that usually more than two measures of topological characteristics are applied to evaluate and differentiate an Internet model. In such cases, one can also combine the canonical variable analysis and Bayesian decision theory to classify the Internet models [29]. Suppose the feature vector is $X = (x_1, x_2, \dots, x_p)^T$, where x_i is a scalar measure, and it is used to classify N networks which are divided into M classes. The objective is to maximize the interclass dispersion while minimizing the intraclass scattering, where the intraclass matrix is defined as

$$S_{\text{intra}} = \sum_{k=1}^{M} \sum_{\zeta \in C_k} \left(X_\zeta - \bar{X}_k\right)\left(X_\zeta - \bar{X}_k\right)^T,$$

while the interclass matrix is defined as

$$S_{\text{inter}} = \sum_{k=1}^{C} N_k \left(\bar{X}_k - \bar{X}\right)\left(\bar{X}_k - \bar{X}\right)^T,$$

where X_ζ is the feature vector of network ζ, $\bar{X}_k$ is the average feature vector of class C_k, $\bar{X}$ is the average feature vector of N networks, and N_k is the number of networks in class C_k, $k = 1, 2, \dots, M$. The original higher-dimensional feature measures can then be projected into a two-dimensional feature space by using a linear transformation $Y = TX_\zeta$, where T is constructed by the eigenvectors associated with the first two largest eigenvalues of the matrix $S_{\text{intra}}^{-1} S_{\text{inter}}$. Finally, in the two-dimensional feature space, a network with unknown classification can be determined to belong to which class, on the basis of the Bayesian decision method. Fig. 8 shows the canonical projection results when the average clustering coefficient, the average distance, and the first largest eigenvalue of the adjacency matrix are involved in the evaluation and comparison of the Internet models. By using the Bayesian decision method, one can find that the MLW model is indeed the most compatible one to the real Internet.

It is also possible to apply the hierarchical clustering algorithm [30] to classify the various Internet models. This method builds a hierarchy by treating every network as a single cluster. Then, in each successive iteration, according to the predefined distance between clusters, the closest pair of clusters are merged, until only one cluster remains. Fig. 9 shows the dendrogram by using the familiar Ward's method when the average clustering coefficient, the average distance, and the first largest eigenvalue of the adjacency matrix are used to classify the Internet models. In the figure, each linkage of distances indicates a point at which two models are merged: the sooner the two networks are merged, the more similar they are. From this figure, one can see that the MLW model is closer to the real Internet than all the other models.

From Figs. 8 and 9, thus, one can gain an overall impression that although a network model (e.g., the MLW model) can represent the network (e.g., the Internet) in terms of topological characteristics, it cannot represent the concerned network performances (e.g., traffic load distribution). It means that the approach using topological metrics to evaluate and differentiate models may lead to incorrect conclusions on network performances concerned by the engineering community.

In summary, the approaches using topological characteristics to discriminate graph models are widely used in the engineering community [31]. However, due to the fact that the intrinsic relations between the network topology and its functionalities are still unknown, the current approaches using topological characteristics to evaluate and differentiate network models may mislead engineers to draw incorrect conclusions on performances of network algorithms and protocols.

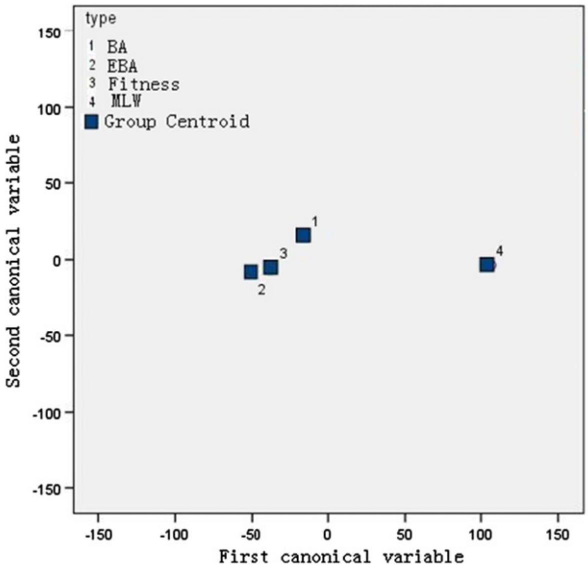

Fig. 8. Classification of the Internet models by using canonical variable analysis.

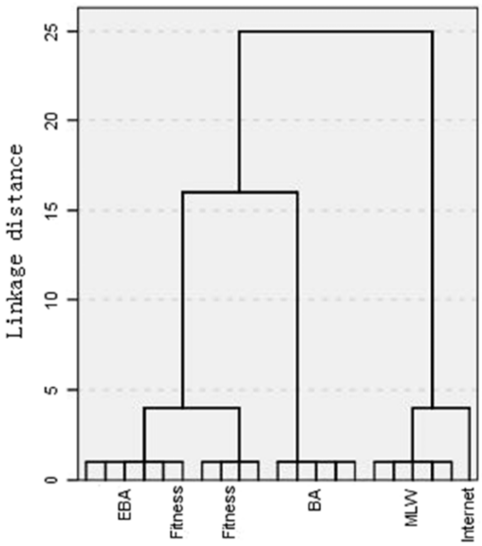

Fig. 9. Dendrogram of the Internet and its models.

Acknowledgments

The authors acknowledge financial support from the National Natural Science Foundation of China under Grants 60704045 and 60775050, Natural Science Key Foundation of China under Grants 10832006 and 60736028, Fundamental Research Funds for the Central Universities under Grant 09Lgpy57, and the Hong Kong GRF Scheme under Grant CityU1114/11E.

References

[1] R. Albert, A.L. Barabási, Statistical mechanics of complex networks, Rev. Modern Phys. 74 (2002) 47–97.
[2] D. Saban, F. Bonomo, N.E. Stier-Moses, Analysis and models of bilateral investment treaties using a social networks approach, Physica A 389 (2010) 3661–3673.
[3] M. Kitsak, M. Riccaboni, S. Havlin, F. Pammolli, H.E. Stanley, Scale-free models for the structure of business firm networks, Phys. Rev. E 81 (2010) 036117.
[4] I.T. Vieira, R.C.H. Cheng, P.R. Harper, V. Senna, Small world network models of the dynamics of HIV infection, Ann. Oper. Res. 178 (2010) 173–200.
[5] J. Yang, C. Yao, W. Ma, G. Chen, A study of the spreading scheme for viral marketing based on a complex network model, Physica A 389 (2010) 859–870.
[6] M. Nicolau, M. Schoenauer, On the evolution of scale-free topologies with a gene regulatory network model, Biosystems 98 (2009) 137–148.

[7] J.C. Nacher, N. Araki, Structural characterization and modeling of ncRNA-protein interactions, Biosystems 101 (2010) 10–19.
[8] K. Sneppen, S. Krishna, S. Semsey, Simplified models of biological networks, Annu. Rev. Biophys. 39 (2010) 43–59.
[9] S.C. Ponten, A. Daffertshofer, A. Hillebrand, C.J. Stam, The relationship between structural and functional connectivity: graph theoretical analysis of an EEG neural mass model, NeuroImage 52 (2010) 985–994.
[10] P.R.V. Boas, F.A. Rodrigues, L.F. Costa, Modeling worldwide highway networks, Phys. Lett. A 374 (2009) 22–27.
[11] X. Wang, D. Loguinov, Understanding and modeling the Internet topology: economics and evolution perspective, IEEE Trans. Netw. 18 (2010) 257–270.
[12] R. Toivonen, L. Kovanen, M. Kivela, J.P. Onnela, J. Saramaki, K. Kaski, A comparative study of social network models: network evolution models and nodal attribute models, Social Networks 31 (2009) 240–254.
[13] M.A. Ayyoub, H. Gupta, Joint routing, channel assignment, and scheduling under general interference models, IEEE Trans. Mob. Comput. 9 (2010) 553–569.
[14] M. Faloutsos, P. Faloutsos, C. Faloutsos, On power-law relationships of the Internet topology, Comput. Commun. Rev. 29 (1999) 251–262.
[15] A.L. Barabási, R. Albert, Emergence of scaling in random networks, Science 286 (1999) 509–512.
[16] R. Albert, A.L. Barabási, Topology of evolving networks: local events and universality, Phys. Rev. Lett. 85 (2000) 5234–5237.
[17] C. Bianconi, A.L. Barabási, Competition and multiscaling in evolving networks, Europhys. Lett. 54 (2001) 436–442.
[18] T. Bu, D. Towsley, On distinguishing between Internet power law topology generators, in: Proc. IEEE INFOCOM, 2002, pp. 638–647.
[19] J.M. Carlson, J. Doyle, Highly optimized tolerance: a mechanism for power laws in designed systems, Phys. Rev. E 60 (1999) 1412.
[20] S. Zhou, Understanding the evolution dynamics of Internet topology, Phys. Rev. E 74 (2006) 016124.
[21] Z.P. Fan, G.R. Chen, Y.N. Zhang, A comprehensive multi-local-world model for complex networks, Phys. Lett. A 373 (2009) 1601–1605.
[22] X. Wang, D. Loguinov, Wealth-based evolution model for the Internet AS-level topology, in: Proc. IEEE INFOCOM, 2006, pp. 1–11.
[23] M.B. Doar, A better model for generating test networks, in: IEEE GLOBECOM, 1996, pp. 86–93.
[24] B. Zhang, R. Liu, D. Massey, L. Zhang, Collecting the Internet AS-level topology, Comput. Commun. Rev. 35 (2005) 53–61.
[25] H. Haddadi, M. Rio, G. Iannaccone, A. Moore, R. Mortier, Network topologies: inference, modeling, and generation, IEEE Commun. Surv. Tutor. 10 (2008) 48–69.
[26] B.M. Waxman, Routing of multipoint connections, IEEE J. Sel. Areas Commun. 6 (1988) 1617–1622.
[27] P. Mahadevan, D. Krioukov, K. Fall, A. Vahdat, Systematic topology analysis and generation using degree correlations, Comput. Commun. Rev. 36 (2006) 135–146.
[28] G.Q. Zhang, Q.F. Yang, S.Q. Cheng, T. Zhou, Evolution of the Internet and its cores, New J. Phys. 10 (2008) 123027.
[29] R. Albert, H. Jeong, A.L. Barabási, Error and attack tolerance in complex networks, Nature 406 (2000) 378–382.
[30] L.F. Costa, F.N. Silva, A pattern recognition approach to complex networks, J. Stat. Phys. 11 (2010) 11015.
[31] L.F. Costa, F.A. Rodrigues, G. Travieso, P.R.V. Boas, Characterization of complex networks: a survey of measurements, Adv. Phys. 56 (2007) 167–242.