PURPOSEFUL RANDOM ATTACKS ON NETWORKS — FORECASTING NODE RANKING NOT BASED ON NETWORK STRUCTURE

Lili Ma

School of Statistics, Capital University of Economics and Business
Beijing, 100070, China
malili@cueb.edu.cn

(Received May 3, 2018; accepted March 20, 2019)

We propose the conception of purposeful random attacks, which can greatly save attacking costs but achieve comparable effects to targeted attacks, based on the hidden degree centrality (HDC) defined according to node features in the one-dimensional circle model of network hidden metric spaces. The macro-matching degree is proposed to research attacking effects. Results show that when the optional node set for attacks is selected as nodes ranked in the top $\beta\%$ according to HDC, the macro-matching degree will be $> 80\%$ with $\beta = 0.5$. The smaller the value of β, the higher the value of the matching degree, showing that random attacks on the optional node set would be performed at most of those really important nodes. Further, the effect of the purposeful random attack becomes better with the growth of parameter α in the circle model. However, after α grows to a fixed value, it would have no influence on the attack effectiveness. Jump phenomena presented by changing curves of the macro-matching degree with parameter γ, another parameter in the circle model, show that networks should be divided into two groups for $\gamma > 2.5$ or $\gamma < 2.5$, and in any group, the effect of the purposeful random attack becomes worse with the growth of γ.

DOI:10.5506/APhysPolB.50.943

1. Introduction

During the last few years, complex systems have been studied widely in the context of the theory and applications in various fields [1, 2], ranging from transportation networks [3–5] to the Internet [6, 7] and human societies [8, 9]. Real-world networks are found to be structured heterogeneously [10]. This common structural characteristics implies that different

nodes of the network could display quite different features and play distinct roles in network structures and network functions [11]. So, the concept of node centrality is proposed in the study of network theory to quantify contributions or importance of network nodes.

Different definitions of node centrality are often proposed to evaluate some kinds of node importance from different views. According to the views, there are a lot of definitions of node centrality [11–18]. Centrality based on network structure is first proposed. The simplest one is the degree centrality (DC) [11], which is characterized by node degree and measures the contributions of nodes to facilitate transportation in networks. For instance, in disease propagation networks, diseases would spread widely when a degree of an infected individual is high. As DC just measures the immediate contribution of a node (node degree), the eigenvector centrality (EC) [12, 13] is proposed as an extension of DC to quantify both the immediate contribution of a node and the contributions of its neighbors. Moreover, as another extension of DC, node subgraph centrality (SC) [14] is proposed by considering the long-range influence transferred from the participation of the node in all subgraphs of the network. The betweenness centrality (BC) [11, 15] is a measurement of node centrality which is in common use and is generally characterized by the number of the shortest paths passing through the node. While BC reflects the ability of a node to control the communications between pairs of nodes, the closeness centrality (CC) [11] shows the capability of a node to escape from the potential control of the others in the network.

The measurements of node centrality described above are all defined based on network structures. Considering both network structures and network dynamics, some definitions of node centrality are suggested. In Ref. [15], the flow-based measure of node centrality (FC) is constructed by restricting the maximum amount of transportation elements (*e.g.*, rumors, data packets, or viruses) passing through the node. Besides, there are some other definitions of node centrality based on the random walk process of the network, such as the power centrality [16], the random-walk centrality [17] and the information centrality [18].

In recent years, the social network draws a lot of attention because of its close relationships with real life and its important applications in real world. In the study of social networks, node centrality is named the social influence of an individual [19–23]. At present, various mobile applications (mobile APPs), such as APPs used for shopping and APPs for making friends, come out and are booming. The study of individual influence is becoming more and more important. In the study of this field, besides those above definitions of node centrality, some definitions are constructed considering both network structures and individual features [24–29]. Considering features of individuals in Twitter, the HITS algorithm is proposed to evaluate the

authority and the centrality of an individual [24, 25]; Personalized PageRank algorithm is proposed considering the degree of preference of topics, the degree of novelty, sensitivity of information, and so on [26–29].

Studies on node centrality and individual influence provide effective methods to research attacks on networks. Because of the scale-free feature, structures of real-world networks could be robust under random attacks but fragile under targeted attacks. As a kind of social network, criminal networks could survive from random attacks of polices, but collapse more easily under attacks aimed at the most important members. Therefore, studies on node centrality have very significant and effective applications in real life. It is easy to see that network topological structure is a necessary condition in calculating most kinds of node centrality. Nevertheless, it is quite hard to get the concrete structure of a real-world network, especially now under the situation with huge amount of data. On the other hand, many real networks are networks with the structures evolving over time, which is getting more and more attention from network researchers [30, 31], and where no information about the actual ranking of node importance in the future is available. In this paper, we aim to propose a mechanism to estimate the ranking of node importance in advance, under some sort of average effect and not based on the actual network structures.

Studies on hidden metric spaces of networks provide some possibility to solve this problem. Real-world networks have lots of common features in structures, dynamic processes and functions. To explain these phenomena, in 2009, Boguñá *et al.* [32] proposed the 'hidden metric space explanation' theory: they claim that a hidden metric space does exist underneath any real network and plays quite a crucial role in shaping the observed network. A node in the space has its own coordinates, which reflect the hidden intrinsic features of the node. Moreover, for the real network, there are some existing algorithms to find the appropriate implicit model of the hidden metric space of the network [33, 34], even for evolving networks [35].

Enlightened by this conception, in this paper, we design a mechanism for forecasting the rank of network nodes, according to the hidden features of network nodes but not related to network structures. Based on the simplest model with all nodes uniformly distributed on a one-dimensional circle [32], we propose the conception of 'hidden degree centrality' of a node. According to the calculation results of this centrality of all nodes, we get the forecasting node rank of the observable network. Depending on the ranking result, we give an optional set of nodes for the random attack on the network and name it the 'purposeful random attack'. We also calculate the degree centrality of nodes and rank the nodes in the observable network based on the structure. Comparing results show that nodes in the optional set are those which really have most important positions in the observable network.

To reflect the effectiveness of the purposeful random attack, we propose the 'macro-matching degree' of the two ranking results. Simulation results show that random attacks at those optional nodes can both work as targeted attacks on the whole network and massively save costs of attacks. On the other hand, we study the relationships between the matching degrees with parameters in the one-dimensional circle model.

2. Hidden metric spaces of networks

At first, the concept of hidden metric space is introduced to study the navigability of complex networks [32, 36]. In many real-world networks, such as social, neural and cell regulatory networks, the networks have quite good navigable abilities where nodes communicate without any global knowledge of network topologies. Boguñá *et al.* [32] proposed the hidden metric space to explain this fact. They suggest that observable networks are underlain by hidden geometric frames which determine network topologies and affect information-routing decisions.

According to the concept of hidden metric space (see Fig. 1) [32], the network can be embedded into a manifold, and all nodes exist in the observable network and the hidden space. While the metric distance between a pair of nodes is the length of the shortest path in the network, the distance of the pair of nodes in the hidden space is abstracted by the similarity between them, such as similar professions, interests or backgrounds between social individuals [37]. Similar nodes are placed closer in the space and with high probability connected in the observable network. With node similarity as the hidden distance between nodes, the hidden metric space can be constructed. In the space, if node A is close to node B and node B is close to node C, then node A is also close to node C under the rule of the triangle

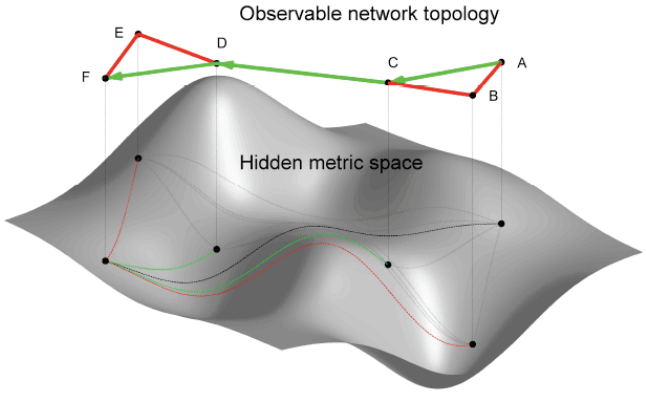

Fig. 1. A sketch map for the conception of hidden metric space.

inequality. Thus, triangle ABC exists in the observed structure with high probability. The theory of hidden metric space provides a feasible explanation for the appearance of most common features of networks, such as the scale-free feature, the high clustering phenomenon, the small-world feature, and so on.

As the simplest model of hidden metric space, a one-dimensional circle model is proposed in Fig. 2 [32] to uniformly place all nodes on it, in which the radius is $R = N/2\pi$ and the number of nodes is N. Each node is given by two hidden parameters (θ, k), where θ is the polar angle uniformly distributed in $[0, 2\pi)$ and k is the expected node degree with a distribution $\rho(k) = (\gamma-1)k_0^{\gamma-1}k^{-\gamma}$, $k > k_0 \equiv (\gamma-2)\langle k\rangle/(\gamma-1)$, $\gamma > 2$. The probability that node (θ, k) and node (θ', k') are connected in the network is

$$r\left(\theta, k; \theta', k'\right) = \left(1 + \frac{d\left(\theta, \theta'\right)}{\mu k k'}\right)^{-\alpha}, \tag{1}$$

where $d(\theta, \theta')$ is the geodesic distance between the two nodes on the circle and $\mu = \frac{\alpha-1}{2\langle k\rangle}$. The form of the connection probability r relies on typical phenomena in real-world networks such as airport networks [37]. Equation (1) reveals that two nodes with smaller distance (nodes which are similar to each other) tend to be connected with higher probability. On the other hand, hub nodes will be connected with high probability regardless of their hidden distance as r is close to 1 when kk' is large; hub nodes will be connected to nodes with low degrees if their distances are medium; low degree nodes will be connected only if they are close enough. These rules above ensure to generate random networks with power-law degree structure $P(k) \sim k^{-\gamma}$ [38]. In Eq. (1), parameter $\alpha > 1$ is considered as the hidden metric strength. The larger the strength α, the more preferred connections between close nodes in the hidden metric space, and then the higher the clustering of the real-world network.

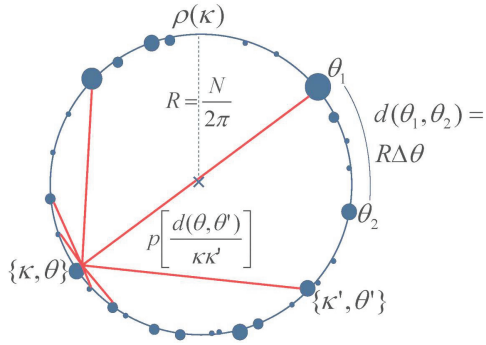

Fig. 2. The one-dimensional circle model of hidden metric space.

A method to map the Internet to a hyperbolic hidden space has already been proposed in [39]. Research on hidden metric spaces of networks attracts great attention in IT and biological fields [40]. Internet researchers worry about scalability limits of routing architecture in the existing Internet. Black holes are appearing everywhere and restrict further developments of the Internet. Discovery of the hidden metric space underneath a network could reveal the basic layout of the network and show how this network really functions. Routing strategies based on such a hidden metric space allow networks to efficiently find communication targets even when they do not know the global topology of the system. It is believed that such routing strategies would remove the bottleneck in the existing Internet. Moreover, hidden metric spaces could be applied to cancer research whose studies rely heavily on gene regulation. Supposing you were able to find the hidden space here, one could then figure out what drives gene regulation networks and what drives them to failure [40].

3. Node centrality and prediction of node ranking

3.1. Node degree centrality

Based on the scale-free feature of a real-world network, just a few nodes are hubs with big degrees, while most nodes are the ones with small degrees. Hubs are considered to play some important roles in networks, such as a social network — the disease would spread massively after an individual with a big degree has been infected. Nodes with big degrees also have crucial effects in protecting the network structure as attacks at hub nodes often lead to collapse of the network. Therefore, to evaluate this kind of node importance, the degree centrality (DC) of a node is proposed as $\mathrm{DC}(i) = k_i/(N-1)$, where k_i is the degree of node i and N is the network size [11]. In a social network, DC reflects the direct influence of an individual [41, 42].

The concept of node centrality finds a very wide range of important applications in the analysis of social networks. Individuals with large values of some kind of node centrality are considered as opinion leaders of the social network. With the rapid development of the Internet, opinion leaders play a more and more prominent role in virtual communities, network groups and information dissemination. They made comments on public opinion and interact with the Internet users and the media. Their opinions often influence the trend of their fans and then the public opinion. So, they are playing increasingly important roles in stimulating the public opinion and promoting the public discussion. Therefore, it is more and more important to find these opinion leaders in social networks. In the research of this area, individuals with the centrality ranked in the first 1% of all the individuals can be seen as the opinion leaders [19, 43]. Thus, node ranking is often studied after the research of node centrality.

3.2. Node hidden degree centrality

Based on the conception of network hidden metric space, we propose a mechanism to reflect the role of a node in the hidden space, similar to the degree centrality defined above. In the one-dimensional circle model, any two nodes have a linking probability. So, we consider all nodes form a weighted complete network with the linking probability as the edge weight between the two nodes. Then, we define the '*hidden degree centrality*' (HDC) of a node i as follows:

$$\mathrm{HDC}(i) = \sum_j r_{ij} \,,$$

where r_{ij} is the linking probability between node i and node j gained from the hidden metric space model. According to the concept of hidden metric space, this definition is totally based on the hidden features of nodes but not the structure of the network.

3.3. Prediction of node ranking

Based on the values of node DC and node HDC, we can give two kinds of node ranking. One is determined by the structure of the network, while the other by the natural features of nodes. In the realworld, the size of data grows rapidly and it becomes quite difficult to know the whole network structure. However, it seems to be getting easier to obtain the features of nodes under current technologies: with just two or three pieces of information about an individual, almost all information about them could be dug out. In China, we call this 'Human flesh search' and it is happening more and more frequently. Therefore, we believe it is feasible to estimate the ranking of nodes based on their natural features but not connections in network structure. Once the forecasting ranking results are proved to be effective, random attacks at the nodes predicted as important ones are going to have amazing effects both on destructive powers and cost savings.

To prove the effectiveness of our mechanism, in Tables I and II, we give some samples of the node ranking based on DC and HDC, respectively, and in the next section, we will research the matching degree of node rankings based on these two quantities. Here, we generate some networks with $N = 50$ based on the one-dimensional circle model. For $\gamma = 2.2$ with $\alpha = 2.5$ and for $\gamma = 2.8$ with $\alpha = 1.1$, 50 networks are generated, respectively, and two of the ranking results (only showing the top 15 nodes) are shown in Tables I and II. From the compared results of the two kinds of node ranking, we find that the ranking, based on node features in the hidden metric space, does have some effects in forecasting in the observable network.

TABLE I

A sample of the node ranking for a network with $N = 50$, $\gamma = 2.2$, $\alpha = 2.5$, showing only the top 15 nodes. The ranking result in the first line is based on the values of node DC, and the result in the second line is for the values of node HDC.

44	8	32	13	0	15	19	48	2	38	23	35	25	26	47
44	8	32	15	13	0	48	38	2	28	19	23	26	25	47

TABLE II

A sample of the node ranking for a network with $N = 50$, $\gamma = 2.8$, $\alpha = 1.1$, showing only the top 15 nodes. The ranking result in the first line is based on the values of node DC, and the result in the second line is for the values of node HDC.

10	26	41	0	2	28	9	49	4	5	31	34	24	25	8
26	10	2	28	43	0	4	41	34	38	20	29	49	25	5

4. Optional node sets for random attacks and simulation results

4.1. Optional node sets for random attacks

Effective attacks on a network are considered to be those which could lead to some degree of damage to network structure. Thus, according to the heterogeneous feature of real-world networks, here we do not care about those nodes ranked in the back. Thinking of opinion leaders in social networks, here we study the matching degree of the node ranking based on DC and the node ranking based on HDC just for the first $\beta\%$ nodes ($\beta \in [0.1, 50]$) rather than for all nodes. If the node ranking based on HDC can be gained before randomly performing attacks on the network, the first $\beta\%$ nodes could be considered as a set of targets and attacks could be carried out randomly in this set. We call this node set an *optional node set* for the random attack, and according to the results in the above section, this optional set contains most of the nodes that really play important roles in the observable network structure.

In order to research the effectiveness of the optional set, we propose the *micro-matching degree* and the *macro-matching degree* of the two kinds of node ranking. For the micro-matching degree, we give the definition as follows:

$$\text{micro-m} = \sum_{i \in V_\beta} \text{micro}(i)/(\beta\% \times N)\,, \tag{2}$$

where N is the number of nodes in the network, and V_β is the set constructed by the top $\beta\%$ nodes according to the first ranking result. The parameter $\text{micro}(i)$ is an indicator function, and for node i, if its position in the second ranking result is the same that in the first ranking result, then $\text{micro}(i) = 1$,

else, the micro$(i) = 0$. On the other hand, our purpose in this paper is to propose a mechanism to provide an optional node set for random attacks on the network. It means that attacks are still randomly carried out in the optional set. Therefore, there is no need to require that the positions of a node in the two ranking results are totally the same. For a node i, one of the top $\beta\%$ nodes according to the first ranking result, if it is also a node belonging to the top $\beta\%$ nodes based on the second ranking result, we consider node i as a macro-matching node in the two kinds of ranking results. Then, we define the macro-matching degree of the two ranking results as follows:

$$\text{macro-m} = \sum_{i \in V_\beta} \text{macro}(i)/(\beta\% * N)\,, \tag{3}$$

where the other parameters mean the same as in Eq. (2), and macro$(i) = 1$ if node i is a macro-matching node in the two kinds of ranking results, else, macro$(i) = 0$. According to this definition, it is not difficult to find out that the macro-matching degree could be considered as a measurement of the effectiveness of the purposeful random attacks we propose in this paper.

Next, we will study the effects of parameter β on the matching degrees of the two ranking results. For $N = 10\,000$, $\gamma = \gamma_0$, $\alpha = \alpha_0$, we generate 50 networks, and for each network with a given value of β, we calculate the micro-matching degree and the macro-matching degree, and then the average values of them for the 50 generated networks. For $\gamma = 2.8$, $\alpha = 1.1$ and for $\gamma = 2.2$, $\alpha = 4.5$, results are shown in Tables III and IV, respectively. Results in the two tables seemingly show that the smaller the value of β, the more effective the corresponding optional set. To further study this problem, for some different values of γ and α, we simulate the changing curves of the micro-matching degree and the macro-matching degree with respect to β. Because targets for attacks on networks should be those nodes with higher importance, we change the values of parameter β from 0.001 to 0.5 in the simulations of this part, and corresponding simulation results are shown in Figs. 3 and 4.

TABLE III

For $N = 10\,000$, $\gamma = 2.8$, $\alpha = 1.1$, the micro-matching degree and the macro-matching degree vary with parameter β.

β	0.1	0.2	0.5	1	2	5	10	20
mi	0.548	0.37	0.178	0.1002	0.054	0.0233	0.0121	0.0061
ma	0.932	0.918	0.9068	0.8872	0.861	0.8075	0.753	0.7045

TABLE IV

For $N = 10\,000$, $\gamma = 2.2$, $\alpha = 4.5$, the micro-matching degree and the macro-matching degree vary with parameter β.

β	0.1	0.2	0.5	1	2	5	10	20
mi	0.802	0.611	0.3612	0.212	0.1189	0.0529	0.0276	0.0142
ma	0.972	0.971	0.966	0.9574	0.9436	0.925	0.8969	0.8508

Figure 3 shows that the micro-matching degree indeed becomes smaller with the increase of parameter β, and drops to less than 0.1 at a very fast speed. On the other hand, for the macro-matching degree, Fig. 4 shows that though it goes down in a fluctuant and slow way with the increase of β, it generally has higher values compared with the micro-matching degree. According to the sharp decline of the micro-matching degree shown in Fig. 3, only quite few nodes on the highest position of the node ranking have good matching results and nodes ranked on the lowest position have no good matching effects. However, in Fig. 4, the ends of the curves show a slight upward tendency (to make it clearer, we list the data of the ends of those curves in Table V). We sum up the reason as the definition of the macro-matching degree: the greater the value of parameter β, the more the number of network nodes included in the optional set, and the less nodes that are excluded, then the higher the probability that a node in the optional set becomes a macro-matching node according to the definition, which would lead to a rise of the macro-matching degree. If all the network nodes were considered in the optional set, any node should be a macro-matching node and the value of the macro-matching degree would have to be 1 which is its

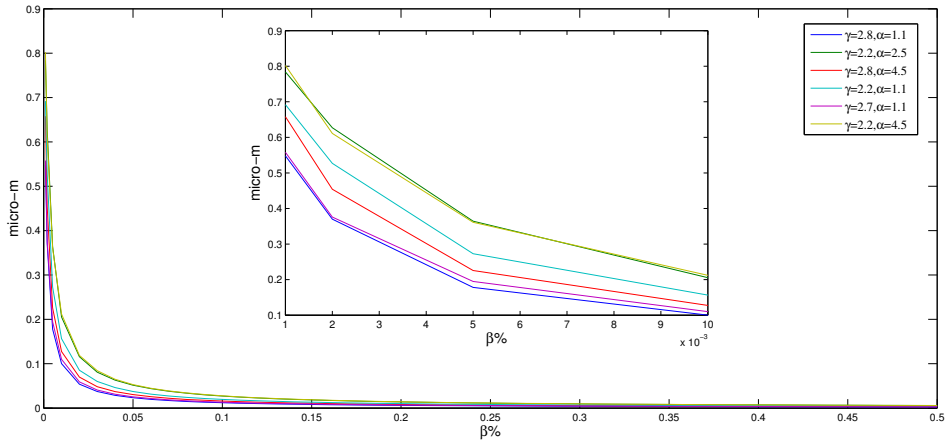

Fig. 3. The micro-matching degree changing with parameter β.

greatest value. So, based on the curves in Fig. 4 and the definition given by Eq. (3), the macro-matching degree should decrease slowly at first and then increase slowly with the increase of parameter β.

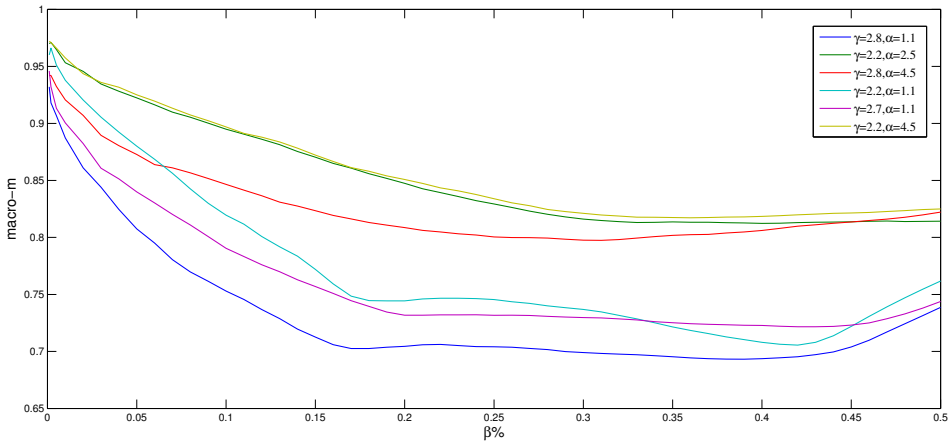

Fig. 4. The macro-matching degree changing with parameter β.

In the research of social networks, nodes ranked in the first 1% according to their centrality could be considered as the opinion leaders. Thus, in the following parts of this paper, we just consider the situations with $\beta = 0.5$ and $\beta = 1$. From the simulation results, we find that the macro-matching degree has relatively large values (about > 0.8 or > 0.75) in these two cases, and it means that the corresponding optional node sets we proposed for random attacks contain more than 80% or 75% of the real important nodes in the network structure. Therefore, with a proper value of β, under the mechanism we provide here, random attacks on networks could greatly save the costs of attacks (just carried out at β% of all the nodes), but achieve comparable effects to targeted attacks.

4.2. The matching degrees varying with parameters in the one-dimensional circle model

In the one-dimensional circle model of the hidden metric space, there are three independent parameters: α (the clustering strength), γ (the exponent of the power-low degree distribution) and $\langle k \rangle$ (the average degree). The average degree $\langle k \rangle$ is often fixed to 6, which is roughly equal to the average degree of some real networks of interest [44, 45], and change α from 1.1 to 5 and γ from 2.1 to 3, which cover their observed ranges in documented complex networks [32]. In this section, we will simulate the matching degrees varying with parameter α and with parameter γ, respectively.

TABLE V

Data of the ends of the curves shown in Fig. 4. The first line in this table shows the corresponding values of (γ, α).

$(2.2, 4.5)$	$(2.2, 2.5)$	$(2.8, 4.5)$	$(2.2, 1.1)$	$(2.7, 1.1)$	$(2.8, 1.1)$
0.821154	0.816059	0.797559	0.736832	0.72969	0.699013
0.819658	0.814818	0.797425	0.734682	0.729384	0.698309
0.818713	0.813831	0.798106	0.731656	0.728581	0.697625
0.817758	0.813067	0.79943	0.72857	0.727661	0.697109
0.817676	0.813247	0.800741	0.725088	0.726118	0.696259
0.817463	0.813629	0.801766	0.721543	0.725171	0.695383
0.81721	0.813281	0.802412	0.718433	0.724318	0.694332
0.817426	0.813328	0.80266	0.715702	0.723785	0.693679
0.817795	0.812905	0.803905	0.712737	0.723437	0.693326
0.818	0.812692	0.80481	0.710405	0.722933	0.69319
0.818425	0.81233	0.80606	0.707985	0.72278	0.693635
0.819088	0.812493	0.807922	0.706317	0.722093	0.694459
0.819857	0.812998	0.809888	0.705525	0.721686	0.695332
0.820433	0.813287	0.811058	0.708048	0.721679	0.697227
0.821095	0.813427	0.812368	0.713786	0.721968	0.6996
0.821409	0.813716	0.813511	0.721933	0.723142	0.703929
0.821904	0.814152	0.814857	0.730778	0.725017	0.70983
0.822732	0.814404	0.816051	0.73917	0.728681	0.717132
0.823505	0.813911	0.817679	0.747014	0.732899	0.724259
0.82445	0.814068	0.819763	0.75455	0.737991	0.731402
0.824956	0.814256	0.82222	0.7618	0.7438	0.738696

4.2.1. The matching degrees varying with parameter α

For $\beta = 0.5$ and $\beta = 1$, we respectively study the changing trends of the matching degrees with parameter α, with some given values of parameter γ, and the results are shown in Figs. 5 and 6.

Results in Fig. 5 present that the micro-matching degree shows some less strong trend to grow with increasing parameter α. By comparison, the changing trend of the macro-matching degree is quite more visible which is shown in Fig. 6: the macro-matching degree has a clear trend of growth with increasing parameter α and, more importantly, phase transitions appear in this figure: when α is greater than a specific value, the value of the macro-matching degree basically no longer changes. For parameters given in Fig. 6, we can assume that the value of the macro-matching degree has no big change when parameter $\alpha > 1.5$. It means that while $\alpha > 1.5$, parameter α has no longer any influence on the macro-matching degree, and then on the effectiveness of the purposeful attacks on networks.

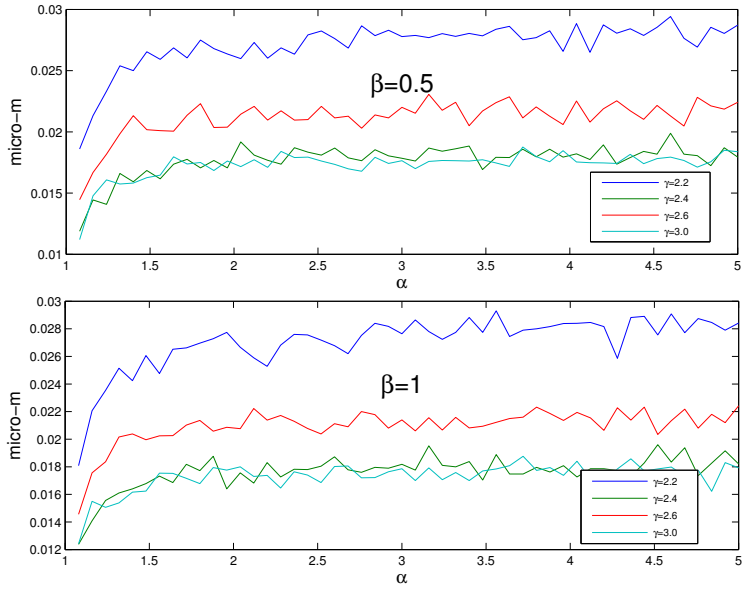

Fig. 5. The micro-matching degree changing with parameter α for $\beta = 0.5$ and $\beta = 1$.

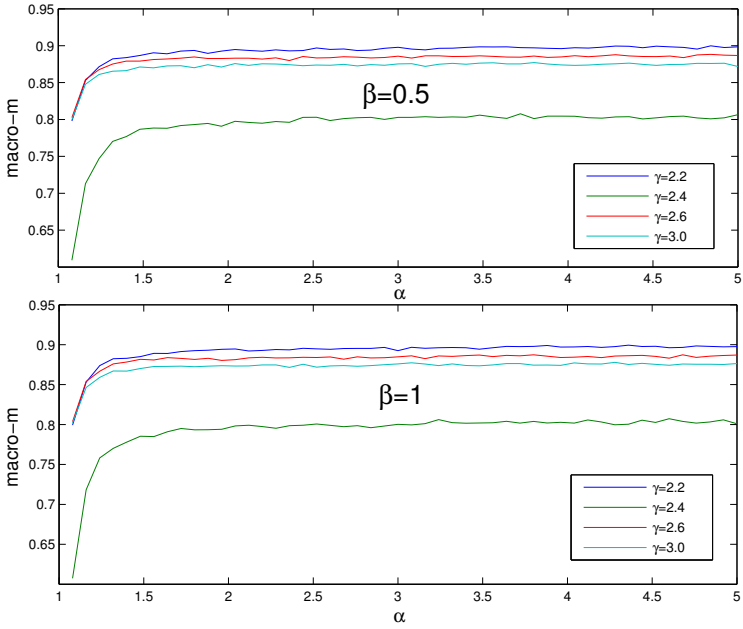

Fig. 6. The macro-matching degree changing with parameter α for $\beta = 0.5$ and $\beta = 1$.

4.2.2. The matching degrees varying with parameter γ

For $\beta = 0.5$ and $\beta = 1$, with $\alpha = 1.1, 2.0, 3.5, 5.0$, we simulate the changing curves of the two matching degrees with the increase of parameter γ and show the corresponding results in Figs. 7 and 8.

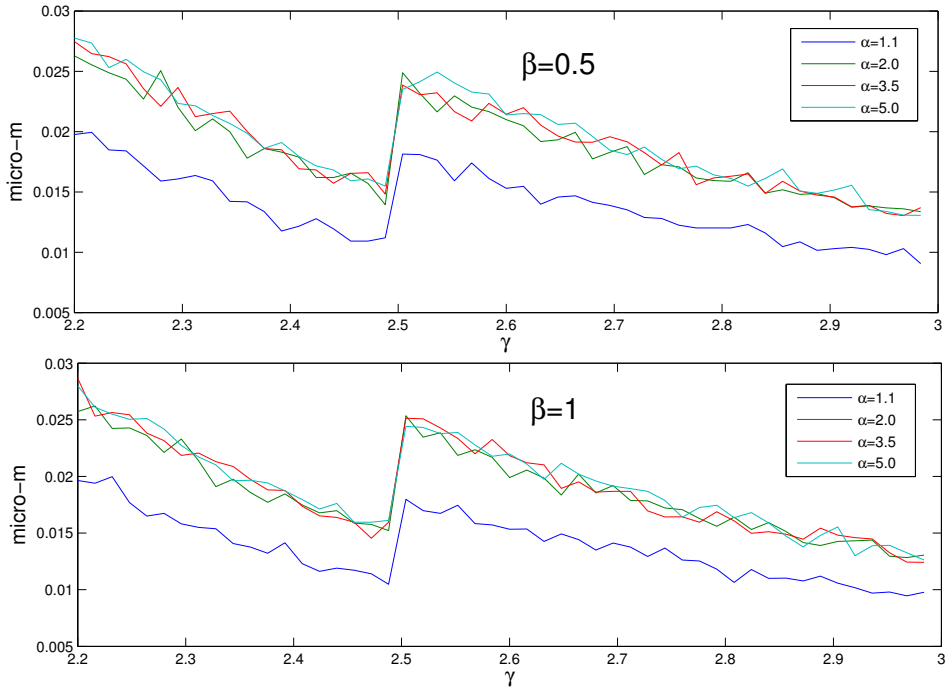

Fig. 7. The micro-matching degree changing with parameter γ for $\beta = 0.5$ and $\beta = 1$.

Results in these two figures show that curves of the matching degrees have clear jump points near $\gamma = 2.5$. For the micro-matching degree, it has a decreasing trend with some fluctuation both before and after the jump point. For the macro-matching degree, it also has a decreasing trend before and after the jump point, which is more obvious than that of the micro-matching degree.

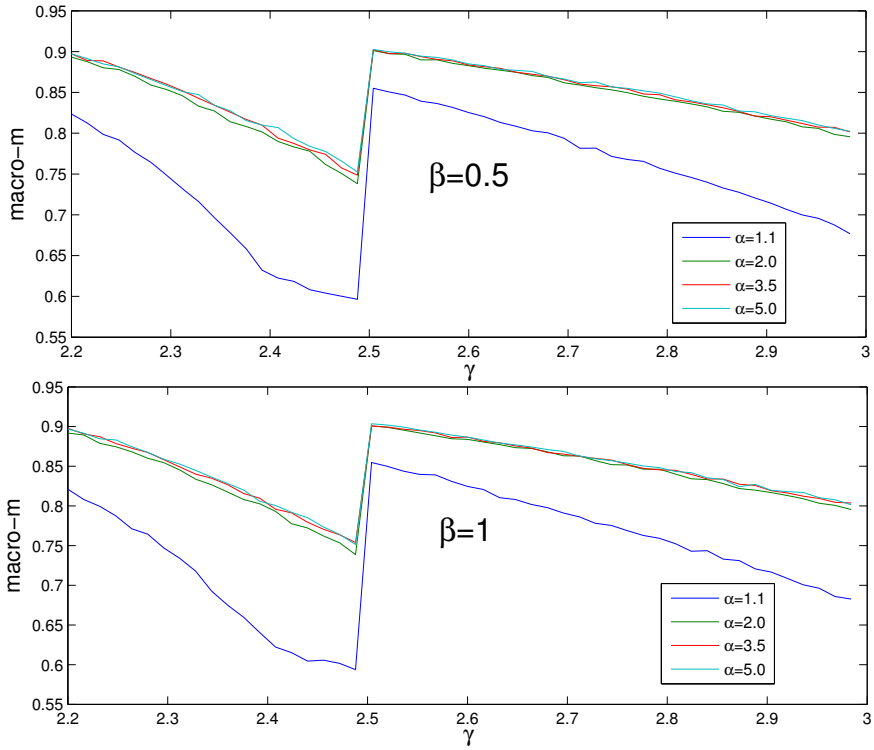

Fig. 8. The micro-matching degree changing with parameter γ for $\beta = 0.5$ and $\beta = 1$.

5. Conclusions

In this paper, we research targeted random attacks on complex networks. If we do not get the concrete structure of a network, we would not know which nodes are the key nodes for the network, and then attacks on the network can only be carried out randomly. It is known that real-world networks have robustness to random attacks. It means that random attacks on these networks cost a lot but cannot achieve significant damage effects. So, in this paper, we propose a mechanism to predict the set of the key nodes for a network, which can considerable save costs of attacks but can work as targeted attacks on the network.

Totally based on node features in the hidden metric space of the network, we put forward the definition of node hidden degree centrality and research the ranking results of nodes according to this centrality. We also calculate the degree centrality of nodes, get the ranking results based on it, and give the definition of the macro-matching degree of these two rankings. According to the simulation results of the macro-matching degree, we find that

while considering the nodes ranked in the first $\beta\%$, most of the key nodes of the network are included in the optional node set that we provide. Our simulations show that when considering the first 1% nodes, the macro-matching degree is going to be more than 75%, when considering the first 0.5% nodes, the macro-matching degree is going to be more than 80%, and the smaller the value of β, the higher the value of the matching degree, which shows that attacks at nodes in the optional set, even if they are random attacks, would be going to be performed at most of those really important nodes. We name it the purposeful random attack, and from the simulation results of this paper, we can conclude that our mechanism for random attacks on networks does not need to know the structure of the network, but can achieve nearly matched effects with targeted attacks, while could greatly save attack costs compared with general random attacks.

Moreover, we study relationships between the matching degrees and the parameters in the hidden metric space of the network by simulations. It shows that the macro-matching degree increases with the growth of the clustering parameter α in the one-dimensional circle model of the hidden metric space, and after α grows to a fixed value, it would basically has no influence on the effectiveness of the attacks according to the mechanism we put forward in this paper. According to simulation results, the curves of the matching degrees have jump points near $\gamma = 2.5$, and before and after the jump points, the matching degrees have decrease trends with the increase of parameter γ. It shows that to research the purposeful random attacks, networks should be divided into two groups according to the value of parameter γ with $\gamma > 2.5$ and $\gamma < 2.5$.

This work is supported by the Scientific Research Level Improvement Quota Project of the Capital University of Economics and Business, China.

REFERENCES

[1] S.N. Dorogovtsev, A.V. Goltsev, J.F.F. Mendes, *Rev. Mod. Phys.* **80**, 1275 (2008).

[2] M.E.J. Newman, *SIAM Rev.* **45**, 167 (2003).

[3] V. Latora, M. Marchiori, *Phys. Rev. Lett.* **87**, 198701 (2001).

[4] R. Guimerá, S. Mossa, A. Turtschi, L.A.N. Amaral, *Proc. Natl. Acad. Sci. USA* **102**, 7794 (2005).

[5] P. Holme, *Adv. Complex Syst.* **6**, 163 (2003).

[6] T.S. Eugene Ng, H. Yan, in: ACM SIGCOMM Workshop on Internet Network Management, 2006.

[7] A.S. Tanenbaum, *Computer Networks*, PH PTR, New Jersey 2004.

[8] S.P. Borgatti, A. Mehra, D. Brass, G. Labianca, *Science* **323**, 892 (2009).

[9] M. Szilagyi, *Qual. Quant.* **25**, 211 (1991).

[10] A.L. Barabási, R. Albert, *Science* **286**, 509 (1999).

[11] L.C. Freeman, *Soc. Networks* **1**, 215 (1979).

[12] G. Canright, K. Engo-Monsen, *Sci. Comput. Program.* **53**, 195 (2004).

[13] S.P. Borgatti, *Soc. Networks* **27**, 1 (2005).

[14] E. Estrada, J.A. Rodríguez-Velázquez, *Phys. Rev. E* **71**, 056103 (2005).

[15] L.C. Freeman, S.P. Borgatti, D.R. White, *Soc. Networks* **13**, 141 (1991).

[16] P.F. Bonacich, *Am. J. Sociol.* **92**, 1170 (1987).

[17] J.D. Noh, H. Rieger, *Phys. Rev. E* **66**, 066127 (2002).

[18] K.A. Stephenson, M. Zelen, *Soc. Networks* **11**, 1 (1989).

[19] E. Katz, P.F. Lazarsfeld, *Personal Influence: The Part Played by People in the Flow of Mass Communications*, The Free Press, New York 1955.

[20] C.C. Aggarwal, *Social Network Data Analytics*, Springer, New York 2012.

[21] S. Aral, D. Walker, *Science* **337**, 337 (2012).

[22] L. Liu, J. Tang, J. Han, S. Yang, *Data Min. Knowl. Disc.* **25**, 511 (2012).

[23] J. Tang, J. Sun, C.Wang, Z. Yang, in: Proceedings of the 15$^{\text{th}}$ ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'09), 2009, pp. 807–816.

[24] J.M. Kleinberg, *J. ACM* **46**, 604 (1999).

[25] D.M. Romero, W. Galuba, S. Asur, B.A. Huberman, in: Proceedings of the 20$^{\text{th}}$ International Conference on World Wide Web (WWW-Poster 2011), 2011, pp. 113–114.

[26] L. Page *et al.*, The PageRank Citation Ranking: Bringing Order to the Web, Technical report, Stanford Digital Library Technologies Project, January 29, 1998, `http://dbpubs.stanford.edu/pub/1999-66`

[27] D. Tunkelang, A Twitter Analog to PageRank, `http://thenoisychannel.com/2009/01/13/a-twitter-analog-to-pagerank/`, 2009.

[28] N. Agarwal, H. Liu, L. Tang, P.S. Yu, in: Proceedings of the International Conference on Web Search and Web Data Mining, 2008, pp. 207–217.

[29] P. Hui, M. Gregory, in: Proceedings of the 1$^{\text{st}}$ Workshop on Social Media Analytics (SOMA '10), 2010, pp. 53–61.

[30] S. Pei, H.A. Makse, *J. Stat. Mech.* **12**, P12002 (2013).

[31] S. Pei *et al.*, *Sci. Rep.* **4**, 5547 (2014).

[32] M. Boguñá, D. Krioukov, K.C. Claffy, *Nature Phys.* **5**, 74 (2009).

[33] A. Muscoloni *et al.*, *Nature Commun.* **8**, 1615 (2017).

[34] W.S. Kennedy, O. Narayan, I. Saniee, `arXiv:1307.0031 [physics.soc-ph]`.

[35] F. Papadopoulos *et al.*, *Nature* **498**, 537 (2012).

[36] J. Kleinberg, *Nature* **406**, 845 (2000).

[37] M.A. Serrano, D. Krioukov, M. Boguñá, *Phys. Rev. Lett.* **100**, 078701 (2008).

[38] M. Boguñá, R.P. Satorras, *Phys. Rev. E* **68**, 036112 (2003).

[39] M. Boguñá, F. Papadopoulos, D. Krioukov, *Nature Commun.* **1**, 62 (2010).

[40] Experts in IT and biological fields consider that new mathematical "hidden metric spaces" principle seems to guide everything from internet routing to neurology, http://www.caida.org/home/

[41] S. Wasserman, K. Faust, *Social Network Analysis: Methods and Applications*, Cambridge University Press, London 1994.

[42] M. Cha, H. Haddadi, F. Benevenuto, K.P. Gummadi, in: Proceedings of the 4$^{\text{th}}$ International AAAI Conference on Weblogs and Social Media, 2010, pp. 10–17.

[43] J. Tang, T. Lou, J. Kleinberg, in: Proceedings of the 5$^{\text{th}}$ ACM Conference on Web Search and Data Mining, 2012, pp. 743–752.

[44] P. Mahadevan *et al.*, *SIGCOMM Comput. Commun. Rev.* **36**, 17 (2006).

[45] M. Boguñá, R.P. Satorras, A.D. Guilera, A. Arenas, *Phys. Rev. E* **70**, 056122 (2004).