Hindawi
Mathematical Problems in Engineering
Volume 2017, Article ID 6108563, 9 pages
https://doi.org/10.1155/2017/6108563

Research Article

Combined Heuristic Attack Strategy on Complex Networks

Marek Šimon, Iveta Dirgová Luptáková, Ladislav Huraj, Marián Host'ovecký, and Jiří Pospíchal

Department of Applied Informatics and Mathematics, University of Ss. Cyril and Methodius, J. Herdu 2, 917 01 Trnava, Slovakia

Correspondence should be addressed to Iveta Dirgová Luptáková; iveta.dirgova@ucm.sk

Received 10 March 2017; Revised 28 June 2017; Accepted 14 August 2017; Published 18 September 2017

Academic Editor: Sebastian Heidenreich

Usually, the existence of a complex network is considered an advantage feature and efforts are made to increase its robustness against an attack. However, there exist also harmful and/or malicious networks, from social ones like spreading hoax, corruption, phishing, extremist ideology, and terrorist support up to computer networks spreading computer viruses or DDoS attack software or even biological networks of carriers or transport centers spreading disease among the population. New attack strategy can be therefore used against malicious networks, as well as in a worst-case scenario test for robustness of a useful network. A common measure of robustness of networks is their disintegration level after removal of a fraction of nodes. This robustness can be calculated as a ratio of the number of nodes of the greatest remaining network component against the number of nodes in the original network. Our paper presents a combination of heuristics optimized for an attack on a complex network to achieve its greatest disintegration. Nodes are deleted sequentially based on a heuristic criterion. Efficiency of classical attack approaches is compared to the proposed approach on Barabási-Albert, scale-free with tunable power-law exponent, and Erdős-Rényi models of complex networks and on real-world networks. Our attack strategy results in a faster disintegration, which is counterbalanced by its slightly increased computational demands.

1. Introduction

Complex networks keep attracting an increasing amount of attention during the past couple of decades. This can be illustrated by a number of documents in Scopus search results for this term in the title, abstract, or key words, from 605 documents in 1986, 2372 documents in 1996, 8086 documents in 2006, and up to 20256 documents in 2016 [1]. The existence of such networks is being discovered in many areas of nature as well as society, for example, in biology as neural networks, networks of protein reactions, or plant immune signaling networks, in transport, in economics, in sociology as citation or rumor spreading networks, in computer science as the Internet, and in physics as power grids [2–6]. Mostly, these networks are considered a positive thing. A number of studies are devoted to measuring the robustness of such networks against a malicious attack or against a random degradation failure causing deletion of a node or of a connection. Such measures are used to increase security of complex systems and where possible, like in computer networks, to increase robustness, for example, by rewiring optimization [7–13].

Only in recent years, more attention has been given to malicious networks. Under such term, terrorist networks, fake-news spreading networks, malnets or botnets used in DDoS attacks, or for spreading worms and viruses, dark networks involved in various criminal activities like illegal arm selling or child pornography, and so forth can be understood [14–20]. Attack strategies on such harmful complex networks (i.e., node deletion and occasionally also edge deletion) are studied in [21–23]. For example, in terrorist networks, a sequence of individuals should be identified, whose arrest will result in the maximum breakdown of communication between remaining individuals in the network. Similar approach should work for disabling Internet access to computers used for illegal activities. Apart from networks, where the aim of the involved individuals is malicious, there exist also networks, where the harm is unintentional, but, which should nevertheless be quickly disabled. These involve spread of disease, where the goal is to design vaccination

strategies to restrain the spread of pandemic diseases, when mass vaccination is an expensive process and only a specific number of people, modeled as nodes of a graph, can be vaccinated. Another example is cascading failures (blackouts) of electric power transmission network, where the goal is to prevent a total breakdown of power network by inhibiting some power transmission points or lines. Similar approach involves, for example, immunization of disease carriers [24, 25] or critical node detection [26–28], where the sequence of deletion order is not taken into account, and only the optimum subset of nodes selected for deletion is important. Lately, a more computationally demanding approach to network disintegration and attack, using stochastic and evolutionary optimization, is applied on smaller scale networks, providing better results than traditional approaches [29–32].

A related topic to edge deleting attacks is also community detection problem, because a network can be most easily dismantled by removing the edges between communities [34]. Therefore, a fast community detection algorithm can be used for edge network attack; and vice versa, approaches useful in edge removing attacks can be used in community detection.

Practically the same approach to the network disintegration measure as in network attacks can be found in Morone et al. [35–37]. They use collective influence algorithm to find the minimal set of influencers. Their algorithm has complexity $O(N \log N)$ in [35, 37], where N is the number of nodes, followed by an algorithm with improved results but worse complexity $O(N^2)$ in [37]. A number of related algorithms were inspired by this approach, a good survey of the topic is in [38].

Lately, Hirsch index and its generalization [39], leading eventually to coreness value, were proposed to be a good indicator of influence of nodes. This assumption was further critically analyzed in [40].

Attack strategies are important not only as a countermeasure against harmful networks but also for potential improvements in useful engineering networks. It is popular to study the robustness of networks, but the network disruptions are usually chosen either at random or by very simple targeting methods. In engineering, it is very important to know the worst-case scenario for vulnerability analysis, which our paper addresses.

In the attack algorithms, apart from the quality of results, which are measured by the level of network disintegration, also the complexity of these algorithms matters. While the approach of Morone et al. [35, 36] can handle hundreds of millions of nodes within hours of computation, tabu search approach [29] can handle a few hundred nodes in the same time, but it should provide better results.

In this paper, we shall describe new heuristics for attack strategies, merge them in a newly designed combination of new and classical attack heuristics, and investigate the effectiveness of this new approach both on model networks and on a couple of real-world collaboration networks. Our approach should find its niche on the Pareto optimal front somewhere between collective influence approaches [35, 36] and stochastic optimization approaches [29], both in the terms of the quality of results and in the computational time.

2. Materials and Methods

2.1. Networks, Their Types, Models, and Measures of Robustness. In the beginning of studies of networks, a model network was considered simply as a large random graph, typically rather sparse (i.e., its number of edges is much smaller than that in a complete graph). Random ER (Erdős-Rényi) graphs [41] start from unconnected nodes, which are then connected with a uniform probability. They have a Gaussian bell-shaped degree (number of connections to other nodes) distribution and couples of nodes have a short average path; that is, almost any node can be reached from any other node by going through a relatively small number of edges. Neighbors of any node are not likely mutually connected (low number of triangles corresponds to low clustering coefficient).

It has been discovered that in most real-world networks the neighbors of a node are likely connected to each other, while the property of having short average paths is satisfied. More exactly, a small-world network is characterized by an average distance growing proportionally to the logarithm of the number N of nodes in the network. First such models by Watts and Strogatz (1998) [42] were created by rewiring (with a certain probability) connections between the nodes in a regular graph. However, such graphs had very narrow degree distribution, while most of discovered small-world networks had so-called "long tail" distribution, where there are a few nodes with a very high degree. A new type of network, a scale-free one, where zooming on any part of the distribution does not change its shape, has a degree distribution where the fraction $P(k)$ of nodes of degree k asymptotically follows $P(k) = k^{-\gamma}$ where parameter γ is usually in the range $2 < \gamma < 3$.

Typical example of a scale-free network is the Barabási-Albert model starting with a few nodes (e.g., a triangle), where one node is added at a time and connected with a given number of nodes which already exist in the network. The new edges are attached to these nodes selected pseudorandomly with a probability of attachment corresponding to their current degree, so-called linear preferential attachment $\prod_{(k_i)} = k_i / \sum_j k_j$.

A simplest type of attack on a network is to delete its node(s) together with its/their connections, which will cause the greatest damage. However, a number of possible selections of a set of m nodes to be deleted from all the network nodes n are a binomial coefficient $C(n, m)$, leading to combinatorial explosion for larger values.

Network damage can be established by various measures. One possible measure is a probability of a presence of a giant component, which Molloy-Reed criterion [43] defined as a threshold of division of average of squared degrees of nodes divided by average of degrees of nodes. However, this criterion, while easily calculable, is derived for random graph and randomly deleted nodes, not for nodes deleted by heuristic methods, which targets nodes pseudorandomly or deterministically. Another measure is an average inverse geodesic (average inverse of the shortest path length between all pairs of nodes) [44]. This measure would be suitable for a slightly damaged network, which is still fully connected as one component. We are interested in the more substantial

destruction of the network. Therefore, we use in our paper a measure of network damage R, Unique Robustness Measure (R-index) [45, 46], defined as

$$R = \frac{1}{N} \sum_{Q=1}^{N} S(Q), \tag{1}$$

where N is the number of nodes in the network and $S(Q)$ is the fraction of nodes in the largest connected component after removing $Q = Nq$ nodes using a given strategy. The variable q is a current fraction of deleted nodes against the total initial number N of network nodes. The R-index thus encompasses the whole attack process, not just one moment of damage at a current fraction q.

2.2. Classical Attack Strategies. Finding the least number of nodes, whose removal would result in unconnected components of the network, is proved in graph theory to be an NP complete problem. A simplified problem is to find such a subset of nodes, that after their removal the remaining nodes shall be isolated. This problem is a reformulation of a node cover of a graph, which is a set of vertices such that each edge of the graph is incident to at least one vertex of the set. To find node cover is one of the famous Karp's 21 NP complete problems [47]. This leads us to the necessity to use heuristics for the network attack.

In the most typical so-called ID attack, the nodes are deleted in descending order of their degrees [48]. The degrees are calculated and ordered only once in the original network, which is the least computationally demanding strategy of all the attack strategies. The calculation of degree centrality requires $O(E)$ time in a sparse matrix representation, where E is the number of connections. A more efficient but slightly more demanding strategy known as RD recalculates the order of degrees after each removal of a node [49]. Similar couples of approaches, that is, calculating the sequence of nodes to be deleted all at once from the original network, or recalculating this sequence after each node removal, can be applied to all other centrality measures, that is, betweenness, closeness, Katz, and eigenvector centrality [50]. After RD approach, the second most effective measure generally was proved to be the betweenness centrality RB, recalculated after deletion of each node. Often used is also betweenness centrality calculated only once for the original network, named IB [50]. The betweenness centrality of a node v is defined as

$$g(v) = \sum_{t \neq u \neq v} \frac{\sigma_{tu}(v)}{\sigma_{tu}}, \tag{2}$$

where σ_{tu} is the number of shortest paths between nodes t and u and $\sigma_{tu}(v)$ is the number of those paths which contain node v. Since the test networks do not have weighted connections, Brandes' algorithm [51] requiring $O(N\ E)$ can be used, where N is the number of nodes.

As in many other areas of optimization of NP problems, there exist first attempts to use a metaheuristic optimization for selection of nodes to be deleted. An example of this approach is a tabu search usage [29]. The approach seems to improve R index measure of the RD attack by roughly 15 percent, but the expense is enormous, as in most metaheuristics. It requires tens of thousands of evaluations (it uses a local optimization, and, as the termination criterion, 1000 calculations are carried out when no improvement is reached; if there is an improvement in the thousands of calculations, the cycle starts all over).

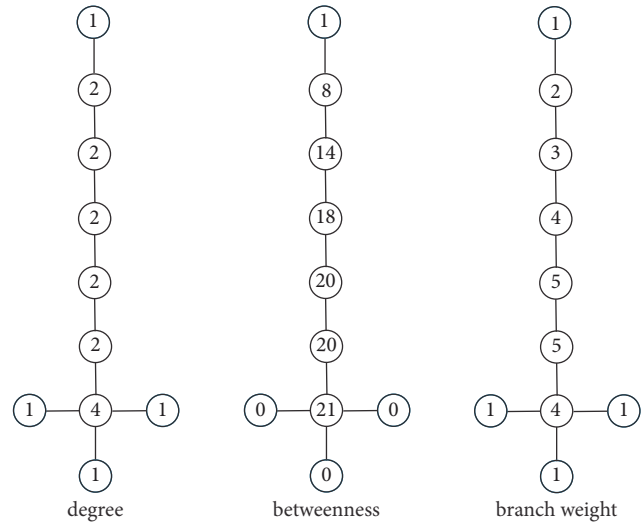

Figure 1: Degree, betweenness, and branch weight evaluation of nodes.

2.3. Branch Removal Strategy. Both the degree and betweenness criterion work very well most of the time to identify the nodes, whose removal is most likely to break the component apart, so that the largest remaining component is as small as possible. However, for an already sparse component with a large branch, these centrality measures may not always be ideal. Let us have a simple component of a network as an example, containing a tree with 10 nodes, where on the end of a linear "network" the last node has four neighbors; see Figure 1. When attack strategy would be guided by maximum degree, the node with degree 4 would be deleted, leaving the largest connected component with six nodes (the "linear part" of the tree above the deleted node). The same node with the maximum betweenness equal to 21 would be selected using the betweenness based attack. However, when we would evaluate each node by a number of nodes, by which the largest common component would be diminished, if we would delete the node, then nodes with values equal to five in the last network in Figure 1 would be selected. This would leave the largest connected component with five nodes which provides better result than both the degree and the betweenness attack.

How to arrive to the branch weight evaluation of nodes? Firstly, all the nodes with a degree equal to 1 will be assigned by weight 1, and all nodes with other degrees will have weight 0. Then, recursively, (1) the nodes will be weighted by the sum of the weights of their neighbors of degree 1. This sum will be increased by 1 (for the node itself), unless the resulting weight would be more than half of the number of nodes of the component; (2) the nodes of degree one will be cut off for

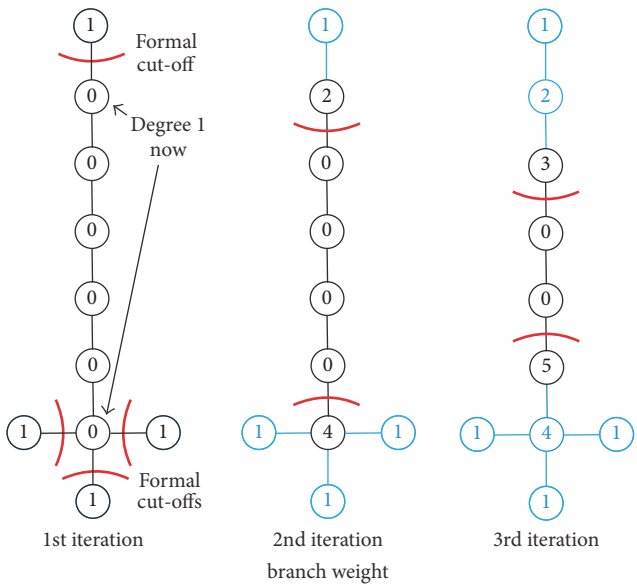

Figure 2: Iterations of branch weight evaluation of nodes: the blue colored vertices are formally cut off, so that their black colored neighbors formally change their degree to 1.

the sake of calculation (so that the degree of their neighbor is decreased by 1, while its weight remains the same).

If the network is a tree with N nodes, the recursive weighting by the sum of neighbors of degree 1 and their cutting off continues until only two nodes remain. When the number of nodes N is even, the weights of two remaining nodes are $N/2$; for odd N, the weights of two remaining nodes are $N/2-1$ and $N/2+1$. The other termination criterion of weighting evaluation is when the evaluated node is a part of a cycle. The iterative node evaluation by branch weighting is shown in Figure 2.

After the third iteration in Figure 2, the evaluation directly above the node with weight 5 is stopped (its weight would be more than a half of the component size), while the zero weighted node below the node weighted 3 is weighted by 4 and then in another iteration the node below is weighted by 5.

The computational complexity of the branch weighting clearly does not exceed the betweenness complexity. Unfortunately, the branch weight strategy can be applied only when at least some nodes of the network are not part of a cycle. This constraint is usually not satisfied for more complex networks, at least at the beginning of the attack; therefore, this attack strategy must be combined with another attack strategy. Moreover, even if a branch exists, it might be more advantageous in further stages to remove a node of high degree and betweenness, which is a part of a cycle, than to remove a node of low degree and betweenness that would cut off say only small branch. This is the reason for combination of the strategies.

2.4. Combination of Heuristics. It is clear that each of the heuristics stresses of different aspects of the problem and their combination might produce better results than any of the heuristics applied separately. However, how to produce the best combination? In multiple-criteria decision-making, the simplest approach is to weight single attributes and produce the resulting evaluation by adding the weighting score. After local optimization of weights, such combination produced the best results for the degree and branch weight heuristics, where the resulting weight of a node was calculated by

$$\text{weight (node)} = \alpha \times \text{degree (node)} + (1-\alpha) \times \text{branch\_weight (node)}. \quad (3)$$

The parameter α is bounded by $0 \le \alpha \le 1$. Another possible approach is a multiplicative score, when the resulting weight is obtained by multiplication of factors and their weights are used as exponents. Empirical local optimization trials resulted in the addition of weighted scores of degree, branch weight, and betweenness. The resulting measure used for selection of a node to be deleted was thus defined as

$$\text{weight (node)} = \alpha \times \text{degree (node)} + (1-\alpha-\beta) \times \text{branch\_weight (node)} + \beta \times \text{betweenness (node)}. \quad (4)$$

Parameters α and β are bounded by $0 \le \alpha \le 1$, $0 \le \beta \le 1$, $0 \le \alpha + \beta \le 1$. This criterion with its weight constants was produced by a local optimization for a set of Barabási-Albert model networks generated with a given set of parameters described further. While the results proved to be advantageous, it is entirely possible that other types of networks might require a different combination or at least slightly different weights α, β.

2.5. Reverse Build-Up Strategy. In the classical attacks, we use greedy heuristics to delete nodes, which would most advantageously disrupt the network. However, we can take another approach. We can start from an empty network, or a disrupted network, where only nodes of degree one and zero exist, and build the network by adding the nodes, which would connect the network as little as possible at a time. When we reverse the sequence of added nodes, we get the sequence of nodes for deletion.

In the beginning, we take the first evaluation of nodes for the complete network by the combined heuristics in our calculation. Then we start from a network with nodes of degree at most one, produced by a combination of previously described heuristics. Recursively, we try to add each of the deleted nodes and select the one, in which addition results in the smallest number of nodes of the largest component of the build-up network. If several nodes satisfy the criterion, we add the node with the smallest preference of the combined heuristics evaluated for the complete network.

While in the beginning of adding nodes, we cannot get worse results than we got during deletion of nodes, at the end of attaching of nodes, Q values might be bigger than those for the original sequence might.

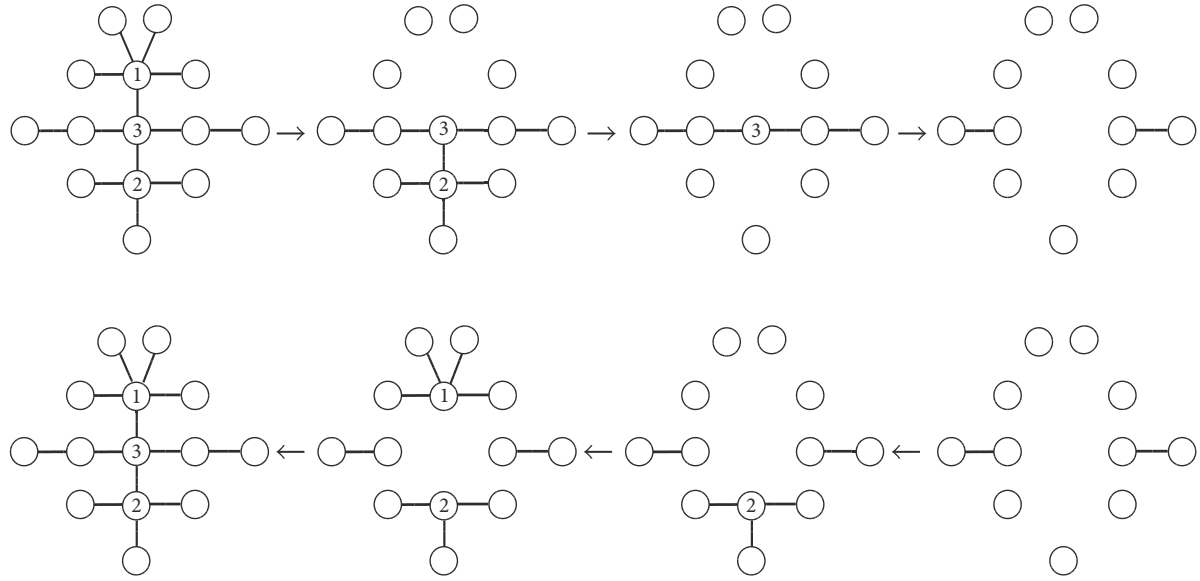

Figure 3: Example of reverse build-up strategy.

Table 1: R-values for various types and combinations of attacks and networks.

Network	Barabási-Albert		Erdős-Rényi		Scale-free $\gamma = 4.5$		Erdos991	polblogs
Attack type	R	SD(R)	R	SD(R)	R	SD(R)	R	R
ID	0.221713	0.008080	0.353849	0.011350	0.309254	0.003846	0.175308	0.121236
IB	0.227784	0.008715	0.358559	0.010636	0.314423	0.006829	0.183182	0.142251
RD	0.197184	0.005145	0.292670	0.006801	0.254578	0.002685	0.135383	0.103740
RB	0.189197	0.008954	0.275701	0.006297	0.239698	0.003942	0.106413	0.074570
Equation (3)	0.191293	0.005200	0.286642	0.007355	0.249797	0.003264	0.135383	0.103740
Equation (4)	0.182394	0.003859	0.275700	0.006298	0.240187	0.004437	0.106396	0.074039
Rev (see (4))	0.178483	0.004562	0.271771	0.008002	0.234166	0.004308	0.103963	0.080134
CI	0.219380	0.006931	0.315197	0.008498	0.293521	0.004947	0.125509	0.100185
H1	0.271769	0.014294	0.407317	0.009088	0.368555	0.007733	0.179723	0.139189
H2	0.287601	0.018629	0.418594	0.007187	0.397841	0.005653	0.212845	0.169600

Let us have as an example a simple tree as the first network in Figure 3. To keep the example simple, we shall use only degree-based strategy RD. In this strategy, the first deleted node has index 1 with degree 5, the second in the resulting network to the right is node indexed 2 with degree 4, and the third deleted node is, for example, node 3 with degree 2. The resulting network on the right has only two components of size 2. In the second row of Figure 3, we continue from the right to the left. From the 3 available deleted nodes, if we add node 2 first, the smallest component has 4 nodes instead of 5. When we add node 1, the greatest component has 5 nodes instead of 10 above. Therefore, when we delete the nodes in sequence $3, 1, 2$ we get the sizes of the largest component $12, 5, 4, 2$ instead of $12, 9, 5, 2$ by sequence $1, 2, 3$. The sequence of the sizes of the largest component $12, 5, 4, 2$ results in smaller R index value. Since in each iteration we require to try to add each of the deleted nodes, the computational complexity of the approach is $O(N^2)$, similar to betweenness centrality.

3. Results and Discussion: Testing the Combined Heuristics Attack

In order to test our proposed heuristic strategies and their combination in the attack, we compared them against the four most popular and successful strategies based on degree and betweenness, namely, RD, RB, ID, and IB, described in Section 2.2, as well as against one of the state-of-the-art strategies (CI strategy in Table 1) based on collective influence [35, 36]. Additionally, the currently popular Hirsch index (H1 strategy in Table 1) and its second-order generalization [40] (H2 strategy in Table 1) were used in tests, but they did not bring improved results compared to other strategies. Our results for Hirsch index and its generalization support results in [38] where strategies using the Hirsch index as well as coreness have worse results in robustness measure R than strategy using degree centrality. To estimate usefulness of the single strategies in the combined attack, we first used a combination of degree centrality and branch removal weight

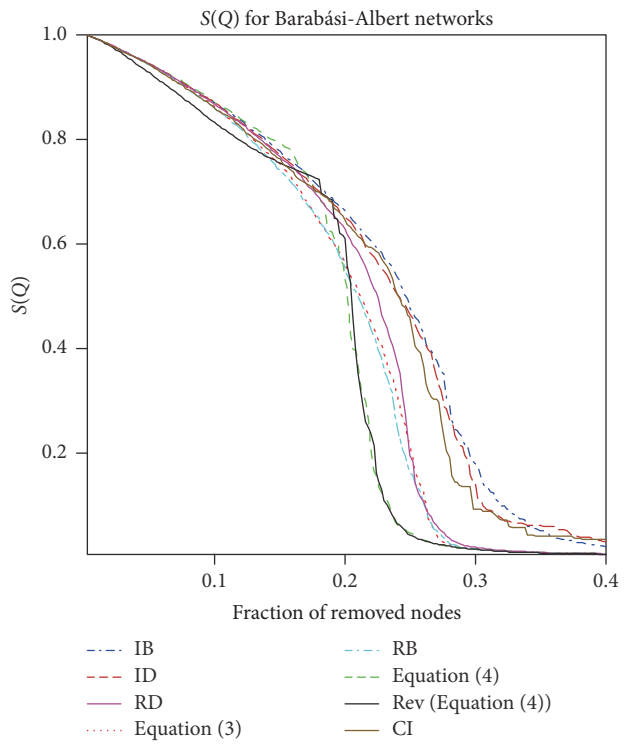

Figure 4: Means of $S(Q)$ values for attacks of all the strategies from Table 1 on Barabási-Albert networks.

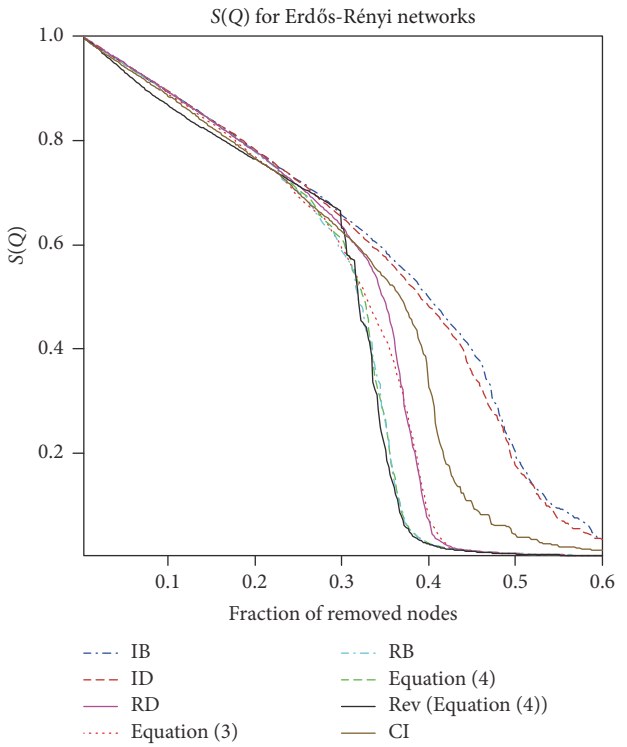

Figure 5: Means of $S(Q)$ values for attacks of all the strategies from Table 1 on Erdős-Rényi networks.

described by (3) with parameter $\alpha = 0.15$, (see (3) strategy in Table 1). To this approach we added first betweenness centrality; the combined strategy is described by (4) with parameters $\alpha = 0.15$ and $\beta = 0.1$ (see (4) strategy in Table 1). When the network would be destroyed to the degree, when only solitary edges and single vertices remain, we then used the nodes deleted in this process in the reverse build-up strategy (Rev (see(4)).

Similar to [29], we tested attack strategies on the networks produced by the BA preferential attachment model, generated by starting with a triangle and adding each time a node together with 3 edges and on ER random network model with $P = 0.012$. Further, we also tested attack strategies on random scale-free networks with a tunable parameter γ. We set the scale-free network with $\gamma = 4.5$ and with 1500 connections [52, 53]. We used 10 randomly generated networks with 500 nodes in all three test sets.

For the real-world network, we used collaboration network Erdos991 from repository [54] with 492 nodes and 1417 edges, originally coming from Pajek dataset [55], and the political blogosphere web, polblogs, with 643 nodes and 2280 edges, also from [54], which originated from [33]. Results of R values for all the attack strategies and all the types of networks can be found in Table 1. Since the real-world network tests provide just single R values, their standard deviation could not be calculated. The averages of $S(Q)$ values for all the tested strategies against the fraction q of removed nodes are shown for the BA networks in Figure 4, for the ER networks in Figure 5, and for the scale free network with $\gamma = 4.5$ in Figure 6. For the collaboration and polblog networks the resulting $S(Q)$ values are shown in Figures 7 and 8.

4. Conclusions

Our combined heuristic attack strategy improved destruction of network measure R for the collaboration network Erdos991 by more than 23 percent, for political blogosphere by 29 percent, for the Barabási-Albert model by more than 9 percent, for another scale-free model with $\gamma = 4.5$ by more than 8 percent, and for the Erdős-Rényi networks by 7 percent, compared to most popular RD attacks. Combined heuristics also achieved better results compared to RB attack, though less substantial. Even a comparison to the state-of-the-art algorithm CI [35, 37] is favorable, but this is counterbalanced by higher complexity of our algorithmic approach. The variability in results for different types of networks suggests that there might exist other types of networks, where the combined heuristic attack might not be advantageous. Moreover, even for networks similar to the Barabási-Albert model, none of the attack heuristics or approaches can be named a winner. While our combination of heuristics provided better results than the most popular and most useful single-heuristic strategy RD; it also required more computational resources for the betweenness, branch removal weight and the build-up strategy. Our current results are likely comparable to tabu search described in [29], while taking substantially less computational time. A suitable

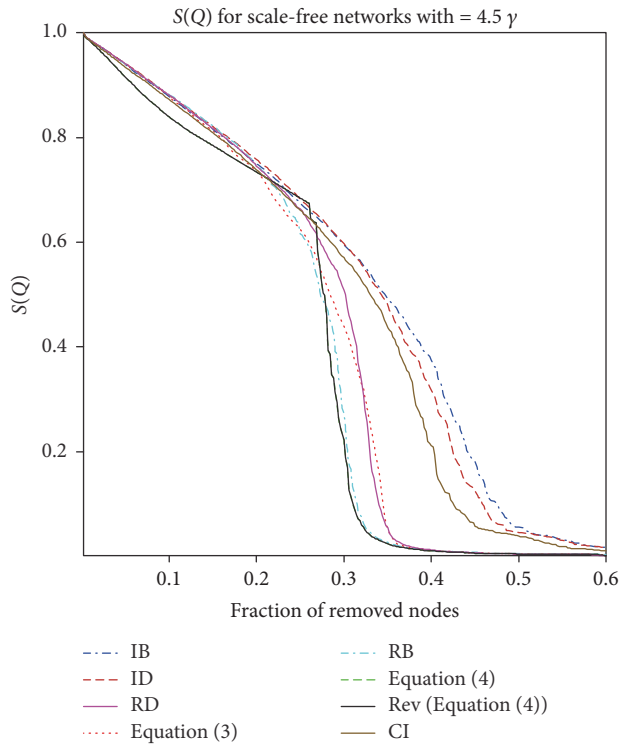

Figure 6: Means of $S(Q)$ values for attacks of all the strategies from Table 1 on scale-free networks with $\gamma = 4.5$.

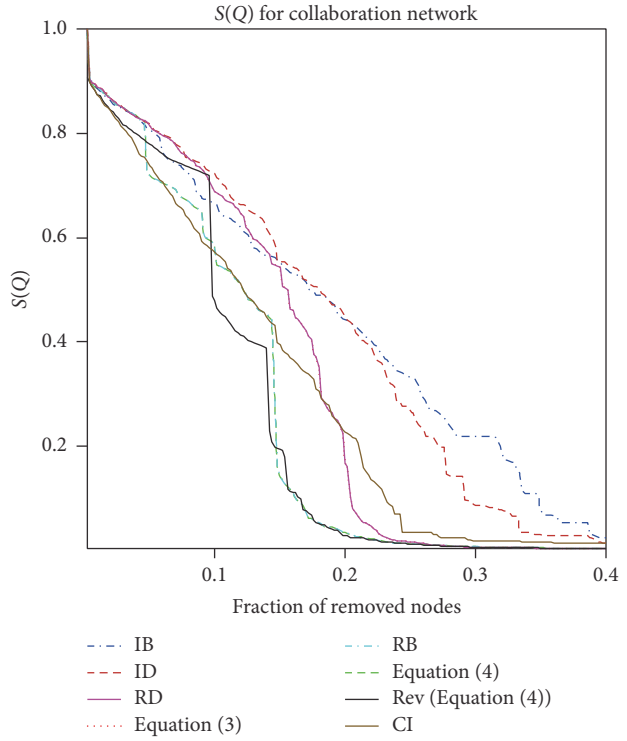

Figure 7: $S(Q)$ values for attacks of all the strategies from Table 1 on collaboration network Erdos991. The RD and (3) lines overlap; the branch removal brings no advantage here.

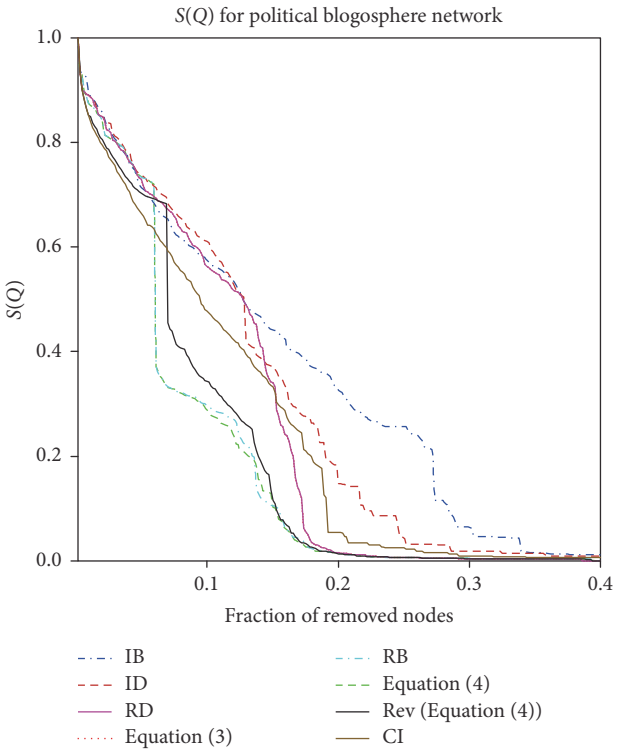

Figure 8: $S(Q)$ values for attacks of all the strategies from Table 1 on political blogosphere, polblog [33]. The RD and (3) lines overlap; the branch removal brings no advantage here; reverse build-up strategy, Rev (see (4)), actually provides worse results than (4), even though at the beginning it is better, as well as the CI strategy.

parametrized and adjusted stochastic evolutionary optimization is likely to provide even better results, at the expense of orders of magnitude growth of computing resources. On the other hand, the classical RD attack requires not only fewer computing resources (it has $O(N)$ complexity) but also substantially less information about the structure of the network compared to all other strategies, heuristic or metaheuristic. The collective influence approach, CI [35, 36], with only slightly worse complexity $O(N \log N)$ than that of RD approach typically provides better results both for model and for real-world networks. Our combined heuristic attack strategy can be currently claimed as Pareto optimal, giving, for networks with few thousands nodes, reasonable tradeoff between execution time and the measure of network destruction.

We do not claim that our current set of methods and/or parameters are optimal. However, our aim is to show that when someone is interested in the best results for certain types of networks, it is worthwhile to try a combination of approaches, such as the case described in our manuscript.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The work was supported by Grant APV SK-SRB-2016-0003: *Adaptation of Parallel WoBInGO Framework for Protection of Cloud and Grid Computing Systems by Computational Intelligence*.

References

[1] Scopus, "abstract and citation database of peer-reviewed literature," 2017, https://www.scopus.com/.

[2] A.-L. Barabási, *Network Science*, Cambridge University Press, 2016.

[3] M. E. J. Newman, *Networks: An Introduction*, Oxford University Press, Oxford, UK, 2010.

[4] M. O. Jackson, *Social and economic networks*, Princeton University Press, Princeton, NJ, USA, 2008.

[5] L. Cabyova and J. Ptacin, "Benchmarking comparison of marketing communication of universities in Slovakia," in *Communication Today*, vol. 1, pp. 54–69, 2014.

[6] C.-H. Huang, T.-H. Chen, and K.-L. Ng, "Graph theory and stability analysis of protein complex interaction networks," *IET Systems Biology*, vol. 10, no. 2, pp. 64–75, 2016.

[7] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[8] G. Paul, T. Tanizawa, S. Havlin, and H. E. Stanley, "Optimization of robustness of complex networks," *European Physical Journal B*, vol. 38, no. 2, pp. 187–191, 2004.

[9] O. Lordan, J. M. Sallan, P. Simo, and D. Gonzalez-Prieto, "Robustness of the air transport network," *Transportation Research Part E: Logistics and Transportation Review*, vol. 68, pp. 155–163, 2014.

[10] Y. Koç, M. Warnier, P. Van Mieghem, R. E. Kooij, and F. M. Brazier, "The impact of the topology on cascading failures in a power grid model," *Physica A. Statistical Mechanics and its Applications*, vol. 402, pp. 169–179, 2014.

[11] M. Korytar and D. Gabriska, "Integrated security levels and analysis of their implications to the maintenance," *Journal of Applied Mathematics, Statistics and Informatics*, vol. 10, no. 2, pp. 33–42, 2014.

[12] M. Zhou and J. Liu, "A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks," *Physica A: Statistical Mechanics and its Applications*, vol. 410, pp. 131–143, 2014.

[13] J. Thomas, S. Ghosh, D. Parek, D. Ruths, and J. Ruths, "Robustness of network controllability to degree-based edge attacks," *Studies in Computational Intelligence*, vol. 693, pp. 525–537, 2017.

[14] J. Xu and H. Chen, "The topology of dark networks," *Communications of the ACM*, vol. 51, no. 10, pp. 58–65, 2008.

[15] P. A. C. Duijn, V. Kashirin, and P. M. A. Sloot, "The relative ineffectiveness of criminal network disruption," *Scientific Reports*, vol. 4, article 4238, 2014.

[16] P. A. Duijn and P. P. Klerks, "Social network analysis applied to criminal networks: recent developments in dutch law enforcement," in *Networks and Network Analysis for Defence and Security*, A. J. Masys, Ed., Lecture Notes in Social Networks, pp. 121–159, Springer International Publishing, Cham, 2014.

[17] M. R. D'Orsogna and M. Perc, "Statistical physics of crime: A review," *Physics of Life Reviews*, vol. 12, pp. 1–21, 2015.

[18] S. Agreste, S. Catanese, P. De Meo, E. Ferrara, and G. Fiumara, "Network structure and resilience of Mafia syndicates," *Information Sciences*, vol. 351, pp. 30–47, 2016.

[19] C. Z. Marshak, M. P. Rombach, A. L. Bertozzi, and M. R. D'Orsogna, "Growth and containment of a hierarchical criminal network," *Physical Review E - Statistical, Nonlinear, and Soft Matter Physics*, vol. 93, no. 2, Article ID 022308, 2016.

[20] N. F. Johnson, P. Manrique, and P. M. Hui, "Modeling insurgent dynamics including heterogeneity: a statistical physics approach," *Journal of Statistical Physics*, vol. 151, no. 3-4, pp. 395–413, 2013.

[21] L. K. Gallos, R. Cohen, F. Liljeros, P. Argyrakis, A. Bunde, and S. Havlin, *Attack Strategies on Complex Networks*, vol. 3993 of *Lecture Notes in Computer Science*, 2006.

[22] M. Bellingeri, D. Cassi, and S. Vincenzi, "Efficiency of attack strategies on complex model and real-world networks," *Physica A: Statistical Mechanics and its Applications*, vol. 414, pp. 174–180, 2014.

[23] T. Nie, Z. Guo, K. Zhao, and Z.-M. Lu, "New attack strategies for complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 424, pp. 248–253, 2015.

[24] R. Pastor-Satorras and A. Vespignani, "Immunization of complex networks," *Physical Review E*, vol. 65, no. 3, Article ID 036104, 2002.

[25] R. Cohen, S. Havlin, and D. Ben-Avraham, "Efficient immunization strategies for computer networks and populations," *Physical Review Letters*, vol. 91, no. 24, Article ID 247901, 2003.

[26] A. Arulselvan, C. W. Commander, L. Elefteriadou, and P. M. Pardalos, "Detecting critical nodes in sparse graphs," *Computers and Operations Research*, vol. 36, no. 7, pp. 2193–2200, 2009.

[27] A. Veremyev, O. A. Prokopyev, and E. L. Pasiliao, "Critical nodes for distance-based connectivity and related problems in graphs," *Networks*, vol. 66, no. 3, pp. 170–195, 2015.

[28] B. Addis, R. Aringhieri, A. Grosso, and P. Hosteins, "Hybrid constructive heuristics for the critical node problem," *Annals of Operations Research*, vol. 238, no. 1-2, pp. 637–649, 2016.

[29] Y. Deng, J. Wu, and Y.-j. Tan, "Optimal attack strategy of complex networks based on tabu search," *Physica A. Statistical Mechanics and its Applications*, vol. 442, pp. 74–81, 2016.

[30] X. Zhang, J. Wu, H. Wang, J. Xiong, and K. Yang, "Optimization of disintegration strategy for multi-edges complex networks," in *Proceedings of the IEEE Congress on Evolutionary Computation (CEC '16)*, pp. 522–528, July 2016.

[31] M. Lozano, C. García-Martínez, F. J. Rodríguez, and H. M. Trujillo, "Optimizing network attacks by artificial bee colony," *Information Sciences*, vol. 377, pp. 30–50, 2017.

[32] R. Aringhieri, A. Grosso, P. Hosteins, and R. Scatamacchia, "A general Evolutionary Framework for different classes of Critical Node Problems," *Engineering Applications of Artificial Intelligence*, vol. 55, pp. 128–145, 2016.

[33] L. A. Adamic and N. Glance, "The political blogosphere and the 2004 U.S. Election: Divided they blog," in *Proceedings of the 3rd International Workshop on Link Discovery (LinkKDD '05)*, pp. 36–43, ACM, 2005.

[34] B. R. Da Cunha, J. C. González-Avella, and S. Gonçalves, "Fast fragmentation of networks using module-based attacks," *PLoS ONE*, vol. 10, no. 11, Article ID e0142824, 2015.

[35] F. Morone and H. A. Makse, "Influence maximization in complex networks through optimal percolation," *Nature*, vol. 524, no. 7563, pp. 65–68, 2015.

[36] "Webpage of Complex Networks and Soft Matter Lab of Hernan Makse at the Levich Institute and Department of Physics of City College of New York," 2015, http://www-levich.engr.ccny.cuny.edu/webpage/hmakse/, http://www-levich.engr.ccny.cuny.edu/~hernanlab/uploads/CI_HEAP.c.

[37] F. Morone, B. Min, L. Bo, R. Mari, and H. A. Makse, "Collective Influence Algorithm to find influencers via optimal percolation in massively large social media," *Scientific Reports*, vol. 6, Article ID 30062, 2016.

[38] L. Lü, D. Chen, X.-L. Ren, Q.-M. Zhang, Y.-C. Zhang, and T. Zhou, "Vital nodes identification in complex networks," *Physics Reports*, vol. 650, pp. 1–63, 2016.

[39] L. Lü, T. Zhou, Q.-M. Zhang, and H. E. Stanley, "The H-index of a network node and its relation to degree and coreness," *Nature Communications*, vol. 7, Article ID 10168, 2016.

[40] R. Pastor-Satorras and C. Castellano, "Topological structure and the H index in complex networks," *Physical Review E*, vol. 95, no. 2, Article ID 022301, 2017.

[41] P. Erdos and A. Rényi, "On Random Graphs. I," *Publicationes Mathematicae*, vol. 6, Article ID 290297, pp. 290–297, 1959.

[42] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[43] M. Molloy and B. Reed, "A critical point for random graphs with a given degree sequence," *Random Structures Algorithms*, vol. 6, no. 2-3, pp. 161–179, 1995.

[44] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Physical Review Letters*, vol. 87, no. 19, Article ID 198701, 2001.

[45] H. J. Herrmann, C. M. Schneider, A. A. Moreira, J. S. Andrade Jr., and S. Havlin, "Onion-like network topology enhances robustness against malicious attacks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2011, no. 1, Article ID P01027, 2011.

[46] C. M. Schneider, A. A. Moreira, J. S. Andrade Jr., S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 108, no. 10, pp. 3838–3841, 2011.

[47] R. M. Karp, "Reducibility among combinatorial problems," in *Complexity of Computer Computations*, R. E. Miller and J. W. Thatcher, Eds., pp. 85–103, Springer, New York, NY, USA, 1972.

[48] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *American Association for the Advancement of Science. Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[49] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E, Statistical, Nonlinear, and Soft Matter Physics*, vol. 65, no. 5, part 2, Article ID 056109, 2002.

[50] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, "Attack robustness and centrality of complex networks," *PLoS ONE*, vol. 8, no. 4, Article ID e59613, 2013.

[51] U. Brandes, "A faster algorithm for betweenness centrality," *Journal of Mathematical Sociology*, vol. 25, no. 2, pp. 163–177, 2001.

[52] F. Chung and L. Lu, "Connected components in random graphs with given expected degree sequences," *Annals of Combinatorics*, vol. 6, no. 2, pp. 125–145, 2002.

[53] Y. S. Cho, J. S. Kim, J. Park, B. Kahng, and D. Kim, "Percolation transitions in scale-free networks under the achlioptas process," *Physical Review Letters*, vol. 103, no. 13, Article ID 135702, 2009.

[54] R. A. Rossi and N. K. Ahmed, "The network data repository with interactive graph analytics and visualization," in *Proceedings of the 29th AAAI Conference on Artificial Intelligence*, 2015.

[55] Pajek data sets, "Vladimir Batagelj and Andrej Mrvar," 2006, http://vlado.fmf.uni-lj.si/pub/networks/data/.