Robustness of Link Prediction Under Network Attacks

Cunlai Pu, Kun Wang, and Yongxiang Xia, *Senior Member, IEEE*

***Abstract*—Link prediction in networks has been a hot topic over the years, while its robustness has not been well discussed in the network literature. In this brief, we study the robustness of mainstream link prediction methods under various kinds of network attacks, including random attack (RDA), centrality based attack (CA), similarity based attack (SA), and simulated annealing based attack (SAA). In the variation of precision, a typical evaluation index of link prediction, we find that for the SA and SAA, a small fraction of link removals significantly degenerates the performance of link prediction. In general, SAA has the highest attack efficiency, followed by the SA and then the CA attack. Interestingly, the performance of some particular CA strategies, such as the betweenness based attack (BA), are even worse than the RDA attack. Furthermore, we discover that the link prediction method with high performance probably has low attack robustness, and vice versa.**

***Index Terms*—Network attacks, robustness, link prediction, structural similarity, complex networks.**

I. Introduction

The LINK prediction problem [1] is originated from the area of data mining, and has achieved great progress with the booming of network science [2]. The goal of link prediction is to estimate the link likelihood of two unconnected nodes based on available network data and analysis tools, such as machine learning [3]–[5] and network theory [6]. Various link prediction methods have been proposed [7], and are broadly divided into four categories: structural similarity based methods (such as the Common Neighbor (CN) [8] and Adamic-Adar (AA) [9] indices), maximum likelihood based methods (such as the hierarchical structure model [10] and stochastic block model [11]), probabilistic models (such as the probabilistic relational model [12] and probabilistic entity-relationship model [13]), and information theory based methods, including the neighbor set information (NSI) [14] and path entropy (PE) [15] indices. The established link prediction methods are widely used in online product recommendation [16], bionetwork reconstruction [17], evolution process prediction of infrastructure networks [18], etc.

Though excellent prediction methods have emerged, their robustness has not been adequately discussed in the literature. Unfortunately, real-world networks suffer from random failures and targeted attacks. For instance, many scale-free networks, such as the Internet, are vulnerable to degree based targeted attacks [19]. A small initial attack can trigger a large-scale cascading failure [20], [21], which is one of the main security issues in power networks. In addition, novel attack strategies have been proposed, such as the edge attacks [22], [23] and path attacks [24]. These random or intentional attacks significantly affect the structure and dynamics of real-world networks [25]. In particular, the predictability of real-world networks keeps changing as the network attack continues. Thus, it is necessary to explore the robustness of link prediction under network attacks.

Recently, Zhang *et al.* [26] studied robustness of several link prediction algorithms in noisy environments. The results of that study show that different prediction algorithms have different behaviors; in general, they are robust to random disturbances. However, their work has the following limitations:

(i) Only the area under the receiver operating characteristic curve (AUC) is considered in the evaluation of prediction accuracy, while the precision, another mainstream index, should be considered in the link prediction problem as well.

(ii) The perturbation methods used are relatively simple, only involving random disturbances. The robustness of link prediction under various targeted attacks needs more attention.

In this brief, we examine the robustness of typical link prediction methods under various network attacks. Our main contributions are as follows:

(i) We investigate link prediction robustness under typical target attacks including the betweenness based attack (BA) [27] and preferential attachment based attack (PA) [28], and find that PA has a higher attack efficiency than BA.

(ii) To further study attack robustness, we propose similarity based attack strategies by considering typical similarity indices, such as the Common Neighbor (CN), Adamic-Adar (AA), and Resource Allocation (RA) [29]. Furthermore, we propose the simulated annealing based attack (SAA) strategy.

Manuscript received June 14, 2019; revised August 19, 2019; accepted August 27, 2019. Date of publication September 6, 2019; date of current version August 4, 2020. This brief was recommended by Associate Editor J. Wu. *(Corresponding author: Cunlai Pu.)*

C. Pu and K. Wang are with the School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China (e-mail: pucunlai@njust.edu.cn; kunwang239@qq.com).

Y. Xia is with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: xiayx@zju.edu.cn).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSII.2019.2938894

(iii) Through simulation, we find that SAA has the largest attack efficiency, followed by similarity based strategies and finally centrality based strategies. Furthermore, we discover that the link prediction method with high performance probably has low robustness, and vice versa.

In the next section, we introduce the evaluation metrics as well as the link prediction methods used in this brief. In Section III, we provide the typical attack strategies and our proposed attack strategies. Section IV presents the experimental results and related analysis. Finally, Section V is our conclusion.

II. Link Prediction Methods and Their Evaluation

We examine the structural similarity based methods of link prediction, which have been popular in recent years. In these methods, each unconnected node pair is given a similarity score according to a certain similarity index, and the node pairs of large similarity scores are assumed to have a large link probability. Different from [26], we use precision, another typical metric, to quantify the accuracy of link prediction.

A. Link Prediction Methods

We select five mainstream prediction methods for our experiments: the Common Neighbor (CN), Adamic-Adar (AA), Resource Allocation (RA), Local Path (LP) [30], and Katz [31]. In the following, the degree of node x is denoted by k_x, and the set of common neighbors of nodes x and y is represented by $\Gamma(x) \cap \Gamma(y)$.

(i) CN: Assuming that the set of neighbor nodes of node x is $\Gamma(x)$, the CN index of nodes x and y is defined as

$$s_{xy}^{CN} = |\Gamma(x) \cap \Gamma(y)|. \tag{1}$$

(ii) AA: This index accounts for the contribution of common neighbors with a penalization term that is dependent on the logarithm of common neighbors' degree,

$$s_{xy}^{AA} = \sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{1}{\log k_z}. \tag{2}$$

(iii) RA: It is originated from the resource allocation problem [32]. Suppose that node x delivers the resource to node y (they are not directly connected) through their common neighbors. Each common neighbor gets one unit of resource from x, and then evenly distributes this unit to all of its neighbors. The similarity between x and y is defined as the amount of resource y receives from x,

$$s_{xy}^{RA} = \sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{1}{k_z}. \tag{3}$$

(iv) LP: This index considers the contribution of paths of lengths 2 and 3, which is defined as:

$$\mathbf{S}^{LP} = \mathbf{A}^2 + \alpha \cdot \mathbf{A}^3. \tag{4}$$

where $\mathbf{A}$ is the adjacency matrix. The (x, y) entry of $\mathbf{A}^i$ is the number of paths of length i between nodes x and y. α is a tunable parameter controlling the contribution of paths with length 3.

(v) Katz: It takes into account all the paths between two nodes, which is

$$s_{xy}^{Katz} = \sum_{l=1}^{\infty} \alpha^l \cdot |paths_{x,y}^{<l>}|. \tag{5}$$

where α is a tunable parameter and $|paths_{x,y}^{<l>}|$ represents the number of paths of length l between nodes x and y.

B. Evaluation Metric

We assume an undirected and unweighted network $G(V, E)$, where V is the set of nodes and E is the set of links. In the link prediction problem, we divide E into a training set E_T and a probe set E_P to evaluate the prediction method. Usually, E_P consists of 10% (or 20%) of links randomly extracted from E, and E_T includes the remaining 90% (or 80%) of links. In E_T, each unconnected node pair is given a similarity score by the similarity index, and then all of the unconnected node pairs are ranked in decreasing order of similarity scores. The precision index for the evaluation of prediction accuracy is defined as:

$$pre = \frac{m}{L}. \tag{6}$$

where m is the number of desired node pairs (whose links are previously removed to the probe set) among the top L unconnected node pairs [6].

III. Network Attack Strategies

Real-world networks suffer from various kinds of failures or attacks. Here we consider representative attack strategies, including the random attack (RDA) and the centrality based attack (CA) [25]. For the category of CA, we study the betweenness based attack (BA) and the preferential attachment based attack (PA). Furthermore, we propose two additional types of attack strategies: the similarity based attack (SA) and the simulated annealing based attack (SAA). Note that all the attack strategies mentioned here are for link attacks, which means removing the targeted links. All of these strategies are described below in detail.

(i) RDA: It is a very simple attack strategy, and usually works as a baseline for other strategies. In RDA, we randomly remove links from the network.

(ii) BA: In this strategy, we use betweenness centrality [27] to evaluate the importance of links. Then, we remove the links of the largest betweenness. The betweenness of link e is

$$BC_e = \sum_{s,t \in V} \frac{\sigma(s, t|e)}{\sigma(s, t)}. \tag{7}$$

where $\sigma(s, t)$ is the number of shortest paths between nodes s and t, and $\sigma(s, t|e)$ is the number of those paths that pass through link e.

(iii) PA: In this strategy, we remove the links of the largest preferential attachment index. Assume the end nodes of link e are nodes x and y, the preferential attachment index of link e is given as [28]:

$$P_e = k_x \cdot k_y. \tag{8}$$

TABLE I
THE STATISTICS OF SEVEN REAL-WORLD NETWORKS, WHERE N IS THE NUMBER OF NODES, E IS THE NUMBER OF LINKS, AND C IS THE ASSORTATIVITY COEFFICIENT

	USAir	PB	C.elegans	Metabolic	Jazz	HVR	Email
N	332	1,222	297	453	198	307	1,133
E	2,126	16,714	2,148	2,025	2,742	2812	5,451
C	-0.208	-0.221	-0.163	-0.226	0.020	0.599	0.078

where k_x and k_y represent the degree of nodes x and y, respectively.

(iv) SA: In this category of attacks, the importance of a link is quantified as the similarity score of its two end nodes. Then, we remove the links of the greatest importance. The CN, RA, and AA indices are used to give the similarity scores of the nodes, and then the corresponding attacks are denoted by SA-CN, SA-RA, and SA-AA respectively. Note that the other similarity indices can also be taken into account.

(v) SAA: This strategy is based on the simulated annealing algorithm [33]. It globally searches the best set of links, by removing which the link prediction accuracy of the network decreases the most. This algorithm is as follows:

a. We randomly select a set of links of a fixed number from the network as the initial solution, and then we set the initial temperature to t_{max}, and the minimum temperature to t_{min}.

b. To update the solution, we randomly select a link (not in the current solution set) from the network and swap it with a random link in the current solution, which provides a new solution.

c. Let P_c (P_n) be the precision of the remaining network corresponding to the current (new) solution. If $P_n < P_c$, we replace the current solution with the new one with probability 1, and otherwise with probability $P = \exp\left((P_c - P_n)/t_c\right)$, where t_c is the current temperature.

d. We update the temperature, $t_c = c \cdot t_c$, where c is the cooling coefficient and has a range in (0, 1). If $t_c < t_{min}$, the algorithm ends; otherwise, it returns to step b.

In SAA, we remove the optimal set of links from the network.

IV. RESULT

We do experiments on various real-world network data downloaded from [34], [35], including the USAir (American Airlines Network), PB (Political Blog Network), C.elegans (Nematode Neural Network), Metabolic (Nematode Metabolism Network), Jazz (Jazz Musician Network), HVR (Malaria Parasite Gene Network), and Email (Email Communication Network). The statistics of these networks are shown in Table I. Note that we ignore link directions and remove self-loops in the network data. When calculating precision, we do 100 times of training and probe set divisions and get the average value. The results of RDA and SAA are the average of 10 independent runs.

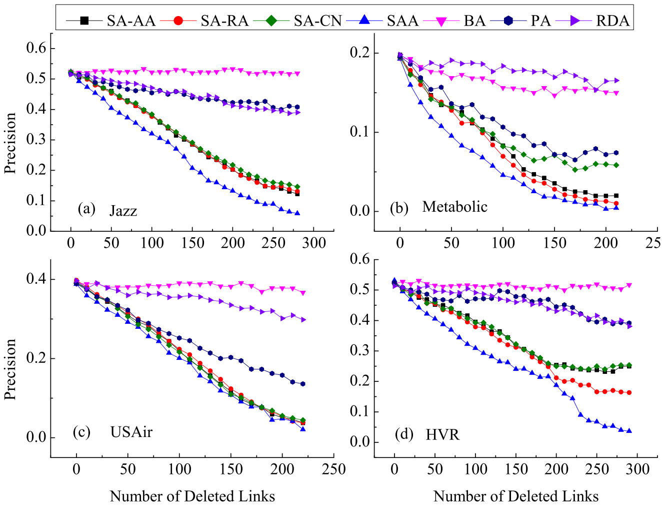

Fig. 1. Precision of the AA index under various attack strategies.

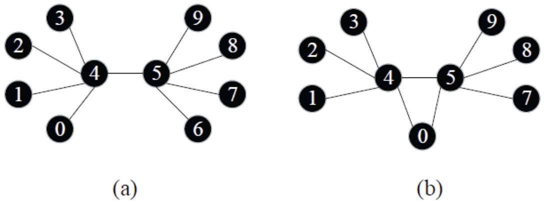

Fig. 2. Two example networks for illustration purpose, whose assortativity coefficient values are. (a) −0.80 and (b) −0.78 respectively.

A. Comparison of Efficiency Among Different Attack Strategies

We first compare the efficiency of the given attack strategies in degenerating the link prediction accuracy. The AA index is used as the prediction method. The experimental results are shown in Fig. 1. In each panel of Fig. 1, the first data point of every curve corresponds to the case of no attacks, whereas the last data point is the result of 10% of the links being removed. Note that we only show the results of four networks due to limited space, and other networks have similar conclusion.

In Fig. 1, we can see that the SAA attack achieves the highest attack efficiency than the others, since it always attacks the optimal link set to suppress precision. The SA attack achieves the second highest attack efficiency. The relatively high efficiency of SA lies in removing links, where two end nodes are structurally similar. This will greatly damage the structural similarity of the whole network, which leads to the decrease of link predictability. Note that the difference of efficiency among distinct SA strategies is not significant.

The CA follows SA with respect to attack efficiency. In CA strategies, the efficiency is different. For instance, PA is more efficient than BA, and in some cases the latter is even worse than RDA. This is unexpected, since the BA attack is efficient in other scenarios [22]. If a link has a large betweenness, it is the intersection of many shortest paths controlling the connectivity and communicability of the network. For example, in Fig. 2(a) link (4, 5) has the largest betweenness and is critical to the network, since it connects two separate communities. However, the end nodes of this link have no common neighbor.

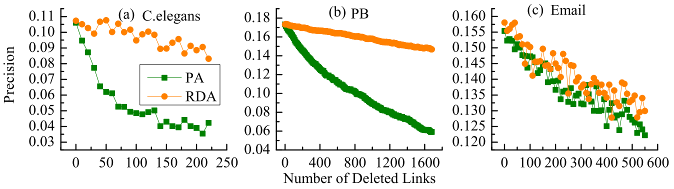

Fig. 3. Comparison of PA and RDA in three real-world networks.

TABLE II

ATTACK COST Φ (%) OF SEVEN REAL-WORLD NETWORKS. IF $\Phi > 10\%$, WE MARK IT AS "−"

	BA	PA	SA-CN	SA-AA	SA-RA	SAA	RDA
Jazz	-	-	6.20	6.20	6.20	5.11	-
Metabolic	-	5.43	4.94	4.44	4.44	2.47	-
USAir	-	7.53	5.64	5.17	5.64	5.17	-
HVR	-	-	6.76	6.76	6.76	4.62	-
PB	-	6.34	3.23	3.17	3.47	2.99	-
C.elegans	-	3.26	2.23	2.33	2.33	1.86	-
Email	-	-	4.40	3.67	3.67	2.94	-

Thus, they should have a very small connection probability according to the rule of similarity based link prediction. Removing this kind of link does not affect link predictability, and may even promote link prediction since these links are outliers of similarity based link prediction.

For PA, we find that attack efficiency in disassortative networks is much larger than assortative networks. To confirm this, we show the results of PA and RDA on three other networks in Fig. 3. We see that the difference of attack efficiency of PA and RDA is larger in disassortative networks. Note that the assortativity coefficient values of networks used in the experiments are given in Table I, where positive value means assortative network, and vice versa. Fig. 2(b) is a small disassortative network for illustration purpose. In this network, link (4, 5) has the largest similarity score according to the AA index. However, for the PA attack this link is the first target to be removed. Therefore, the prediction performance of AA index decreases significantly when the network is under the PA attack.

To quantify the efficiency of an attack strategy, we study the fraction of links to be removed in order to decrease the precision by half, which is named as the attack cost and can be expressed as

$$\Phi = \frac{E'}{E}. \tag{9}$$

where E' is the number of links that need to be removed to decrease the precision by half, and E is the total number of links in the network. Based on this definition, we know that the smaller attack cost means a larger attack efficiency. We still use the AA index as the link prediction method. The attack cost Φ of seven real-world networks for different attack strategies is given in Table II, in which "-" means $\Phi > 10\%$.

As can be seen from this table, for most of the attack strategies, removing only a small portion of links can reduce the prediction accuracy by half, which indicates that the influence of network attacks on link prediction cannot be ignored. In other words, real-world networks are pretty vulnerable to network attacks in terms of link prediction. In addition, we can clearly see the difference of efficiency of distinct attack strategies, which is consistent with Fig. 1.

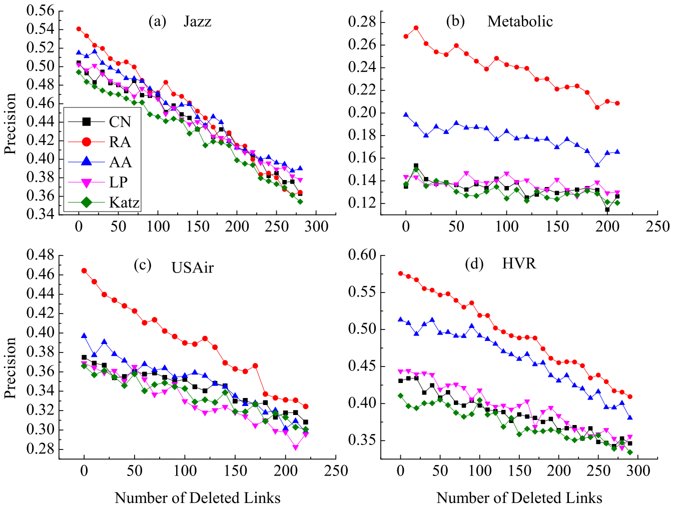

Fig. 4. Precision of different link prediction methods under the RDA attack strategy.

B. Comparison of Robustness Among Different Prediction Methods

Furthermore, we compare the robustness of different link prediction methods. Here we use RDA as the attack strategy for all of the prediction methods. The experimental results are shown in Fig. 4. The first data point of each curve corresponds to the case of no attacks, and the last point is the result of the random removal of 10% links. From Fig. 4, we observe that the precision of all the link prediction methods decreases as the number of removed links increases. For the considered network data, RA has the largest prediction accuracy, followed by AA. The prediction accuracy of CN, LP, and Katz is relatively low with a small difference. In order to quantify the robustness of a link prediction method against network attacks, we provide a new index of attack robustness as follows:

$$\Omega = \frac{1}{L} \cdot \sum_{i=1}^{L} \frac{|pre(i \cdot \Delta m) - pre(0)|}{pre(0)}. \tag{10}$$

where Δm is a given constant ($\Delta m = 10$ in the experiments), and i is a variable ranging in $[0, L]$. $pre(*)$ is the result of precision when the number of removed links is $*$. Attack robustness Ω measures the average decrease rate of precision under network attacks, and the small Ω means a large attack robustness. According to the results of Fig. 4, we calculate the attack robustness Ω of the five considered link prediction methods, the results of which are shown in Table III.

We can see that although the RA index has the highest prediction accuracy, its Ω value is also the largest among all the prediction methods, which indicates that RA has the smallest attack robustness. In contrast, the prediction accuracy of CN is not very prominent. However, its Ω value is smaller than RA, which means that CN is more robust than RA against

TABLE III
ATTACK ROBUSTNESS Ω (%) OF LINK PREDICTION METHODS ON DIFFERENT REAL-WORLD NETWORKS

	CN	AA	RA	LP	Katz
Jazz	12.19	12.12	15.92	11.64	12.84
Metabolic	3.78	9.63	10.64	4.62	5.81
USAir	7.91	11.54	15.68	10.21	8.21
HVR	10.30	9.91	13.69	10.48	8.78
PB	7.50	7.72	11.23	6.60	6.32
C.elegans	9.90	11.24	13.09	10.31	6.54
Email	4.61	10.23	8.62	10.13	7.62

network attacks. These results provide support for a comprehensive consideration of the performance of link prediction methods in real applications.

V. CONCLUSION

In summary, we study the robustness of link prediction methods under network attacks, which is a new dimension for the evaluation of link prediction methods. Specifically, we consider the random attack (RDA) and the centrality based attacks (CA), including the betweenness based attack (BA) and the preferential attachment based attack (PA). Furthermore, we propose the similarity based attack (SA), which attacks links based on similarity scores of their end nodes, and the simulated annealing based attack (SAA).

Through our experiments, we observe that network attacks have a great impact on link prediction accuracy, as measured by the precision index. Generally speaking, attacking a small portion of links may result in a significant decrease of prediction accuracy, except for the random and betweenness based attacks. For all of these attack strategies, SAA has the highest attack efficiency, followed by SA, then CA, and finally RDA. Note that in the category of centrality based attacks, BA has a low attack efficiency, which is even worse than RDA.

For all the considered similarity indices, we find that the RA index achieves a better prediction performance than the others, but it is very vulnerable to network attacks. On the other hand, the CN index has a relatively large robustness against attacks compared to the others, although its prediction accuracy is just adequate. These results indicate that along with accuracy, the robustness of link prediction methods should also be considered in real applications.

REFERENCES

[1] D. Liben-Nowell and J. Kleinberg, "The link-prediction problem for social networks," *J. Amer. Soc. Inf. Sci. Technol.*, vol. 58, no. 7, pp. 1019–1031, 2007.

[2] A.-L. Barabási *et al.*, *Network Science*. Cambridge, U.K.: Cambridge Univ. Press, 2016.

[3] M. Nasim, R. Charbey, C. Prieur, and U. Brandes, "Investigating link inference in partially observable networks: Friendship ties and interaction," *IEEE Trans. Comput. Social Syst.*, vol. 3, no. 3, pp. 113–119, Sep. 2016.

[4] L. Duan, S. Ma, C. Aggarwal, T. Ma, and J. Huai, "An ensemble approach to link prediction," *IEEE Trans. Knowl. Data Eng.*, vol. 29, no. 11, pp. 2402–2416, Nov. 2017.

[5] C. Fu *et al.*, "Link weight prediction using supervised learning methods and its application to Yelp layered network," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 8, pp. 1507–1518, Aug. 2018.

[6] L. Lü and T. Zhou, "Link prediction in complex networks: A survey," *Physica A Stat. Mech. Appl.*, vol. 390, no. 6, pp. 1150–1170, 2011.

[7] V. Martínez, F. Berzal, and J.-C. Cubero, "A survey of link prediction in complex networks," *ACM Comput. Surveys*, vol. 49, no. 4, p. 69, 2017.

[8] F. Lorrain and H. C. White, "Structural equivalence of individuals in social networks," *J. Math. Soc.*, vol. 1, no. 1, pp. 49–80, 1971.

[9] L. A. Adamic and E. Adar, "Friends and neighbors on the Web," *Soc. Netw.*, vol. 25, no. 3, pp. 211–230, 2003.

[10] A. Clauset, C. Moore, and M. E. J. Newman, "Hierarchical structure and the prediction of missing links in networks," *Nature*, vol. 453, no. 7191, p. 98, 2008.

[11] R. Guimerà and M. Sales-Pardo, "Missing and spurious interactions and the reconstruction of complex networks," *Proc. Nat. Acad. Sci. USA*, vol. 106, no. 52, pp. 22073–22078, 2009.

[12] J. Neville, *Statistical Models and Analysis Techniques for Learning in Relational Data*, Univ. Massachusetts Amherst, Amherst, MA, USA, 2006.

[13] "Probabilistic entity-relationship models, PRMS, and plate models," in *Introduction to Statistical Relational Learning*. Cambridge, MA, USA: MIT Press, 2007, pp. 201–238.

[14] B. Zhu and Y. Xia, "An information-theoretic model for link prediction in complex networks," *Sci. Rep.*, vol. 5, Sep. 2015, Art. no. 13707.

[15] Z. Xu, C. Pu, and J. Yang, "Link prediction based on path entropy," *Physica A Stat. Mech. Appl.*, vol. 456, pp. 294–301, Aug. 2016.

[16] G. Linden, B. Smith, and J. York, "Amazon.com recommendations: Item-to-item collaborative filtering," *IEEE Internet Comput.*, vol. 7, no. 1, pp. 76–80, Jan./Feb. 2003.

[17] M. J. Herrgård *et al.*, "A consensus yeast metabolic network reconstruction obtained from a community approach to systems biology," *Nat. Biotechnol.*, vol. 26, no. 10, pp. 1155–1160, 2008.

[18] L. Mei *et al.*, "Predicting the evolution process of infrastructure networks with an NSIPA link prediction method," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, to be published.

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

[20] B. Schäfer, D. Witthaut, M. Timme, and V. Latora, "Dynamically induced cascading failures in power grids," *Nat. Commun.*, vol. 9, no. 1, p. 1975, 2018.

[21] H. Tu, Y. Xia, H. H.-C. Iu, and X. Chen, "Optimal robustness in power grids from a network science perspective," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 1, pp. 126–130, Jan. 2019.

[22] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 65, May 2002, Art. no. 056109.

[23] I. Mishkovski, M. Biey, and L. Kocarev, "Vulnerability of complex networks," *Commun. Nonlin. Sci. Numer. Simulat.*, vol. 16, no. 1, pp. 341–349, 2011.

[24] C.-L. Pu and W. Cui, "Vulnerability of complex networks under path-based attacks," *Physica A Stat. Mech. Appl.*, vol. 419, pp. 622–629, Feb. 2015.

[25] R. Cohen and S. Havlin, *Complex Networks: Structure, Robustness and Function*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[26] P. Zhang, X. Wang, F. Wang, A. Zeng, and J. Xiao, "Measuring the robustness of link prediction algorithms under noisy environment," *Sci. Rep.*, vol. 6, Jan. 2016, Art. no. 18881.

[27] U. Brandes, "On variants of shortest-path betweenness centrality and their generic computation," *Soc. Netw.*, vol. 30, no. 2, pp. 136–145, 2008.

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

[29] T. Zhou, L. Lü, and Y. C. Zhang, "Predicting missing links via local information," *Eur. Phys. J. B*, vol. 71, no. 4, pp. 623–630, 2009.

[30] L. Lü, C.-H. Jin, and T. Zhou, "Similarity index based on local paths for link prediction of complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 80, no. 4, 2009, Art. no. 046122.

[31] L. Katz, "A new status index derived from sociometric analysis," *Psychometrika*, vol. 18, no. 1, pp. 39–43, 1953.

[32] Q. Ou, Y.-D. Jin, T. Zhou, B.-H. Wang, and B.-Q. Yin, "Power-law strength-degree correlation from resource-allocation dynamics on weighted networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 75, Feb. 2007, Art. no. 021102.

[33] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi, "Optimization by simulated annealing," *Science*, vol. 220, no. 4598, pp. 671–680, 1983.

[34] *Link Prediction Group*. Accessed: Mar. 4, 2018. [Online]. Available: http://www.linkprediction.org/

[35] C. U. A. Clauset and A. Ray. *The Index of Complex Networks*. Accessed: Mar. 10, 2018. [Online]. Available: https://icon.colorado.edu/