Topological Approach to Measure Network Recoverability

He, Zhidong; Sun, Peng; Van Mieghem, Piet

DOI
10.1109/RNDM48015.2019.8949119

Publication date
2019

Document Version
Accepted author manuscript

Published in
Proceedings of 2019 11th International Workshop on Resilient Networks Design and Modeling, RNDM 2019

Topological approach to measure network recoverability

Zhidong He, Peng Sun, and Piet Van Mieghem
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology, The Netherlands
E-mails: Z.He, P.Sun-1, P.F.A.VanMieghem@tudelft.nl

***Abstract*—Network recoverability refers to the ability of a network to return to a desired performance level after suffering malicious attacks or random failures. This paper proposes a general topological approach and recoverability indicators to measure the network recoverability in two scenarios: 1) recovery of damaged connections and 2) any disconnected pair of nodes can be connected to each other. Our approach presents the effect of the random attack and recovery processes on the network performance by the robustness envelopes of realizations and the histograms of two recoverability indicators. By applying the effective graph resistance and the network efficiency as robustness metrics, we employ the proposed approach to assess 10 real-world communication networks. Numerical results verify that the network recoverability is coupled to the network topology, the robustness metric and the recovery strategy. We also show that a greedy recovery strategy could provide a near-optimal recovery performance for the investigated robustness metrics.**

***Index Terms*—Robusteness; multiple failure; Recoverability**

I. Introduction

In communication networks, disaster-based failures and damage to optical fiber cables can partially overload data delivery, resulting in un-availability of communication services [1]. The causes for such massive failures include: human errors, malicious attacks, large-scale disasters, and environmental challenges [2]. Calculating the performance of networks under such challenges can provide significant insight into the potential damage they can incur, as well as provide a foundation for creating more robust infrastructure networks.

Network robustness is interpreted as a measure of the network's response to perturbations or challenges imposed on the network [3], which has been studied extensively in recent years. Van Mieghem *et al.* [3] propose a framework for computing topological network robustness by considering both a network topology and a service for which the network is designed. In communication networks, Cholda *et al.* [4] survey various robustness frameworks and present a general framework classification, while Pašić *et al.* [5] present the FRADIR framework that incorporates reliable network design, disaster failure modeling and protection routing. A wide range of metrics based on the underlying topology have been proposed to measure network robustness [6], and further a structural robustness comparison of several telecommunication networks under random nodal removal was presented in [7].

In a board sense, network robustness is also related to the ability of a network to return to a desired performance level after suffering malicious attacks and random failures [8]. We define such network capability as *network recoverability*[1] in this paper. Several recovery mechanisms have been investigated under different circumstances [9], particularly in complex networks applications. Majdandzic *et al.* [10] model cascading failures and spontaneous recovery as a stochastic contiguous spreading process and exhibit a phase switching phenomenon. The recovery strategies based on the centrality metrics of network elements (e.g., nodes or links) are investigated in [8][11], which show that a centrality metric-based strategy may not exist to improve all the network performance aspects simultaneously. A progressive recovery approach [12], that consists in choosing the right sequence of links to be restored after a disaster in communication networks, proposes to maximize the weighted sum of the total flow over the entire process of recovery [13], as well as to minimize the total cost of repair under link capacity constraints [14].

Although the above papers [8]–[14] have contributed to this field, a general framework or methodology for quantifying the recovery capability of a real communication network is still lacking. In this paper, we propose a topological approach and two recoverability indicators to measure the network recoverability in two different scenarios, link-based Scenario A and energy-based Scenario B. Specifically, Scenario A assumes that any disconnected pair of nodes can be connected to each other in the recovery process, which can describe the recovery process for logical networks. Scenario B restricts the under-repaired links to the damaged links in the attack process, which describes the recovery process for physical networks.

The proposed approach involves three concepts: the network topology, the robustness metric and the recovery strategy. For a communication network G, we apply the network efficiency E_G and the effective graph resistance r_G as the robustness metrics for case studies. The network efficiency E_G gives an indication of the efficiency of information exchange on networks under shortest path routing [15], while the effective graph resistance determines the overall diffusivity of information spreading in a communication network [16]. Besides a random recovery strategy and some strategies based on topological properties, we also consider a greedy recovery strategy. In the greedy strategy, the damaged element (a node or a link) which improves the network performance most has

[1]Sometimes *network restoration* is used

the highest priority to be recovered. We test our approach in 10 real telecommunication networks, including logical networks and backbone networks located in different areas, and verify that the proposed approach and the proposed recoverability indicators can assess the performance of different recovery strategies and compare the recoverability of different networks.

The rest of this paper is organized as follows: Section II introduces the topological approach for measuring the network recoverability in two scenarios. Section III presents the main concepts in the evaluation of network recoverability. The experimental results are exhibited in Section IV. Section V concludes the paper.

II. Topological Approach for Measuring Network Recoverability

In this section, we introduce an approach for measuring the network recoverability in two scenarios.

A. R-value and challenge

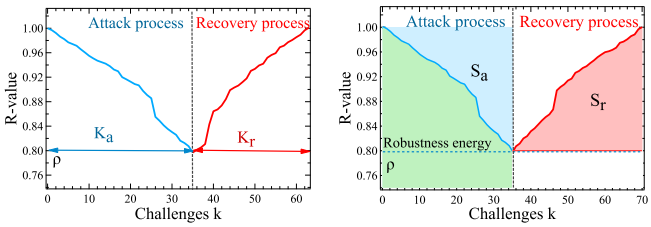
We inherit the framework and some definitions proposed for network robustness [3], [17] and extend the methodology for the network recoverability. A given network determined by a service and an underlying topology is translated into a mathematical object, defined as the R-value, on which computations can be performed [3]. The R-value takes the service into account and is normalized to the interval $[0, 1]$. Thus, $R = 1$ reflects complete functionality in an unattacked network, and $R = 0$ corresponds to absence of performance in a completely destroyed network.

A challenge is an event that changes the network and thus changes the R-value. We assume that a sequence of elementary changes do not coincide in time. Here, we confine an elementary challenge to a link removal in an attack process or a link addition in a recovery process. Since every perturbation has an associated R-value, any realization consisting of a number M of elementary challenges can be described by a sequence of R-values denoted $\{R[k]\}_{1\leq k\leq M}$, where k is the sequence number of challenges.

B. Scenario A: recovery of any alternative link

We define R_G as the robustness metric of the network $G(N, L)$ with N nodes and L links. Attacks on a network only consist of link removals in the network by a determined strategy, which usually degrades the robustness of the network. We remove links, one by one, until the R-value R_{G_a} first reaches or drops below a constant ρ, where $\rho \in [0, 1]$ is a prescribed R-threshold for the robustness metric that can be tolerated [3]. The above process is called the attack or failure process. The number of removed links in the attack process, i.e., *attack challenges*, is denoted by K_a.

Then we launch the recovery process from the remaining network $G_a(N, L - K_a)$. Scenario A assumes that the recovery links can be established between any two nodes in the complement of the graph after attacks. The process of one realization is illustrated in Figure 1a. Specifically, we recover the network by adding links, one by one, to the remaining network G_a by a recovery strategy until the robustness metric R-value first reaches or excesses $R_{G_r} = 1$. The network after the recovery process is denoted by $G_r(N, L - K_a + K_r)$, where K_r is the number of *recovery challenges* (adding K_r links). We define the *Link Ratio* denoted η_L as the ratio of the number of attack challenges and the recovery challenges, i.e.,



(a) Scenario A (b) Scenario B

Fig. 1: Illustration of the attack process and the recovery process in an Erdős-Rényi (ER) random graph $G_{0.1}(100)$ with link density $p = 0.1$ and network size $N = 100$ in one realization. The R-threshold is $\rho = 0.8$.

$$\eta_L(G, \rho) = \frac{K_a}{K_r} \tag{1}$$

which indicates the efficiency of the recovery process in one realization. A Link Ratio $\eta_L(G, \rho) > 1$ implies that the network can be recovered by less challenges than the number K_a of attack challenges. Otherwise, the network is more difficult to recover than to destroy.

Scenario A can characterize the recovery process in a connection oriented network with logical connections [18], e.g., a virtual circuit for transporting data or a wireless backhaul network, where the links in a logical network represent the duplex channel between two devices. After such networks are attacked by denial-of-service attacks (DoS) or signal blocking, one should establish several connections or reconfigure several new channels to maintain the network's overall performance. In this case, the overhead cost of the recovery measures mainly depends on the total number of dispatched connections, which corresponds to the number K_r of recovery challenges in Scenario A.

C. Scenario B: recovery of attacked links

The attack process in Scenario B is the same as in Scenario A. In the recovery process in Scenario B, we add all the links which are removed in the attack process, one by one, until the underlying topology returns to the original. Scenario B describes recovery processes in the physical communication network, e.g., optical backbone networks and power grids supplying to communication networks. In these networks, the recovery measure for each connection, e.g., repairing fiber optic cables, usually requires a relatively long period. During the recovery process, the network still provides services with a degraded performance. Thus, the network recoverability is related to the network performance (or the robustness metric) throughout the recovery process.

One realization of the attack and recovery process is illustrated in Figure 1b. In Scenario B, the number of attack challenges and the number of recovery challenges are the

same, i.e., $K_a = K_r$, and hence, $\eta_L = 1$ in (1). Therefore, we propose another recoverability indicator in Scenario B. The *robustness energy* $S(G, \rho)$ of a network G is the sum of the R-value in the attack process $S(G, \rho) = \sum_{k=0}^{K_a} R[k]$, which expresses the robustness performance of network under successive attacks [17]. Thus, the energy of attack challenges is computed by $S_a(G, \rho) = \sum_{k=0}^{K_a}(1 - R[k]))$, which indicates the cumulative degradation of network performance due to the attacks. In the recovery process, the energy of recovery challenges $S_r(G, \rho) = \sum_{k=0}^{K_a}(R[k] - \rho)$ represents the benefit of the network performance by the recovery measures. The *Energy Ratio* denoted η_E in Scenario B is defined as the ratio between the energy of recovery challenges S_r and the energy of attack challenges S_a in each realization for a determined R-threshold ρ, which follows

$$\eta_E(G, \rho) = \frac{S_r}{S_a} \tag{2}$$

An Energy Ratio $\eta_E(G, \rho) > 1$ implies the benefit of recovery measures can compensate the loss of network performance by the attacks, which indicates a high network recovery capability. Conversely, an Energy Ratio $\eta_E(G, \rho) < 1$ implies a low recoverability.

D. Comparison via envelopes and the recoverability indicators

Any realization of attack and recovery processes can be expressed as a sequence of R-values denoted $\{R[k]\}$. To investigate the recovery behavior, we need to know how many challenges k are needed to make R-value decrease to a predefined threshold ρ and increase to its original value, which confines us to investigate the number of challenges K as a function of a specific R-value r, i.e., $\{K[r]\}$. Thus, each value in $\{K[r]\}$ is the number of challenges that is needed to change R-value to a specific R-value r for each realization. The *envelope* is constructed using all sequences $\{K[r]\}$ for $r \in \{r_1, r_2, \ldots, r_H\}$, where $r_j = \rho + \frac{j(1-\rho)}{H}$ is a sampled value and $H = 1000$ is the total sample number. The boundaries of the envelope are given by the extreme number of challenges K

$$K_{\min}[r] \in \{\min(K[r_1]), \min(K[r_2]) \ldots, \min(K[r_H])\} \tag{3}$$
$$K_{\max}[r] \in \{\max(K[r_1]), \max(K[r_2]) \ldots, \max(K[r_H])\} \tag{4}$$

which gives the best- and worst-case of robustness metrics for a network after a given number of recovery challenges. The expected number of challenges K leading the topological approach r_j is

$$K_{avg}[r] \in \{E(K[r_1]), E(K[r_2]) \ldots, E(K[r_H])\} \tag{5}$$

Since $K[r]$ defines a probability density function (PDF), we are interested in the percentiles of $K[r]$

$$K_{m\%}[r] \in \{K_{m\%}[r_1], K_{m\%}[r_2] \ldots, K_{m\%}[r_H]\} \tag{6}$$

where $K_{m\%}[r]$ are the points at which the cumulative distribution of $K[r]$ crosses $\frac{m}{100}$, namely $K_{m\%}[r] = t \Leftrightarrow \Pr[K[r] \leq t] = \frac{m}{100}$.

We apply the envelope to present the behavior of the attack and recovery processes on a network [3], [17]. The envelope profiles a rough PDF of the random variables of the number of challenges K, which is the probability of a random variable to fall within a particular region. The area of the envelope can be regarded as the variation of the robustness impact of a certain series of challenges, which quantifies the uncertainty or the amount of risk due to perturbations.

We propose two recoverability indicators, the Link Ratio $\eta_L(G, \rho)$ and the Energy Ratio $\eta_E(G, \rho)$, for different scenarios, respectively. Since an attack process and a recovery process could be random under the random strategy, the recoverability indicators are random variables. We can compare the recoverability of different networks by the average recoverability indicators for simplicity. For example, the average Link Ratio $E[\eta_L(G_1, \rho)] > E[\eta_L(G_2, \rho)]$ for two different networks G_1 and G_2 implies that the network G_1 usually has a better recoverability than G_2 in Scenario A for the robustness threshold ρ.

Besides the average recoverability indicators, we are also concerned about the variance of the recoverability indicators $Var[\eta(G, \rho)]$, which indicates how likely the recoverability is to shift upon the random strategy. A smaller variance of the recoverability indicators $Var[\eta(G, \rho)]$ implies a narrower uncertainty of the recoverability indicators, thus a better recoverability.

III. Robustness metric and recovery strategy

In this section, we introduce the main factors of a specific recovery process, which involve robustness metrics, recovery strategies and network topologies.

A. Robustness metrics

A group of topological metrics are proposed to measure the network robustness [6] and the correlation of some metrics in random graphs and functional brain networks are investigated in [19]. We select 20 real telecommunication networks in the specialized databases [20], and show the correlation between metrics. As metrics, we include the network efficiency E_G, the spectral radius of adjacency matrix λ_1, the algebraic connectivity μ_{N-1}, the diameter φ, the effective graph resistance r_G, the ratio μ_1/μ_{N-1}, the average hopcount $E[H]$ among all node pairs, the clustering coefficient c_G in Figure 2. Considering services of communication networks, we select 1) the network efficiency E_G and 2) the effective graph resistance r_G as the robustness metrics that characterize the performance of end-to-end transmissions. Figure 2 shows that these two path-based metrics, the network efficiency E_G and the effective graph resistance r_G, are comparatively lowly correlated (i.e., $\rho_{\text{Pearson}}(E_G, r_G) = -0.63$).

1) **Network efficiency E_G.** We assume that the hopcount $h(i, j)$, i.e., the number of links in the shortest path from node i to j, indicates the overhead of data delivery from end to end. Thus, the reciprocal of the hopcount $1/h(i, j)$ implies the amount of packages for one unit overhead, which can be interpreted as the efficiency of the communication between two nodes. If there is no path from i to j, $h(i, j) = \infty$ and $1/h(i, j) = 0$. For a whole network, the efficiency of a given

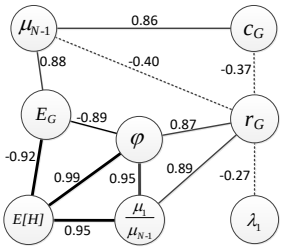


Fig. 2: Correlation of several topological properties in 20 real telecommunication networks. The Pearson correlation coefficients ρ_{Pearson} are marked if the correlation is strong enough, i.e., $|\rho_{\text{Pearson}}| > 0.8$ (by solid lines) or weak enough, i.e., $|\rho_{\text{Pearson}}| < 0.4$ (by dash lines).

network can be computed by the mean of the reciprocals of all the hopcount $h(i,j)$ in a network, i.e.,

$$E_G = \frac{\sum_{i \neq j \in G} 1/h(i,j)}{\binom{N}{2}} \tag{7}$$

which is defined as network efficiency [15]. Network efficiency quantifies how efficient the exchange of information across the whole network under the shortest-path routing [21]. The network efficiency of a network monotonically decreases with the successive link removals.

2) **Effective graph resistance** r_G**.** The effective graph resistance [22], [23], [16], [24] origins from the field of electric circuit analysis, which is defined as the accumulated effective resistance between all pairs of nodes. The effective graph resistance refers to the average power dissipated in a resistor network with random infected currents, which can indicate the overall diffusivity of information spreading in a communication network. Also, the effective graph resistance r_G determines the onset of congestion in a communication network. Specifically, let δ be the average total input rate of the network. It can be shown [25] that the maximum acceptable value of δ, which ensures that all links are within their transmission capacity, is upper bounded by $\binom{N}{2} r_G^{-1}$.

To generalize the impact of attacks on the robustness metrics, we apply the reciprocal of the effective graph resistance r_G^{-1} as the R-value, which decreases for link removals in an attack process and increases in a recovery process. In this paper, we also assume that the removed links leading to the network disconnection have the supreme priority and can be restored instantly. Thus, we numerically exclude the realizations of attack processes that disconnect the network and lead to $r_G^{-1} = 0$.

B. Attack and recovery strategies

For simplicity and generality, we consider a *random attack* strategy in attack processes. The random attack strategy implies that the attacks or failures occur independently on links randomly and uniformly, which is consistent with the random failure stage in a product life cycle. The R-value $R[k]$ for a determined number of attack challenges k is a random variable. We consider three different strategies for recovery measures, i.e., random recovery, metric-based recovery and greedy recovery:

1) **Random recovery:** The random recovery strategy refers to the strategy that the links are added randomly and uniformly, one by one, in recovery processes, which can describe a self-repairing process after attacks or recovery measures without scheduling.

2) **Metric-based recovery:** The metric-based strategy determines the sequence of adding links by the topological metrics of links. The performance of a network is usually restricted by its structural "bottleneck", i.e., the effective graph resistance is related to the algebraic connectivity and the minimum degree [19]. A good recovery strategy tends to remedy such bottleneck. Thus, we consider two metrics of links between node i and j: the minimum product of degree $d_i d_j$, and the minimum product of eigenvector centrality $c_i c_j$. For each challenge in a recovery process, we select and restore the link l_{ij}^* with the minimum $d_i d_j$ or $c_i c_j$.

3) **Greedy recovery:** The greedy recovery strategy involves adding the link l^* that makes R-value increase most in each challenges, i.e.,

$$l^* = \arg\max_{l \in G^c} R(G+l) - R(G) \tag{8}$$

where G^c is the complement of the current network G. The greedy strategy is a practical and intuitive recovery strategy, where the current optimal link for improving the performance of the network has the priority to be recovered during a recovery process.

Networks	N	L	$E[D]$	λ_1	μ_{N-1}	φ	ρ_D	E_G
DFN	58	87	3.00	5.43	0.25	6	-0.11	0.36
Cernet	41	58	2.83	4.78	0.22	5	-0.35	0.40
Bt_US	36	76	4.22	5.85	0.41	6	0.03	0.44
GtsCe	149	193	2.59	3.81	0.01	21	-0.09	0.16
Cogentco	197	243	2.47	3.79	0.01	28	0.03	0.14
TataNld	145	186	2.57	3.27	0.01	28	-0.21	0.15
ATT_US	25	56	4.48	5.76	0.65	5	-0.02	0.51
Coronet	100	136	2.72	3.30	0.05	15	0.04	0.20
GEANT	40	61	3.05	4.32	0.14	8	-0.20	0.36
Renater	43	56	2.60	3.88	0.10	9	-0.15	0.33

TABLE I: Topological properties, explained in Section 3.1, of the 10 real telecommunication networks.

C. Telecommunication networks

We select 10 real communication networks for case study. The topological properties of the 10 real telecommunication networks are described in Table 1. These 10 telecommunication networks include logical networks (representing the IP layer) and backbone transport networks (connected with optical fiber). This set of networks was selected in specialized databases [20], covering the telecommunication systems located in different areas of the world, i.e., DFN (German backbone X-WiN network), Cernet (China education and research network), Bt_US (Internet provided by BT in the US), GtsCe (GTS network in central Europe), Cogentco (IP backbone network provided by Cogentco), TataNld (Tata national long distance network), ATT_US (IP MPLS backbone network provided by AT&T), Coronet (IP backbone network provided by Cogent), GEANT (IP backbone network provided by GEANT), Renater (Internet provided by Renater).

IV. Results and discussion

In this section, detailed results and analysis on the real-world network via the proposed approach for assessing network recoverability are presented. For some evaluation items,

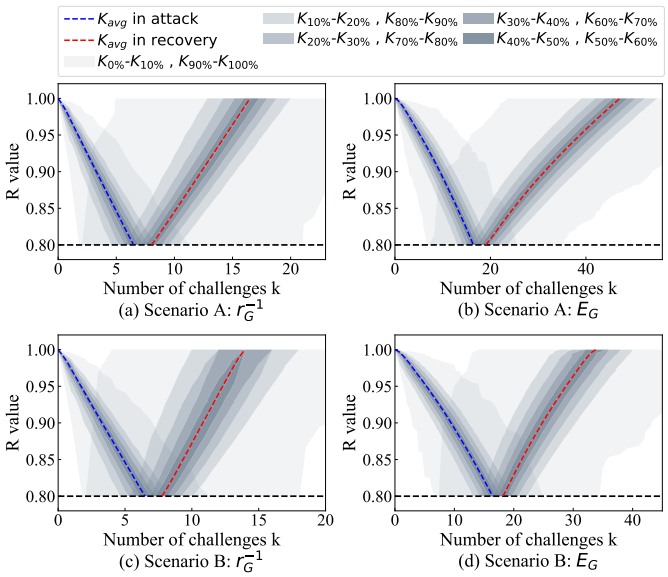


Fig. 3: Envelopes of the challenges for two scenarios and two robustness metrics (i.e., the inverse of the effective graph resistance r_G^{-1} and the network efficiency E_G) in DFN network, by random recovery strategy. Each envelope is based on 10^4 realizations.

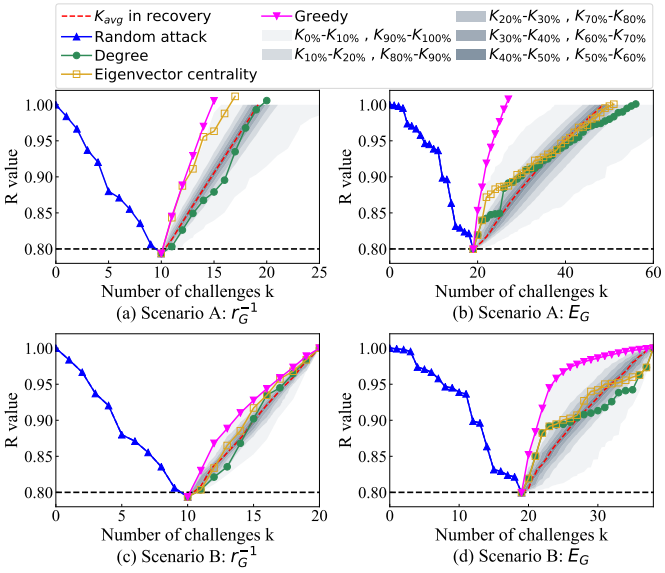


Fig. 4: Comparisons of different recovery strategies for one realization of attacks in DFN network. Two scenarios and two robustness metrics (i.e., the inverse of the effective graph resistance r_G^{-1} and the network efficiency E_G) are applied. Each envelope is based on 10^4 realizations.

we only present results for a specific network, i.e., DFN. We set the R-threshold as $\rho = 0.8$ in the following simulations. The approach translates easily to other networks or other robustness metrics.

A. Envelope examples and comparison

Each realization of processes consists of an attack process and a following recovery process. Figure 3 exemplifies the envelopes of the challenges in DFN network for two scenarios and two robustness metrics, r_G^{-1} and E_G, respectively, under the random recovery strategy. The envelopes for the attack processes are similar in different scenarios while Scenario A usually needs more challenges to recover the robustness metrics than Scenario B, if the random recovery strategy is employed. The total number of challenges $K_a + K_r$ could cover a wide range of values since the number of challenges $K_a + K_r$ is influenced by two random processes (i.e., attack and recovery).

Figure 3a and Figure 3c also illustrates that the function R-value of the average number of challenges $R[K_{avg}]$ for the robustness metric r_G^{-1} is almost linear, in both the attack process and the recovery process. For the robustness metric E_G, the function $R[K_{avg}]$ is slightly concave, illustrated in Figure 3b and Figure 3d. We will show that the concavity of the function $R[K_{avg}]$ could help to explain the behavior of the recoverability indicators.

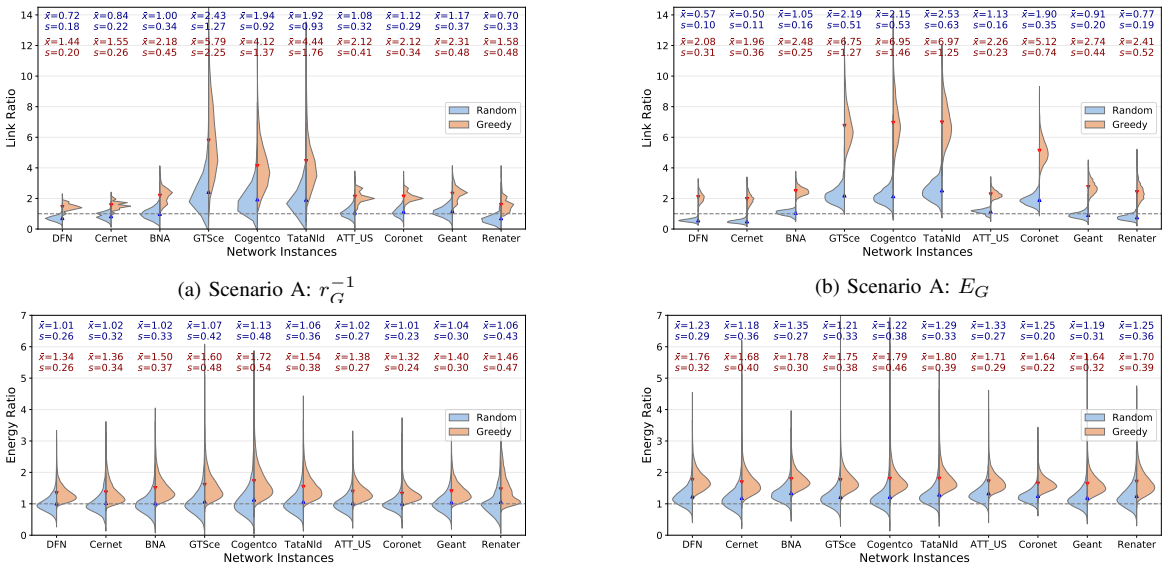
B. Comparison of recovery strategies

The envelope computation can be applied to compare the performance of different recovery strategies for a specific realization of attacks. Figure 4 shows different recovery strategies (e.g., random, minimum $d_i d_j$, minimum $c_i c_j$, greedy) for one realization of attack processes under random attack strategy in DFN network. The envelope of recovery processes by random recovery for the network efficiency E_G covers a larger surface than that of the inverse of the effective graph resistance r_G^{-1}. This implies that the network efficiency E_G in different realizations could deviate more from one another under the random recovery, and the performance of random recovery is more difficult to be guaranteed. The average challenge sequence $\{K_{avg}\}$ under the random recovery can be a standard to evaluate the performance of other recovery strategies.

Figure 4 shows that the performance of metric-based strategies, e.g., minimum degree product and minimum eigenvector centrality product, is not guaranteed. Especially for the network efficiency E_G, the metric-based strategies outperform the average of random strategy in the initial stage of recovery processes but degrade for more recovery challenges. Meanwhile, we notice that the greedy recovery usually upper bounds the random recovery envelopes. The R-value as a function of the number of challenges k under the greedy strategy is concave in the recovery process, which demonstrates the diminishing returns property of the recovery measures. Since the optimal recovery strategy is usually an NP-hard problem, we suspect that the greedy recovery can be a practical near-optimal recovery strategy for both robustness metrics, i.e., r_G^{-1} and E_G.

C. Overview of the Link Ratio and the Energy Ratio

We employ the proposed approach and the recoverability indicators η (including the Link Ratio η_L and the Energy Ratio η_E) to evaluate the 10 real telecommunication networks. Figure 5 shows the recoverability indicators under two different scenarios, two robustness metrics and two recovery strategies for 10 networks by violin plots. Violin plots are similar to box plots, except that they show the probability density of the ratios η at different values, which presents more insights about the ratios η under random circumstances. Moreover, violin



(a) Scenario A: r_G^{-1}

(b) Scenario A: E_G

(c) Scenario B: r_G^{-1}

(d) Scenario B: E_G

Fig. 5: Violin plots of the Link Ratio η_L in Scenario A and the Energy Ratio η_E in Scenario B. The average ratios $\tilde{x} = E[\eta]$ and the standard deviations $s = \sqrt{Var[\eta]}$ are presented on the top of each subplot. The blue surface and blue notes represent the random recovery strategy, and the red surface and blue notes represent the greedy recovery strategy. The average ratios are marked as triangle markers. Each histogram of η is based on 10^4 realizations.

plots can be applied to compare the performance of any two different strategies, e.g., the random and the greedy.

Figure 5 shows that almost all histograms of the ratio η, regardless of the scenarios, the strategies and the metrics, exhibit heavy-tailed distributions, while the greedy strategy presents a longer tail. Also, the ratio η has a wider range of values under the greedy strategy, which implies the greedy strategy has a higher probability to lead to a large ratio η, as well as a better recovery performance.

For both robustness metrics in Scenario A, DFN, Cernet and Renater have an average Link Ratio $E[\eta_L] < 1$ for the random strategy, which implies a relatively low recovery capability. By contrast, GTSce, Cogentco and TataNld have a large average Link Ratio $E[\eta_L] > 1$, which outperform other networks much under both the random strategy and the greedy strategy. The network with a larger average Link Ratio usually has a larger diameter φ, then the new established links in Scenario A could shorten the diameter φ and increase the topological approach (r_G^{-1} or E_G) more.

The Energy Ratio η_E presents different behaviors of the Link Ratio η_L compared with Scenario A. The average Energy Ratios $E[\eta_E]$ for the robustness metric r_G^{-1} approximate 1 under the random strategy, which can be explained by the fact that the function $R[K_{avg}]$ is almost linear (illustrated in Section 4.1), and thus the energy $S_a \approx S_r$. Since the function $R[K_{avg}]$ is concave for the robustness metric E_G^{-1} and thus the energy $S_a < S_r$, the average Energy Ratios $E[\eta_E]$ for different networks are slightly larger than 1. The average Energy Ratio $E[\eta_E]$ in Scenario B under the greedy strategy is usually located in the tail of the distribution of the Link Ratio η_L under the random strategy, which demonstrates that the greedy strategy can update the recoverability of networks much.

D. Relation between Scenario A and Scenario B

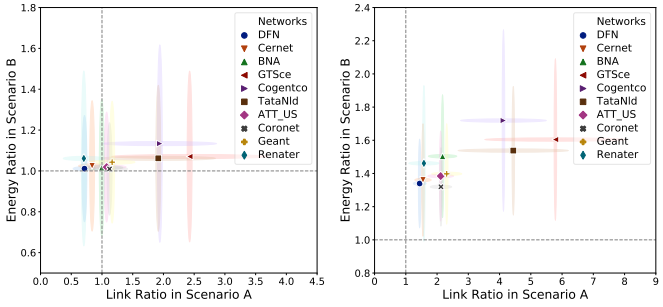
To compare the recoverability among different networks, we employ the SA-SB plots to show the relation of the Link Ratio in Scenario A and the Energy Ratio in Scenario B under a determined recovery strategy. SA-SB plots are divided as 4 quadrants by the reference lines of the Link Ratio $\eta_L = 1$ and the Energy Ratio $\eta_E = 1$ in order to easily assess the recoverability by the location of the average ratios $E[\eta_L]$ and $E[\eta_E]$. Figure 6 shows the average ratios $E[\eta]$ and the standard deviations $\sqrt{Var[\eta]}$ for the real-world networks in SA-SB plots.

Figure 6 shows that the recoverability under two different scenarios has a weak correlation, e.g., a Link Ratio η_L in Scenario A does not lead to a higher η_L in Scenario B. We can also observe that all the average Energy Ratios $E[\eta_E]$ are located in the first and the second quadrant, which demonstrates a good recoverability of tested networks in Scenario B. However, the average Link Ratios $E[\eta_L]$ in the second quadrant suggest the topological improvement for these networks in Scenario A.

For a determined robustness metric, both the average Link Ratio $E[\eta_L]$ and the Energy Ratio $E[\eta_E]$ can be increased by applying the greedy strategy, but the performance can be different. For example, the average Link Ratio $E[\eta_L]$ of Cogentco is larger than that of TataNld under the random strategy but smaller than that of TataNld under the greedy strategy, which implies that the performance of a recovery strategy strongly depends on the network topology.

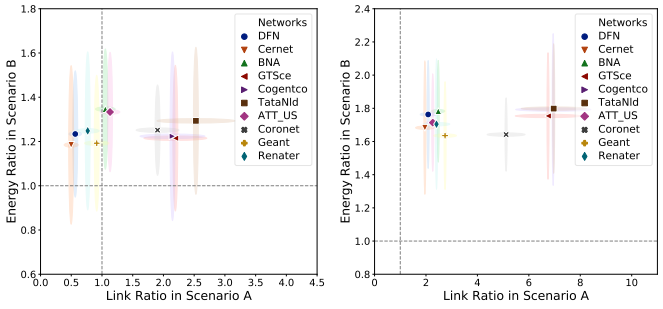
V. Summary

This paper proposes a topological approach for evaluating the network recoverability in two scenarios, which extends the application of the framework [3] of network robustness.



(a) Random recovery: r_G^{-1}

(b) Greedy recovery: r_G^{-1}



(c) Random recovery: E_G

(d) Greedy recovery: E_G

Fig. 6: SA-SB plots of the Link Ratio η_L and the Energy Ratio η_E for two robustness metrics (i.e., the inverse of the effective graph resistance r_G^{-1} and the network efficiency E_G). The dark markers represent the average ratios $E[\eta]$, and the cross indicates the value range $\left[E[\eta] - \sqrt{Var[\eta]}, E[\eta] + \sqrt{Var[\eta]}\right]$.

We assess the recoverability of 10 real communication networks for two different path-based robustness metrics, i.e., the network efficiency and the effective graph resistance. In accordance with the results, the network recoverability presents different behaviors between link-based Scenario A and energy-based Scenario B. All the telecommunication networks have a healthy recovery capability in Scenario B under the random recovery strategy, i.e. the average Energy Ratio $E[\eta_E] > 1$, while three of the networks (DFN, Cernet and Renater) suggest topological improvements for the recoverability in Scenario A, i.e., the average Link Ratio $E[\eta_L] < 1$. The goodness of the recoverability in Scenario B can be explained by the concavity of the R-value as a function of the number of challenges. The network recoverability is also strongly related to the recovery strategy. Comparing the performance of different recovery strategies, the greedy recovery strategy exhibits a good performance for the investigated robustness metrics and thus improves the network recoverability.

Acknowledgment

We are grateful to Prof. Jose L. Marzo and Prof. Robert Kooij for useful comments.

References

[1] J. L. Marzo, S. G. Cosgaya, N. Skorin-Kapov, C. Scoglio, and H. Shakeri, "A study of the robustness of optical networks under massive failures," *Optical Switching and Networking*, vol. 31, pp. 1–7, 2019.

[2] E. K. Çetinkaya and J. P. Sterbenz, "A taxonomy of network challenges," in *2013 9th International Conference on the Design of Reliable Communication Networks (DRCN)*. IEEE, 2013, pp. 322–330.

[3] P. Van Mieghem, C. Doerr, H. Wang, J. M. Hernandez, D. Hutchison, M. Karaliopoulos, and R. Kooij, "A framework for computing topological network robustness," *Delft University of Technology, Report20101218*, 2010.

[4] P. Cholda, A. Mykkeltveit, B. E. Helvik, O. J. Wittner, and A. Jajszczyk, "A survey of resilience differentiation frameworks in communication networks," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 4, pp. 32–55, 2007.

[5] A. Pašić, R. Girão-Silva, B. Vass, T. Gomes, and P. Babarczi, "Fradir: A novel framework for disaster resilience," in *2018 10th International Workshop on Resilient Networks Design and Modeling (RNDM)*. IEEE, 2018, pp. 1–7.

[6] J. L. Marzo, E. Calle, S. G. Cosgaya, D. Rueda, and A. Mañosa, "On selecting the relevant metrics of network robustness," in *2018 10th International Workshop on Resilient Networks Design and Modeling (RNDM)*. IEEE, 2018, pp. 1–7.

[7] D. F. Rueda, E. Calle, and J. L. Marzo, "Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements," *Journal of Network and Systems Management*, vol. 25, no. 2, pp. 269–289, 2017.

[8] X. Pan and H. Wang, "Resilience of and recovery strategies for weighted networks," *PloS one*, vol. 13, no. 9, p. e0203894, 2018.

[9] T. Afrin and N. Yodo, "A concise survey of advancements in recovery strategies for resilient complex networks," *Journal of Complex Networks*, 2018.

[10] A. Majdandzic, B. Podobnik, S. V. Buldyrev, D. Y. Kenett, S. Havlin, and H. E. Stanley, "Spontaneous recovery in dynamical networks," *Nature Physics*, vol. 10, no. 1, p. 34, 2014.

[11] W. Sun and A. Zeng, "Target recovery in complex networks," *The European Physical Journal B*, vol. 90, no. 1, p. 10, 2017.

[12] J. Wang, C. Qiao, and H. Yu, "On progressive network recovery after a major disruption," in *2011 IEEE INFOCOM Proceedings*. IEEE, 2011, pp. 1925–1933.

[13] K. Al Sabeh, M. Tornatore, and F. Dikbiyik, "Progressive network recovery in optical core networks," in *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*. IEEE, 2015, pp. 106–111.

[14] D. Z. Tootaghaj, H. Khamfroush, N. Bartolini, S. Ciavarella, S. Hayes, and T. La Porta, "Network recovery from massive failures under uncertain knowledge of damages," in *2017 IFIP Networking Conference (IFIP Networking) and Workshops*. IEEE, 2017, pp. 1–9.

[15] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Physical review letters*, vol. 87, no. 19, p. 198701, 2001.

[16] P. Van Mieghem, K. Devriendt, and H. Cetinay, "Pseudoinverse of the laplacian and best spreader node in a network," *Physical Review E*, vol. 96, no. 3, p. 032311, 2017.

[17] S. Trajanovski, J. Martín-Hernández, W. Winterbach, and P. Van Mieghem, "Robustness envelopes of networks," *Journal of Complex Networks*, vol. 1, no. 1, pp. 44–62, 2013.

[18] P. Van Mieghem, *Data Communications Networking*. Purdue University Press, 2006.

[19] C. Li, H. Wang, W. De Haan, C. Stam, and P. Van Mieghem, "The correlation of metrics in complex networks with applications in functional brain networks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2011, no. 11, p. P11018, 2011.

[20] S. Knight, H. Nguyen, N. Falkner, R. Bowden, and M. Roughan, "The internet topology zoo," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 9, pp. 1765 –1775, october 2011.

[21] Y. T. Woldeyohannes and Y. Jiang, "Measures for network structural dependency analysis," *IEEE Communications Letters*, vol. 22, no. 10, pp. 2052–2055, 2018.

[22] W. Ellens, F. Spieksma, P. Van Mieghem, A. Jamakovic, and R. Kooij, "Effective graph resistance," *Linear Algebra and its Applications*, vol. 435, no. 10, pp. 2491–2506, 2011.

[23] X. Wang, J. L. Dubbeldam, and P. Van Mieghem, "Kemeny's constant and the effective graph resistance," *Linear Algebra and its Applications*, vol. 535, pp. 231–244, 2017.

[24] X. Wang, E. Pournaras, R. E. Kooij, and P. Van Mieghem, "Improving robustness of complex networks via the effective graph resistance," *The European Physical Journal B*, vol. 87, no. 9, p. 221, 2014.

[25] A. Tizghadam and A. Leon-Garcia, "Autonomic traffic engineering for network robustness," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 1, pp. 39–50, 2010.