DomiRank Centrality: revealing structural fragility of complex networks via node dominance

Marcus Engsig*
Directed Energy Research Centre, Technology Innovation Institute, Abu Dhabi, United Arab Emirates.

Alejandro Tejedor†
Institute for Biocomputation and Physics of Complex Systems (BIFI), Universidad de Zaragoza, 50018 Zaragoza, Spain
Department of Theoretical Physics, University of Zaragoza, Zaragoza 50009, Spain and
Department of Civil and Environmental Engineering, University of California, Irvine, Irvine, CA 92697, USA.

Yamir Moreno‡
Institute for Biocomputation and Physics of Complex Systems (BIFI), University of Zaragoza, 50018 Zaragoza, Spain
Department of Theoretical Physics, University of Zaragoza, Zaragoza 50009, Spain and
CENTAI Institute, Turin 10138, Italy.

Efi Foufoula-Georgiou§
Department of Civil and Environmental Engineering, University of California, Irvine, Irvine, CA 92697, USA. and
Department of Earth System Science, University of California Irvine, Irvine, CA, USA

Chaouki Kasmi¶
Directed Energy Research Centre, Technology Innovation Institute, Abu Dhabi, United Arab Emirates

(Dated: May 17, 2023)

Determining the key elements of interconnected infrastructure and complex systems is paramount to ensure system functionality and integrity. This work quantifies the dominance of the networks' nodes in their respective neighborhoods, introducing a novel centrality metric, DomiRank, that integrates local and global topological information via a tunable parameter. We present an analytical formula and an efficient parallelizable algorithm for DomiRank centrality, making it applicable to massive networks. DomiRank systematically outperforms other centrality metrics in generating targeted attacks that effectively compromise network structure and disrupt its functionality for synthetic and real-world topologies. Moreover, we show that DomiRank-based attacks inflict more enduring damage in the network, hindering its ability to rebound, and thus, impairing system resilience. DomiRank centrality capitalizes on the competition mechanism embedded in its definition to expose the fragility of networks, paving the way to design strategies to mitigate vulnerability and enhance the resilience of critical infrastructures.

I. INTRODUCTION

Complex systems consist of many interacting components, with dynamics and emergent behavior being system properties. However, not all the constituents of such systems are equivalently central to their structure and dynamics, and in some systems, a few elements might be critical to ensure the integrity of the complex system's structure or functionality [1–10]. Our capacity to accurately and efficiently identify key elements of such complex systems is at the core of actions as diverse as providing the most suitable website on an internet search [11], defining a vaccination scheme to mitigate the spreading of a disease [12–15], or ensuring the integrity and functionality of transportation networks and critical infrastructures [16–20].

Network theory, by abstracting complex systems as a collection of nodes (system constituents) and links (interactions), has been instrumental in providing a general framework to assess different aspects of the relative importance of nodes in a network, yielding different node centrality definitions depending on the evaluated aspects, ranging from considering only the number of links a node has (degree centrality), aggregating the importance of a node's neighborhood (e.g., eigenvector [21], Katz [22], and PageRank [11] centralities) to considering the relative position of the node in the network (e.g., closeness and betweenness [23] centralities) or the role of the node in a dynamic process (e.g., current-flow [24], entanglement[25], and random-walk [26] centralities). The performance of these centralities is often benchmarked against each other in evaluating their capacity to generate targeted attacks to dismantle the

* marcus.w.engsig@gmail.com
† alej.tejedor@gmail.com
‡ yamir.moreno@gmail.com
§ efi@uci.edu
¶ chaouki.kasmi@tii.ae

network's structure or disrupt its functionality. In fact, centrality metrics have a pivotal role in designing mitigation strategies to enhance network robustness and resilience, critical emerging properties of utmost importance to maintain our day-to-day privileges and necessities, which heavily rely on interconnected infrastructures such as the internet [1, 27, 28] or the power grid [29–31].

In this work, we propose a novel centrality, the 'DomiRank' centrality. Intuitively, it quantifies the degree of dominance of nodes in their respective neighborhoods. Thus, high scores of DomiRank centrality are associated with nodes surrounded by a large number of unimportant (e.g., typically low-degree) nodes, which they dominate. This new centrality gives importance to nodes based on how locally *dominant* they are, where the extent of the *dominance* effect can be modulated through a tuneable parameter (σ). Contrary to other centralities such as eigenvector or PageRank, and due to an implicit competition mechanism in the definition of DomiRank, connected nodes tend to have more disparate scores in terms DomiRank centrality. We demonstrate that the inherent properties of DomiRank make both synthetic and real-world networks particularly fragile to the DomiRank centrality-based attacks, outperforming all other centralities-based attacks. Furthermore, we show that the DomiRank-based attack outperforms most of the computationally feasible iterative (recomputed after each node removal) attack methods (i.e., degree, PageRank, eigenvector, and Katz), and it causes more enduring damage than the efficient iterative betweenness attack. We provide both an analytical formula and a computationally efficient iterative algorithm for DomiRank, enabling it to be computed on graphical processing units (GPUs) with a parallelizable computational cost scaling with the number of links, allowing the centrality to be computed for massive sparse networks.

II. DEFINING DOMIRANK

We define DomiRank centrality, denoted $\mathbf{\Gamma} \in \mathbb{R}_{N\times 1}$, as the stationary solution of the following dynamical process

$$\frac{\partial \mathbf{\Gamma}(t)}{\partial t} = \alpha A(\theta \mathbf{1}_{N\times 1} - \mathbf{\Gamma}(t)) - \beta \mathbf{\Gamma}(t), \tag{1}$$

where $A \in \mathbb{R}_{N\times N}$ is the adjacency matrix of the network $\mathcal{N}$ and $\{\alpha, \beta, \theta \in \mathbb{R} : \lim_{t\to\infty} \mathbf{\Gamma}(t) = \mathbf{\Gamma} \in \mathbb{R}_{N\times 1}\}$.

From a simple model perspective, $\mathbf{\Gamma}(t)$ can be interpreted as the evolving fitness of the individuals in a population subject to competition. Two different processes can alter the fitness of each individual: (*i*) *Natural relaxation* - fitness naturally converges to zero at a rate proportional to a constant β; (*ii*) *Competition* – Individuals compete with each neighbor for a limited amount of resources, with their fitness reflecting their capacity to successfully maintain those resources. An individual's fitness tends to increase by being connected to neighbors whose fitness are below the threshold for domination (θ), and decreases otherwise. Thus, the fitness of each individual changes proportionally to $(\sum_{i\in\text{neighbors}} \theta - \Gamma_i(t))$, where the proportionality constant is denoted by α and represents the degree of competition between neighboring individuals.

Notably, the fitness score of a given individual k is a function of (*i*) *its number of neighbors:* the larger the number of neighbors of k, the more resources at stake, and therefore the larger the potential of k to increase/decrease its fitness, and; (*ii*) *its neighbors' neighborhood:* having neighbors lacking dominance in their respective neighborhoods (excluding individual k) due to either the absence of neighbors or the presence of dominant neighbors increases the fitness of individual k. In other words, a given individual results in having a high value of fitness via the dominance of its neighborhood, either due to the direct dominance of its neighbors (quasi-solitary individuals) or via collusion (joint dominance) emerging from the synergetic action of several individuals in suppressing the fitness of a common neighbor while incrementing their respective fitness. The DomiRank centrality is thus based on the concept of dominance to provide scores to nodes that contextualize their importance in their neighborhood.

From Eq. 1, we note that the centrality converges when $\alpha A(\theta \mathbf{1}_{N\times 1} - \mathbf{\Gamma}(t)) = \beta \mathbf{\Gamma}(t)$, for which the analytical expression (see appendix for proof) of the DomiRank centrality $\mathbf{\Gamma} \in \mathbb{R}_{N\times 1}$ is given by:

$$\mathbf{\Gamma} = \theta\sigma(\sigma A + I_{N\times N})^{-1} A \mathbf{1}_{N\times 1}, \tag{2}$$

where $\{\sigma = \frac{\alpha}{\beta} \in \mathbb{R} : \det(\sigma A + I_{N\times N}) \neq 0\}$. A convergence interval can be defined for σ, such that it is bounded as follows:

$$\sigma(\mathcal{N}) \in \left(0, \frac{-1}{\lambda_N}\right), \tag{3}$$

where λ_N represents the minimum (largest negative) eigenvalue of A. Also note that the threshold for domination, θ, only plays a rescaling role on the resulting DomiRank centrality, and therefore, we choose $\theta = 1$ without loss of generality.

The DomiRank Centrality is thus modulated by the ratio $\sigma = \frac{\alpha}{\beta}$. To provide further insight into the effect of this parameter on the scores of the centrality, we explore the DomiRank distribution values for varying values of σ computed for a very simple network (see Fig. 1). As $\sigma \to 0$, the competition between the different nodes vanishes, and the importance of the nodes reduces to their degree (see Figure 1a,d and Eq. 2). Conversely, as $\sigma \to \frac{-1}{\lambda_N}$, the competition is maximum, and each node is either dominating its neighbors or dominated by one of its neighbors (see Fig. 1c). Interestingly, at this end of the spectrum, the number of neighbors still plays a role, but the network structure is the key feature defining the scores, where the synergistic competitive action of not

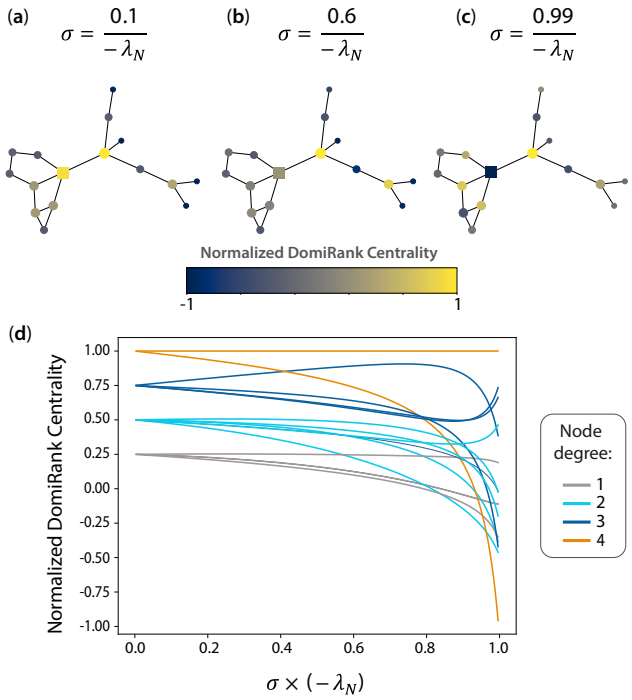

FIG. 1. **DomiRank for different levels of competition (σ).** DomiRank centrality displayed on the nodes of a simple network with $N = 15$ nodes for (a) low, (b) medium, and (c) large values of σ. Panel d shows the DomiRank centrality as a function of σ, wherein each solid line represents a specific node (color encoding node degree).

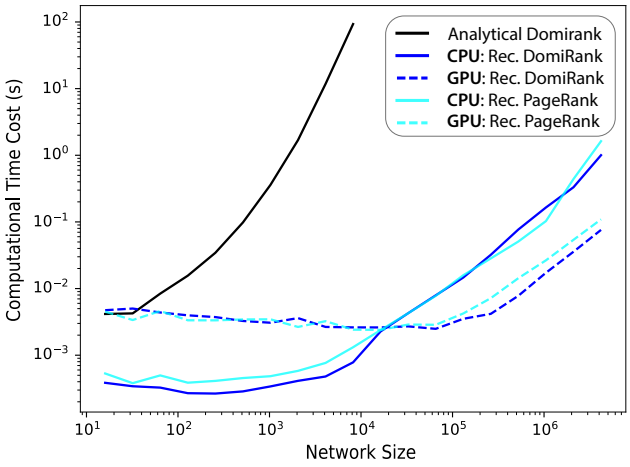

FIG. 2. **Computational cost of DomiRank.** Mean (30 samples) computational costs to compute DomiRank analytically (black solid line) and estimate it recursively on a multi-threaded CPU and on the GPU, as a function of the network size N. The mean DomiRank computational cost is also compared with the mean computational cost for estimating PageRank on the same multi-threaded CPU and GPU. The convergence criterion is evaluated using the $L1$ error between two consecutive iterations - i.e., $||\mathbf{\Gamma}(t) - \mathbf{\Gamma}(t+dt)||_1 < \epsilon$, with a threshold set to $\epsilon = 1 \times 10^{-6}$ (note that for the chosen convergence threshold, the Spearman correlation to the analytic solution is > 0.9999999).

directly connected nodes might result in their joint dominance in their respective neighborhoods. On that note, Figure 1c,d shows how a node with a relatively high degree (square node) results in the lowest value of DomiRank centrality. This low value is the result of the joint domination by its four neighbors, which despite having the same or lower degree as the dominated node, are able to increase their relative fitness by dominating their respective non-overlapping unfit neighborhoods and, together, the mentioned node. Intermediate values of σ (e.g., see Fig. 1b) represent different domination strategies based on utilizing different balances of local node-based (low σ) and global network-structure-based (high σ) properties.

Beyond the interpretability of DomiRank and its versatility via its parameter σ, one of the key advantages of the proposed centrality is that it can be calculated efficiently through iteration in a parallelizable algorithm (see Fig. 2),

$$\mathbf{\Gamma}(t + dt) = \mathbf{\Gamma}(t) + \beta[\sigma A(\mathbf{1}_{N\times 1} - \mathbf{\Gamma}(t)) - \mathbf{\Gamma}(t)]dt, \quad (4)$$

with a computational cost C:

$$C(t, A) = t(m + 5N), \quad (5)$$

which scales with $\mathcal{O}(m)$, where m is the number of links, and thus the DomiRank scales with $\mathcal{O}(N^2)$ in the worst case (fully connected graph). Importantly, eq. 5 can be distributed among κ cores given that $\kappa \leq m$ for sparse matrices, which allows for parallel computation and efficient execution on GPUs. Fig. 2 shows the computational costs of calculating DomiRank (analytically and recursively) and PageRank (recursively) for different network sizes showing: (i) the high computational cost for the analytic computation of DomiRank, as it requires matrix inversion, (ii) the comparable computational cost of the DomiRank to that of PageRank on both CPU and GPU infrastructure, and (iii) that the latency of computing DomiRank on the GPU is the computational bottleneck unless the number of links is significantly larger the number of GPU cores, i.e., $m >> \kappa$. Thus, DomiRank centrality is computable even for massive (sparse) networks, allowing computational time costs under one second for networks consisting of millions of nodes.

III. EVALUATING DOMIRANK

In order to gain further insight into the capabilities of DomiRank, and to benchmark its performance with respect to the other most commonly used centralities, we examine the efficacy of targeted attacks based on DomiRank centrality for different network topologies, analyzing its ability to dismantle the network structure and functionality, and contrasting its performance with those

of the attacks based on other centralities.

A. Structural Network robustness

In this section, we evaluate the structural robustness of different networks, both synthetic and real-world topologies, under sequential node removal (attacks) based on different centrality metrics, and compare the results with those obtained based on DomiRank. To evaluate network robustness, we use its most commonly used proxy, the evolution of the relative size of the largest connected component (LCC) [32–35], whilst the network is undergoing sequential node removal. We compare the robustness of the different networks for the different attacks by directly comparing the resulting LCC curves, and for simplicity and enhanced comparability, we also use the area under that curve as a summary indicator of robustness (the larger the area, the more robust is the network under that particular attack).

We start our analysis with synthetic toy networks, consisting of a reduced number of nodes, but wherein their graphical representation still allows us to visually identify patterns on the centrality distributions for different topologies, gaining insight into the interpretation of DomiRank and its performance when compared with different centralities. Particularly, we perform targeted attacks based on DomiRank and nine other centralities for three different topologies: 2D-regular lattice [36], Erdős-Rényi [37], and a Barabasi-Albert [38] networks. Note that for each topology, the range of σ was explored to determine its optimal value to dismantle the network (i.e., minimize area under the LCC curve). Fig. 3a,b,c reveals that the DomiRank centrality-based attack dismantles these three networks more efficiently than all other tested centrality-based attacks. More particularly, DomiRank excels at dismantling regular networks (Fig. 3a). It is not surprising that for this topology, DomiRank centrality produces the most effective attack for large values of σ, wherein network structure is overweighed to the detriment of local node properties. This value of σ leads to a DomiRank distribution wherein if a node is important (*dominating* node), all of its adjacent nodes are not important (*dominated* node), and vice-versa. Applying a similar DomiRank-based attack strategy to a more heterogeneous network, such as Erdős-Rényi (see Fig. 3b), still leads to the highest fragility of the network, also capitalizing on the built-in competition mechanism of DomiRank (high value of σ) that penalizes connections between nodes labeled as highly central, reducing those instances to situations wherein connected nodes possess disjoint neighborhoods to exert their respective dominance. For most of the other centrality metrics, including Betweeness, Eigenvector, PageRank and Katz, highly central nodes permeate their centrality to their direct connections (see Fig. 3e). However, that *by-contact* importance only reflects the centrality of their truly important neighbor, yielding attack sequences less efficient than DomiRank. As the networks display more hub-dominated topologies (e.g., scale-free), we expect that the optimal value of σ for the most efficient attack decreases, emphasizing nodal properties (degree) with respect to the neighborhood structure. In the toy example for a network generated by a Barabasi-Albert model (see Fig. 3c), DomiRank still outperforms other centrality-based attacks in dismantling the network. In this case, the improvement is incremental since the most relevant information to destroy the network is local (node degree), and most of the centralities converge to a similar nodal ranking.

We further investigate the efficacy of the attack strategies based on the DomiRank centrality by dismantling larger synthetic networks ($N = 1000$) with varying degrees ($2 < \bar{k} < 40$) for numerous topologies. Particularly, we analyze the robustness of Watts-Strogatz [39], stochastic-block-model [40], Erdős-Rényi, random geometric graph [41], and Barabasi-Albert networks, under nine different targeted attack strategies based on different centralities, including DomiRank, which revealed itself as the most efficient at dismantling all synthetic networks (Fig. 4a-f). As hinted from our previous analysis of the toy networks, the margin by which the DomiRank-based attack outperforms the other strategies relates to the topological properties of the networks, which also dictate the optimal value of σ. Thus, for the Barabasi-Albert topology (hub-dominated) DomiRank offers only an incremental improvement in the efficiency at dismantling the network (see Fig. 4f). On the other hand, for networks with meso-to-macro scale structural features (e.g., regularity or modularity) that dominate over the local node-based properties, DomiRank centrality significantly outperforms all other centralities (Fig. 4d). This also occurs for the Erdős-Rényi (Fig. 4b,e) and Watts-Strogatz networks (Fig. 4a).

Real networks introduce several properties that are hard to produce simultaneously using generative models. Therefore for a more thorough and general benchmark of DomiRank, we analyze various real networks topologies of various sizes: (g) hub-dominated transport network (RyanAir connections) [42], (h) neural network (C-elegans) [3, 43, 44], (i) spatial network (power-grid of the Western States of the United States of America) [39], (j) citation network (high-energy-physics arXiv) [45, 46], (k) massive social network (LiveJournal users and their connections) [46], and (l) massive spatial transport network (Full US roads) [45]. Our results are consistent with the results for synthetic networks, showing that the DomiRank is able to dismantle the networks more efficiently than all the other centrality-based attacks tested (see Fig. 4g-l). Another interesting phenomenon, also observed for the synthetic networks, is that the DomiRank-based attacks remove links more efficiently than previous methods (see SM). This means that for many of these networks, not only is the DomiRank better at reducing the size of the largest cluster size, but it also more severely cripples its connectivity, yielding not only to an overall faster

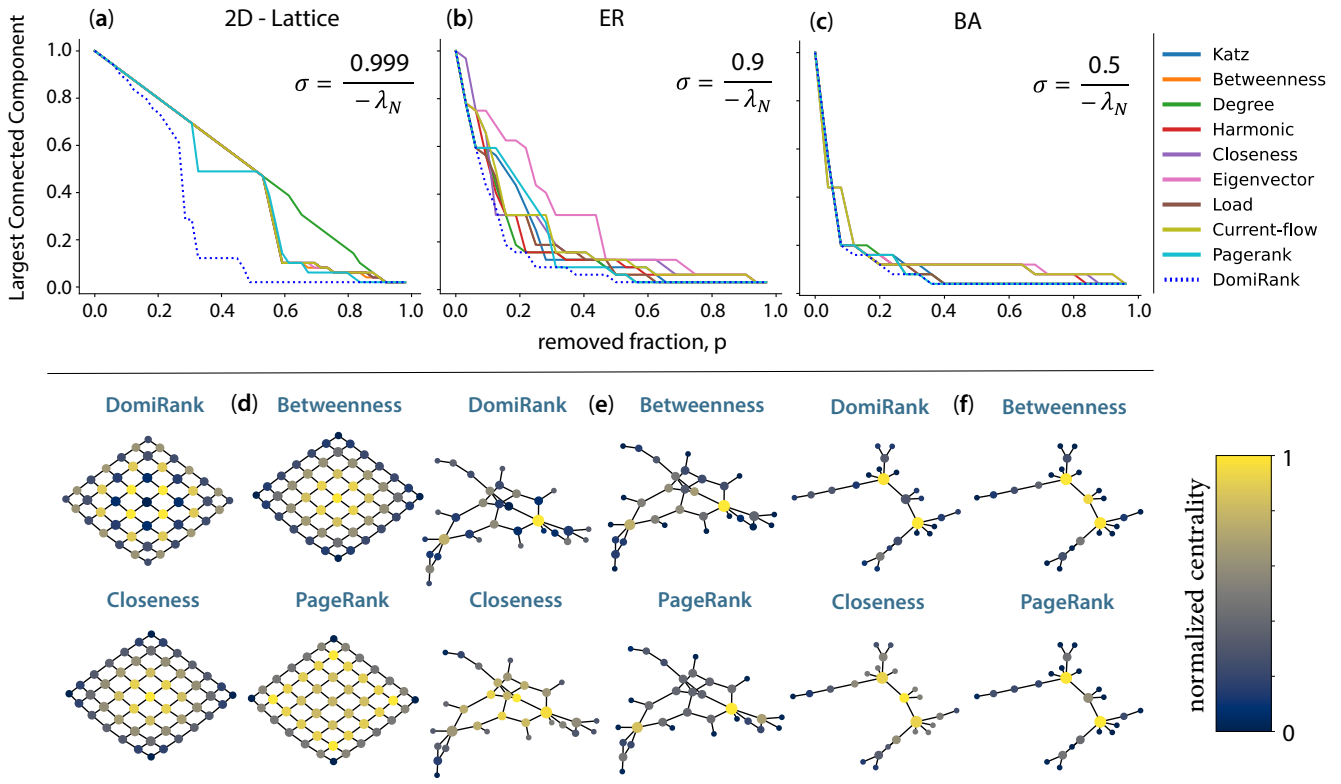

FIG. 3. **Comparing DomiRank with other centralities on toy networks.** Evolution of the relative size of the largest connected component (robustness) whilst undergoing sequential node removal according to their descending scores of DomiRank, betweenness, closeness, and PageRank centralities for toy networks: (a) 2D regular lattice ($N = 49$), (c) Erdős-Rényi (ER; $N = 32$), and (e) Barabasi-Albert (BA; $N = 25$). Panels d,e, and f show the graphical representation of the networks, where the nodes are colored according to the value of their centralities.

but also a more thorough dismantling of the network. However, we note that for the social network analyzed (Fig 4k), the PageRank-based attack outperforms the one based on DomiRank. We attribute this phenomenon to the presence of structural heterogeneity in the network topology (i.e., different structures in different subgraphs of the network). This heterogeneity hinders the assessment of node importance by DomiRank with a single value of σ for the whole network. In the SM material, we provide evidence showing that, indeed, heterogeneity can lead DomiRank to underperform, hinting also potential approaches to address the evaluation of networks exhibiting heterogeneity.

Also note that the results shown in Fig. 4h,j,l correspond to directed graphs. In the case of directed graphs, the adjacency matrix used in the definition of DomiRank (e.g., Eq. 2) should correspond to the reverse of the graph relevant for the transfer of resources (e.g., information, traffic, etc.) to be consistent with the underlying concept of dominance.

The analysis of synthetic networks and real-world topologies has demonstrated the capacity of DomiRank to integrate local (node) and mesoscale information of the network, which, together with the competition mechanism embedded in its definition, produces centrality distributions that efficiently dismantle the networks by avoiding redundant scores in neighboring nodes (importance by-contact). This apparent handicap for other centralities could be addressed at the cost of recomputing the centrality distributions after each node removal. Note that this cost is prohibitive for distance-based or process-based metrics such as closeness, betweenness, or load centralities, even for networks of modest sizes as, for instance, betweenness has a computational complexity that scales with $\mathcal{O}(Nm)$ and $\mathcal{O}(Nm + N^2 \log N)$ for unweighted and weighted graphs respectively [47]. Despite this limitation, and for the sake of completeness, we also benchmark the DomiRank centrality distribution (computed once before the beginning of the attack) with the targeted attacks based on sequentially recomputed centralities.

Fig. 5a-d displays the increase in performance of various centrality-based attacks when recomputed iteratively, particularly for betweenness centrality. In fact, for all the synthetic topologies tested, iterative betweenness and load centralities lead to the most efficient attacks at dismantling networks by a large margin. Notably, the attacks based on pre-computed DomiRank centrality gener-

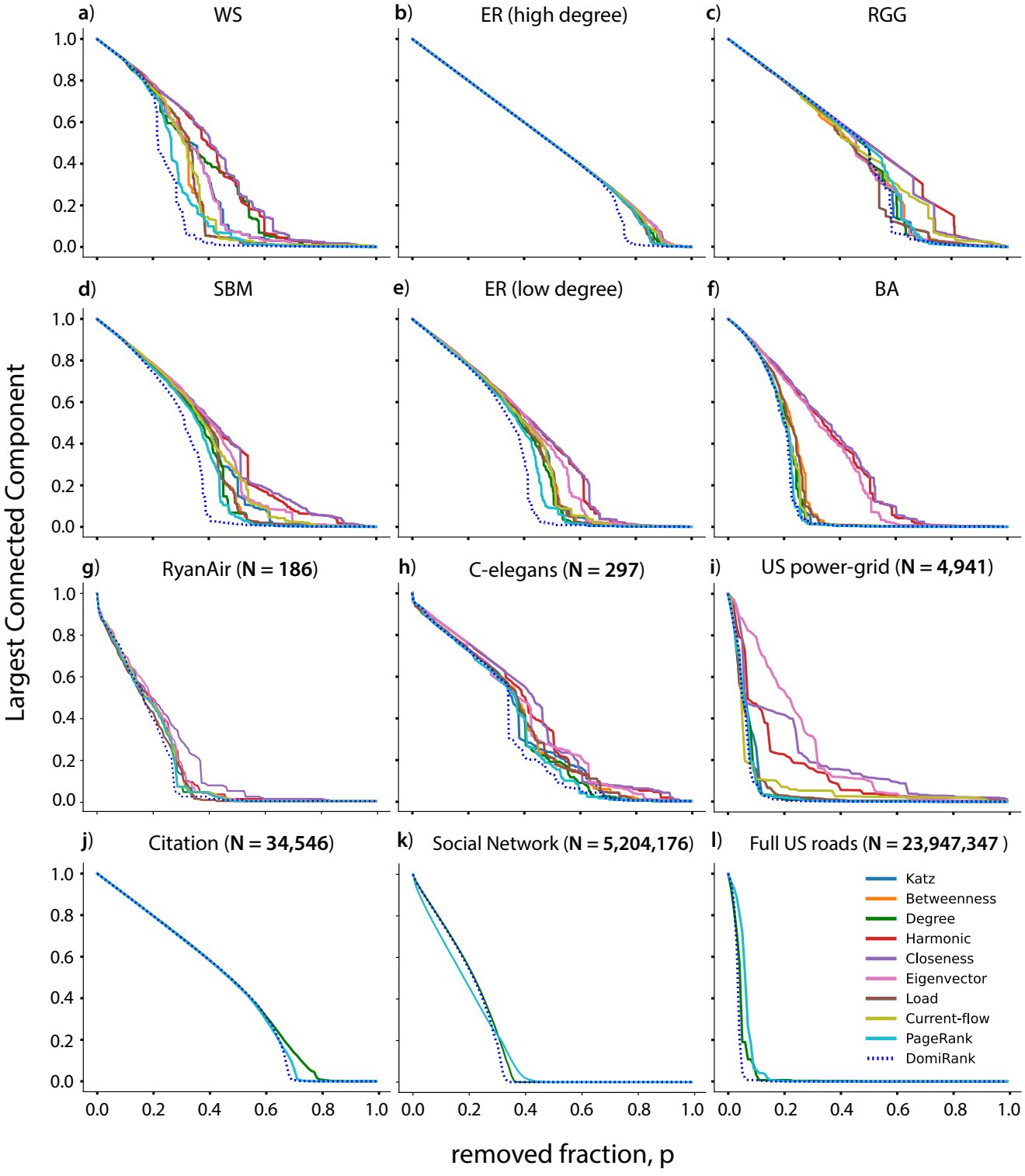

FIG. 4. **Centrality-based attacks on synthetic and real-world networks.** Evolution of the relative size of the largest connected component (robustness) whilst undergoing sequential node removal according to descending scores of various centrality measures for different synthetic networks of size $N = 1000$: (a) Watts-Strogratz (WS; small-world, $\bar{k} = 4$), Erdős-Rényi (ER) with (b) high ($\bar{k} = 20$) and (e) low link density ($\bar{k} = 6$), (c) random geometric graph (RGG; $\bar{k} = 16$), (d) stochastic block model (SBM; $\bar{k} = 7$), and (f) Barabasi-Albert (BA; $\bar{k} = 6$). The performance of the attacks based on the different centrality metrics is also shown for different real networks: (g) hub-dominated transport network (airline connections, $\bar{k} = 16$), (h) neural network (worm, $\bar{k} = 29$), (i) spatial network (power-grid, $\bar{k} = 3$), (j) citation network ($\bar{k} = 25$), (k) massive social network ($\bar{k} = 19$), and (l) massive spatial transport network (roads, $\bar{k} = 5$). Note that for panels j, k, and l, where massive networks are shown, only a few attack strategies are displayed due to the impossibility of computation of the rest.

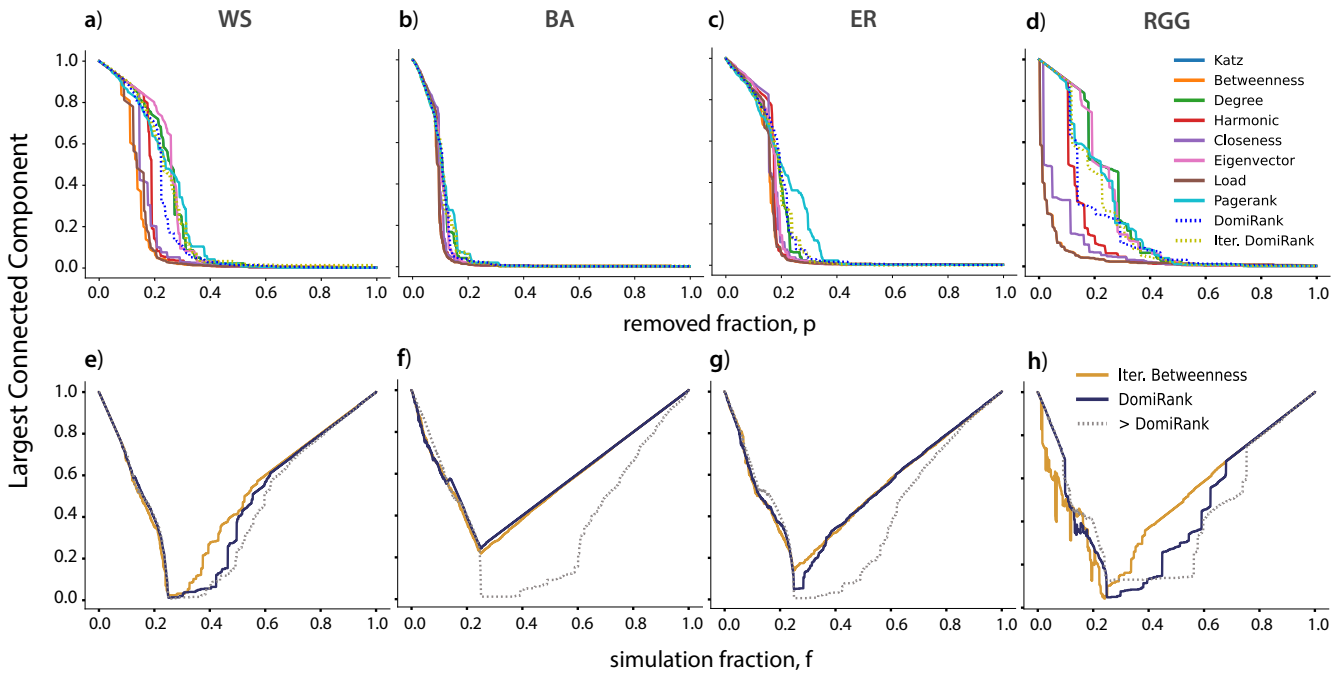

FIG. 5. **Assessing the effect of iterative centrality-based attacks and recovery mechanisms on network resilience.** Panels a-d show the evolution of the relative size of the largest connected component (robustness) of various synthetic networks of size $N = 500$, namely; (a) Watts-Strogatz (WS; $\bar{k} = 4$), (b) Barabasi-Albert (BA; $\bar{k} = 6$), (c) Erdős-Rényi (ER; $\bar{k} = 5$), and (d) random geometric graph (RGG; $\bar{k} = 7$), undergoing sequential node removal based on iterative attack strategies and the pre-computed DomiRank. Panels e-h show the evolution of the relative size of the largest connected component for the same networks undergoing sequential node removal based on pre-computed DomiRank (optimal and high σ) and iterative betweenness, where a stochastic first-in-first-out node recovery (stack recovery implementation) process with a probability of recovery $p = 0.25$ each time step is implemented.

ally outperform other attacks based on iterative centralities that are computationally feasible for medium, large, and massive networks - i.e., iterative degree, PageRank, eigenvector, Katz. Note that attacks based on iterative DomiRank centrality perform worse than the ones obtained from a single computation, which is actually expected as DomiRank leads to attack strategies aiming to cause structural damage, which requires the joint removal of several nodes. Therefore by recomputing DomiRank every time step, no coherent strategy emerges as the network structure becomes a moving target, i.e., the structure is re-evaluated at a faster rate (every node removal) than the time needed to remove the number of nodes necessary to inflict the structural damage. Attacks based on iterative betweenness centrality excel at destroying the LCC by finding *bottle-neck* nodes instrumental in mediating most of the shortest paths and, thus, focusing on simply fragmenting the network. As a result of these fundamental differences in the aim of the two centralities, we expect that despite the DomiRank-based attack being less efficient at dismantling the network than those based on iterative betweenness, it causes more severe and enduring damage, making it more difficult to recover from when compared with the damage produced by an iterative betweenness attack. The first indirect piece of evidence supporting this hypothesis is that DomiRank-based attacks remove links more efficiently than other attack strategies (see SM). To test the hypothesis more directly, we implemented two simple recovery mechanisms to evaluate from which of the attacks the network was less prompt to recover. Both recovery mechanisms assign a probability p to a given removed node to recover every time step, wherein the first strategy selects the nodes in the same order that they were removed (results shown in Fig. 5e-h), while for the second strategy, nodes are selected at random from the pool of removed nodes (see results in SM). Our results show that for all the networks, except for the random geometric graph (probably due to network modularity), when a recovery mechanism is put in place, the attack based on a single computation of DomiRank centrality has a comparative dismantling ability than the attack based on iterative betweenness, as shown by the deterioration trend of the LCC in Fig. 5e-h. Moreover, for all the analyzed topologies, the DomiRank-based attack causes longer-lasting effects, as the recovery mechanism requires a larger fraction of reinstated nodes to obtain an equivalent recovery in terms of LCC. The superior ability of the DomiRank strategy to inflict more severe damage is grounded in its aim to dismantle the inherent network structure via the dominance

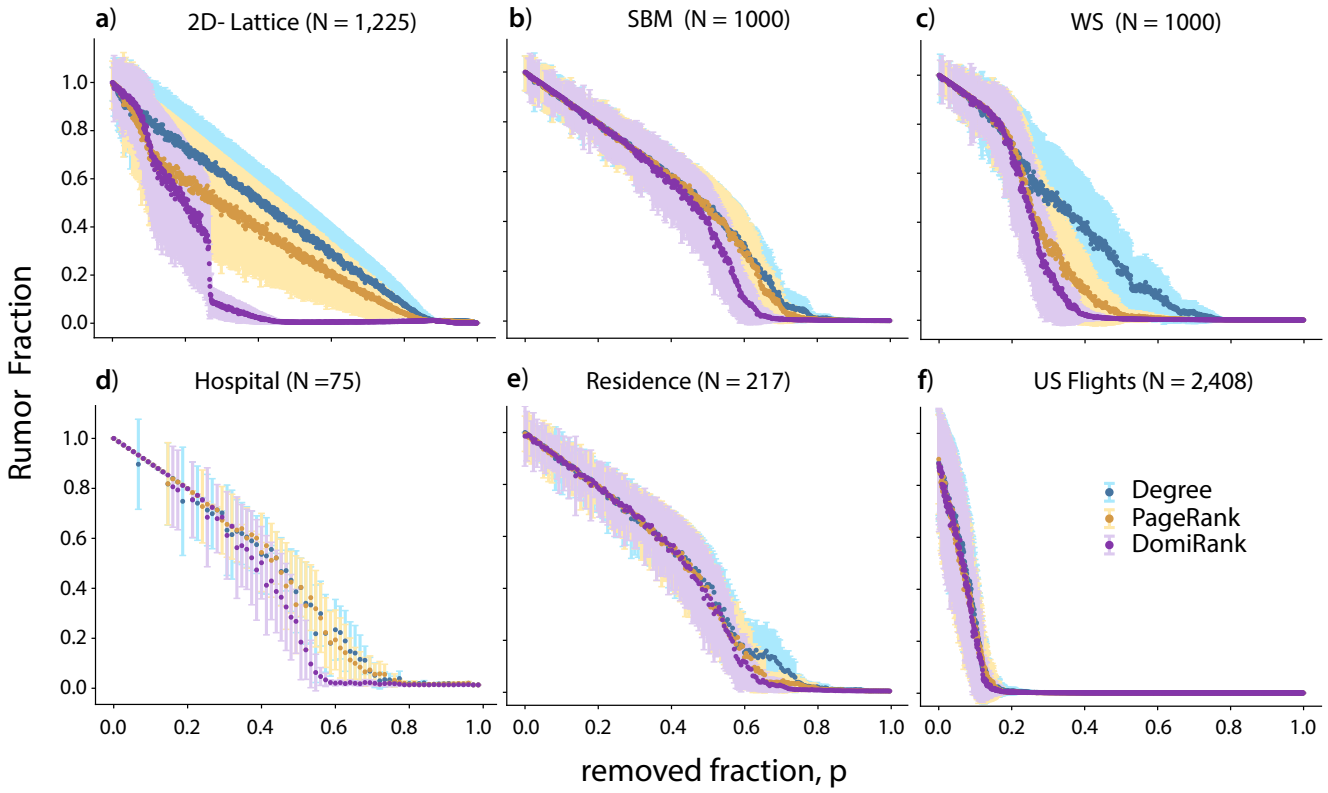

FIG. 6. **Functional robustness of synthetic and real-world networks under centrality-based attacks.** Average rumor spread fraction (error-bars representing the standard deviation) of 1000 rumor spreading simulations as a function of the subsequent network stage resulting of sequential node removal according to degree, PageRank, and DomiRank strategies, for three synthetic networks: (a) 2D regular lattice ($\bar{k} = 4$), (b) stochastic-block-model (SBM; $\bar{k} = 8$), and (c) Watts-Strogatz (WS; $\bar{k} = 6$), and three real networks: (d) a contact-tracing social network [48] (Hospital; $\bar{k} = 30$), (e) a survey based social network [49] (Residence; $\bar{k} = 16$), and (f) a hub-dominated transport network [45] (US flights; $\bar{k} = 4$) .

mechanism. To further demonstrate this point, Fig. 5e-h also displays a high-σ DomiRank-based attack (boosted dominance), where the pace at which the networks recovered was increasingly impeded. Thus, the DomiRank centrality provides a trade-off between the celerity and the severity of the attack through modulation of σ, highlighting its applicability to design vaccination schemes and other mitigation strategies.

B. DomiRank on functional robustness

Sequential node failure caused by random or targeted attacks can compromise not only the structure but also the dynamics taking place on the network, i.e., the functional robustness of the network. In this section, we benchmark the ability of DomiRank-based attacks to disrupt a rumor-spreading dynamic [50] on different network topologies. We implement an epidemic-like model for spreading rumors, where each node represents an individual, who can be in three potential states with respect to the rumor: ignorant, active spreader, and stifler (have heard the rumor but is no longer spreading it) [51]. More specifically, the rumor-spreading dynamic takes four arguments: (i) the network $\mathcal{N}$, (ii) the origin of the rumor (node), (iii) the probability of persuading someone of the rumor (ρ_r), and (iv) the probability of becoming a stifler (ρ_s). We implement this model on the subsequent networks originating from sequences of node removal according to different centrality-based targeted attacks, choosing the fraction of persons that believe the rumor at the end of the process as the proxy for functional robustness.

Fig. 6 showcases the ability of the DomiRank centrality to halt a rumor-spreading process in comparison to degree and PageRank centralities. Our results highlight that for real and particularly synthetic networks, the DomiRank-based attacks are the most efficient at disrupting network functionality. This is a result of the fact that the DomiRank-based attacks aim to dismantle the network by crippling the structure of the network with a more significant deletion of links than most of the other centrality-based attacks (see SM).

The ability of DomiRank to highlight the set of nodes to effectively establish firewalls to mitigate the propa-

gation of rumors is conceptually generalizable to other dynamic processes, such as information transport or epidemic spreading, to name a few, prompting the idea that the DomiRank could be used for establishing efficient vaccination schemes.

IV. CONCLUDING REMARKS

This work presents a new centrality metric, called DomiRank, which evaluates nodal importance by integrating different aspects of the network's topology according to a single tunable parameter that controls the trade-off between local (nodal) and mesoscale (structural) information considered. Thus, the competition mechanism embedded in the definition of DomiRank offers a novel perspective on identifying highly important nodes for network functionality and integrity by contextualizing the relevance of nodes in their respective neighborhoods, taking into account emergent synergies between not directly connected nodes over overlapping neighborhoods (i.e., joint dominance).

One key feature of DomiRank centrality is its low computational cost and fast convergence. On this front, the DomiRank centrality is competitive with the PageRank centrality, whilst, being parallelizable, which allows for efficient execution on GPU infrastructure, making it applicable on massive sparse networks.

We show the superior ability of DomiRank to generate effective targeted attacks to dismantle the network structure and disrupt its functionality, offering an outstanding trade-off between the celerity and the severity of the attack and, therefore, significantly reducing network resilience. DomiRank could be further customized to account for localizing heterogeneity in the topology of massive real-world networks, enhancing the assessment of nodal importance in such systems. Also, we anticipate that hybrid attack strategies, where DomiRank is recomputed at different stages of the attack process, might also increase its performance. Moreover, analyzing the robustness of networks in the light of the recently introduced Idle Network (connectivity of the removed nodes by an attack) [42, 52] could be particularly illuminating as the DomiRank's parameter exerts a direct control on the fragmentation of the Idle network.

Finally, we want to highlight the broad applicability of DomiRank centrality to different domains, as via its versatile dominance mechanism, it is anticipated to be instrumental for tasks as diverse as improving SPAM detection, establishing effective vaccination schemes, or assessing vulnerabilities in transportation networks, just to name a few. Thus, DomiRank, by revealing fundamental aspects of network fragility, can spur further research to develop more effective mitigation strategies to improve our overall understanding of complex systems resilience.

APPENDIX

Proof: *We define the dominance centrality* $\mathbf{\Gamma}$ *as the stationary solution of equation 1:*

$$\frac{1}{\beta}\frac{\partial \mathbf{\Gamma}(t)}{\partial t} = \sigma A(\theta \mathbf{1}_{N\times 1} - \mathbf{\Gamma}(t)) - \mathbf{\Gamma}(t), \tag{6}$$

By definition, the centrality only exists if $\mathbf{\Gamma}(t)$ *converges to* $\mathbf{\Gamma}$*, and thus;*

$$\lim_{t\to\infty} \frac{\partial \mathbf{\Gamma}(t)}{\partial t} = 0, \tag{7}$$

which implies,

$$\lim_{t\to\infty} [\sigma A(\theta \mathbf{1}_{N\times 1} - \mathbf{\Gamma}(t)) - \mathbf{\Gamma}(t)] = 0 \tag{8}$$

thus, we can solve eq. 8 in the following manner;

$$\sigma\theta A \mathbf{1}_{N\times 1} - \lim_{t\to\infty} [(\sigma A + I_{N\times N})\mathbf{\Gamma}(t)] = 0, \tag{9}$$

and therefore,

$$\lim_{t\to\infty} \mathbf{\Gamma}(t) := \mathbf{\Gamma} = \sigma\theta(\sigma A + I_{N\times N})^{-1} A \mathbf{1}_{N\times 1}, \tag{10}$$

[1] R. Albert, H. Jeong, and A.-L. Barabási, Error and attack tolerance of complex networks, Nature **406**, 378 (2000).

[2] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Network robustness and fragility: Percolation on random graphs, Phys. Rev. Lett. **85**, 5468 (2000).

[3] H. Jeong, S. P. Mason, A.-L. Barabási, and Z. N. Oltvai, Lethality and centrality in protein networks, Nature **411**, 41 (2001).

[4] M. De Domenico, A. Solé-Ribalta, S. Gómez, and A. Arenas, Navigability of interconnected networks under random failures, Proceedings of the National Academy of Sciences **111**, 8351 (2014).

[5] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, Complex networks: Structure and dynamics, Physics reports **424**, 175 (2006).

[6] A. V. Goltsev, S. N. Dorogovtsev, J. G. Oliveira, and J. F. F. Mendes, Localization and spreading of diseases in complex networks, Phys. Rev. Lett. **109**, 128702 (2012).

[7] J. Gao, B. Barzel, and A.-L. Barabási, Universal resilience patterns in complex networks, Nature **530**, 307 (2016).

[8] N. Crua Asensio, E. Muñoz Giner, N. S. de Groot, and M. Torrent Burgas, Centrality in the host–pathogen interactome is associated with pathogen fitness during infection, Nature Communications **8**, 14092 (2017).

[9] H. Farooq, Y. Chen, T. T. Georgiou, A. Tannenbaum, and C. Lenglet, Network curvature as a hallmark of

brain structural connectivity, Nature Communications **10**, 4937 (2019).
[10] D. Guilbeault and D. Centola, Topological measures for identifying and predicting the spread of complex contagions, Nature Communications **12**, 4430 (2021).
[11] L. Page, S. Brin, R. Motwani, and T. Winograd, *The PageRank citation ranking: Bringing order to the web.*, Tech. Rep. (Stanford InfoLab, 1999).
[12] M. Kitsak, L. K. Gallos, S. Havlin, F. Liljeros, L. Muchnik, H. E. Stanley, and H. A. Makse, Identification of influential spreaders in complex networks, Nature Physics **6**, 888 (2010).
[13] M. Salathé, M. Kazandjieva, J. W. Lee, P. Levis, M. W. Feldman, and J. H. Jones, A high-resolution human contact network for infectious disease transmission, Proceedings of the National Academy of Sciences **107**, 22020 (2010).
[14] Z. Wang, C. T. Bauch, S. Bhattacharyya, A. d'Onofrio, P. Manfredi, M. Perc, N. Perra, M. Salathé, and D. Zhao, Statistical physics of vaccination, Physics Reports **664**, 1 (2016).
[15] R. Pung, J. A. Firth, Spurgin, Singapore CruiseSafe working group, and CMMID COVID-19 working group, Using high-resolution contact networks to evaluate SARS-CoV-2 transmission and control in large-scale multi-day events, Nature Communications **13**, 1956 (2022).
[16] R. Guimerà, S. Mossa, A. Turtschi, and L. A. N. Amaral, The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles, Proceedings of the National Academy of Sciences **102**, 7794 (2005).
[17] Z. Wu, L. A. Braunstein, S. Havlin, and H. E. Stanley, Transport in weighted networks: Partition into superhighways and roads, Phys. Rev. Lett. **96**, 148702 (2006).
[18] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, Defending critical infrastructure, Interfaces **36**, 530 (2006).
[19] R. Carvalho, L. Buzna, F. Bono, E. Gutiérrez, W. Just, and D. Arrowsmith, Robustness of trans-european gas networks, Phys. Rev. E **80**, 016106 (2009).
[20] Y. Duan and F. Lu, Robustness of city road networks at different granularities, Physica A: Statistical Mechanics and its Applications **411**, 21 (2014).
[21] P. Bonacich, Factoring and weighting approaches to status scores and clique identification, Journal of mathematical sociology **2**, 113 (1972).
[22] L. Katz, A new status index derived from sociometric analysis, Psychometrika **18**, 39 (1953).
[23] L. C. Freeman, A set of measures of centrality based on betweenness, Sociometry , 35 (1977).
[24] U. Brandes and D. Fleischer, Centrality measures based on current flow., in *Stacs*, Vol. 3404 (Springer, 2005) pp. 533–544.
[25] A. Ghavasieh, M. Stella, J. Biamonte, and M. De Domenico, Unraveling the effects of multiscale network entanglement on empirical systems, Communications Physics **4**, 129 (2021).
[26] G. F. de Arruda, A. L. Barbieri, P. M. Rodríguez, F. A. Rodrigues, Y. Moreno, and L. d. F. Costa, Role of centrality for the identification of influential spreaders in complex networks, Phys. Rev. E **90**, 032812 (2014).
[27] R. V. Solé, M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde, Robustness of the european power grids under intentional attack, Phys. Rev. E **77**, 026102 (2008).
[28] J. C. Doyle, D. L. Alderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger, The "robust yet fragile" nature of the internet, Proceedings of the National Academy of Sciences **102**, 14497 (2005).
[29] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE control systems magazine **21**, 11 (2001).
[30] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, Resilience of the internet to random breakdowns, Phys. Rev. Lett. **85**, 4626 (2000).
[31] B. Schäfer, D. Witthaut, M. Timme, and V. Latora, Dynamically induced cascading failures in power grids, Nature Communications **9**, 1975 (2018).
[32] S. Trajanovski, J. Martín-Hernández, W. Winterbach, and P. Van Mieghem, Robustness envelopes of networks, Journal of Complex Networks **1**, 44 (2013).
[33] M. Ventresca and D. Aleman, Network robustness versus multi-strategy sequential attack, Journal of Complex Networks **3**, 126 (2014).
[34] M. J. Williams and M. Musolesi, Spatio-temporal networks: reachability, centrality and robustness, Royal Society Open Science **3**, 160196 (2016).
[35] O. Cats and P. Krishnakumari, Metropolitan rail network robustness, Physica A: Statistical Mechanics and its Applications **549**, 124317 (2020).
[36] N. Biggs, N. L. Biggs, and B. Norman, *Algebraic graph theory*, 67 (Cambridge university press, 1993).
[37] P. Erdös and A. Rényi, On random graphs I, Publicationes Mathematicae Debrecen **6**, 290 (1959).
[38] A.-L. Barabási and R. Albert, Emergence of scaling in random networks, Science **286**, 509 (1999).
[39] D. J. Watts and S. H. Strogatz, Collective dynamics of 'small-world' networks, Nature **393**, 440 (1998).
[40] P. W. Holland, K. B. Laskey, and S. Leinhardt, Stochastic blockmodels: First steps, Social networks **5**, 109 (1983).
[41] E. N. Gilbert, Random graphs, The Annals of Mathematical Statistics **30**, 1141 (1959).
[42] A. Tejedor, A. Longjas, I. Zaliapin, S. Ambroj, and E. Foufoula-Georgiou, Network robustness assessed within a dual connectivity framework: joint dynamics of the active and idle networks, Scientific Reports **7**, 8567 (2017).
[43] T. Manke, L. Demetrius, and M. Vingron, An entropic characterization of protein interaction networks and cellular robustness, Journal of The Royal Society Interface **3**, 843 (2006).
[44] R. A. Rossi and N. K. Ahmed, The network data repository with interactive graph analytics and visualization, in *AAAI* (2015).
[45] J. Kunegis, Konect: the koblenz network collection, in *Proceedings of the 22nd international conference on world wide web* (2013) pp. 1343–1350.
[46] J. Leskovec, J. Kleinberg, and C. Faloutsos, Graph evolution: Densification and shrinking diameters, ACM transactions on Knowledge Discovery from Data (TKDD) **1**, 2 (2007).
[47] U. Brandes, A faster algorithm for betweenness centrality, Journal of mathematical sociology **25**, 163 (2001).
[48] P. Vanhems, A. Barrat, C. Cattuto, J.-F. Pinton, N. Khanafer, C. Régis, B.-a. Kim, B. Comte, and N. Voirin, Estimating potential infection transmission routes in hospital wards using wearable proximity sensors, PloS one **8**, e73970 (2013).

[49] L. C. Freeman, C. M. Webster, and D. M. Kirke, Exploring social structure using dynamic three-dimensional color images, Social networks **20**, 109 (1998).
[50] Y. Moreno, M. Nekovee, and A. F. Pacheco, Dynamics of rumor spreading in complex networks, Physical review E **69**, 066130 (2004).
[51] L. Zhao, J. Wang, Y. Chen, Q. Wang, J. Cheng, and H. Cui, Sihr rumor spreading model in social networks, Physica A: Statistical Mechanics and its Applications **391**, 2444 (2012).
[52] M. Engsig, A. Tejedor, and Y. Moreno, Robustness assessment of complex networks using the idle network, Phys. Rev. Res. **4**, L042050 (2022).

ACKNOWLEDGMENTS

Y.M was partially supported by the Government of Aragón, Spain and "ERDF A way of making Europe" through grant E36-20R (FENOL), and by Ministerio de Ciencia e Innovación, Agencia Española de Investigación (MCIN/AEI/10.13039/501100011033) Grant No. PID2020-115800GB-I00. A.T. thanks the Spanish Ministry of Universities and the European Union Next Generation EU/PRTR for their support through the Maria Zambrano program. A.T. and E.F-G. were partially supported by the National Science Foundation through the Collaborative Research Program Grant EAR1811909 and the United Kingdom Research & Innovation Living Deltas Hub NES008926. E. F-G also acknowledges partial support by NASA through the Global Precipitation Measurement Mission program (Grant 80NSSC22K0597). The funders had no role in the study design, data collection, analysis, the decision to publish, or the preparation of the manuscript.

CONTRIBUTIONS

M.E and A.T developed the methods. M.E. implemented the code and conducted the experiments. M.E and A.T analyzed the data. M.E. and A.T. wrote the initial manuscript. All authors discussed the results, revised the manuscript, and approved the final version of the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

Supplementary Material: DomiRank Centrality: revealing structural fragility of complex networks via local dominance

Marcus Engsig*

Directed Energy Research Centre, Technology Innovation Institute, Abu Dhabi, United Arab Emirates.

Alejandro Tejedor†

Institute for Biocomputation and Physics of Complex Systems (BIFI), Universidad de Zaragoza, 50018 Zaragoza, Spain

Department of Theoretical Physics, University of Zaragoza, Zaragoza 50009, Spain and

Department of Civil and Environmental Engineering, University of California, Irvine, Irvine, CA 92697, USA.

Yamir Moreno‡

Institute for Biocomputation and Physics of Complex Systems (BIFI), University of Zaragoza, 50018 Zaragoza, Spain

Department of Theoretical Physics, University of Zaragoza, Zaragoza 50009, Spain and

CENTAI Institute, Turin 10138, Italy.

Efi Foufoula-Georgiou§

Department of Civil and Environmental Engineering, University of California, Irvine, Irvine, CA 92697, USA. and

Department of Earth System Science, University of California Irvine, Irvine, CA, USA

Chaouki Kasmi¶

Directed Energy Research Centre, Technology Innovation Institute, Abu Dhabi, United Arab Emirates

(Dated: May 17, 2023)

I. LINK REMOVAL DURING ATTACKS

Our results have shown that attack strategies based on DomiRank centrality are more efficient in deteriorating the connectivity of the network in terms of the largest connected component than any other centrality-based attack. In this section (see Fig. 1), we also show that DomiRank-based attacks are able to remove links more efficiently than other attacks for synthetic and real-world networks, providing further evidence about the capacity of the DomiRank to highlight the nodes structurally important for the integrity of the network's connectivity.

The efficiency of DomiRank-based attacks in deteriorating network structural connectivity, both in terms of the largest connected component and sparsifying the number of connections, underlies the also outstanding capacity of this attack to severely impair the functionality of networks (see main text Fig. 6).

II. HETEROGENEOUS NETWORKS

Figure 4 in the main text shows the evolution of the largest connected component for different synthetic and real-world networks as they are attacked based on various centrality metrics. DomiRank-based attacks outperform all other attacks for all the networks analyzed but in one case. That case corresponds to a massive social network (LiveJournal users and their connections - see Figure 4k in the main text), where the DomiRank-based attack, although very competitive, does not perform better than the PageRank-based attack.

In this section, we pose the hypothesis that the presence of heterogeneity (different structural properties) in different subgraphs of the network could lead to underperformance for DomiRank-based attacks. The rationale behind this statement is straightforward in the light of previous results. As shown in the analysis of synthetic networks in Fig. 3 and Fig 4 of the main text, DomiRank excels in highlighting the important nodes with different values of σ depending on the network structure. Thus, for hub-dominated networks, a relatively low value of σ provides the most effective ordering of nodes for designing attack strategies. On the other hand, more regular networks such as lattices or random graphs require large

* marcus.w.engsig@gmail.com
† alej.tejedor@gmail.com
‡ yamir.moreno@gmail.com
§ efi@uci.edu
¶ chaouki.kasmi@tii.ae

values of σ, which allow for a larger integration of the information in the network structure for assessing the relative importance of each node. Consequently, if a network consists of different subgraphs (e.g., communities) with different topological properties might require different σ for each subgraph, since an *average* global value of σ would lead to suboptimal results.

In order to address this issue, we could substitute the σ parameter in DomiRank definition by a diagonal matrix (without additional computational cost), where the entries of $\sigma_{i,i}$ are corresponding to the optimal σ for the community that node i belongs to. We can mathematically describe this new diagonal matrix σ as follows, given T communities $C_j, j \in [1, T]$;

$$(\sigma)_{i,i} = \sum_{j=1}^{T} \sigma_j \mathbb{1}_{i \in C_j}. \tag{1}$$

Moreover, in order to guarantee the convergence of DomiRank, Eq. 1 takes the final form:

$$(\sigma)_{i,i} = \min \left[\sum_{j=1}^{T} \sigma_j \mathbb{1}_{i \in C_j}, \frac{-1}{\lambda_N} \right] \tag{2}$$

where λ_N is the minimum (largest negative) eigenvalue of the whole network.

To test this hypothesis, we generate synthetic networks consisting of two subgraphs, each of them generated with a different model (e.g., Barabasi-Albert and random geometric graph), establishing links between both subgraphs (10% of the nodes establish a connection with a node in the other subgraph). Fig. 2 displays the results for the attacks based on the previous centralities (including DomiRank), as well as the results obtained from a DomiRank where nodes in different subgraphs are evaluated with different values of σ to account for heterogeneity in networks. As expected, in the cases where the two merged networks are characterized by disparate values of σ for optimal attack strategies (i.e., large heterogeneity), we obtain a larger gain by considering the diagonal-matrix-based σ in the definition of DomiRank. Thus, for instance, Fig. 2a shows a significant improvement in the performance of the attack strategy when heterogeneity is considered in the definition of DomiRank for a network consisting in the combination of a subgraph generated by a Barabasi-Albert model with relatively low degree ($\bar{k} = 4$) and random-geometric-graph ($\bar{k} = 5$). Additionally, from Fig. 2c we see that by combining two subgrphaps characterized by comparable optimal σ values like the Erdős-Rényi and Watts Strogatz networks, the gain is just incremental. Note that when the difference in the optimal value of σ does not significantly differ between the

two subgraphs (e.g., Erdos-Reyni and 2D-Lattice - See fig. 2 d), the traditional DomiRank computed in the whole network might offer better performance than the community-based version, as it accounts for the links connecting the two sub-graphs.

Consequently, massive networks, consisting of multiple communities with different properties, might require the adoption of the definition of DomiRank that account for that heterogeneity (i.e., using the diagonal-matrix-based σ) to design more efficient attack strategies for dismantling the networks, as the traditional definition of DomiRank could underperform.

Thus, by combining the various algorithms to detect communities in massive networks, and this newly defined σ could potentially lead to further gains in designing strategies to dismantle networks' structure and functionality without incurring unaffordable computational costs.

III. NETWORKS UNDERGOING RANDOM-RECOVERY

Complementing the results shown in Figure 5 in the main text, we show how a different recovery mechanism affects the evolution of the largest connected component under various attacks. Particularly we implement a random recovery mechanism, for which at every time step, a node is selected at random (with uniform probability) from the pool of the removed nodes. This selected node is recovered with probability p. Note that, if a given node is recovered cannot be subject to any further attack. Our results using a random recovery mechanism are consistent with those shown in Figure 5 in the main text, where a sequential recovery mechanism was implemented. Notably, the high-σ DomiRank-based attack (Fig. 3) inflicts more enduring damage (i.e., longer time to recover the same relative size of the largest connected component) than the iterative betweenness when the network has a random recovery process, despite the fact that the iterative betweenness-based-attacks are superior in dismantling the structure of the network. Fig. 3a-d also showcases that when a network has a random recovery process, a low-σ DomiRank-centrality-based attack can result in an incrementally more rapid deterioration of the largest-connected-component than iterative betweenness. This fundamentally shows a key property of DomiRank-based attacks, i.e., the inherent trade-off between the efficiency of network dismantling and the endurance of the damage by modulating the parameter σ from low to high.

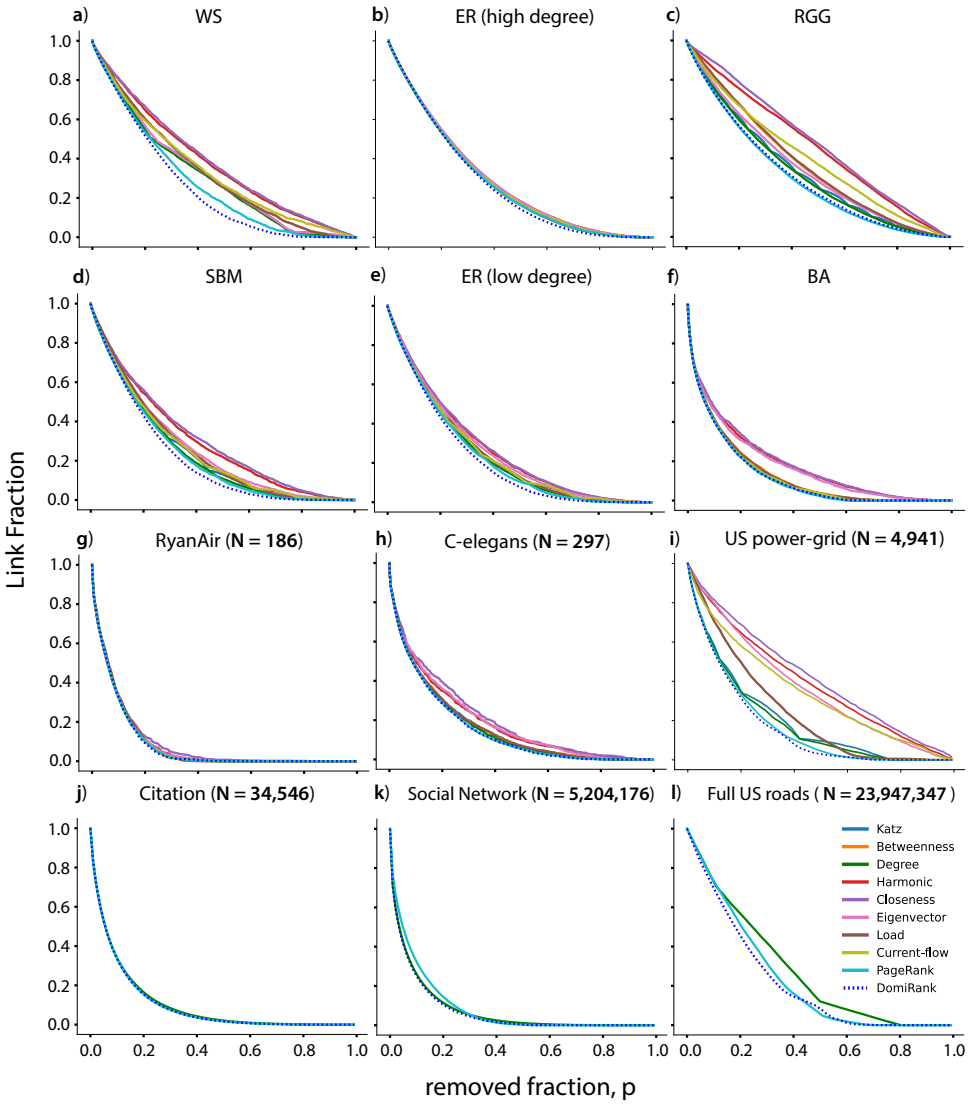

FIG. 1. **Link-removal on synthetic and real-world networks under centrality-based attacks.** Evolution of the remaining link fraction whilst undergoing sequential node removal according to descending scores of various centrality measures for different synthetic networks of size $N = 1000$: (a) Watts-Strogatz (WS; $\bar{k} = 4$), Erdős-Rényi (ER) with (b) high ($\bar{k} = 20$) and (e) low link density ($\bar{k} = 6$), (c) random geometric graph (RGG; $\bar{k} = 16$), (d) stochastic block model (SBM; $\bar{k} = 7$), and (f) Barabasi-Albert (BA; $\bar{k} = 6$). The performance of the attacks based on the different centrality metrics is also shown for different real networks: (g) hub-dominated transport network (airline connections, $\bar{k} = 16$), (h) neural network (worm, $\bar{k} = 29$), (i) spatial network (power-grid, $\bar{k} = 3$) , (j) citation network ($\bar{k} = 25$), (k) massive social network ($\bar{k} = 19$), and (l) massive spatial transport network (roads, $\bar{k} = 5$). Note that for panels j, k, and l, where massive networks are shown, only a few attack strategies are displayed due to the impossibility of computation of the rest.

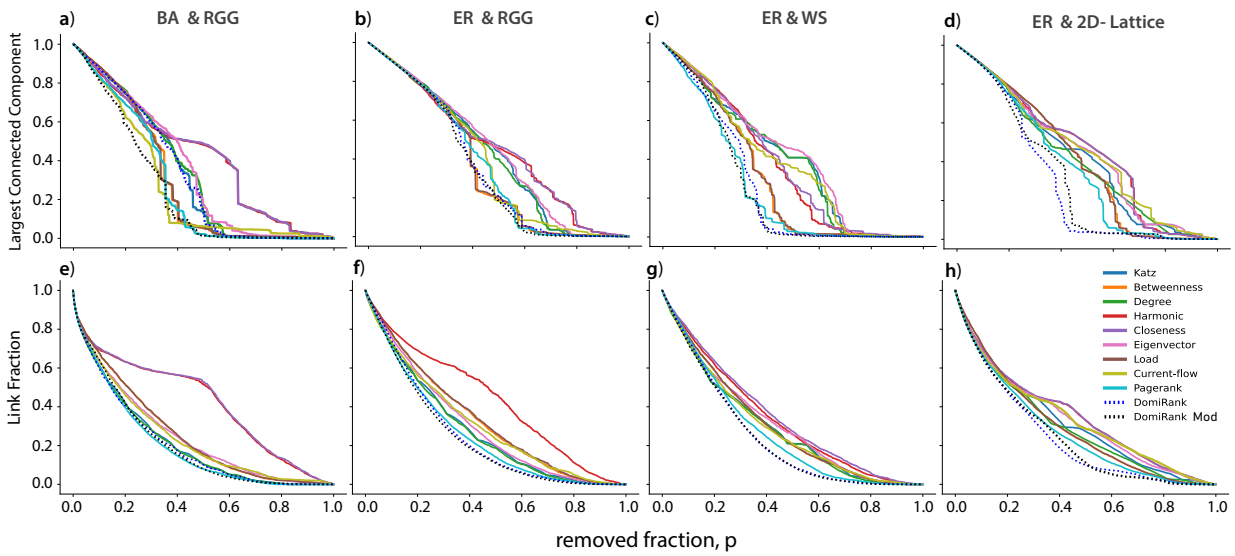

FIG. 2. **The effect of heterogeneity on the performance of centrality-based attacks on synthetic networks.** Panels a-d show the evolution of the relative size of the largest connected component (robustness) and panels e-h show the evolution of the remaining link fraction (connectivity), whilst undergoing sequential node removal according to descending scores of various centrality measures for different coupled synthetic networks (heterogeneous) of size $N = 1000$: (a,e) Barabasi-Albert (BA) and random geometric graph (RGG), (b,f) Erdős-Rényi (ER) and random geometric graph (RGG), (c,g) Erdős-Rényi (ER) and Watts-Strogatz (WS), and (d,h) Erdős-Rényi (ER) and a 2D-lattice. Here we have three different DomiRank-based-attacks corresponding to two different σ (i) the optimal σ for the entire network (denoted in the legend as DomiRank), and (ii) the capped optimal diagonal matrix σ as per eq. 2 (denoted in the legend as DomiRank Mod).

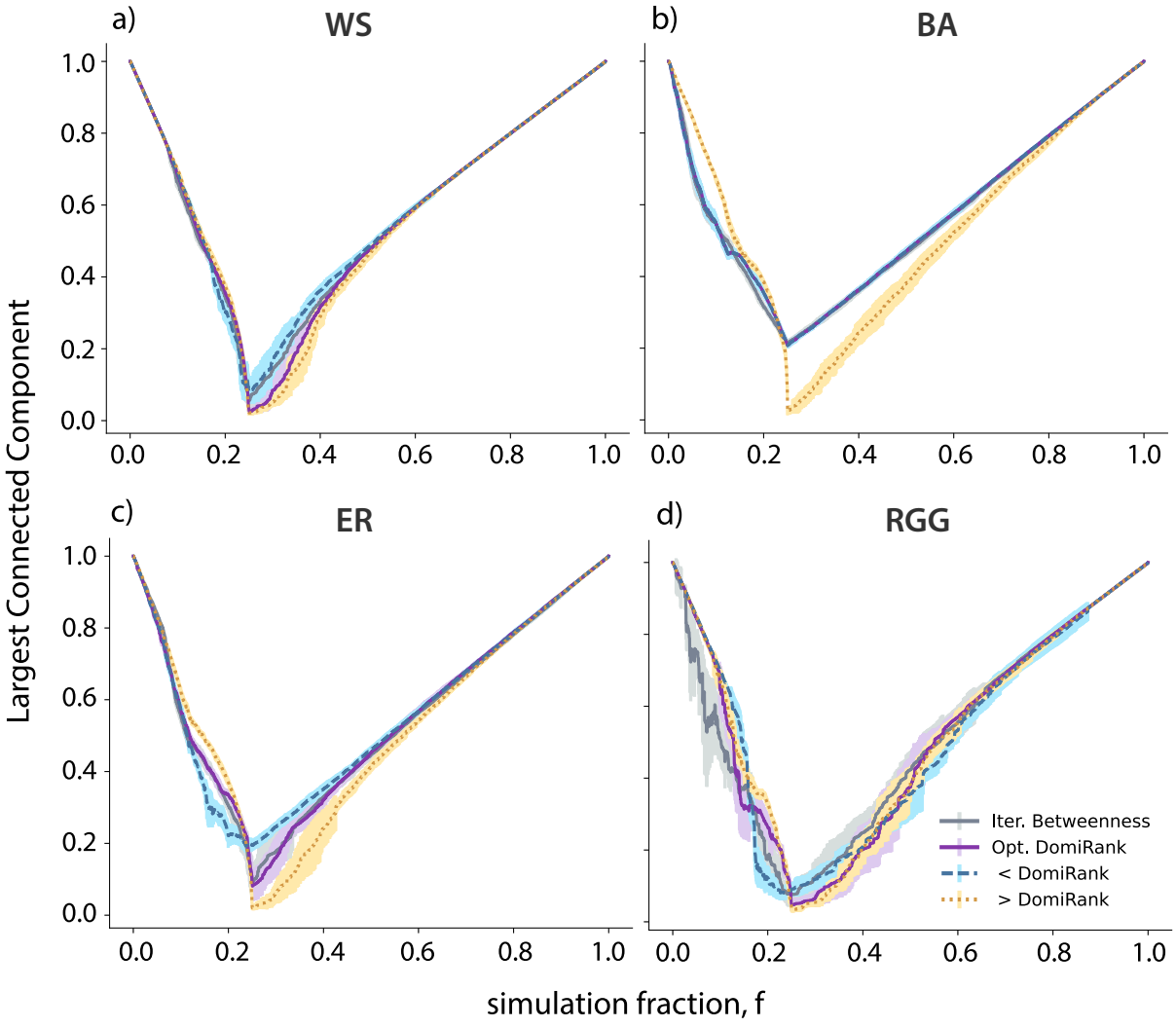

FIG. 3. **Evaluating the effect of random recovery during iterative betweenness-based and DomiRank attacks.** Evolution of the relative size of the largest connected component for various synthetic networks of size $N = 500$, namely (a) Watts-Strogatz (WS; $\bar{k} = 4$), (b) Barabasi-Albert (BA; $\bar{k} = 6$), (c) Erdős-Rényi (ER; $\bar{k} = 5$), and (d) random geometric graph (RGG; $\bar{k} = 7$), undergoing sequential node removal based on pre-computed DomiRank (optimal, low ($<$), and high ($>$) σ) and iterative betweenness, while a random node recovery process is ongoing; specifically, at each time step there is a probability of 0.25 to recover a random (already removed) node.