# Robustness Assessment of Complex Networks using the Idle Network*

Marcus Engsig†
*Department of Science and Engineering, Sorbonne University Abu Dhabi, Abu Dhabi, United Arab Emirates.*

Alejandro Tejedor‡
*Department of Science and Engineering, Sorbonne University Abu Dhabi, Abu Dhabi, United Arab Emirates. 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), Universidad de Zaragoza, 50018 Zaragoza, Spain*

*Departamento de Física Teórica, Universidad de Zaragoza, 50009 Zaragoza, Spain and Institute for Scientific Interchange, ISI Foundation, Turin, Italy*

(Dated: April 28, 2022)

The robustness of interconnected systems such as airports, power grids, or the internet is an essential property for those systems to sustain their functionality in the face of random failures or targeted malicious attacks. Complex networks offer a suitable framework to develop methodologies to assess robustness in terms of system connectivity. However, current approaches to estimate network robustness only consider the connectivity of the nodes unaffected by the attack: the Active Network. Here we propose to incorporate the properties of the emerging connectivity of the nodes affected by the attack: the Idle Network. Our results demonstrate that there is pertinent and non-redundant information in the Idle Network, which enables us to more accurately assess network robustness.

The representation of complex systems as networks, where system components are abstracted as nodes and their interactions as links, has allowed us to further our understanding of system structure and dynamics in fields as diverse as biology, engineering, economics, and geosciences [1–9]. Particularly, network theory has been instrumental in developing methodologies to assess the robustness of interconnected systems such as power grids, the internet, and airports, in the face of random failures or targeted attacks[10–14] The robustness of a network can be defined as the ability of the network to maintain functionality whilst undergoing an attack (sequential node removal). In a world where critical infrastructures and their connectivity are potential targets of malicious attacks, it is paramount to identify the key network properties that determine robustness for a given attack. Since the pioneering work by *Albert et al.* [15], a vast literature has presented methodologies and metrics to quantify network robustness [11, 12, 15–20]. However, current methodologies to assess network robustness focus mainly on the connectivity of the nodes unaffected (Active Network) by the attack, while the connectivity of the affected nodes (Idle Network) has received minimal attention. In this study, we demonstrate the benefit of including information about the Idle Network in assessing network robustness.

Let us formally define the *Active* and *Idle Networks*, which naturally emerge from an attack process acting on a network [21]. Attacking a network is synonymous to a process of *sequential node removal*. Consider an initial network

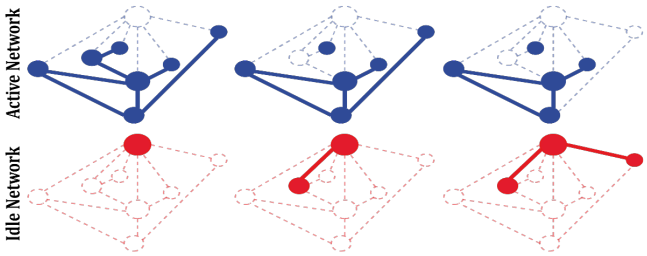



FIG. 1. The evolution of the Active and Idle networks under an attack strategy $D$ consisting of 3 node removals at $t = 1, 2, 3$.

* A footnote to the article title
† marcus.w.engsig@gmail.com
‡ alej.tejedor@gmail.com

$\mathcal{N}$ that consists of $N$ nodes, denoted $\{n_i\} : i = 1, ...N$, connected by a set of links $\{(n_i, n_j)\}$. The sequential node removal process starts at $t = 0$ with the original network $\mathcal{N}$, and an attack strategy $D$, that is a function of the original network $\mathcal{N}$. For every discrete time step $t > 0$, the attack eliminates a chosen node $n_i$ and all its corresponding links $(n_i, \cdot)$, resulting in a new network, formed by the set of nodes and links that is unaffected by the attack; we denote this the Active Network $\mathcal{N}_A(t)$. The attack process also gives rise to the Idle Network $\mathcal{N}_I(t)$, which consists of the entire set of nodes removed from the Network $\mathcal{N}$ up to time $t$, and the links originally existing among them (see Fig.1). We can mathematically express a given attack strategy $D$ acting on a network $\mathcal{N}$, as the decomposition of $\mathcal{N}$ into the Active $\mathcal{N}_A(t)$ and Idle $\mathcal{N}_I(t)$ networks .

$$D : N \to \{N_A(t), N_I(t)\}, \quad t = 1, ...N \tag{1}$$

It is clear that with respect to the nodes, the Active and Idle networks are complementary, implying that the union of the nodes in $\mathcal{N}_A(t)$ and $\mathcal{N}_I(t)$ is the set of nodes in $\mathcal{N}$. However, this is not the case for the connectivity of the nodes, as it is neither complementary nor symmetric. When a node is removed, all its links are removed from the Active Network, however, from that set of newly removed links, only those which connect to the already existing Idle Network's nodes are added to the Idle Network. We argue that the information about the connectivity of the affected nodes by an attack, which is readily available in the Idle Network, provides important information on the effectiveness of the attack and, therefore, on the robustness of the attacked network. Thus, our research hypothesis can be stated as follows: *there exists non-redundant information on the robustness of a network undergoing an attack in the Idle Network structure.*

To test this hypothesis, we will extract indicators from the Active and Idle Networks to benchmark our capacity to assess network robustness using only Active indicators (traditional approach) versus incorporating Idle indicators as well. Particularly, we choose 2 simple indicators to model robustness: (i) The *largest cluster size* $C$ which quantifies the effect of the attack in breaking down (building up) the active (idle) network in terms of its size without encompassing the effectiveness of the connectivity of these networks. More specifically, $C$ is the ratio of the number of nodes in the largest cluster (set of connected nodes) over the number of nodes $N$ in the initial network. (ii) The *link fraction* $L$ is the number of links in the Active (Idle) network, normalized by the total number of links in the initial network $\mathcal{N}$. This indicator describes how the attack removes (adds) links and thus provides information about how well-connected the nodes are in the Active (Idle) Network. Both of these indicators are normalized to be between $[0, 1]$, and are monotonically decreasing (increasing). These indicators were chosen such that, in complement, they have information on the overall functionality of the network and, therefore, on its robustness.

Following previous studies [22–25], we utilize the *efficiency*, $E$, as a proxy for robustness. Recall that $E$ of a network $\mathcal{N}$ with $N$ nodes is defined as the standardized sum of the reciprocal of the shortest paths $d_{i,j}$ between all pair of nodes $i$ and $j$;

$$E = \frac{1}{N(N-1)} \sum_{i,j \in \mathcal{N}, i \neq j} \frac{1}{d_{i,j}} \tag{2}$$

Note that, if two nodes $i, j$ are disconnected, then $\frac{1}{d_{i,j}} = 0$, as the distance between the two nodes is infinite. $E$ is normalized to always start at 1, by dividing all values of $E$ for a single evolution by the value of the efficiency for the intact network. We underline that $E$ is a property of the Active Network, as it is solely a function of the *adjacency matrix* of the Active Network.

Given the two indicators and the proxy for robustness, we transform our hypothesis into a regression problem. Thus, we evaluate the difference in estimation accuracy achieved via a neural network when only active indicators are included in the training set, and when Idle indicators are also included. More specifically, we use a forward-feeding and back-propagating artificial neural network with 3 hidden layers of 10 neurons per layer, each with `ReLu` activation functions; set to optimize validation squared residual loss. Each neural network was implemented with a dataset of 200 attack sequences, with a $\frac{3}{4}$ train, $\frac{1}{8}$ test, and $\frac{1}{8}$ validation split. The output of the neural network is the estimation of the efficiency as the proxy for robustness. In order to verify our hypothesis, the estimation accuracy must increase when the neural network is granted the Active and Idle indicators, compared to the estimation produced using the Active indicators alone.

Our study investigates different stochastically generated synthetic network topologies and attack strategies to test our hypothesis systematically and with all generality. Namely, we test the robustness estimation for random (Erdos Renyi [26]), scale-free (using a configuration model [27]), and small world (Strogatz-Watts [1]) topologies, undergoing three different attack strategies: targeted (degree), random failure, and random spreading [21]. Furthermore, the different topologies were explored for varying initial link densities, as characterized by $\bar{k}$ (average degree of the initial network $\mathcal{N}$). The tested link densities for all of the synthetic topologies correspond to $\bar{k} \in \{3, 6, 12, 24\}$. Thus, we have explored 36 combinations of topologies, attacks, and link densities. For each of these combinations, 200 different

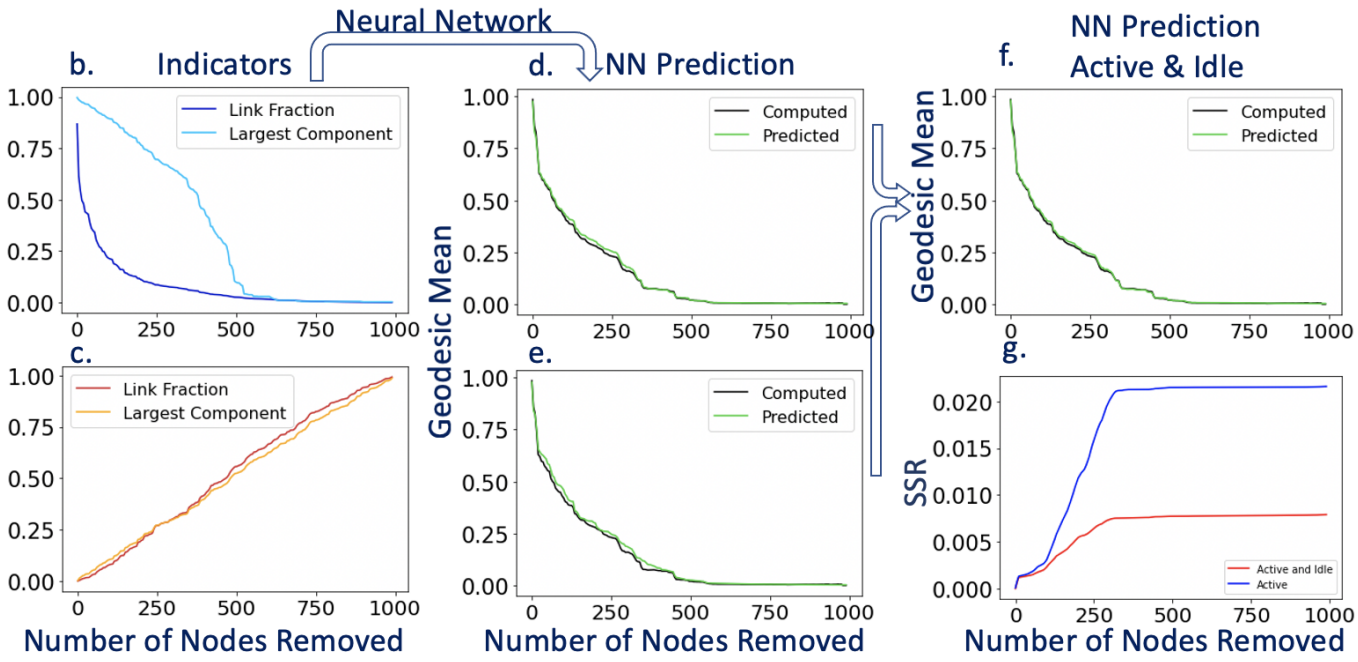



FIG. 2. Evolution of the (b) Active and (c) Idle indicators (largest component and link fraction) for a random network with $N = 1000$ nodes ($\bar{k} = 12$), undergoing a random attack. Prediction of the evolution of the efficiency via a NN using unique indicators from the (d) Active or (e) Idle Networks. (f) Prediction of the efficiency via a neural network trained with both the Active and the Idle indicators. The mean and standard deviation of the sum of the squared residuals ($SSR$) for 25 random topologies undergoing random attacks is also reported in panels (d-f), and its evolution is displayed in panel (g).

stochastic topologies were generated and exposed to a full attack evolution, where the indicators and efficiency were calculated at the different stages of the attack (see *Supplemental Material (SM)*).

Figure 2 displays a representative case to illustrate our results. As expected, the estimation of network robustness (Fig. 2d) using Active indicators (Fig. 2b) is quite accurate ($SSR = 0.02 \pm 0.03$). Noticeably, the Idle indicators alone (Fig. 2c) allowed us to estimate fairly well ($SSR = 0.10 \pm 0.10$) the trend of the evolution of the efficiency as shown in Figure 2e. Most importantly, as hypothesized, by combining the indicators of the Active and Idle networks, we obtained a more accurate estimation of network robustness ($SSR = 0.01 \pm 0.01$) (Fig. 2f). Additionally, the increased accuracy in the estimation is consistent throughout all stages of the attack (Fig. 2g). Our results for the whole data set of network topologies and attacks demonstrate systematically that Active indicators, when combined with Idle indicators, increase the accuracy in the estimation of robustness, verifying our hypothesis.

Guided by the following observation made from the data set of topologies and attacks analyzed in this work (see SM): "the more complex (i.e., more variable at different scales) the Efficiency curves are, the higher the improvement in the accuracy of robustness assessment by acknowledging idle indicators", we investigate the potential role of idle information in distilling variability in the data set to improve network robustness estimation. To this goal, we systematically explore the effect of variability in the training set in estimating robustness. More specifically, we trained neural networks with training sets with increasing variability by combining different topologies, attacks, and link densities (including a data set consisting of all combinations), and we compared the estimation accuracy when only active indicators are considered, and when active and idle indicators are both included.

Fig. 3 shows the model outputs for the most generalized case: data for all the three topologies, four densities, and three attacks are included in the training set. The results are apparent, the inclusion of idle indicators (see 3 f and g) produce exceedingly good predictions when compared with those achieved via only active indicators (see 3 a and b). When the difference between the model output and the true value of robustness (SSR) is computed as a function of the attack stage (see 3 h and g), a consistent pattern is observed: active and idle indicators combined outperformed the active indicators alone during the most significant part of the attack sequence.

As expected, a general trend is also observed (see SM): the more heterogeneous the training set is, the less accurate is the estimation of network robustness done by all three neural networks (trained with: active indicators only, idle indicators only, and active and idle indicators). However, the rate of performance deterioration is not similar, in fact, it is not comparable. As soon as variability is introduced in the training set, the neural network using the

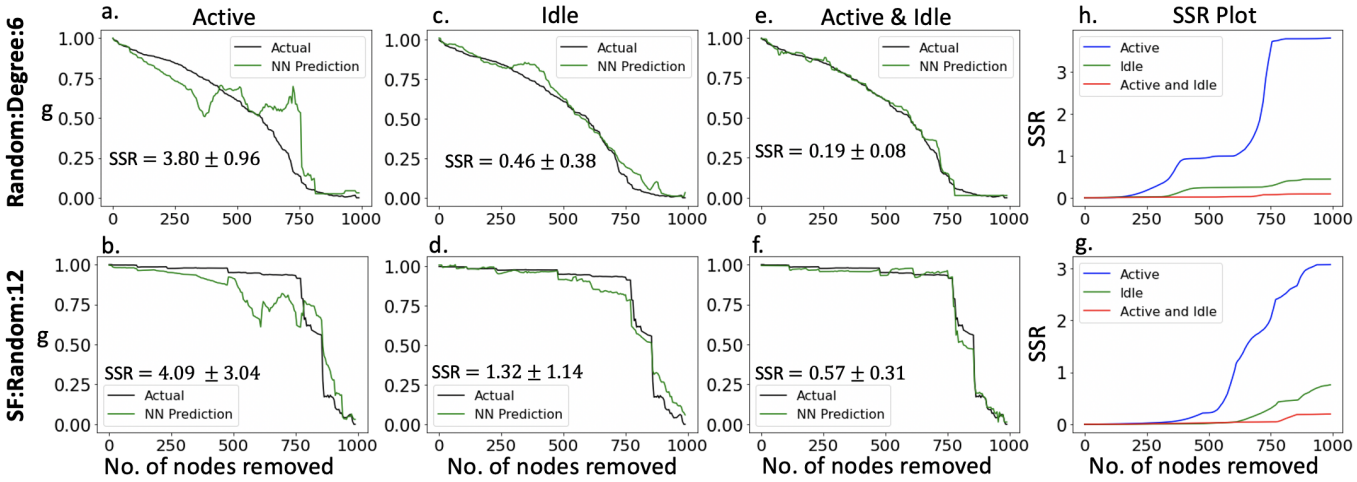



FIG. 3. Performance of a neural network trained with the entire combined data set of topologies, attacks, and densities all-together. (a,c,e) Performance of 3 different neural networks for the Active, Idle, and the Active and Idle indicators, respectively on an Erdos Renyi topology with $\bar{k} = 6$ undergoing random attack. (b,d,f) Performance of 3 different neural networks for the Active, Idle, and the Active and Idle indicators, respectively on configuration scale free model of $\bar{k} = 12$ undergoing a random attack. The mean and standard deviation of the sum of the squared residuals ($SSR$) for 25 synthetic topologies undergoing their respective attacks is also reported. (h,g) Cumulative value of SSR as a function of the attack stage for the Erdos Renyi and Scale free topologies, respectively.

Active indicators exclusively is not able to estimate even the general trend, let alone the variability. Whereas the neural network trained using both the Active and Idle indicators is able to estimate the general trend very well and a majority of the variability. This trend is consistent for all of the topologies tested (see Fig. 3 and SM).

Two further remarks are noteworthy from this part of the work: (i) In a surprising number of times, the robustness estimations obtained via the neural networks trained exclusively with Idle indicators are significantly more accurate than those produced by the neural networks trained only with active indicators, highlighting the non-redundant relevant information content in the idle network. (ii) In select cases, the Neural Network trained with all topologies, densities, and attacks outperforms in terms of accuracy the estimation of robustness made by a Neural Network trained purely for a specific topology, attack, and link density, highlighting the value of idle indicators in interpreting the overall variability in the dataset to improve estimations for specific cases. Therefore, we claim that the joint information of the Idle and Active Network allows the neural networks to *navigate* the variability in the training set to maintain an enhanced accuracy in assessing network robustness.

Our previous results have clearly demonstrated that the Idle network contains intrinsic information, useful for improving the assessment of network robustness. However, the degree of improvement in that assessment varies depending on the attack and network topology. Acknowledging that the used synthetic networks lack some properties often exhibited by real-world networks (e.g., modularity etc.), here, we further test the relevance of idle network information in assessing robustness of real networks. To do that, we simulate stochastic targeted degree attacks on real-world topologies, where the probability of removing a given node is proportional to its original degree. We also evaluate the role of idle information in generalizing the estimation robustness for an unseen attack (e.g., based on betweenness centrality). Particularly, we first train a neural network using only active indicators resulting from 200 node removal sequences obtained by following a stochastic targeted degree attack strategy. Our results show a fairly good estimation of our proxy of robustness (See Fig.4a -Little Rock Lake Food Web [28]). However, suppose that trained neural network is used to estimate the network robustness of the same network topology under a stochastic targeted betweenness attack. In that case, the estimation fails to reproduce the evolution of the true value during the vast majority of the attack sequence (see Fig.4b). On the other hand, if a neural network is trained with the active and idle indicators of the same 200 node removal sequences (stochastic targeted degree attacks), not only we obtain better accuracy in estimating network robustness under stochastic targeted degree attacks (see Fig.4c -Little Rock Lake Food Web), but also that neural network provides an exceptionally well-maintained accuracy in the estimation of network robustness for a previously unseen attack (stochastic targeted betweenness attack) for the vast majority (and relevant) part of the attack sequence (See Fig.4d -Little Rock Lake Food Web). These results have been tested for several real-world networks (Little Rock Lake Food Web [28], Budapest Connectome [29], and Ryanair connections [21] - See SM), corroborating our two previous findings, namely, (i)idle network information systematically improves our capacity to estimate network robustness, and (ii) idle information allows us to retain accuracy in network robustness

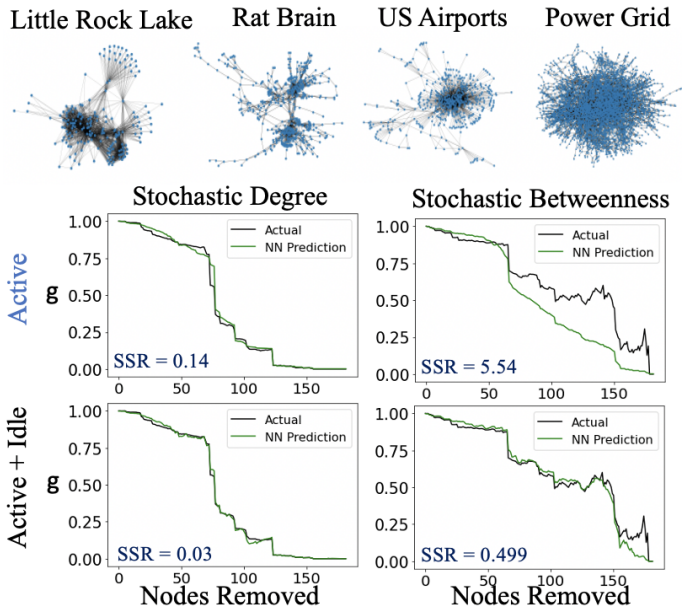



FIG. 4. This figure displays the estimation of robustness done by a neural network trained with stochastic targeted degree attacks on the Little Rock Lake network. The Neural network was trained with 200 full attack evolutions. This Neural Network attempts to predict a stochastic betweenness attack on the same topology. Similarly, the sum of squared residuals is displayed, without uncertainty as it was for a single iteration.

estimation under scenarios of enhanced variability, both in the training set and out-of-sample (e.g., altered attack strategies).

Obviously, the information gained via idle networks indicators is limited. Actually, the key role of idle indicators is to partially harness the existing information in the internal variability of the training set to gain estimation power (i) in the face of variability in the training set (either from its intrinsic stochastic variability or due to the inclusion of different topologies and attacks in the training set), and (ii) for unforeseen attacks and topological features that generate variability compatible with that observed in the training set. Thus, the idle network information is instrumental for our model (neural network) to interpret variability and improve the robustness assessment. However, if the variability in the data set is minimal (e.g., targeted attack in a sparse scale-free network), the gain achieved by including idle indicators would also be incremental. Furthermore, the indicators chosen in this study (size of the largest cluster and link fraction) could be particularly clumsy in properly encoding the data set variability for certain network topologies (e.g., spatial networks such as the power grid [1]), and therefore, these idle indicators might be ineffective in enhancing network robustness assessment in those cases.

We want to finally remark that this study uses a neural network as a tool to turn our hypothesis into a regression problem. The chosen methodology to estimate our proxy of robustness is not intended to be optimal but to demonstrate the information content and role of the idle network in the assessment of network robustness. Thus, for example, we anticipate that using convolutional neural networks may improve the accuracy of robustness estimation. Such further improvements in the accuracy of estimating Efficiency can lead to important implications of our work, since neural networks trained for generalized data sets would offer a light way to estimate network Efficiency, which otherwise is a computationally very demanding quantity to be calculated.

Assessing network robustness accurately is essential to ensure the correct and sustained functionality of many natural and engineered systems. Our study shows that there is non-redundant and pertinent information on the robustness of a network in the so-called Idle network. The inclusion of Idle information in models to assess network robustness allows us to improve the accuracy of our estimations for a specific network topology and attack and equips models with the capability to interpret in-sample and out-sample variability to preserve estimation power amid noise and unseen variability. Thus, evaluating network robustness in the light of the Idle Network constitutes a conceptual paradigm shift that could improve the quality and accuracy of its assessment and might lead to new strategies to

guide enhanced network resilience.


[1] D. J. Watts and S. H. Strogatz, Collective dynamics of 'small-world' networks, Nature **393**, 440 (1998).
[2] A.-L. Barabási and R. Albert, Emergence of scaling in random networks, Science **286**, 509 (1999), http://science.sciencemag.org/content/286/5439/509.full.pdf.
[3] M. Newman, *Networks: An Introduction* (Oxford University Press, Inc., New York, NY, USA, 2010).
[4] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, Complex networks: Structure and dynamics, Physics Reports **424**, 175 (2006).
[5] A. Barrat, M. Barthlemy, and A. Vespignani, *Dynamical Processes on Complex Networks*, 1st ed. (Cambridge University Press, New York, NY, USA, 2008).
[6] I. Rodriguez-Iturbe and A. Rinaldo, *Fractal River Basins: Chance and Self-Organization, 2nd ed* (Cambridge Univ Press, New York, 2001) p. 547.
[7] E. Bullmore and O. Sporns, Complex brain networks: graph theoretical analysis of structural and functional systems, Nature Reviews Neuroscience **10**, 186 (2009).
[8] M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter, Multilayer networks, J. Complex Netw. **2**, 203 (2014).
[9] A. Tejedor, A. Longjas, D. Edmonds, T. Georgiou, I. Zaliapin, A. Rinaldo, and E. Foufoula-Georgiou, Entropy and optimality in river deltas, Proc. Natl. Acad. Sci. U.S.A. (2017).
[10] 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).
[11] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, Resilience of the internet to random breakdowns, Phys. Rev. Lett. **85**, 4626 (2000).
[12] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, Breakdown of the internet under intentional attack, Phys. Rev. Lett. **86**, 3682 (2001).
[13] D. R. Wuellner, S. Roy, and R. M. D'Souza, Resilience and rewiring of the passenger airline networks in the united states, Phys. Rev. E **82**, 056101 (2010).
[14] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, Mitigation of malicious attacks on networks, Proceedings of the National Academy of Sciences **108**, 3838 (2011), https://www.pnas.org/doi/pdf/10.1073/pnas.1009440108.
[15] R. Albert, H. Jeong, and A.-L. Barabási, Error and attack tolerance of complex networks, **406**.
[16] 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).
[17] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, Attack vulnerability of complex networks, Phys. Rev. E **65**, 056109 (2002).
[18] A. E. Motter and Y.-C. Lai, Cascade-based attacks on complex networks, Phys. Rev. E **66**, 065102 (2002).
[19] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature **464**, 1025 (2010).
[20] B. Min, S. D. Yi, K.-M. Lee, and K.-I. Goh, Network robustness of multiplex networks with interlayer degree correlations, Phys. Rev. E **89**, 042811 (2014).
[21] 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).
[22] S. Trajanovski, J. Martín-Hernández, W. Winterbach, and P. Van Mieghem, Robustness envelopes of networks, Journal of Complex Networks **1**, 44 (2013), https://academic.oup.com/comnet/article-pdf/1/1/44/1369171/cnt004.pdf.
[23] M. Ventresca and D. Aleman, Network robustness versus multi-strategy sequential attack, Journal of Complex Networks **3**, 126 (2014), https://academic.oup.com/comnet/article-pdf/3/1/126/1323613/cnu010.pdf.
[24] M. J. Williams and M. Musolesi, Spatio-temporal networks: reachability, centrality and robustness, Royal Society Open Science **3**, 160196 (2016), https://royalsocietypublishing.org/doi/pdf/10.1098/rsos.160196.
[25] O. Cats and P. Krishnakumari, Metropolitan rail network robustness, Physica A: Statistical Mechanics and its Applications **549**, 124317 (2020).
[26] P. L. Erdos and A. Rényi, On the evolution of random graphs, Transactions of the American Mathematical Society **286**, 257 (1984).
[27] M. Catanzaro, M. Boguñá, and R. Pastor-Satorras, Generation of uncorrelated random scale-free networks, Phys. Rev. E **71**, 027103 (2005).
[28] N. D. Martinez, Artifacts or attributes? effects of resolution on the little rock lake food web, Ecological Monographs **61**, 367 (1991), https://esajournals.onlinelibrary.wiley.com/doi/pdf/10.2307/2937047.
[29] B. Szalkai, C. Kerepesi, B. Varga, and V. Grolmusz, The budapest reference connectome server v2.0, Neuroscience Letters **595**, 60 (2015).

# Supplementary Information

## Section A: Specifically Trained Neural Networks

The table below displays the sum of squared residuals (SSR) of the specifically trained neural networks, for all the possible combinations of topology, attack scheme, and link density.

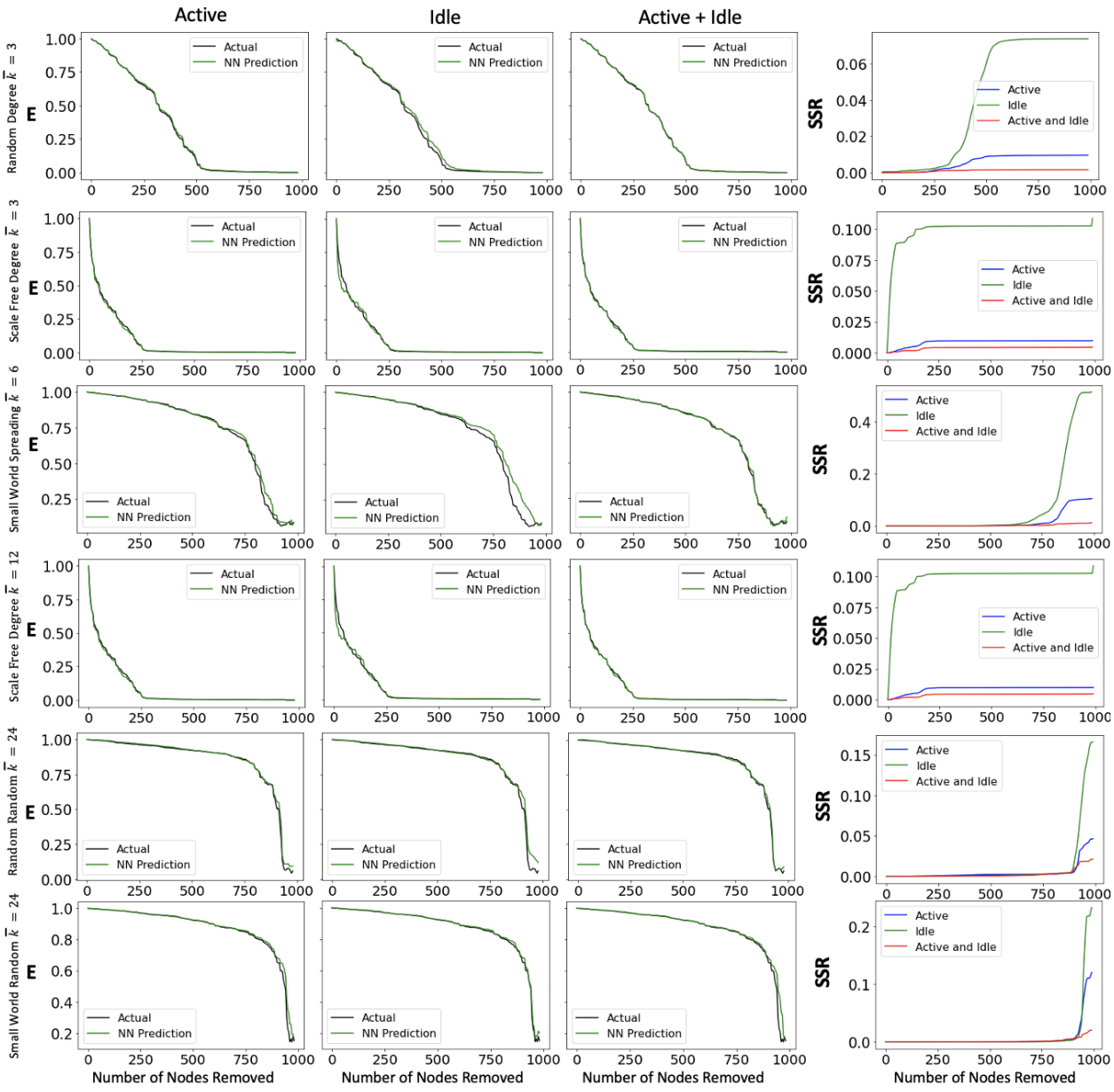
| | | SF Degree | SF Connecte | SF Random | SW Degree | SW Connecte | SW Random | R Degree | R Connected | R Random |
|---|---|---|---|---|---|---|---|---|---|---|
| Kbar = 3 | Active | 0.02 ± 0.03 | 0.2 ± 0.13 | 3.79 ± 3.47 | 0.01 ± 0.01 | 0.13 ± 0.12 | 0.04 ± 0.03 | 0.01 ± 0.02 | 0.09 ± 0.10 | 0.06 ± 0.03 |
| | Idle | 0.10 ± 0.10 | 0.47 ± 0.29 | 6.15 ± 5.16 | 0.03 ± 0.05 | 0.25 ± 0.23 | 0.14 ± 0.08 | 0.05 ± 0.07 | 0.17 ± 0.15 | 0.15 ± 0.10 |
| | Active + Idle | 0.01 ± 0.01 | 0.1 ± 0.09 | 0.42 ± 0.29 | 0.01 ± 0.03 | 0.08 ± 0.06 | 0.03 ± 0.02 | 0.006 ± 0.00 | 0.05 ± 0.10 | 0.03 ± 0.02 |
| Kbar = 6 | Active | 0.04 ± 0.05 | 0.12 ± 0.07 | 0.67 ± 0.50 | 0.02 ± 0.01 | 0.06 ± 0.04 | 0.04 ± 0.02 | 0.02 ± 0.01 | 0.05 ± 0.03 | 0.04 ± 0.03 |
| | Idle | 0.11 ± 0.011 | 0.33 ± 0.21 | 0.42 ± 0.33 | 0.04 ± 0.02 | 0.14 ± 0.11 | 0.09 ± 0.06 | 0.06 ± 0.04 | 0.12 ± 0.09 | 0.12 ± 0.10 |
| | Active + Idle | 0.03 ± 0.02 | 0.07 ± 0.05 | 0.27 ± 0.21 | 0.01 ± 0.004 | 0.02 ± 0.01 | 0.02 ± 0.006 | 0.003 ± 0.00 | 0.01 ± 0.01 | 0.01 ± 0.004 |
| Kbar = 12 | Active | 0.02 ± 0.01 | 0.08 ± 0.04 | 0.92 ± 0.57 | 0.02 ± 0.02 | 0.06 ± 0.05 | 0.04 ± 0.02 | 0.01 ± 0.01 | 0.05 ± 0.04 | 0.06 ± 0.07 |
| | Idle | 0.06 ± 0.05 | 0.13 ± 0.08 | 0.45 ± 0.26 | 0.06 ± 0.05 | 0.14 ± 0.10 | 0.13 ± 0.08 | 0.05 ± 0.03 | 0.12 ± 0.09 | 0.13 ± 0.13 |
| | Active + Idle | 0.01 ± 0.006 | 0.05 ± 0.03 | 0.17 ± 0.14 | 0.01 ± 0.006 | 0.02 ± 0.01 | 0.01 ± 0.009 | 0.002 ± 0.00 | 0.02 ± 0.02 | 0.03 ± 0.02 |
| Kbar = 24 | Active | 0.01 ± 0.01 | 0.05 ± 0.02 | 0.70 ± 0.75 | 0.04 ± 0.03 | 0.09 ± 0.07 | 0.09 ± 0.09 | 0.02 ± 0.02 | 0.10 ± 0.15 | 0.06 ± 0.08 |
| | Idle | 0.04 ± 0.01 | 0.1 ± 0.09 | 0.19 ± 0.12 | 0.07 ± 0.05 | 0.16 ± 0.14 | 0.15 ± 0.12 | 0.07 ± 0.05 | 0.17 ± 0.18 | 0.15 ± 0.14 |
| | Active + Idle | 0.008 ± 0.00 | 0.04 ± 0.02 | 0.12 ± 0.132 | 0.02 ± 0.02 | 0.03 ± 0.02 | 0.03 ± 0.05 | 0.01 ± 0.005 | 0.05 ± 0.09 | 0.03 ± 0.03 |

## Section B: Deterioration of Predictive Power through Generalization

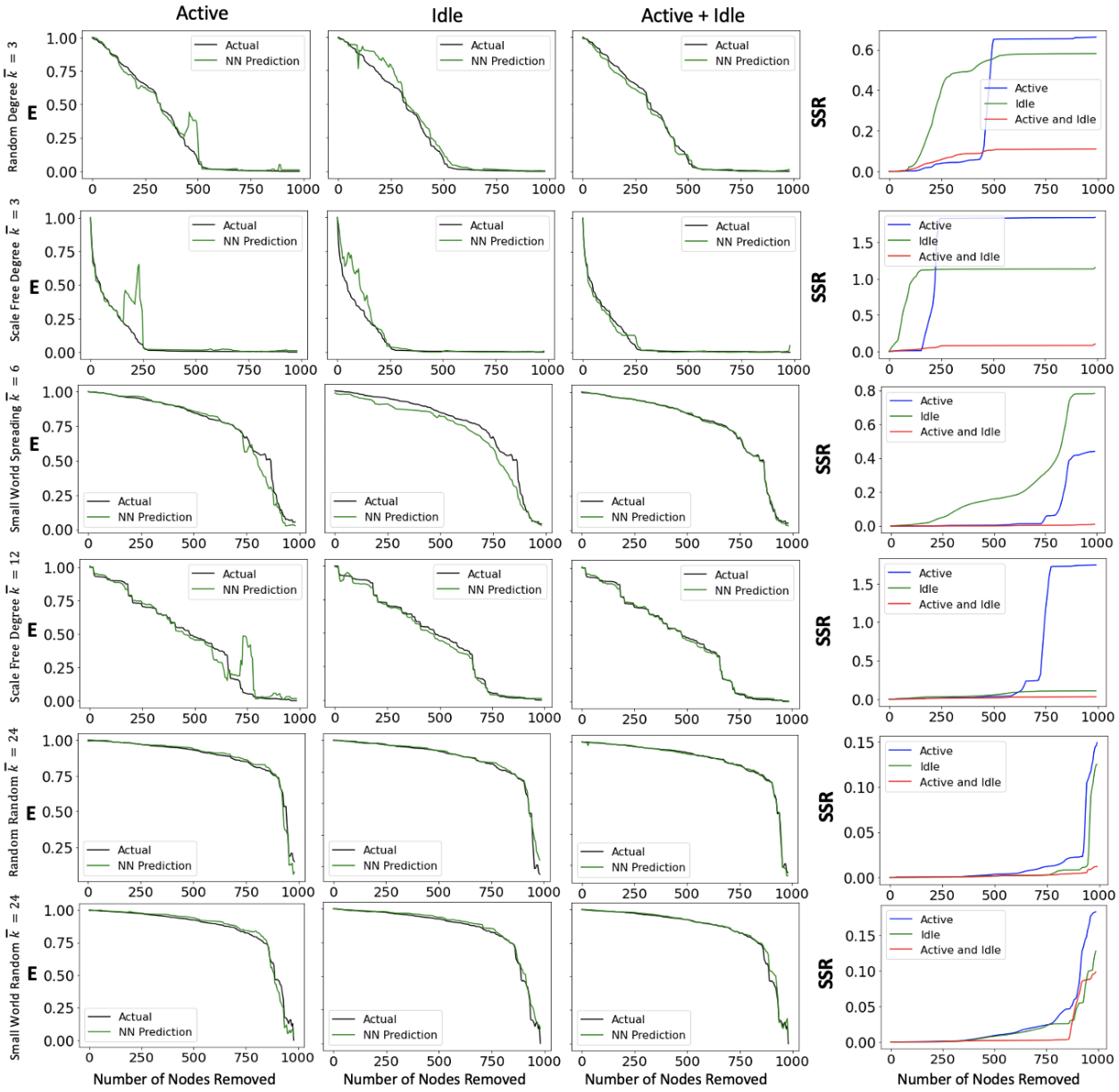
This table displays the sum of squared residuals (SSR) for 6 combinations of topology, attack, and link density, for the specific, generalized for link density, and generalized for topology, attack scheme, and link density neural networks. These are the SSR for the following 3 figures.

| | Specific | | | Generalized Kbar | | | Completely Generalized | | |
|---|---|---|---|---|---|---|---|---|---|
| | Active | Idle | Active + Idle | Active | Idle | Active + Idle | Active | Idle | Active + Idle |
| SF Connecte | 0.07 ± 0.03 | 0.12 ± 0.08 | 0.05 ± 0.02 | 1.30 ± 0.53 | 0.18 ± 0.13 | 0.06 ± 0.04 | 3.79 ± 1.47 | 0.97 ± 0.59 | 0.23 ± 0.09 |
| SF Degree 3 | 0.02 ± 0.03 | 0.10 ± 0.10 | 0.01 ± 0.01 | 2.39 ± 0.99 | 1.09 ± 0.56 | 0.13 ± 0.04 | 7.36 ± 1.70 | 1.07 ± 0.59 | 0.08 ± 0.04 |
| SW Random | 0.09 ± 0.09 | 0.15 ± 0.12 | 0.03 ± 0.05 | 0.15 ± 0.12 | 0.21 ± 0.18 | 0.05 ± 0.08 | 0.78 ± 0.16 | 3.20 ± 0.46 | 0.07 ± 0.05 |
| SW Connecte | 0.06 ± 0.04 | 0.14 ± 0.11 | 0.02 ± 0.01 | 0.40 ± 0.21 | 0.66 ± 0.35 | 0.03 ± 0.02 | 1.26 ± 0.53 | 0.89 ± 0.34 | 0.13 ± 0.05 |
| R Random 2 | 0.06 ± 0.07 | 0.15 ± 0.14 | 0.03 ± 0.02 | 0.12 ± 0.09 | 0.22 ± 0.19 | 0.06 ± 0.04 | 0.95 ± 0.34 | 3.24 ± 0.62 | 0.08 ± 0.05 |
| R Degree 3 | 0.01 ± 0.02 | 0.05 ± 0.07 | 0.006 ± 0.00 | 0.59 ± 0.21 | 0.50 ± 0.26 | 0.14 ± 0.04 | 5.70 ± 1.30 | 5.24 ± 2.21 | 0.09 ± 0.02 |

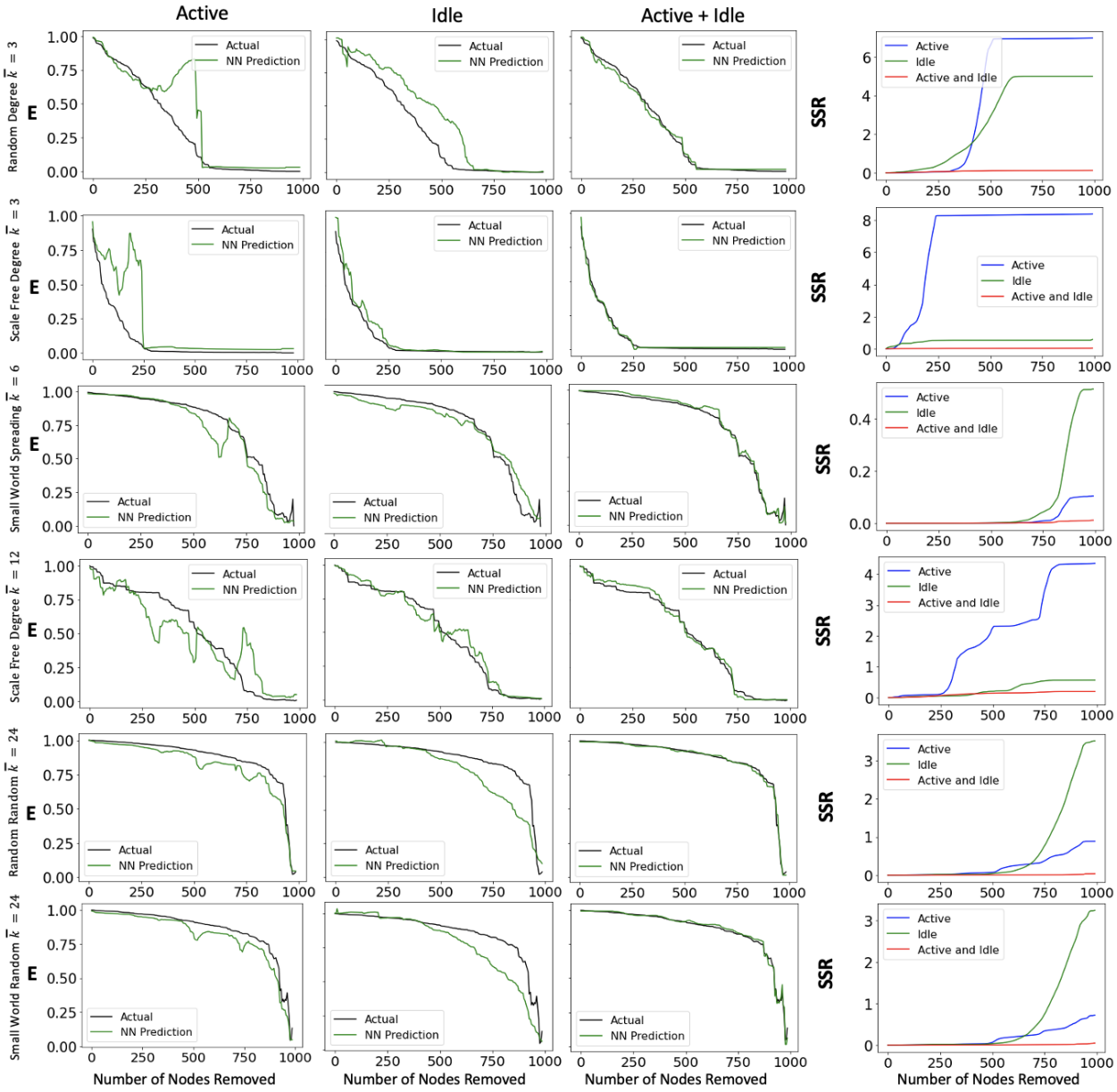
The figure below demonstrates the specifically trained neural networks for 6 combinations of topology, attack, and link density, along with the sum of squared residuals curves.



The figure below demonstrates the generalized neural networks for a specific link density, predicting 6 different combinations of topology, attack, and link density, along with the sum of squared residuals curves.



The figure below demonstrates the completely generalized neural networks for all topologies, attack schemes, and link densities, predicting 6 different combinations of topology, attack, and link density, along with the sum of squared residuals curves.



## Section C: Neural Network Generalized for Link Density.

The table below displays the errors of the link density generalized neural networks, trained with all topologies and attacks for a specific link density, for all the possible combinations of Topology, Attack Scheme, and Link Density.

| | | SF Degree | SF Connecte | SF Random | SW Degree | SW Connecte | SW Random | R Degree | R Connected | R Random |
|---|---|---|---|---|---|---|---|---|---|---|
| Kbar = 3 | Active | 2.39 ± 0.99 | 1.97 ± 1.64 | 1.48 ± 1.29 | 0.57 ± 0.17 | 0.77 ± 0.34 | 0.57 ± 0.36 | 0.59 ± 0.21 | 0.39 ± 0.29 | 0.30 ± 0.10 |
| | Idle | 1.09 ± 0.56 | 0.93 ± 1.69 | 3.69 ± 3.73 | 3.26 ± 1.02 | 1.47 ± 0.51 | 0.58 ± 0.34 | 0.50 ± 0.26 | 2.21 ± 1.18 | 0.46 ± 0.27 |
| | Active + Idle | 0.13 ± 0.04 | 0.49 ± 1.07 | 0.60 ± 0.50 | 0.12 ± 0.05 | 0.43 ± 0.80 | 0.24 ± 0.10 | 0.14 ± 0.05 | 0.15 ± 0.12 | 0.11 ± 0.03 |
| Kbar = 6 | Active | 2.08 ± 1.49 | 1.24 ± 0.69 | 1.75 ± 1.59 | 0.40 ± 0.13 | 0.40 ± 0.21 | 0.12 ± 0.05 | 0.44 ± 0.17 | 0.18 ± 0.12 | 0.16 ± 0.09 |
| | Idle | 0.38 ± 0.14 | 0.35 ± 0.22 | 1.21 ± 1.13 | 0.50 ± 0.16 | 0.66 ± 0.35 | 0.22 ± 0.10 | 0.14 ± 0.08 | 0.36 ± 0.21 | 0.21 ± 0.19 |
| | Active + Idle | 0.03 ± 0.02 | 0.08 ± 0.05 | 0.28 ± 0.17 | 0.02 ± 0.01 | 0.03 ± 0.02 | 0.03 ± 0.02 | 0.01 ± 0.01 | 0.03 ± 0.02 | 0.02 ± 0.01 |
| Kbar = 12 | Active | 1.80 ± 1.57 | 1.30 ± 0.53 | 1.30 ± 1.23 | 0.32 ± 0.09 | 0.23 ± 0.13 | 0.13 ± 0.09 | 0.52 ± 0.17 | 0.16 ± 0.10 | 0.19 ± 0.12 |
| | Idle | 0.10 ± 0.05 | 0.18 ± 0.13 | 0.54 ± 0.37 | 0.25 ± 0.16 | 0.27 ± 0.20 | 0.22 ± 0.15 | 0.12 ± 0.05 | 0.24 ± 0.22 | 0.17 ± 0.12 |
| | Active + Idle | 0.02 ± 0.01 | 0.06 ± 0.04 | 0.26 ± 0.24 | 0.04 ± 0.02 | 0.02 ± 0.01 | 0.03 ± 0.01 | 0.020 ± 0.00 | 0.02 ± 0.01 | 0.03 ± 0.02 |
| Kbar = 24 | Active | 2.42 ± 2.16 | 1.05 ± 0.40 | 3.46 ± 2.83 | 0.17 ± 0.04 | 0.20 ± 0.17 | 0.15 ± 0.12 | 0.29 ± 0.19 | 0.15 ± 0.14 | 0.12 ± 0.09 |
| | Idle | 0.05 ± 0.01 | 0.15 ± 0.12 | 0.81 ± 0.50 | 0.17 ± 0.11 | 0.18 ± 0.17 | 0.21 ± 0.18 | 0.09 ± 0.06 | 0.19 ± 0.17 | 0.22 ± 0.19 |
| | Active + Idle | 0.01 ± 0.01 | 0.05 ± 0.03 | 0.63 ± 0.34 | 0.06 ± 0.02 | 0.04 ± 0.02 | 0.05 ± 0.08 | 0.03 ± 0.01 | 0.06 ± 0.07 | 0.06 ± 0.04 |

## Section D: Neural Network Generalized for Topology, Attack Scheme, and Link Density.

The table below displays the errors of the completely generalized neural networks, trained with all topologies, attacks, and link densities, for all the possible combinations of topology, attack scheme, and link density.

| | | SF Degree | SF Connecte | SF Random | SW Degree | SW Connecte | SW Random | R Degree | R Connected | R Random |
|---|---|---|---|---|---|---|---|---|---|---|
| Kbar = 3 | Active | 7.36 ± 1.70 | 8.45 ± 1.18 | 2.70 ± 2.86 | 4.49 ± 0.55 | 0.72 ± 0.34 | 1.26 ± 0.58 | 5.70 ± 1.30 | 0.84 ± 0.37 | 0.84 ± 0.20 |
| | Idle | 1.07 ± 0.59 | 0.50 ± 0.24 | 13.56 ± 6.29 | 4.75 ± 1.42 | 3.21 ± 0.99 | 16.59 ± 1.95 | 5.24 ± 2.21 | 2.62 ± 0.89 | 15.45 ± 2.66 |
| | Active + Idle | 0.08 ± 0.04 | 0.24 ± 0.26 | 0.50 ± 0.32 | 0.11 ± 0.03 | 0.40 ± 0.26 | 0.41 ± 0.17 | 0.09 ± 0.02 | 0.17 ± 0.12 | 0.15 ± 0.05 |
| Kbar = 6 | Active | 6.48 ± 2.87 | 6.15 ± 1.91 | 4.00 ± 3.80 | 2.99 ± 0.74 | 1.26 ± 0.53 | 0.66 ± 0.16 | 3.80 ± 0.80 | 0.62 ± 0.26 | 0.64 ± 0.22 |
| | Idle | 0.70 ± 0.26 | 0.76 ± 0.40 | 3.03 ± 1.77 | 2.74 ± 0.71 | 0.89 ± 0.34 | 2.77 ± 0.65 | 0.46 ± 0.38 | 0.68 ± 0.30 | 2.88 ± 1.02 |
| | Active + Idle | 0.28 ± 0.15 | 0.25 ± 0.10 | 0.73 ± 0.60 | 0.29 ± 0.10 | 0.13 ± 0.05 | 0.67 ± 0.27 | 0.19 ± 0.08 | 0.10 ± 0.04 | 0.24 ± 0.10 |
| Kbar = 12 | Active | 3.81 ± 1.95 | 3.79 ± 1.47 | 4.09 ± 3.04 | 1.76 ± 0.36 | 1.33 ± 0.61 | 0.38 ± 0.13 | 2.83 ± 0.70 | 0.34 ± 0.12 | 0.33 ± 0.08 |
| | Idle | 0.27 ± 0.09 | 0.97 ± 0.59 | 1.32 ± 1.14 | 0.32 ± 0.15 | 1.71 ± 0.33 | 0.80 ± 0.24 | 1.70 ± 0.61 | 1.17 ± 0.27 | 0.79 ± 0.22 |
| | Active + Idle | 0.19 ± 0.08 | 0.23 ± 0.09 | 0.57 ± 0.31 | 0.19 ± 0.08 | 0.10 ± 0.04 | 0.26 ± 0.09 | 0.20 ± 0.05 | 0.07 ± 0.03 | 0.22 ± 0.08 |
| Kbar = 24 | Active | 2.98 ± 1.37 | 4.65 ± 0.83 | 11.14 ± 5.39 | 1.66 ± 0.23 | 1.28 ± 0.51 | 0.78 ± 0.16 | 2.75 ± 0.26 | 0.91 ± 0.30 | 0.95 ± 0.34 |
| | Idle | 0.11 ± 0.04 | 4.70 ± 1.60 | 8.06 ± 3.08 | 1.62 ± 0.29 | 4.08 ± 0.74 | 3.20 ± 0.46 | 3.39 ± 0.69 | 3.9 ± 0.73 | 3.24 ± 0.62 |
| | Active + Idle | 0.13 ± 0.03 | 0.56 ± 0.13 | 1.53 ± 0.82 | 0.12 ± 0.06 | 0.09 ± 0.04 | 0.07 ± 0.05 | 0.10 ± 0.03 | 0.10 ± 0.08 | 0.08 ± 0.05 |

## Section E: Neural Network for Real Complex Networks.

The figure below shows the results of neural networks being trained with stochastic attacks (degree, degree, between attacks), being used to predict out of sample stochastic attacks (between, between, degree), for three real networks (US airports, Budapest connectome, Power Grid).