Supplementary Information: A Framework of Hierarchical Attacks to Network Controllability

Yang Lou[1], Lin Wang[2,3], and Guanrong Chen[1]

[1]Department of Electrical Engineering, City University of Hong Kong, Hong Kong, China
[2]Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China
[3]Key Laboratory of System Control and Information Processing, Ministry of Education, Shanghai 200240, China

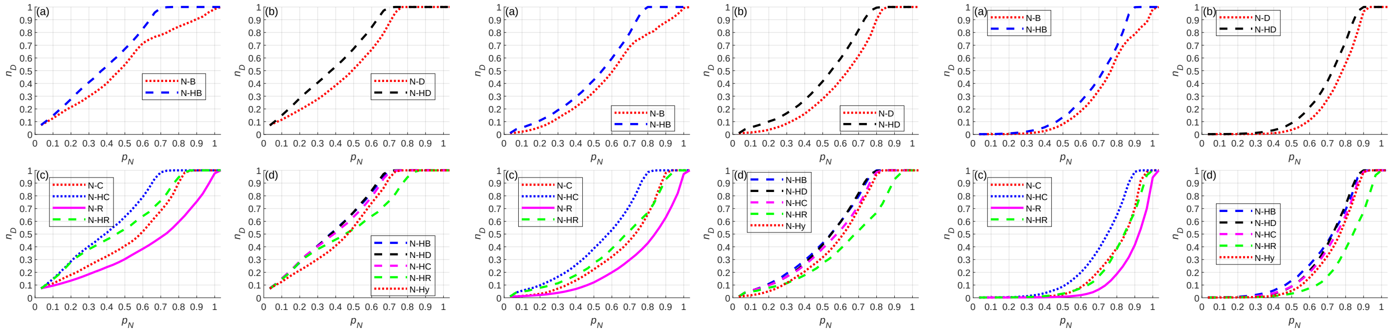
Emails: Y. Lou (felix.lou@my.cityu.edu.hk); L. Wang (wanglin@sjtu.edu.cn); G. Chen (eegchen@cityu.edu.hk)

Source code of this work is available in: https://fylou.github.io/sourcecode.html

Contents

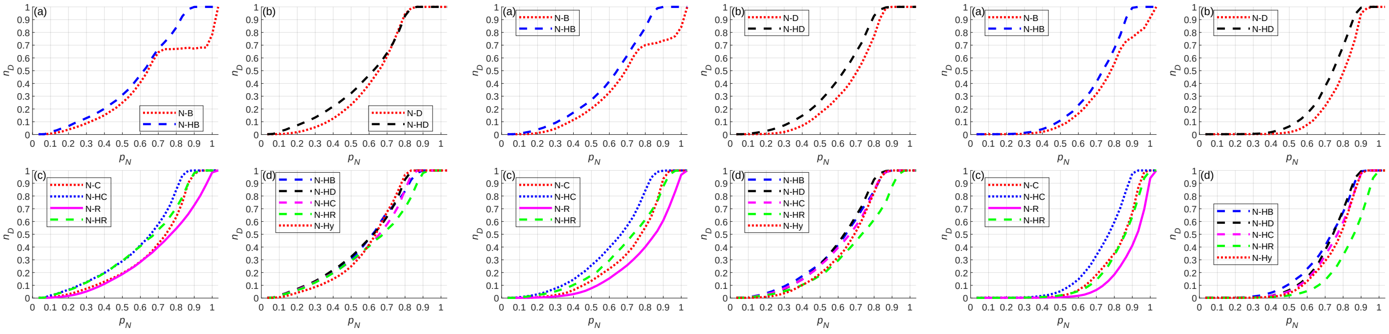
1 Controllability Curves Under Various Attack Simulations

Figures S1–S9 ... ... $N = 500$ and $\langle k \rangle = 3$, 5, and 10, node-removal attacks
Figures S10–S18 ... ... $N = 1000$ and $\langle k \rangle = 3$, 5, and 10, node-removal attacks
Figures S19–S27 ... ... $N = 1500$ and $\langle k \rangle = 3$, 5, and 10, node-removal attacks
Figures S28–S36 ... ... $N = 500$ and $\langle k \rangle = 3$, 5, and 10, edge-removal attacks
Figures S37–S45 ... ... $N = 1000$ and $\langle k \rangle = 3$, 5, and 10, edge-removal attacks
Figures S46–S54 ... ... $N = 1500$ and $\langle k \rangle = 3$, 5, and 10, edge-removal attacks
Figures S55 and S56 ... ... nine real-world networks under node- and edge-removal attacks.



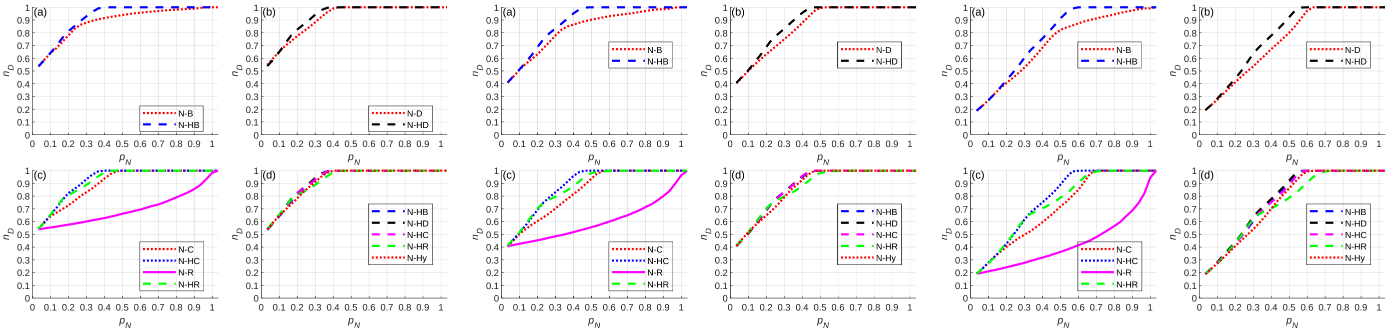
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S1: Node-removal attacks on $N = 500$ ER



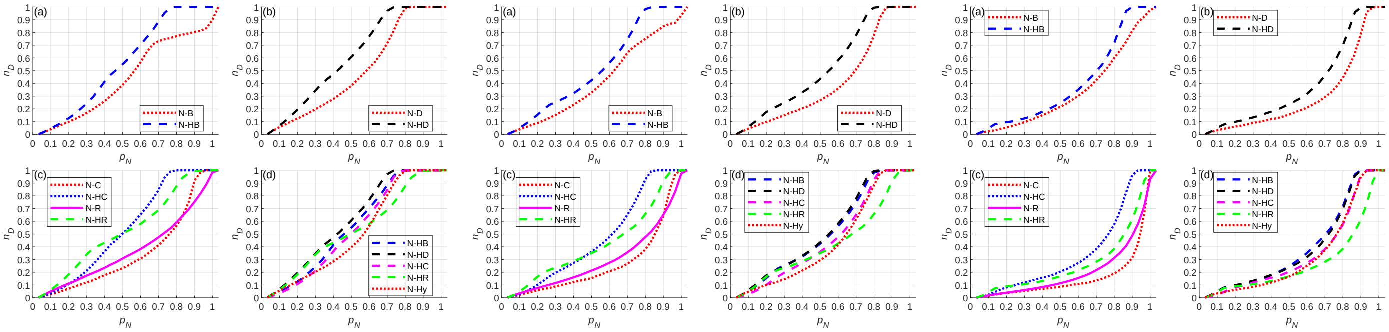
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S2: Node-removal attacks on $N = 500$ SW



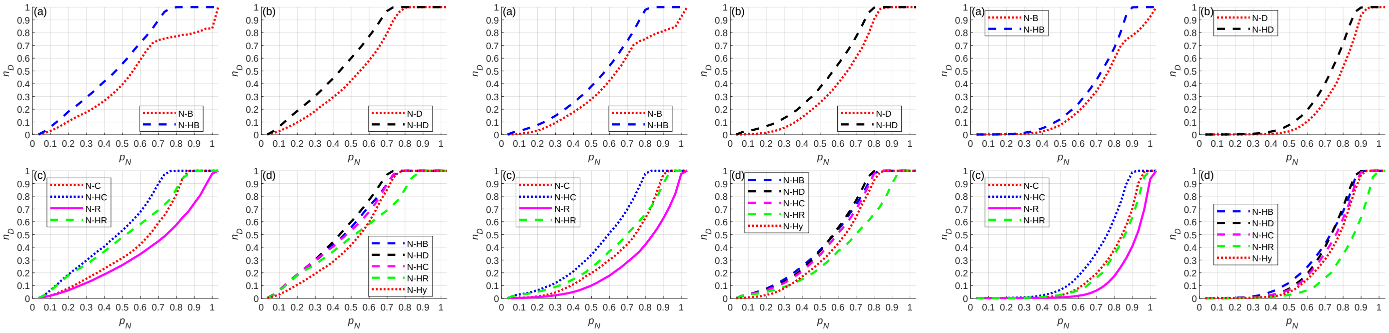
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S3: Node-removal attacks on $N = 500$ SF



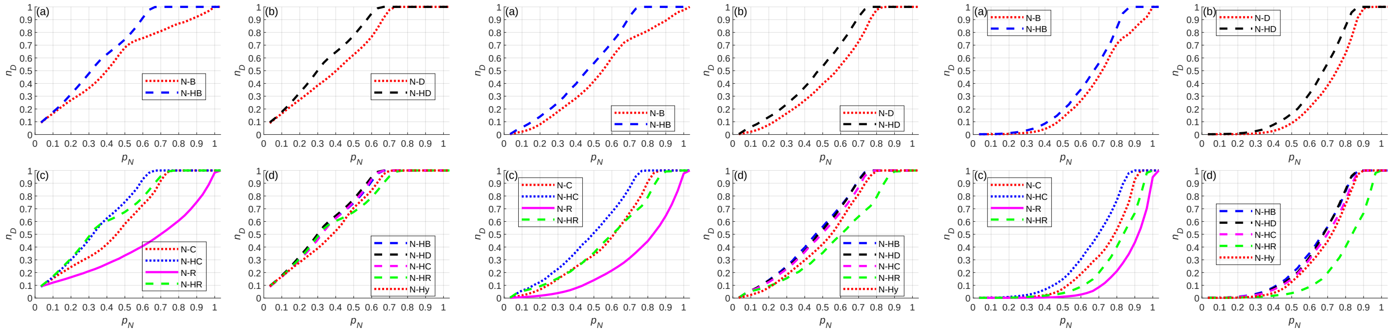
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S4: Node-removal attacks on $N = 500$ QS



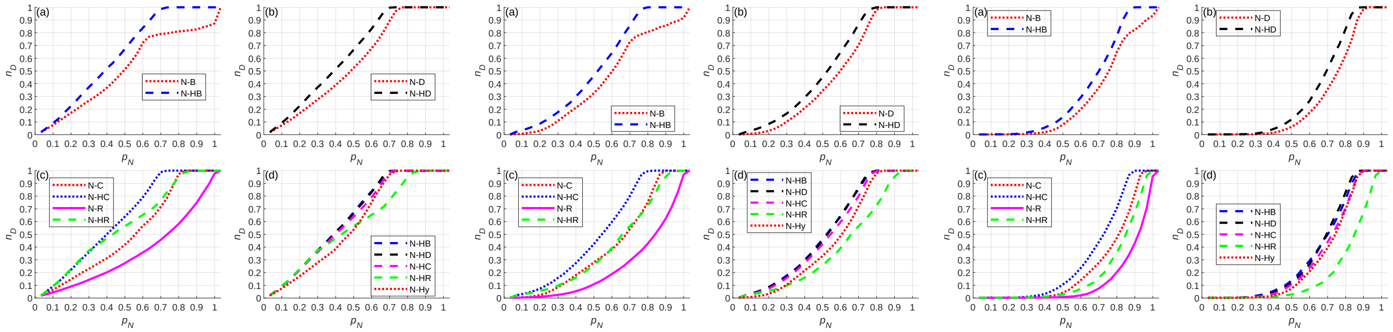
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S5: Node-removal attacks on $N = 500$ QR



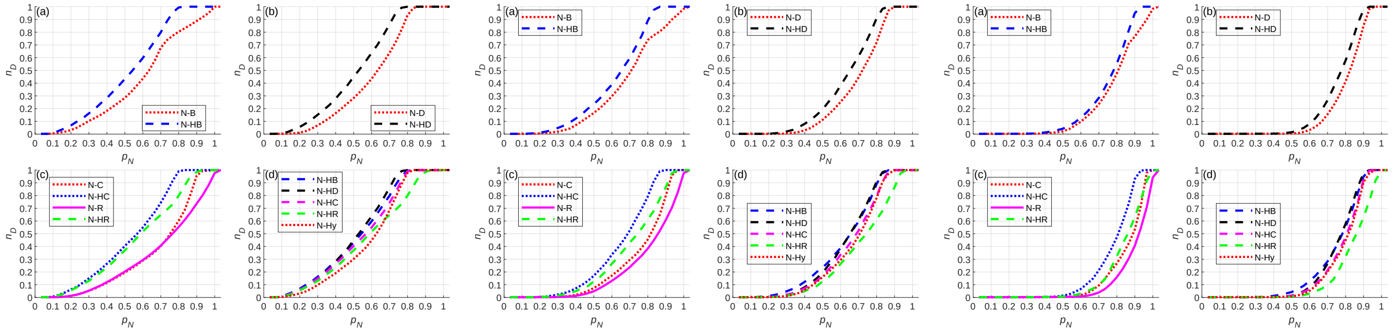
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S6: Node-removal attacks on $N = 500$ RT



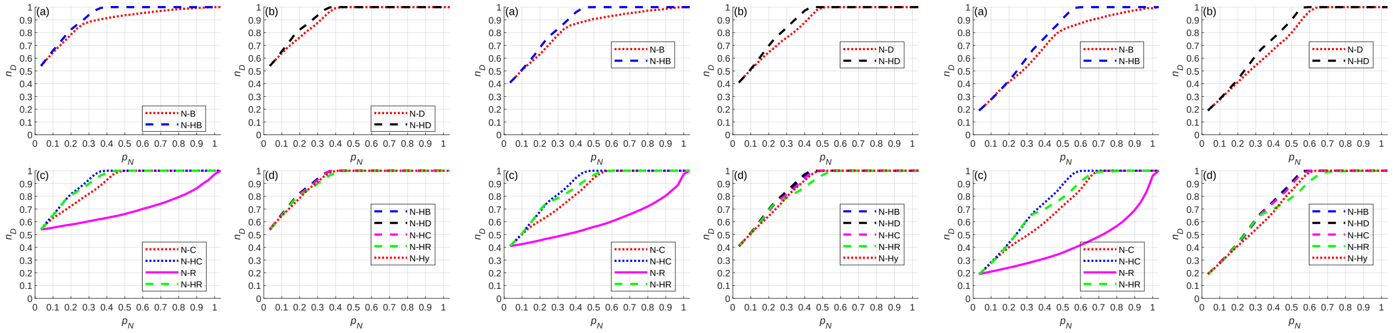
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S7: Node-removal attacks on $N = 500$ RR



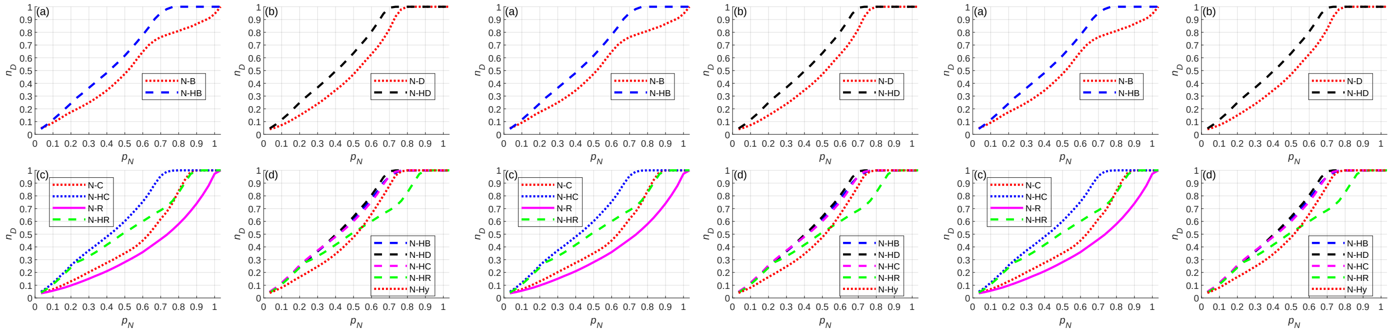
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S8: Node-removal attacks on $N = 500$ HO



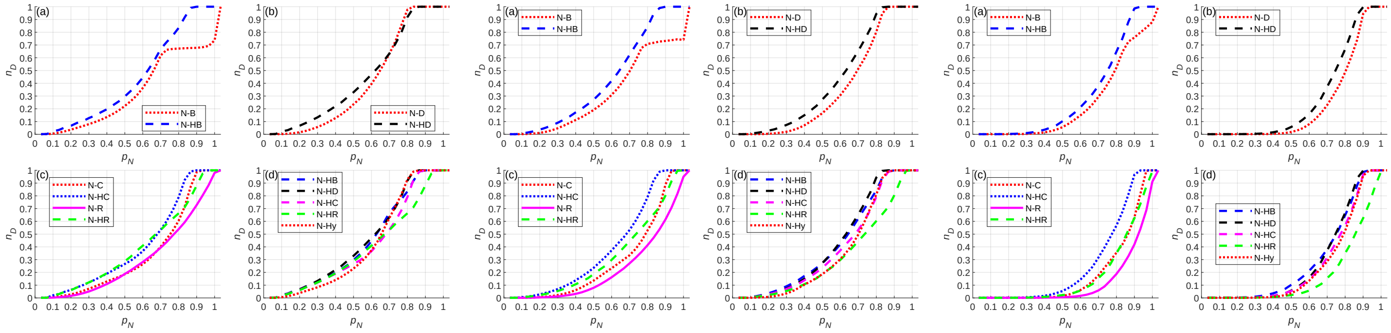
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S9: Node-removal attacks on $N = 500$ OL



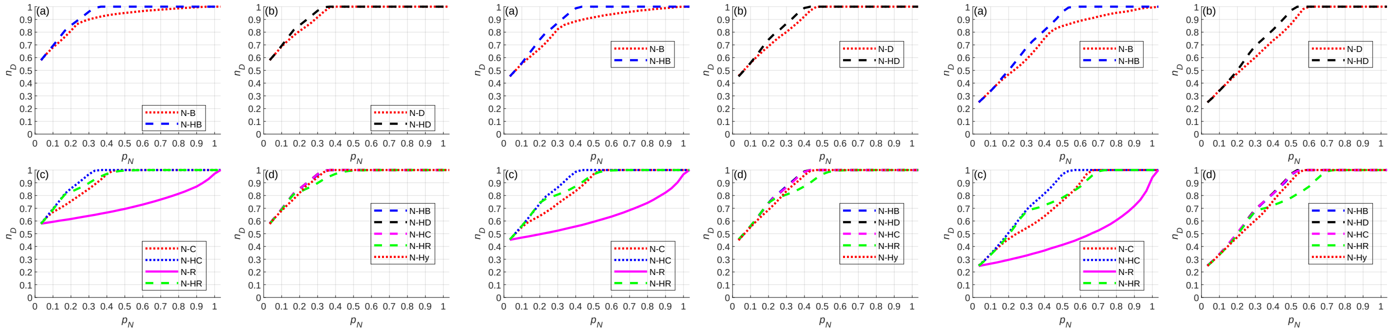
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S10: Node-removal attacks on $N = 1000$ ER



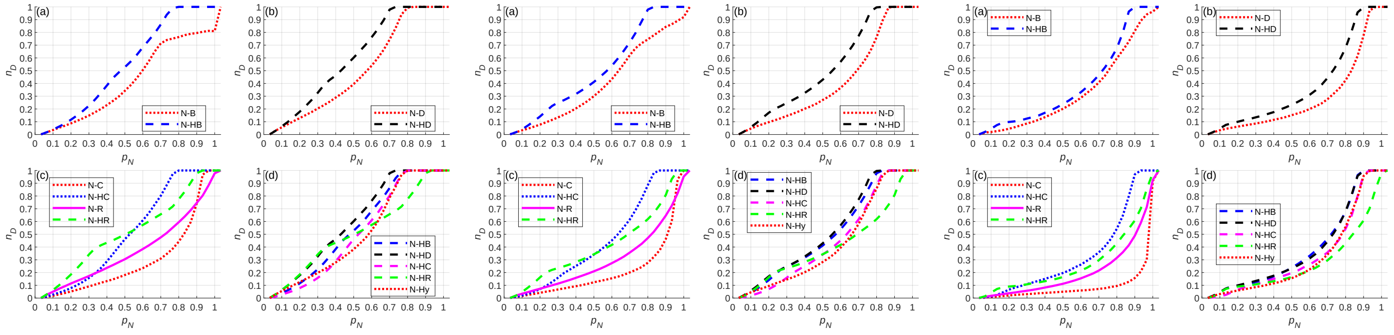
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S11: Node-removal attacks on $N = 1000$ SW



(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S12: Node-removal attacks on $N = 1000$ SF

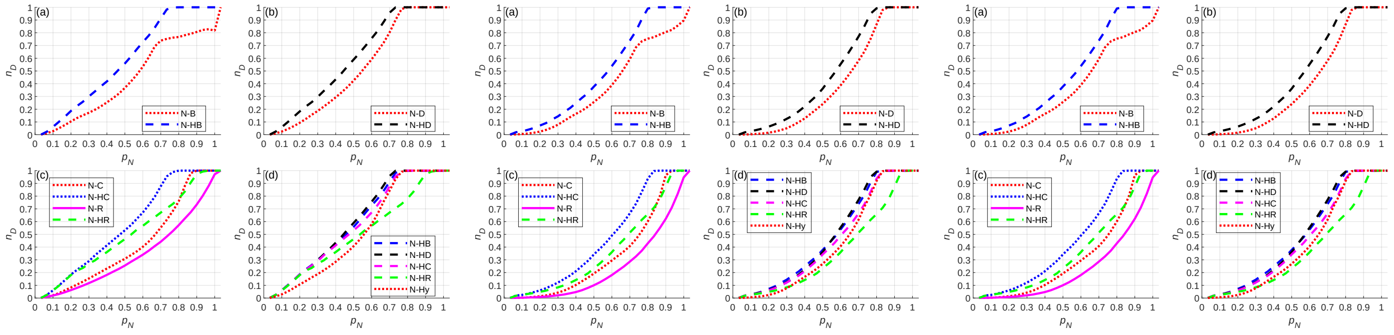


(a) $\langle k \rangle = 3$

(b) $\langle k \rangle = 5$

(c) $\langle k \rangle = 10$

Figure S13: Node-removal attacks on $N = 1000$ QS

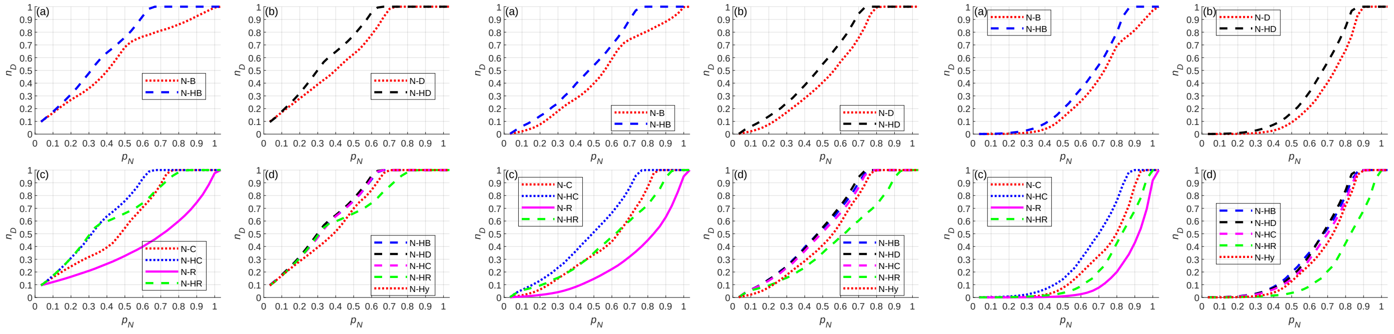


(a) $\langle k \rangle = 3$

(b) $\langle k \rangle = 5$

(c) $\langle k \rangle = 10$

Figure S14: Node-removal attacks on $N = 1000$ QR

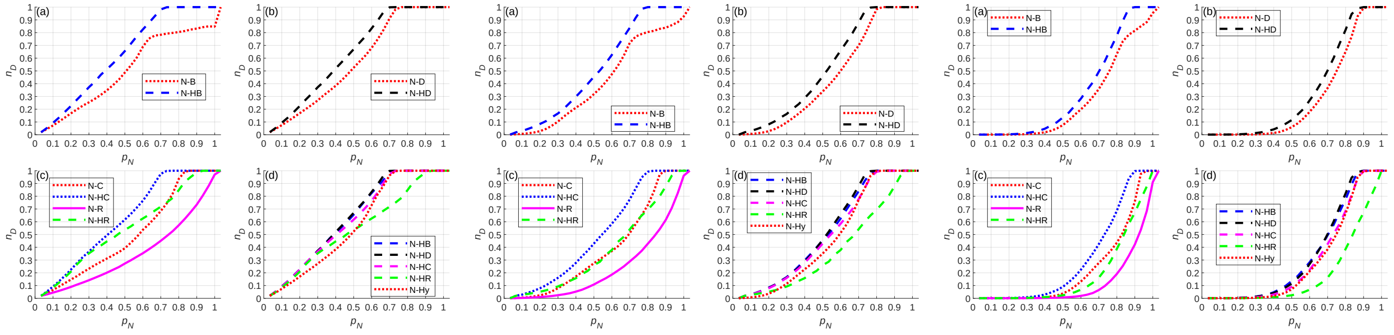


(a) $\langle k \rangle = 3$

(b) $\langle k \rangle = 5$

(c) $\langle k \rangle = 10$

Figure S15: Node-removal attacks on $N = 1000$ RT

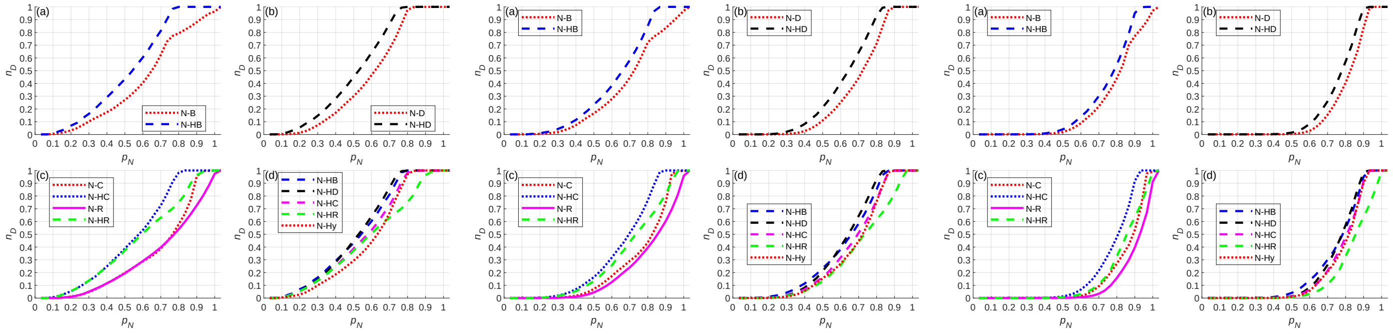


(a) $\langle k \rangle = 3$

(b) $\langle k \rangle = 5$

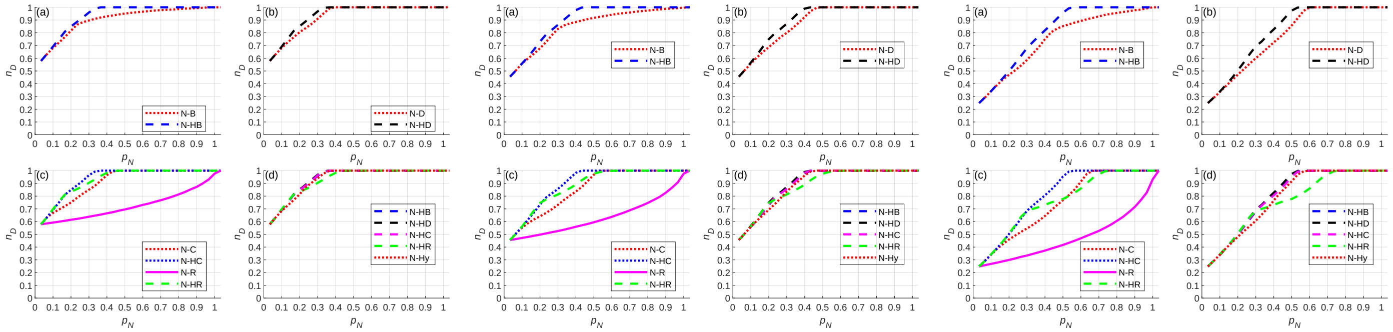
(c) $\langle k \rangle = 10$

Figure S16: Node-removal attacks on $N = 1000$ RR



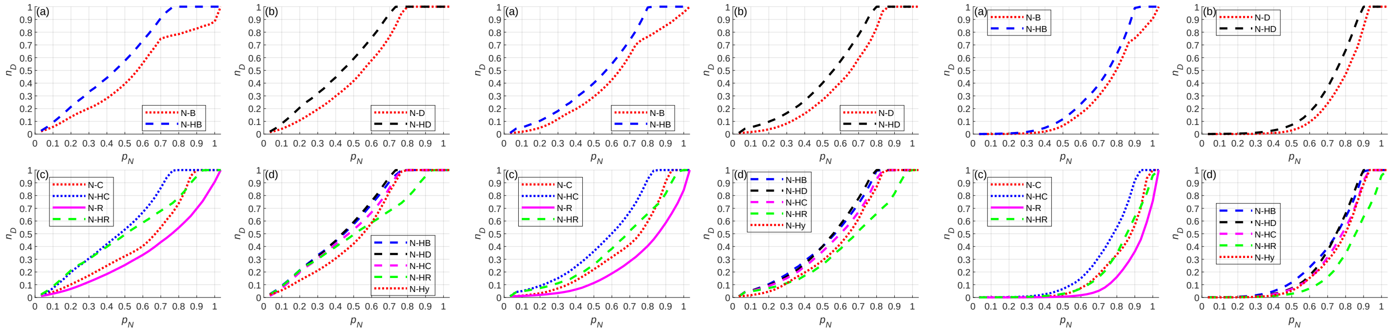
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S17: Node-removal attacks on $N = 1000$ HO



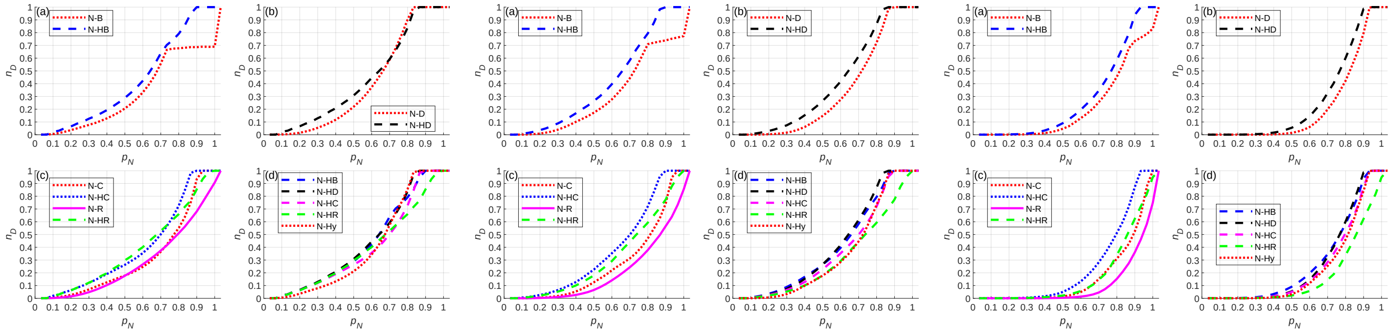
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S18: Node-removal attacks on $N = 1000$ OL



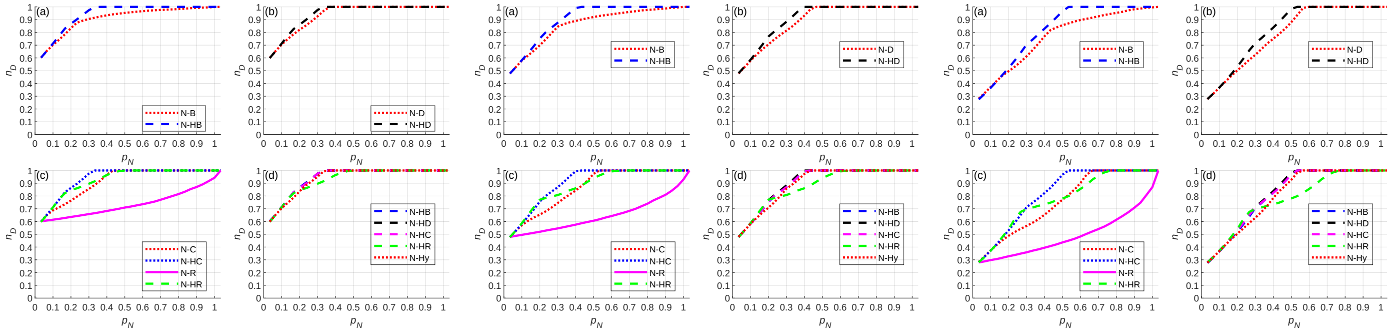
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S19: Node-removal attacks on $N = 1500$ ER



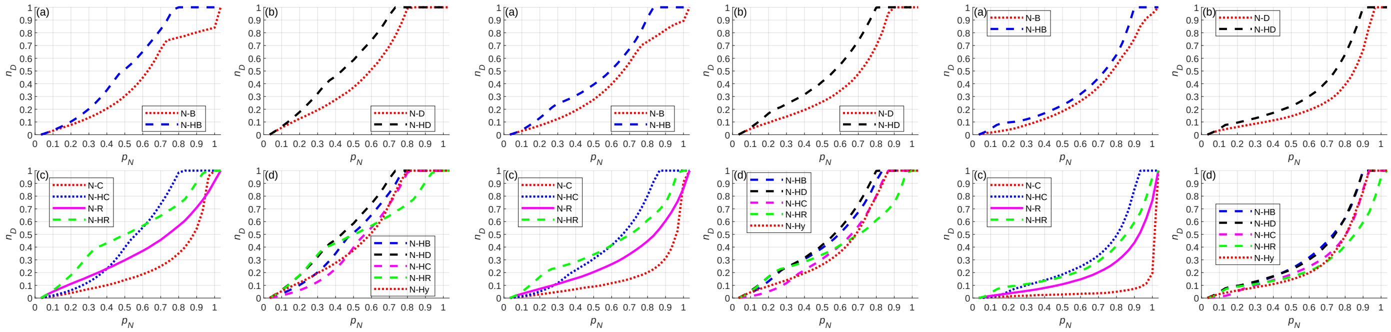
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S20: Node-removal attacks on $N = 1500$ SW



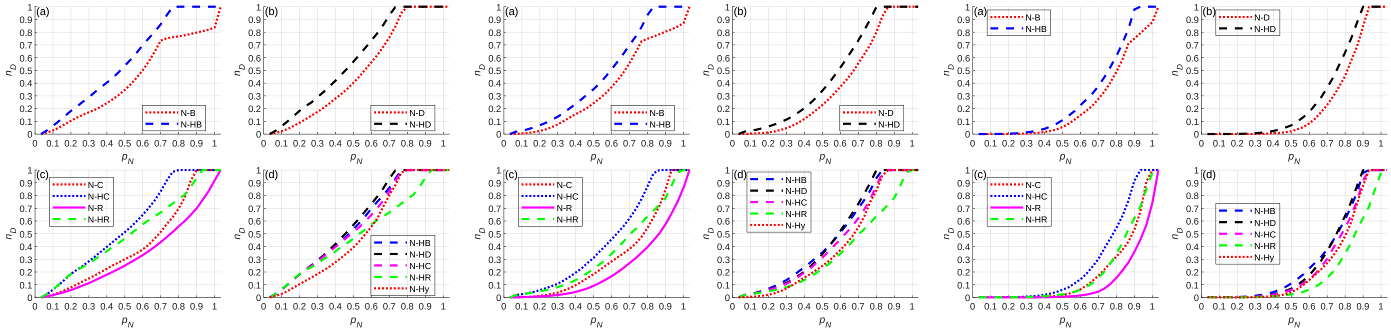
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S21: Node-removal attacks on $N = 1500$ SF



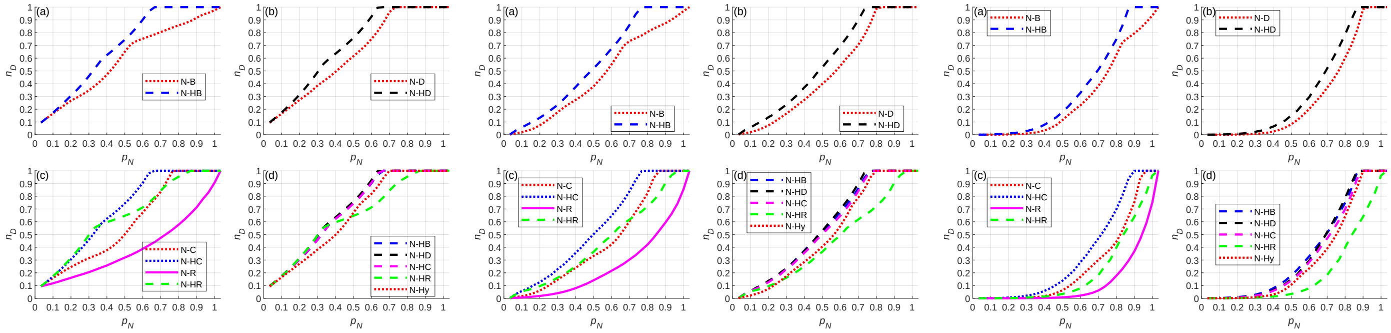
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S22: Node-removal attacks on $N = 1500$ QS



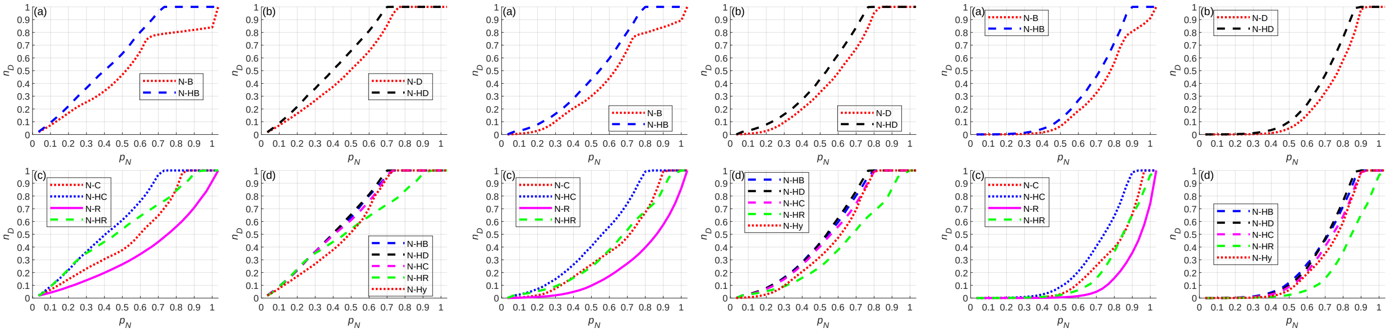
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S23: Node-removal attacks on $N = 1500$ QR



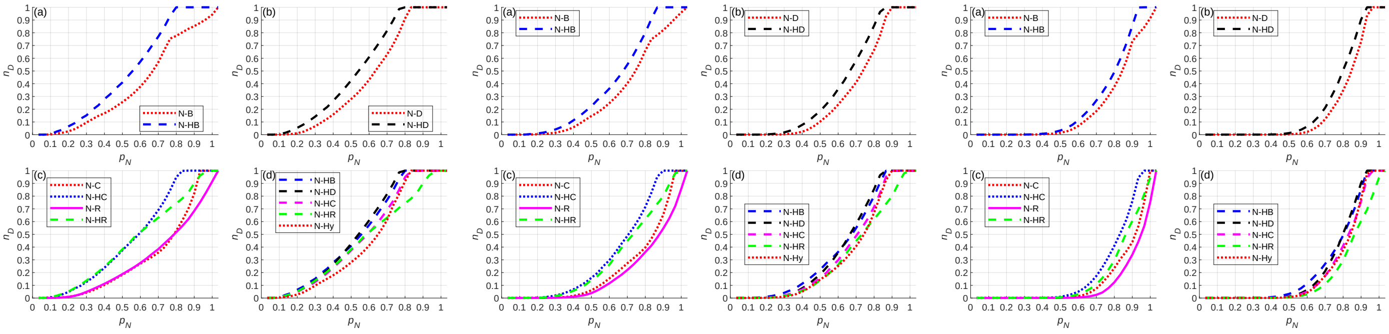
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S24: Node-removal attacks on $N = 1500$ RT



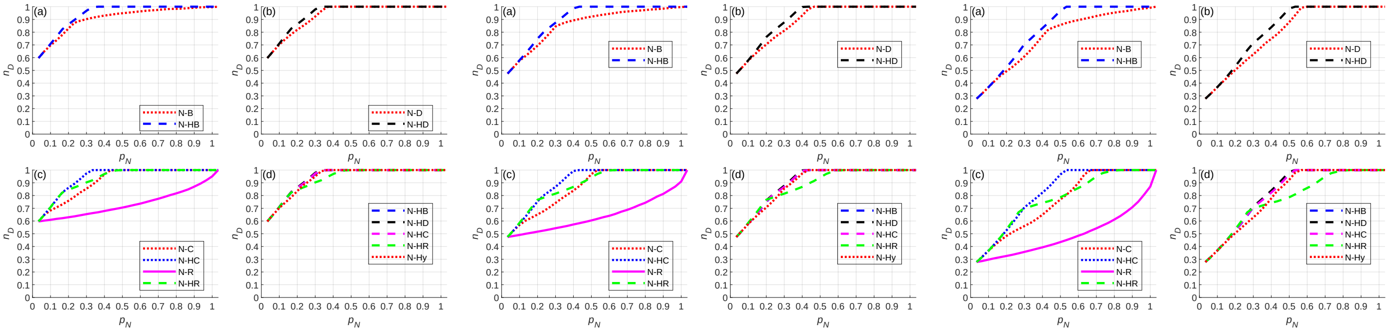
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S25: Node-removal attacks on $N = 1500$ RR



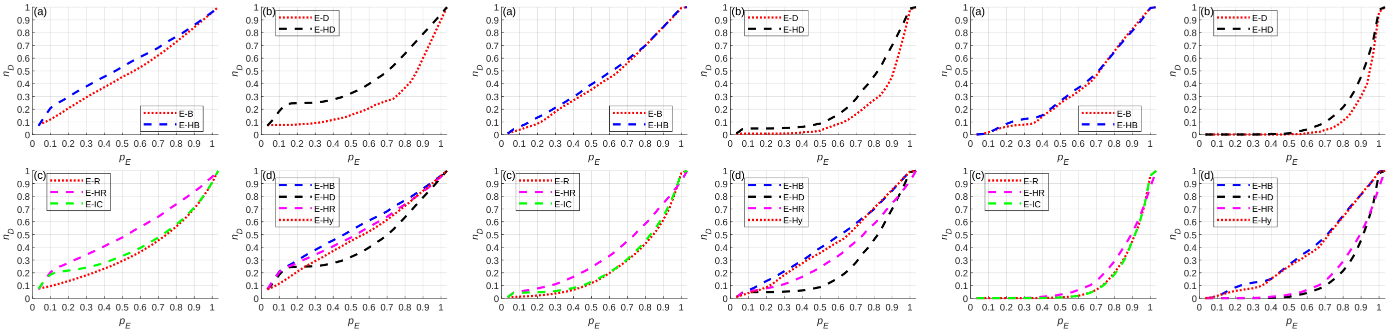
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S26: Node-removal attacks on $N = 1500$ HO



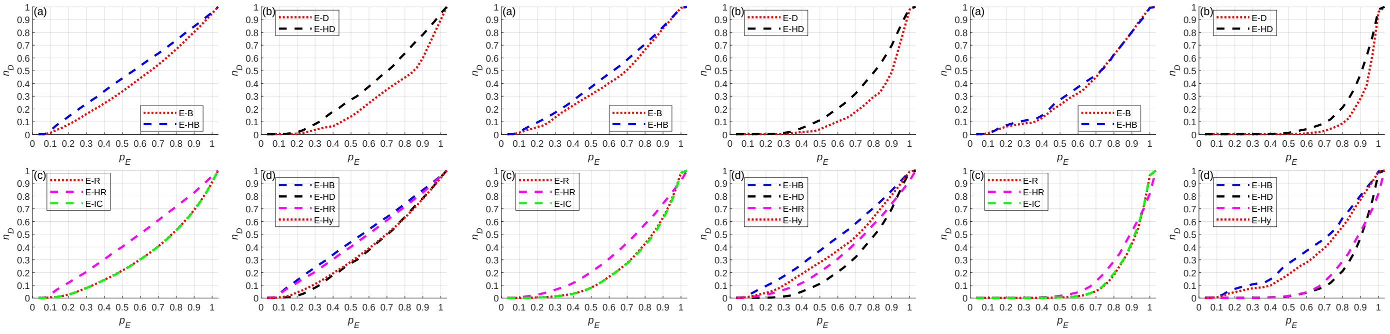
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S27: Node-removal attacks on $N = 1500$ OL



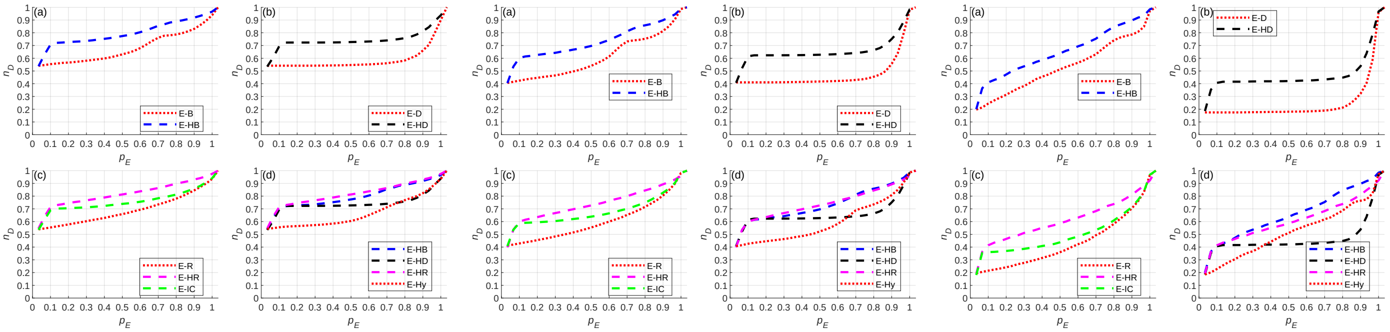
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S28: Edge-removal attacks on $N = 500$ ER



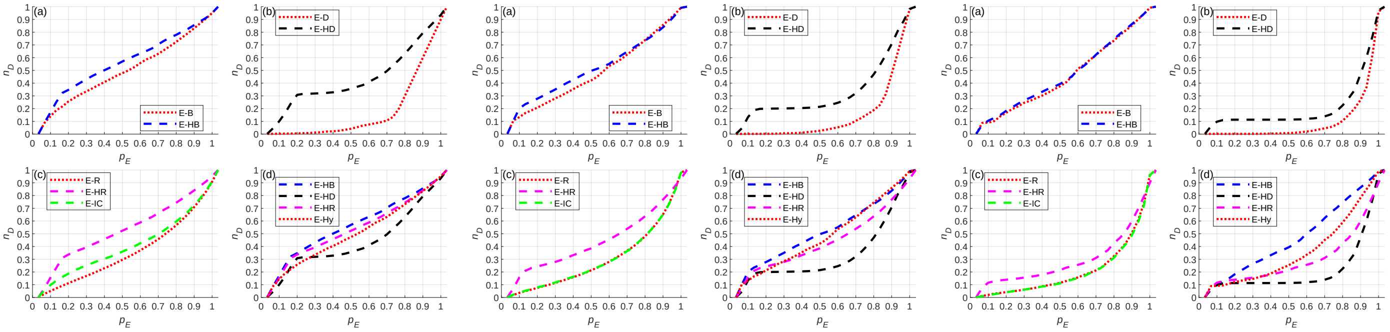
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S29: Edge-removal attacks on $N = 500$ SW



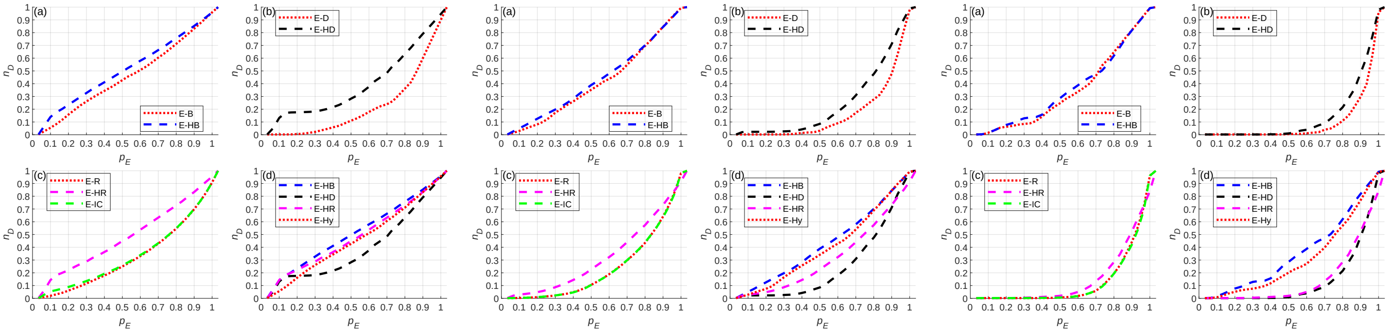
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S30: Edge-removal attacks on $N = 500$ SF



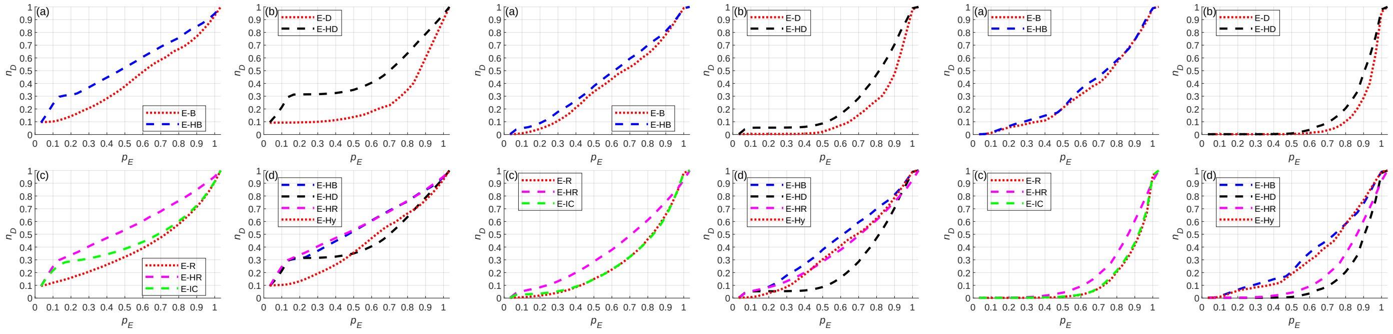
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S31: Edge-removal attacks on $N = 500$ QS



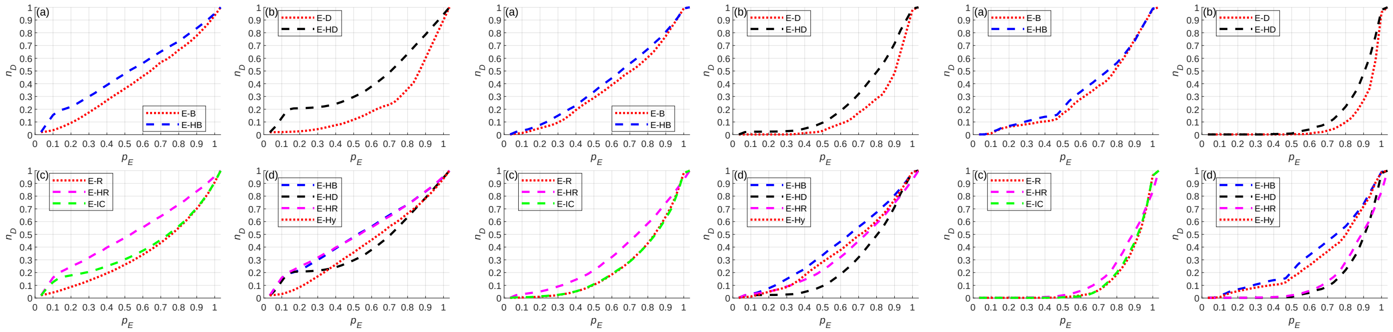
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S32: Edge-removal attacks on $N = 500$ QR



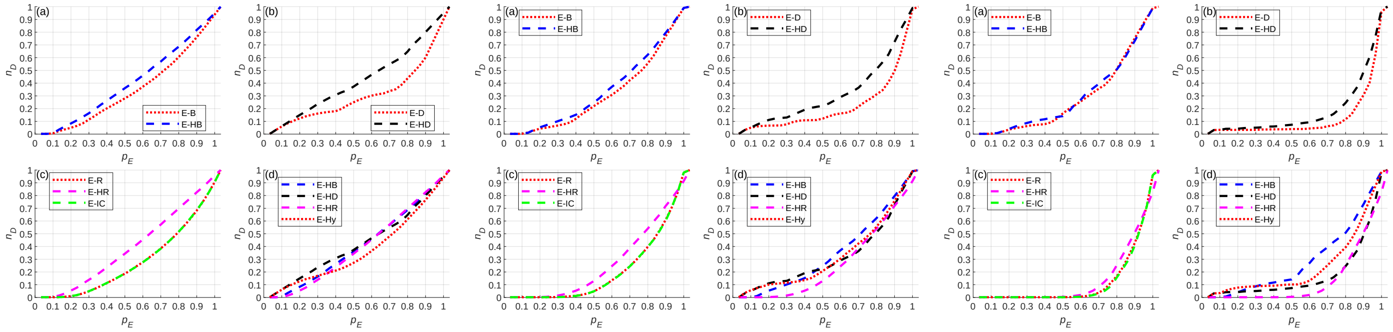
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S33: Edge-removal attacks on $N = 500$ RT



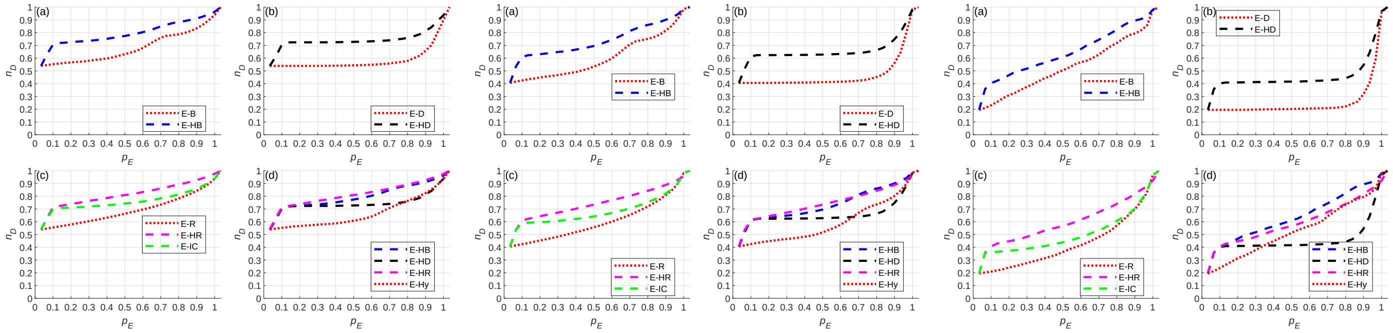
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S34: Edge-removal attacks on $N = 500$ RR



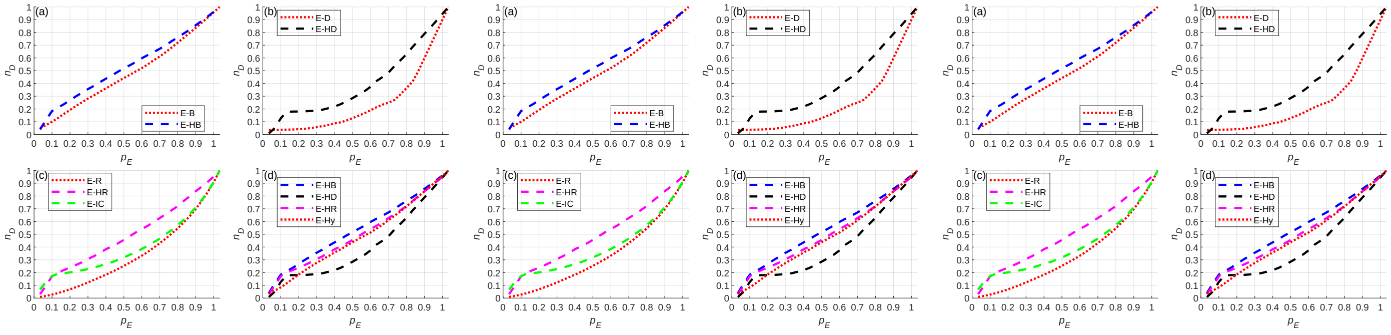
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S35: Edge-removal attacks on $N = 500$ HO



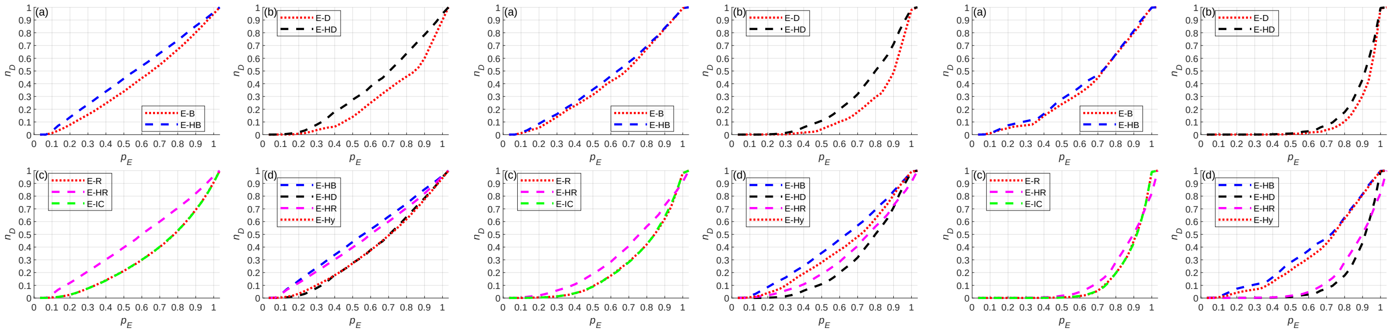
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S36: Edge-removal attacks on $N = 500$ OL



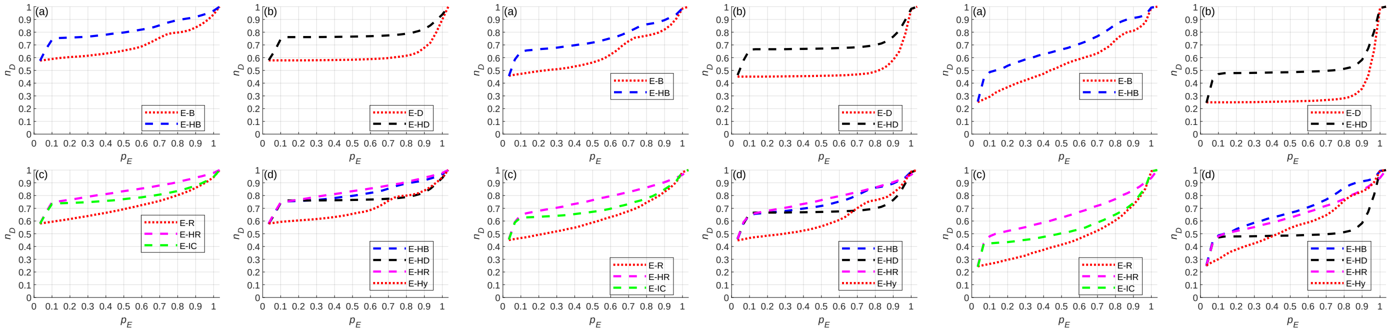
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S37: Edge-removal attacks on $N = 1000$ ER



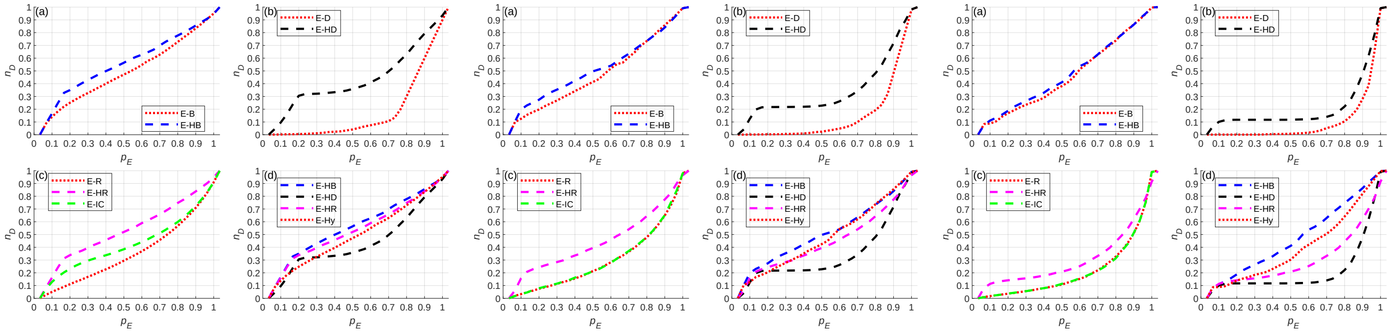
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S38: Edge-removal attacks on $N = 1000$ SW



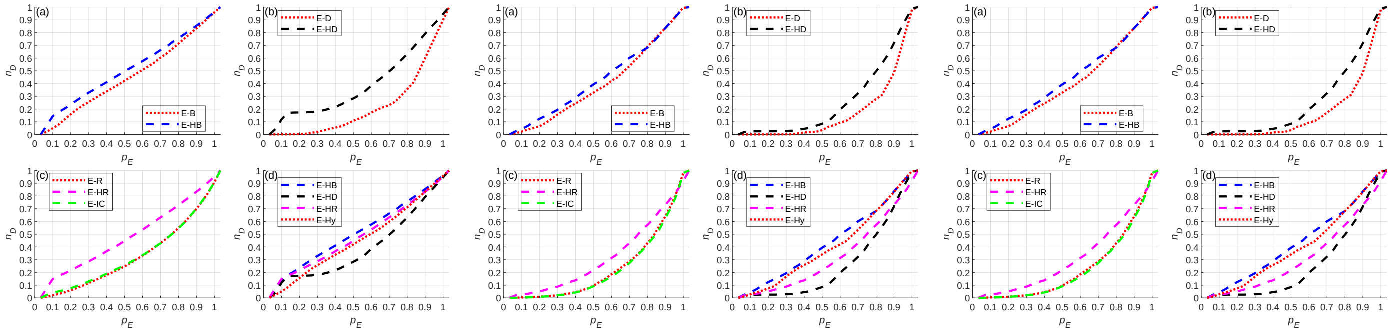
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S39: Edge-removal attacks on $N = 1000$ SF



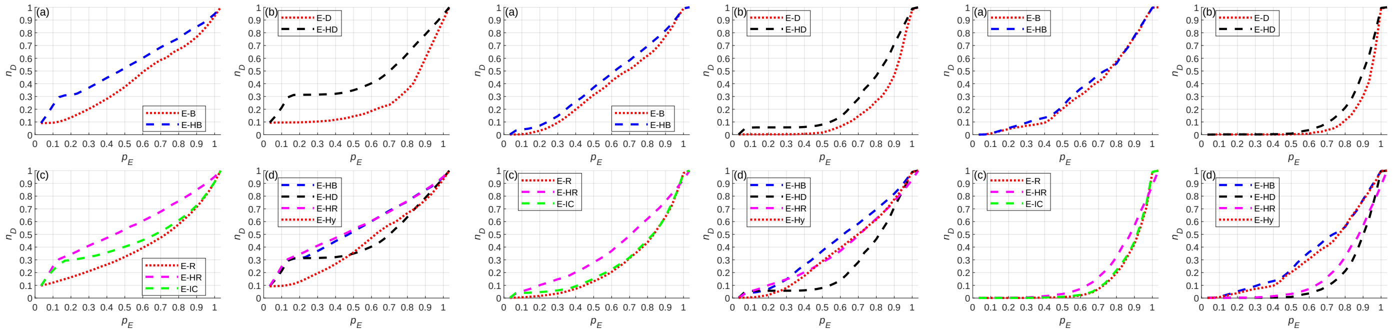
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S40: Edge-removal attacks on $N = 1000$ QS



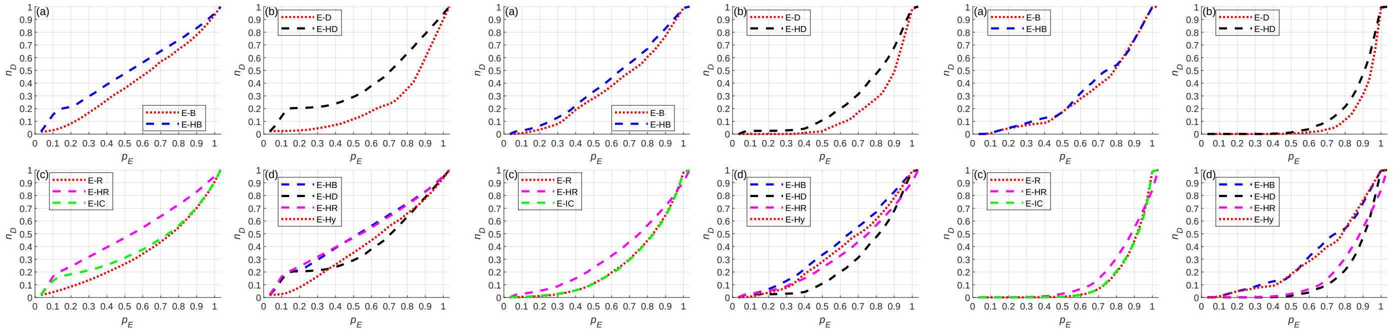
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S41: Edge-removal attacks on $N = 1000$ QR



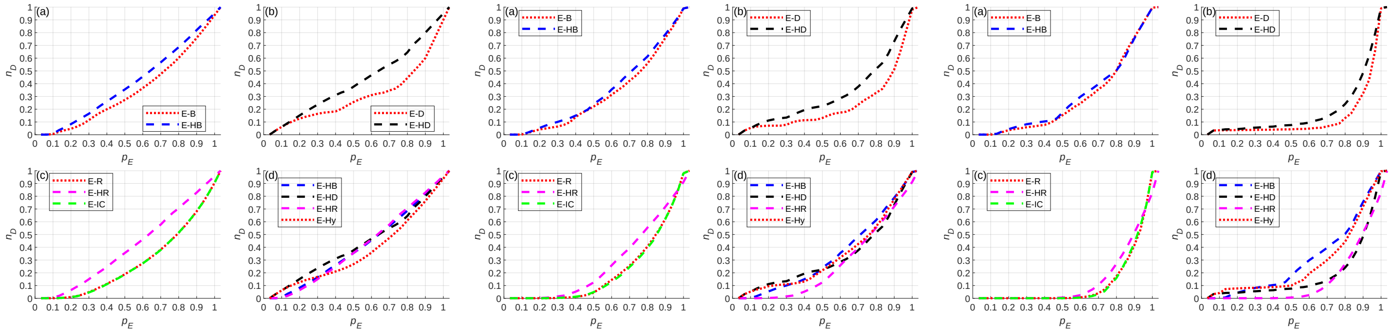
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S42: Edge-removal attacks on $N = 1000$ RT



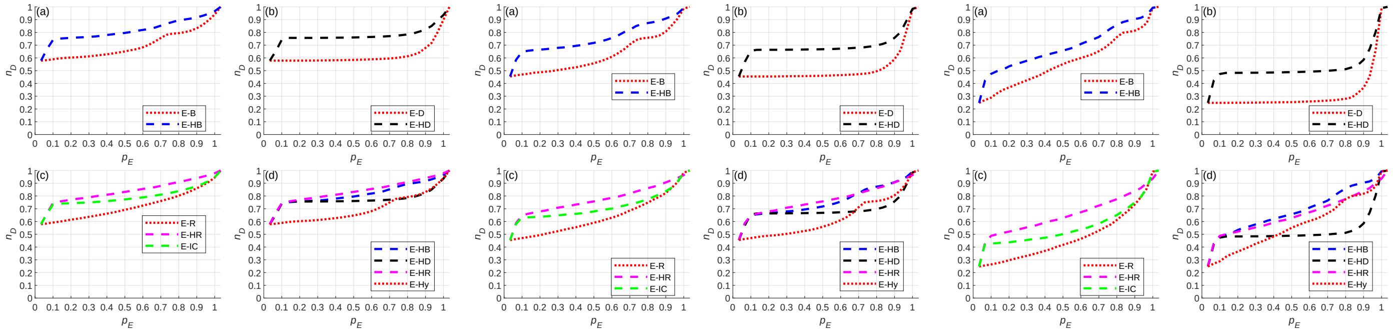
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S43: Edge-removal attacks on $N = 1000$ RR



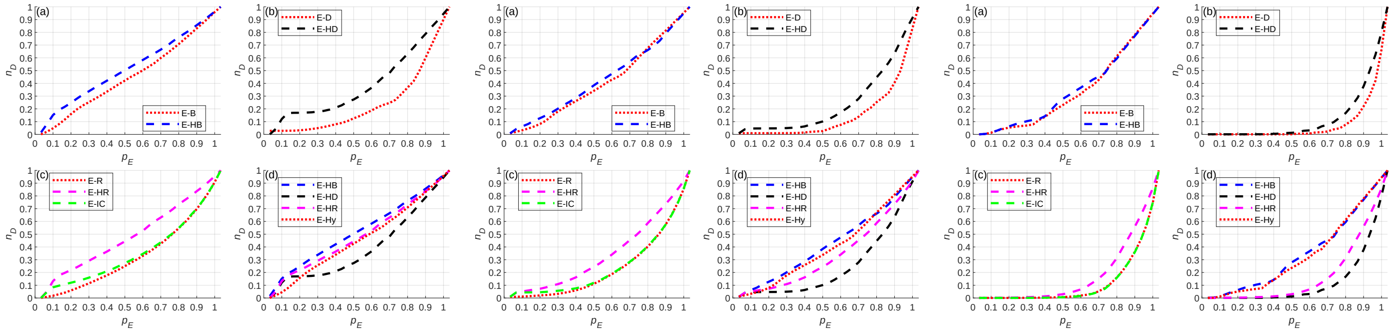
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S44: Edge-removal attacks on $N = 1000$ HO



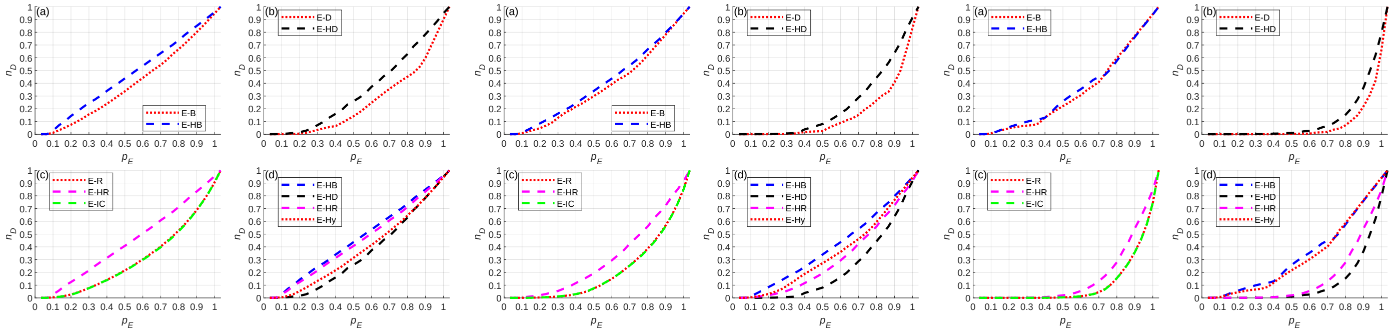
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S45: Edge-removal attacks on $N = 1000$ OL



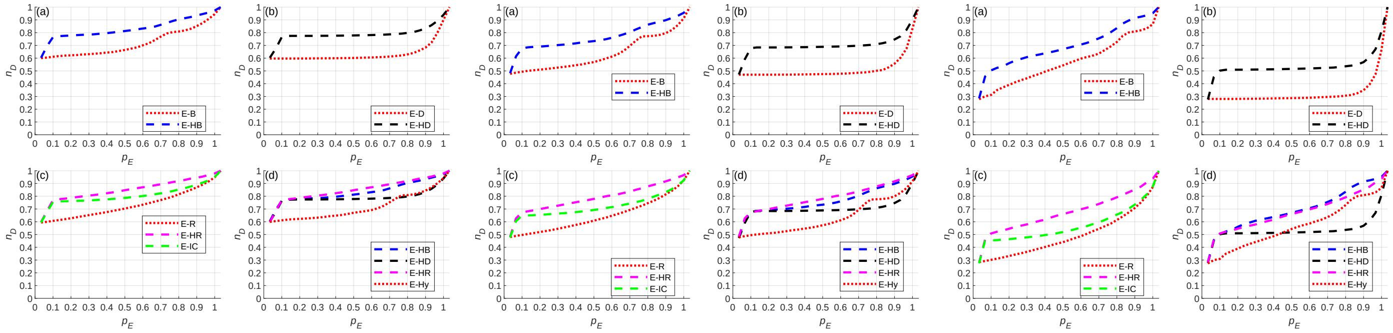
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S46: Edge-removal attacks on $N = 1500$ ER



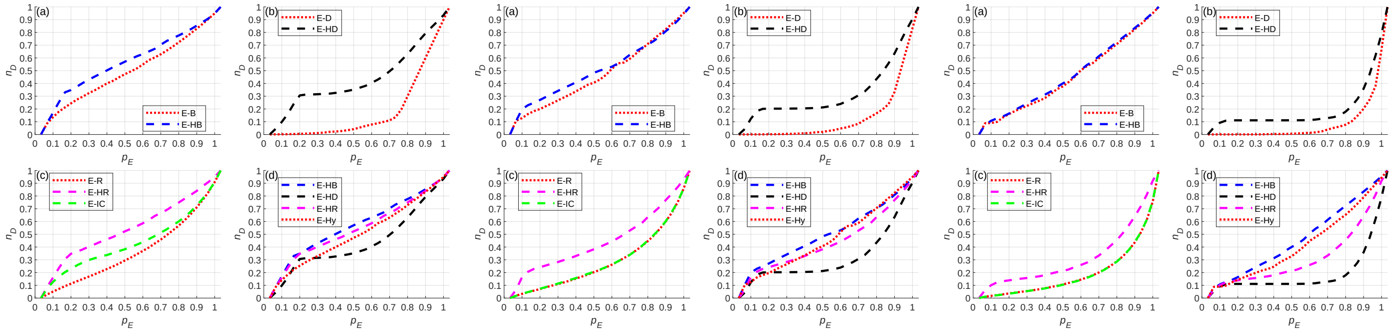
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S47: Edge-removal attacks on $N = 1500$ SW



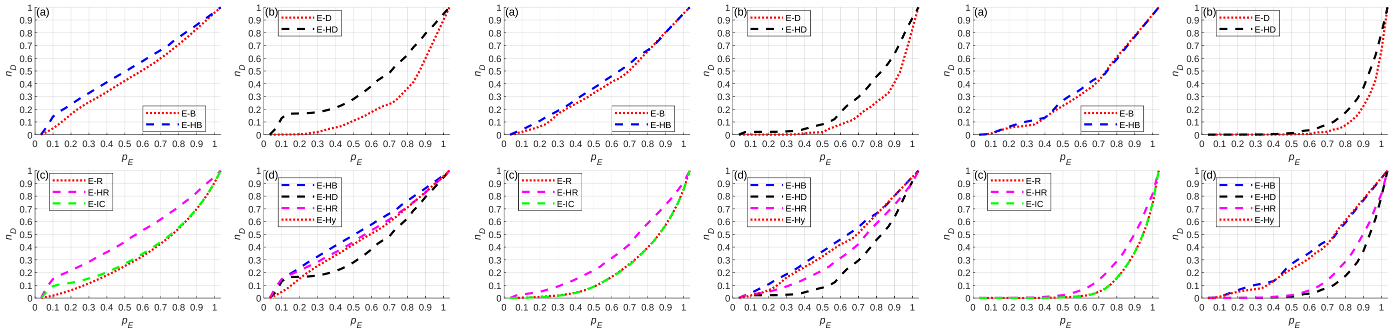
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S48: Edge-removal attacks on $N = 1500$ SF



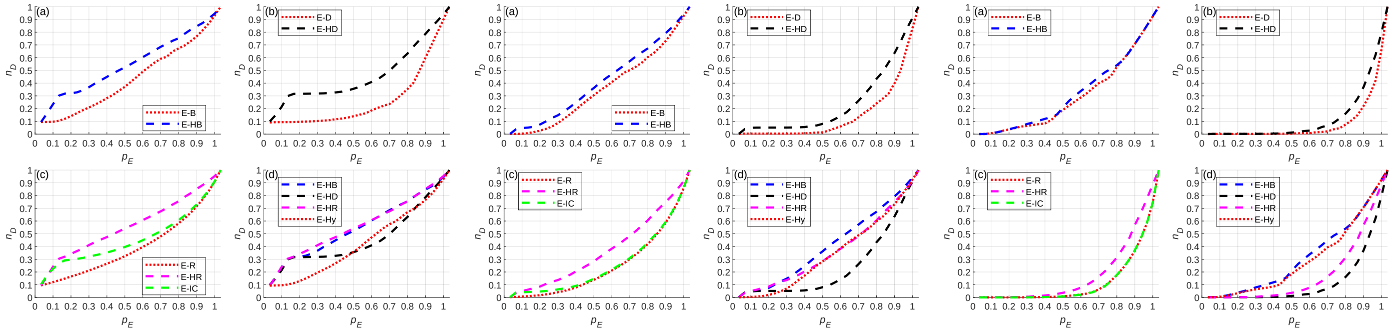
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S49: Edge-removal attacks on $N = 1500$ QS



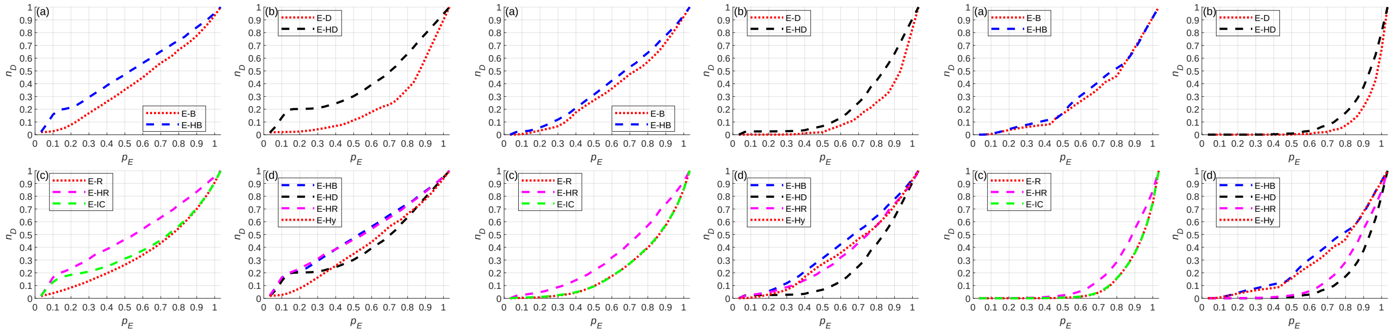
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S50: Edge-removal attacks on $N = 1500$ QR



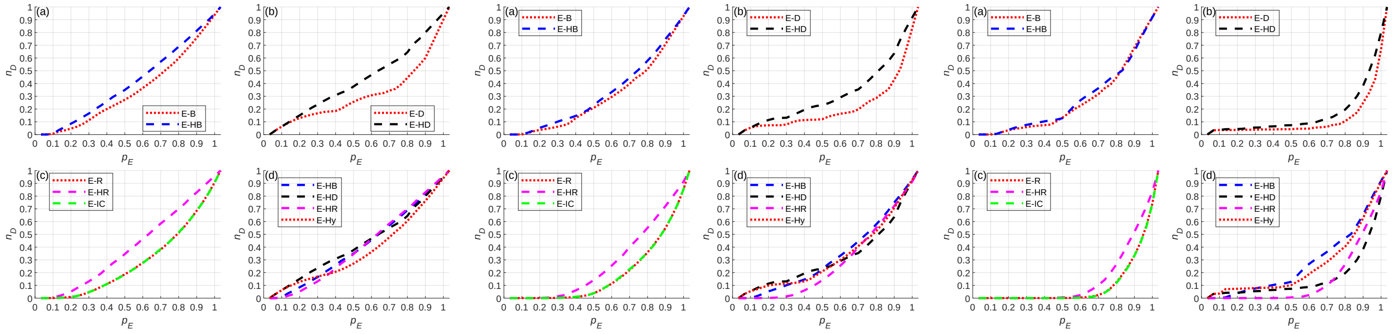
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S51: Edge-removal attacks on $N = 1500$ RT



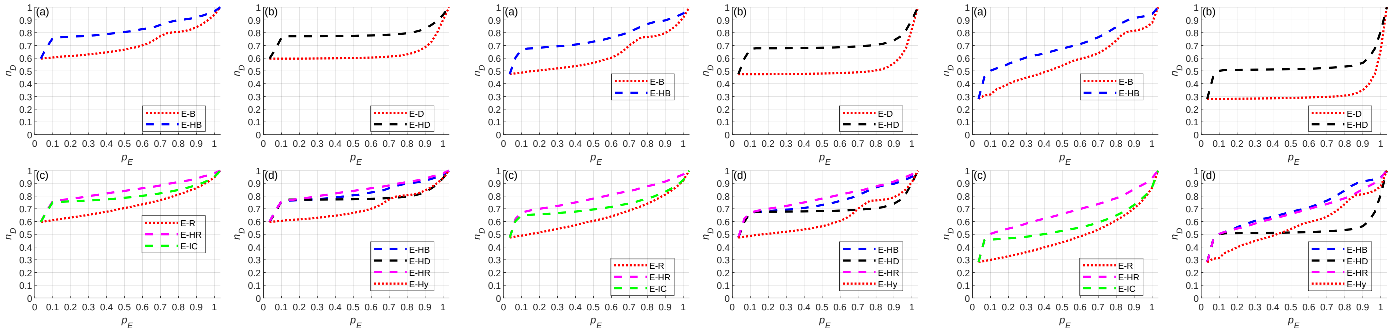
(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S52: Edge-removal attacks on $N = 1500$ RR



(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S53: Edge-removal attacks on $N = 1500$ HO



(a) $\langle k \rangle = 3$ (b) $\langle k \rangle = 5$ (c) $\langle k \rangle = 10$

Figure S54: Edge-removal attacks on $N = 1500$ OL

2 Generation Methods for Complex Networks

Nine typical directed synthetic network models are adopted for simulation, namely the Erdös–Rényi random graph (ER) [1], Newman–Watts small-world (SW) network [2], generic scale-free (SF) network [3–5], q-snapback network (QS) [6], q-snapback with redirected edges (QR) [7], random triangle (RT) network [8], and random rectangle (RR) network [8], extremely homogeneous (HO) network [9], and onion-like (OL) network [10]. The HO networks are empirically with the optimal controllability robustness [9].

The detailed generation methods and parameter settings of the nine synthetic networks are introduced as following.

2.1 ER: Erdös–Rényi Random Graph Networks

An ER network is generated as follows:

1. Start with N isolated nodes.
2. Pick up all possible pairs of nodes from the N given nodes, denoted by i and j ($i \neq j$, $i, j = 1, 2, ..., N$), once and once only. Connect each pair of nodes by a directed edge with probability $p_{RG} \in [0, 1]$, where the edge has the same probability directing from i to j, or j to i.

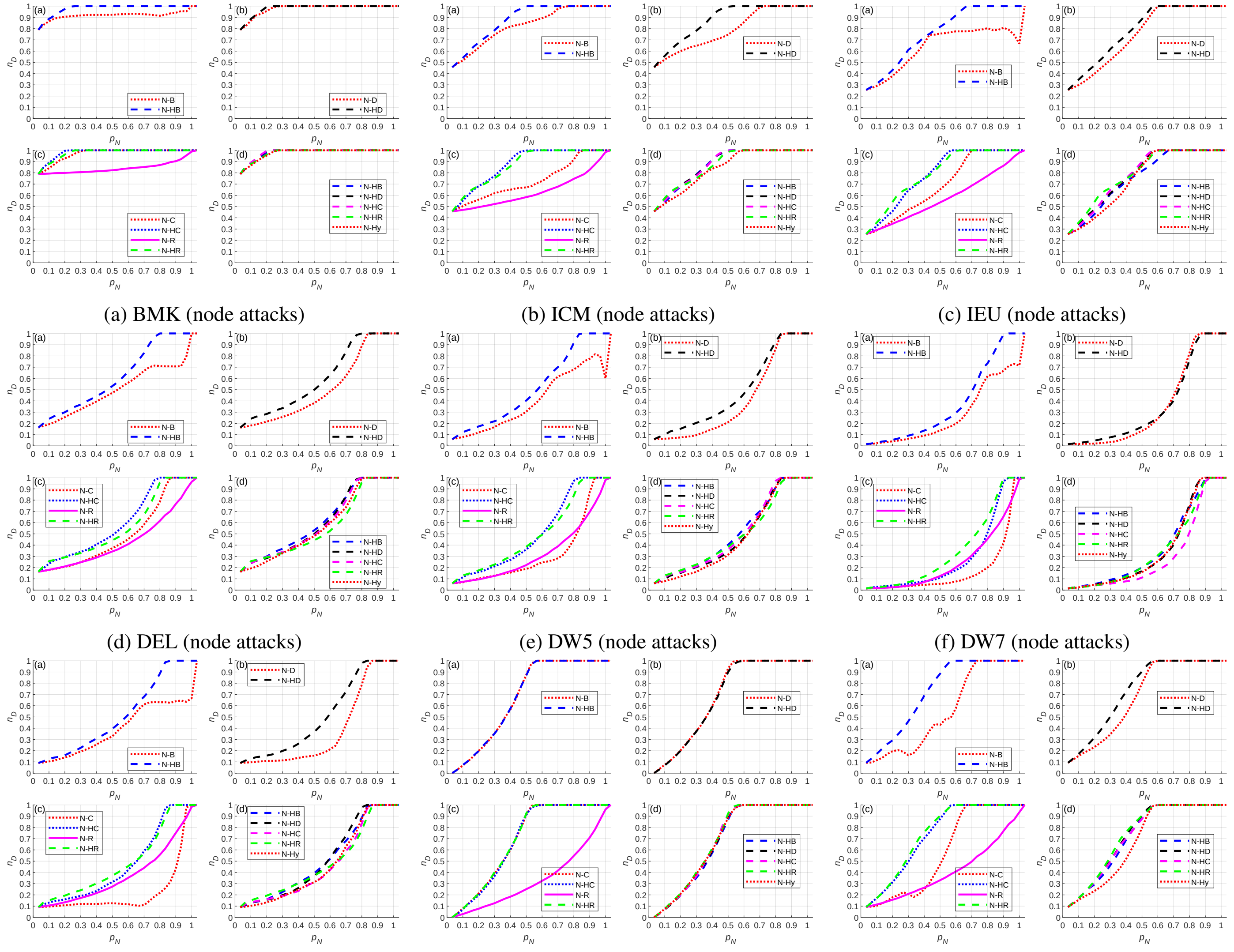
Given the numbers of N and M, let $p_{RG} = \frac{M}{N(N-1)}$. To exactly control the number of generated edges to be M, uniformly-randomly adding or removing edges can be performed. Here, when adding an edge, the direction can be random.

2.2 SW: Newman–Watts Small-world Networks

An SW network is generated as follows:

1. Start with a directed N-node loop having K connected nearest-neighbors on each side of each node.
2. Additional edges with random directions are added without removing any existing edges.

Set $K = 2$ in the following, namely, a node i is connected to its two nearest neighbors on each side, with nodes $i - 1$, $i + 1$, $i - 2$ and $i + 2$, via edges $A_{i-1,i}$, $A_{i,i+1}$, $A_{i-2,i}$ and $A_{i,i+2}$.



(a) BMK (node attacks)

(b) ICM (node attacks)

(c) IEU (node attacks)

(d) DEL (node attacks)

(e) DW5 (node attacks)

(f) DW7 (node attacks)

(g) LSH (node attacks)

(h) OLM (node attacks)

(i) RAJ (node attacks)

Figure S55: Node-removal attacks on real-world networks

2.3 SF: Scale-Free Networks

An SF network is generated as follows:

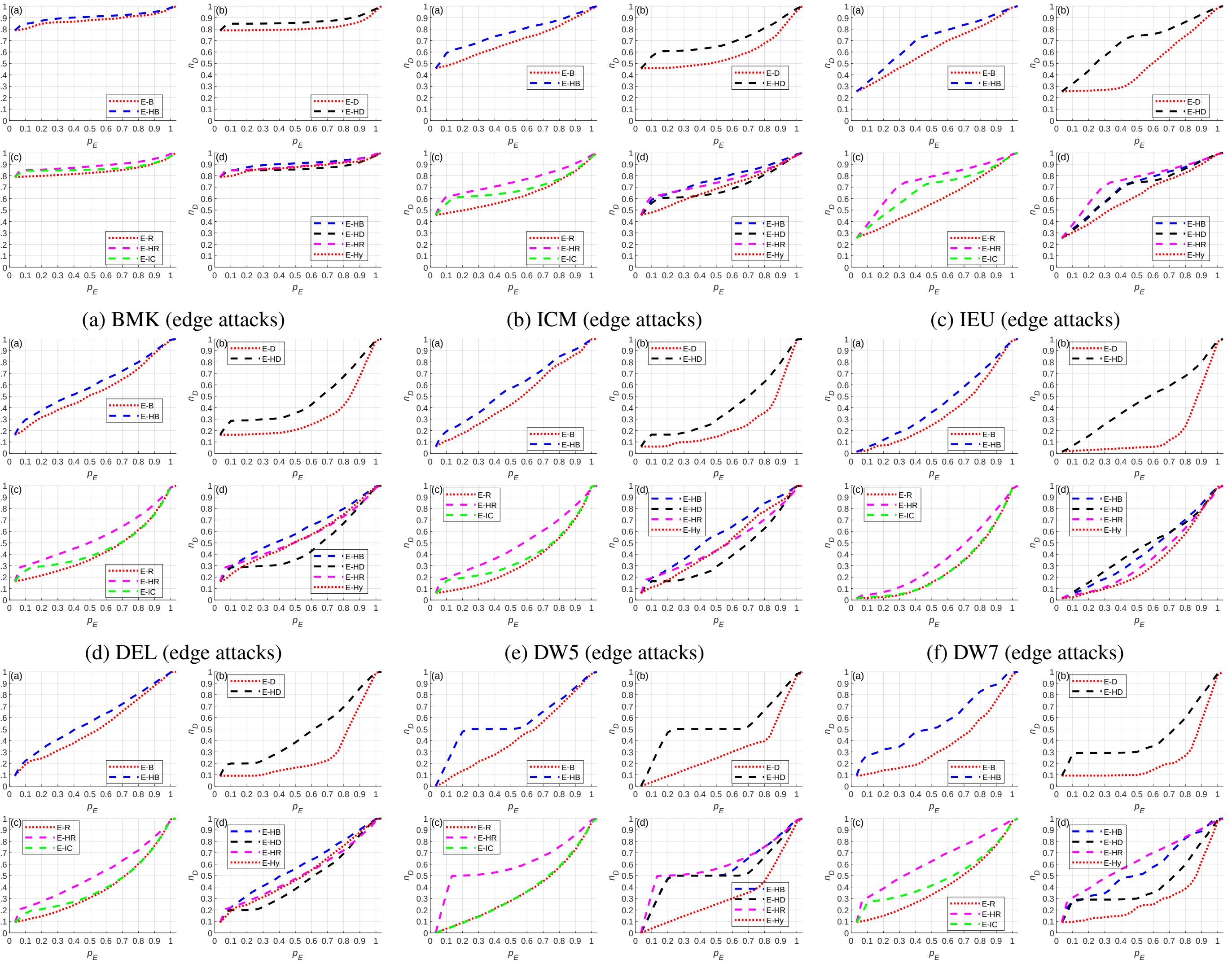
1. Start with N isolated nodes.
2. A weight $w_i = (i + \theta)^{-\sigma}$ is assigned to node i, with $\sigma \in [0, 1)$ and $\theta \ll N$.
3. Two nodes i and j ($i \neq j$, $i, j = 1, 2, ..., N$) are randomly picked from the pool with a probability proportional to the weights w_i and w_j, respectively. Then, an edge A_{ij} from i to j is added (if the two nodes are already connected, do nothing).
4. Repeat Step 3), until M edges have been added.

The resulting network has a power-law distribution $k^{-\gamma}$ with $\gamma = 1 + \frac{1}{\sigma}$, where k is the degree variable, which is independent of θ. Here, σ is set to 0.999, and thus $\gamma = 2.001$.

2.4 QS: *q*-Snapback Networks

Consider a q-snapback network (QS) with only one layer r_{QS} for simplicity. This QS is generated as follows:

1. Start with a directed chain of N nodes, where each node i ($i = 1, 2, ..., N - 1$) has an edge $A_{i,i+1}$.



(a) BMK (edge attacks)

(b) ICM (edge attacks)

(c) IEU (edge attacks)

(d) DEL (edge attacks)

(e) DW5 (edge attacks)

(f) DW7 (edge attacks)

(g) LSH (edge attacks)

(h) OLM (edge attacks)

(i) RAJ (edge attacks)

Figure S56: Edge-removal attacks on real-world networks

2. For each node $i = r_{QS} + 1, r_{QS} + 2, \ldots, N$, it connects backward to the previously-appeared nodes $i - l \times r_{QS}$ ($l = 1, 2, \ldots, \lfloor i/r_{QS} \rfloor$), with the same probability $q \in [0, 1]$.

In the following experimental study, r_{QS} is set to 2. Given $N = 1000$ and $M = 5000$, q is estimated to be 0.008 for fair comparisons. To exactly generate M edges, uniformly-randomly edge-adding with random direction should be applied.

2.5 QR: q-Snapback Networks with Redirected Edges

Consider a QR with only one layer r_{QR} for simplicity. This QR is generated as follows:

1. Start with a directed chain of N nodes, where each node i ($i = 1, 2, ..., N - 1$) has an edge $A_{i,i+1}$.

2. For each node $i = r_{QR} + 1, r_{QR} + 2, \ldots, N$, it connects backward to the previously-appeared nodes $i - l \times r_{QR}$ ($l = 1, 2, \ldots, \lfloor i/r_{QR} \rfloor$), with the same probability $q \in [0, 1]$. With a probability p_{re}, this snapback edge is redirected.

In the following experimental study, r_{QS} is set to 2. Given $N = 1000$ and $M = 5000$, q is estimated to be 0.008 for fair comparisons. To exactly generate M edges, uniformly-randomly edge-adding with random direction should be applied. In the experiments, p_{re} is set to 0.5.

2.6 RT: Random Triangle Networks

Triangular structure, which has been observed benefit to the robustness of controllability [6] and network stability [11,12], is frequently observed in real-life situations.

A directed random triangle network (RTN) is generated as follows:

1. Start with $N-3$ isolated nodes, with the other 3 nodes connected in a directed triangle.
2. Randomly pick up two nodes, i and j, without edge A_{ij} or A_{ji} (otherwise, do nothing). Then, randomly pick up a node k from all the neighbors of node j. If there is an edge A_{jk}, then add two edges A_{ij} and A_{ki}; otherwise (e.g., with an edge A_{kj}), add two edges A_{ji} and A_{ik}.
3. Repeat Step 2), until M edges have been added.

2.7 RR: Random Rectangle Networks

The above directed RTN is extended to a random rectangle network (RRT), as follows:

1. Start with $N-4$ isolated nodes, and the other 4 nodes are connected in a directed rectangle.
2. Randomly pick up three nodes, i, j and k, without edges between any pair of them (otherwise, do nothing). Then, randomly pick up a node w from the neighbors of node k. If there is an edge A_{kw}, then add edges A_{wi}, A_{ij}, and A_{jk}; otherwise (e.g., with an edge A_{wk}), add edges A_{ki}, A_{ij}, and A_{jw}.
3. Repeat Step 2), until M edges have been added.

2.8 HO: Extremely Homogeneous Networks

The in- and out-degree distributions of a directed HO network satisfy the following condition:

$$\lfloor M/N \rfloor \leq k_i^{in,out} \leq \lceil M/N \rceil\,, \quad i = 1, 2, \ldots, N, \tag{1}$$

where N is the number nodes; M is the number edges; $k_i^{in,out}$ means both in- and out-degrees, in which as a standard notation the floor function $\lfloor x \rfloor$ returns the greatest integer less than or equal to x, and the ceiling function $\lceil x \rceil$ returns the least integer greater than or equal to x.

An HO network is generated as follows:

1. Given an ER network.
2. Perform random edge rectification (RER) until both the in- and out-degree distributions satisfy Eq. (1).

The random edge rectification (RER) operator is performed as follows: For any node i, if its in- or out-degree does not satisfy Eq. (1), edge rectification is needed. There are four possible edge rectification operations:

1. If $k_i^{out} < \lfloor M/N \rfloor$, then find another node k with out-degree greater than $\lceil M/N \rceil$, and randomly pick one of its out-edges, $A_{k,l}$. Delete this edge $A_{k,l}$ and add an edge $A_{i,l}$. This increases k_i^{out} by one and decreases k_k^{out} by one.
2. If $k_i^{out} > \lceil M/N \rceil$, then randomly pick one of its out-edges $A_{i,j}$, and find another node k with out-degree less than $\lfloor M/N \rfloor$. Delete this edge $A_{i,j}$ and add an edge $A_{k,j}$. This decreases k_i^{out} by one and increases k_k^{out} by one.
3. If $k_i^{in} < \lfloor M/N \rfloor$, then find another node k with in-degree greater than $\lceil M/N \rceil$, and randomly pick one of its in-edges $A_{l,k}$. Delete this edge $A_{l,k}$ and add an edge $A_{l,i}$. This increases k_i^{in} by one and decreases k_k^{in} by one.
4. If $k_i^{in} > \lceil M/N \rceil$, then randomly pick one of its in-edges $A_{j,i}$, and find another node k with in-degree less than $\lfloor M/N \rfloor$. Delete this edge $A_{j,i}$ and add an edge $A_{j,k}$. This decreases k_i^{in} by one and increases k_k^{in} by one.

2.9 OL: Onion-like Networks

An OL network is generated as follow:

1. Given an SF network.
2. Perform random edge-swapping with degree reservation [10]. If the *connected robustness* measure improves after swapping, then keep it; otherwise, discard the swapping. Until the *connected robustness* measure stagnates.

The degree distribution of the resultant OL follows the same power-law distribution as the SF network.

3 Comparison of Overall Controllability

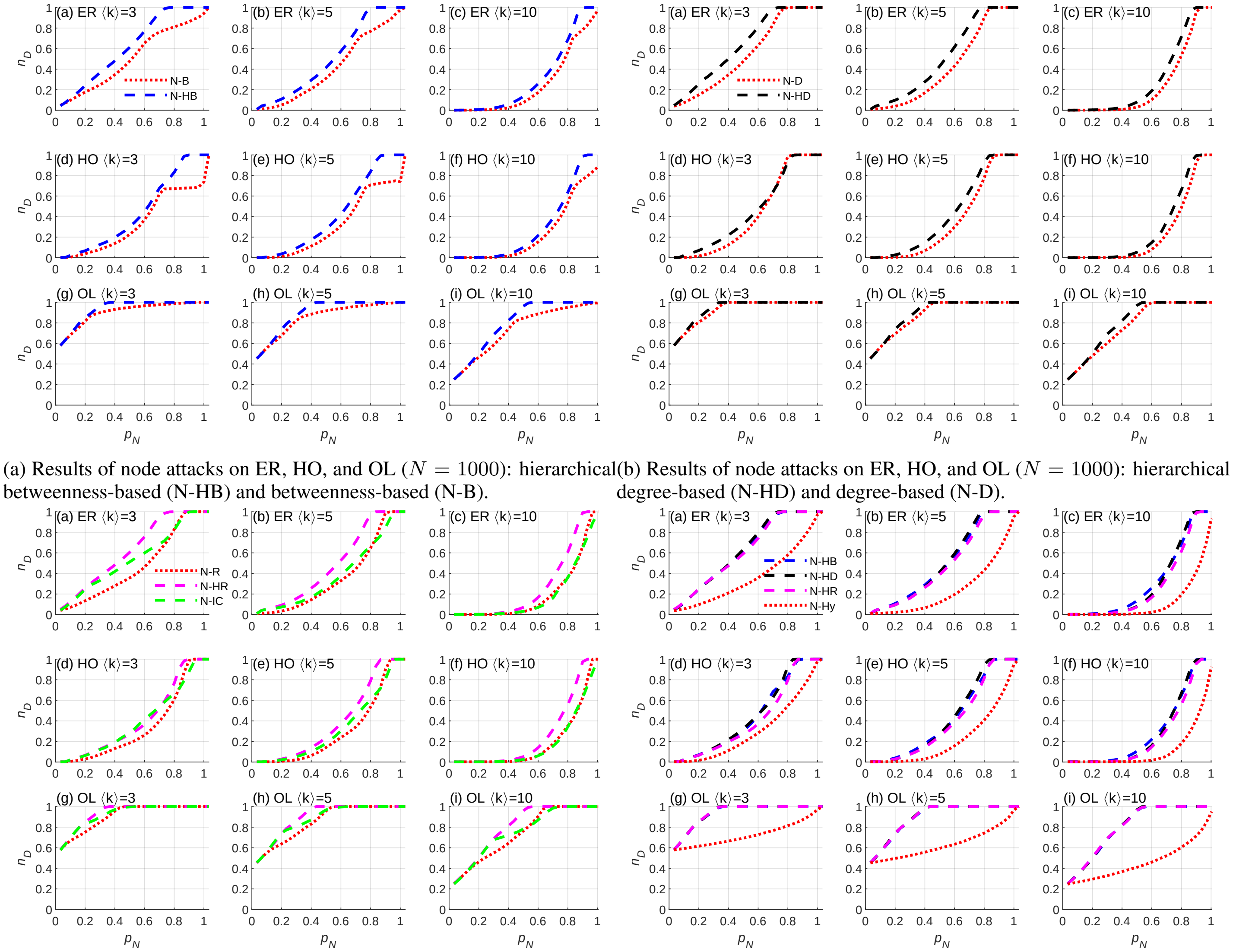
Table 1: Comparison of attack strategies on the nine synthetic networks ($N = 500$), where B represents betweenness; D represents degree; C represents closeness; R represents random; Hy represents hybrid; IC represents initial critical edges; HB represents hierarchical betweenness; HD represents hierarchical degree; HC represents hierarchical closeness; HR represents hierarchical random.

N=500		Node Attack						Edge Attack					
		HB/B	HD/D	HC/C	HR/R	HB/Hy	HD/Hy	HB/B	HD/D	HR/R	HB/Hy	HD/Hy	HR/IC
$\langle k \rangle$=3	ER	1.184	1.138	1.241	1.490	1.090	1.092	1.120	1.584	1.377	1.125	0.892	1.255
	SW	1.251	1.093	1.196	1.291	1.035	1.060	1.157	1.350	1.435	1.264	0.977	1.440
	SF	1.036	1.011	1.030	1.309	1.005	1.007	1.165	1.257	1.177	1.191	1.111	1.075
	QS	1.268	1.200	1.504	1.408	1.103	1.181	1.120	2.252	1.462	1.118	0.878	1.300
	QR	1.289	1.172	1.291	1.470	1.108	1.135	1.114	1.699	1.443	1.112	0.867	1.398
	RT	1.155	1.105	1.134	1.632	1.056	1.061	1.254	1.704	1.401	1.286	1.078	1.228
	RR	1.223	1.120	1.228	1.564	1.081	1.089	1.216	1.688	1.441	1.222	1.005	1.297
	HO	1.240	1.192	1.410	1.427	1.141	1.145	1.146	1.351	1.375	1.092	1.134	1.374
	OL	1.039	1.016	1.027	1.306	1.008	1.011	1.162	1.264	1.171	1.189	1.114	1.066
$\langle k \rangle$=5	ER	1.196	1.209	1.315	1.518	1.135	1.120	1.064	1.432	1.324	1.066	0.651	1.265
	SW	1.257	1.179	1.311	1.429	1.104	1.126	1.068	1.389	1.294	1.138	0.737	1.320
	SF	1.052	1.026	1.051	1.429	1.011	1.013	1.200	1.372	1.221	1.221	1.098	1.089
	QS	1.226	1.253	1.657	1.390	1.175	1.182	1.072	2.067	1.423	1.064	0.714	1.399
	QR	1.265	1.185	1.338	1.507	1.136	1.140	1.060	1.413	1.320	1.067	0.659	1.339
	RT	1.176	1.169	1.191	1.623	1.096	1.102	1.129	1.519	1.332	1.154	0.750	1.318
	RR	1.239	1.165	1.301	1.576	1.119	1.124	1.110	1.435	1.327	1.108	0.739	1.315
	HO	1.213	1.188	1.366	1.427	1.174	1.149	1.070	1.408	1.239	1.037	0.986	1.241
	OL	1.052	1.025	1.048	1.420	1.013	1.014	1.211	1.385	1.226	1.228	1.101	1.092
$\langle k \rangle$=10	ER	1.204	1.203	1.373	1.441	1.180	1.128	1.058	1.416	1.221	1.047	0.473	1.233
	SW	1.209	1.208	1.309	1.414	1.146	1.113	1.025	1.350	1.143	1.123	0.501	1.084
	SF	1.074	1.057	1.092	1.722	1.025	1.039	1.213	1.784	1.387	1.234	0.884	1.221
	QS	1.169	1.311	1.982	1.286	1.174	1.151	1.014	1.805	1.356	1.260	0.589	1.389
	QR	1.240	1.199	1.320	1.376	1.161	1.109	1.030	1.338	1.158	1.100	0.500	1.192
	RT	1.183	1.193	1.302	1.486	1.125	1.112	1.033	1.321	1.306	1.047	0.514	1.290
	RR	1.192	1.188	1.293	1.450	1.118	1.136	1.062	1.305	1.137	1.107	0.538	1.191
	HO	1.212	1.208	1.375	1.337	1.190	1.148	1.067	1.367	1.122	1.192	0.753	1.140
	OL	1.075	1.038	1.085	1.711	1.023	1.029	1.209	1.688	1.382	1.211	0.870	1.182

Table 2: Comparison of attack strategies on the nine synthetic networks ($N = 500$), where B represents betweenness; D represents degree; C represents closeness; R represents random; Hy represents hybrid; IC represents initial critical edges; HB represents hierarchical betweenness; HD represents hierarchical degree; HC represents hierarchical closeness; HR represents hierarchical random.

N=1500		Node Attack						Edge Attack					
		HB/B	HD/D	HC/C	HR/R	HB/Hy	HD/Hy	HB/B	HD/D	HR/R	HB/Hy	HD/Hy	HR/IC
$\langle k \rangle$=3	ER	1.286	1.177	1.322	1.534	1.134	1.144	1.139	1.587	1.448	1.135	0.863	1.352
	SW	1.290	1.082	1.221	1.334	1.065	1.086	1.163	1.327	1.423	1.215	0.925	1.433
	SF	1.033	1.010	1.029	1.258	1.006	1.006	1.157	1.235	1.161	1.160	1.101	1.058
	QS	1.314	1.213	1.880	1.387	1.082	1.199	1.131	2.237	1.463	1.123	0.879	1.241
	QR	1.323	1.171	1.361	1.484	1.130	1.158	1.125	1.694	1.440	1.128	0.873	1.347
	RT	1.161	1.102	1.178	1.638	1.061	1.075	1.258	1.694	1.399	1.285	1.080	1.213
	RR	1.250	1.123	1.261	1.579	1.085	1.094	1.230	1.706	1.426	1.236	1.023	1.273
	HO	1.283	1.184	1.478	1.471	1.155	1.172	1.152	1.335	1.374	1.092	1.142	1.374
	OL	1.034	1.011	1.030	1.260	1.005	1.006	1.150	1.232	1.154	1.150	1.098	1.055
$\langle k \rangle$=5	ER	1.228	1.206	1.349	1.586	1.151	1.158	1.049	1.550	1.436	1.055	0.649	1.374
	SW	1.309	1.201	1.347	1.491	1.150	1.175	1.077	1.421	1.422	1.138	0.692	1.428
	SF	1.045	1.021	1.046	1.354	1.009	1.012	1.203	1.359	1.220	1.200	1.103	1.098
	QS	1.260	1.283	2.433	1.394	1.176	1.230	1.071	2.269	1.517	1.073	0.705	1.505
	QR	1.273	1.199	1.367	1.553	1.159	1.162	1.065	1.513	1.439	1.063	0.645	1.450
	RT	1.206	1.154	1.234	1.723	1.104	1.117	1.144	1.566	1.453	1.179	0.726	1.381
	RR	1.243	1.144	1.298	1.621	1.117	1.132	1.118	1.450	1.442	1.125	0.711	1.432
	HO	1.240	1.189	1.450	1.537	1.167	1.159	1.086	1.452	1.408	1.026	0.986	1.404
	OL	1.045	1.019	1.047	1.359	1.009	1.011	1.204	1.340	1.218	1.207	1.107	1.087
$\langle k \rangle$=10	ER	1.234	1.219	1.380	1.547	1.166	1.129	1.040	1.446	1.456	1.037	0.416	1.466
	SW	1.268	1.226	1.416	1.562	1.164	1.134	1.037	1.411	1.382	1.049	0.421	1.387
	SF	1.065	1.036	1.081	1.556	1.020	1.025	1.214	1.617	1.352	1.219	0.945	1.180
	QS	1.202	1.339	4.723	1.344	1.229	1.218	1.027	2.060	1.552	1.104	0.484	1.557
	QR	1.254	1.221	1.418	1.600	1.177	1.150	1.038	1.438	1.405	1.036	0.422	1.397
	RT	1.239	1.196	1.312	1.624	1.152	1.140	1.058	1.414	1.497	1.066	0.461	1.501
	RR	1.241	1.182	1.349	1.636	1.134	1.139	1.064	1.441	1.380	1.071	0.492	1.373
	HO	1.218	1.192	1.418	1.539	1.159	1.121	1.046	1.384	1.384	1.080	0.671	1.400
	OL	1.069	1.037	1.083	1.565	1.022	1.026	1.210	1.610	1.366	1.210	0.934	1.179

4 Other Supplementary Materials



(a) Results of node attacks on ER, HO, and OL ($N = 1000$): hierarchical betweenness-based (N-HB) and betweenness-based (N-B).

(b) Results of node attacks on ER, HO, and OL ($N = 1000$): hierarchical degree-based (N-HD) and degree-based (N-D).

(c) Results of node attacks on ER, HO, and OL ($N = 1000$): random (N-R), hierarchical random (N-HR) and initial critical (N-IC).

(d) Results of node attacks on ER, HO, and OL ($N = 1000$): three hierarchical attacks (N-HB, N-HD and N-HR) and hybrid (N-Hy).

Figure S57: Node-removal attacks on ER, HO, and OL ($N = 1000$).

References

[1] P. Erdös and A. Rényi, "On the strength of connectedness of a random graph," *Acta Mathematica Hungarica*, vol. 12, no. 1-2, pp. 261–267, 1964.

[2] M. E. Newman and D. J. Watts, "Renormalization group analysis of the small-world network model," *Physics Letters A*, vol. 263, no. 4-6, pp. 341–346, 1999.

[3] C.-L. Pu, W.-J. Pei, and A. Michaelson, "Robustness analysis of network controllability," *Physica A: Statistical Mechanics and its Applications*, vol. 391, no. 18, pp. 4420–4425, 2012.

[4] K.-I. Goh, B. Kahng, and D. Kim, "Universal behavior of load distribution in scale-free networks," *Physical Review Letters*, vol. 87, no. 27, p. 278701, 2001.

[5] F. Sorrentino, "Effects of the network structural properties on its controllability," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 17, no. 3, p. 033101, 2007.

[6] Y. Lou, L. Wang, and G. Chen, "Toward stronger robustness of network controllability: A snapback network model," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 9, pp. 2983–2991, 2018.

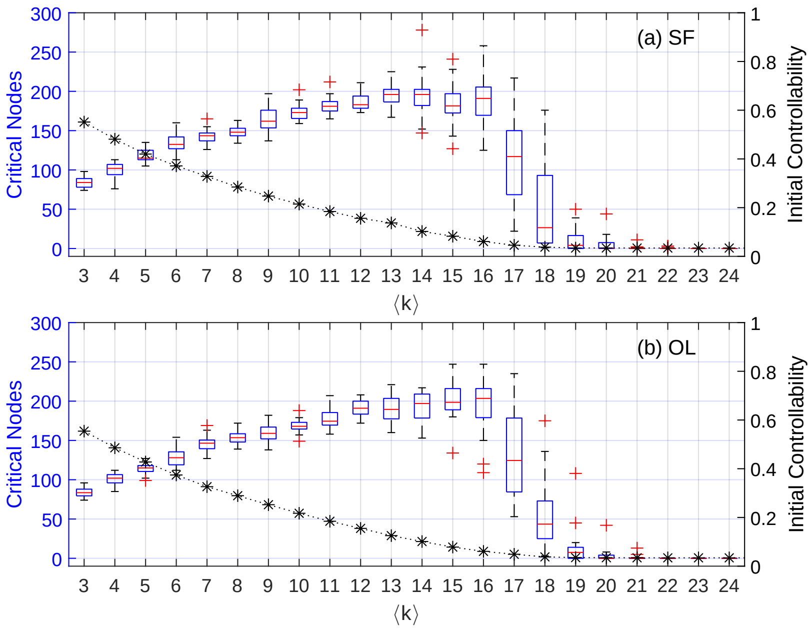


Figure S58: Number of critical nodes (boxplots) and initial controllability (stars *) against the average degree of (a) SF and (b) OL networks.

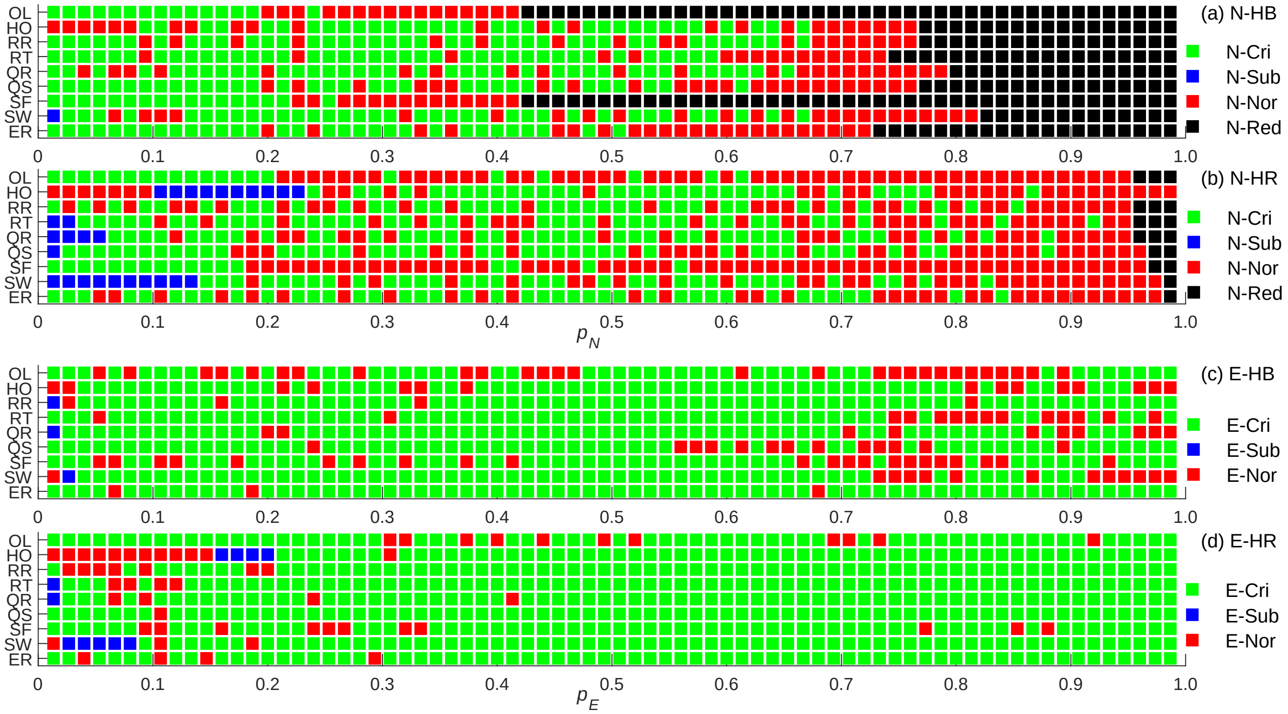


Figure S59: [color online] Types of the removed (a) nodes under N-HB attacks; (b) nodes under N-HR attacks; (c) edges under E-HB attacks; and (d) edges under E-HR attacks. The network configuration is $N = 1000$ and $\langle k \rangle = 5$.

[7] ——, “Enhancing controllability robustness of q-snapback networks through redirecting edges,” *Research*, vol. 2019, no. 7857534, 2019.

[8] G. Chen, Y. Lou, and L. Wang, “A comparative study on controllability robustness of complex networks,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 5, pp. 828–832, 2019.

[9] Y. Lou, L. Wang, K.-F. Tsang, and G. Chen, “Towards optimal robustness of network controllability: An empirical necessary condition,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2020, doi:10.1109/TCSI.2020.2986215.

[10] H. J. Herrmann, C. M. Schneider, A. A. Moreira, J. S. Andrade Jr, and S. Havlin, “Onion-like network topology enhances robustness against malicious attacks,” *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2011, no. 01, p. P01027, 2011.

[11] P. Schultz, J. Heitzig, and J. Kurths, “Detours around basin stability in power networks,” *New Journal of Physics*, vol. 16, no. 12, p. 125001, 2014.

[12] J. Nitzbon, P. Schultz, J. Heitzig, J. Kurths, and F. Hellmann, “Deciphering the imprint of topology on nonlinear dynamical network stability,” *New Journal of Physics*, vol. 19, no. 3, p. 033029, 2017.