Mitigation of malicious attacks on networks

Christian M. Schneider[a,1], **André A. Moreira**[b], **José S. Andrade, Jr.**[a,b], **Shlomo Havlin**[c], **and Hans J. Herrmann**[a,b]

[a]Computational Physics for Engineering Materials, IfB, ETH Zurich, Schafmattstrasse 6, 8093 Zurich, Switzerland; [b]Departamento de Física, Universidade Federal do Ceará, Campus do Pici, 60451-970 Fortaleza, Ceará, Brazil; and [c]Minerva Center and Department of Physics, Bar-Ilan University, 52900 Ramat-Gan, Israel

Edited* by H. Eugene Stanley, Boston University, Boston, MA, and approved January 3, 2011 (received for review July 2, 2010)

Terrorist attacks on transportation networks have traumatized modern societies. With a single blast, it has become possible to paralyze airline traffic, electric power supply, ground transportation or Internet communication. How and at which cost can one restructure the network such that it will become more robust against a malicious attack? We introduce a new measure for robustness and use it to devise a method to mitigate economically and efficiently this risk. We demonstrate its efficiency on the European electricity system and on the Internet as well as on complex networks models. We show that with small changes in the network structure (low cost) the robustness of diverse networks can be improved dramatically whereas their functionality remains unchanged. Our results are useful not only for improving significantly with low cost the robustness of existing infrastructures but also for designing economically robust network systems.

percolation | power grid

The vulnerability of modern infrastructures stems from their network structure having very high degree of interconnectedness that makes the system resilient against random attacks but extremely vulnerable to targeted raids (1–17). We developed an efficient mitigation method and discovered that with relatively minor modifications in the topology of a given network and without increasing the overall length of connections, it is possible to mitigate considerably the danger of malicious attacks. Our efficient mitigation method against malicious attacks is based on developing and introducing a unique measure for robustness. We show that the common measure for robustness of networks in terms of the critical fraction of attacks at which the system completely collapses, the percolation threshold, may not be useful in many realistic cases. This measure, for example, ignores situations in which the network suffers a significant damage, but still keeps its integrity. Besides the percolation threshold, there are other robustness measures based, for example, on the shortest path (18–20) or on the graph spectrum (21). They are, however, less frequently used for being too complex or less intuitive. In contrast, our unique robustness measure, which considers the size of the largest component during all possible malicious attacks, is as simple as possible and only as complex as necessary. Due to the ample range of our definition of robustness, we can assure that our process of reconstructing networks maintains the infrastructure as operative as possible, even before collapsing.

Model

Modeling Attack on Infrastructures. We begin by demonstrating the efficiency of our unique approach to improve the performance of two of the most fragile, but critical infrastructures, namely, the power supply system in Europe (22) as well as the global Internet at the level of service providers, the so-called point of presence (PoP) (23). The breakdown of any of these networks would constitute a major disaster due to the strong dependency of modern society on electrical power and Internet. In Fig. 1 *A* and *B* we show the backbone of the European Union (EU) power grid and the location of the European PoP and their respective vulnerability in Fig. 1 *C* and *D*. The dotted lines in Fig. 1 *C* and *D* represent the size of the largest connected component of the networks after a fraction q of the most connected nodes have been removed. Instead of using the static approach to find the q most connected nodes at the beginning of the attack, we use a dynamical approach. In this case the degrees are recalculated during the attack, which corresponds to a more harmful strategy (24). As a consequence, in their current structure, the shutdown of only 10% of the power stations and a cut of 12% of PoP would affect 90% of the network integrity. To avoid such a dramatic breakdown and reduce the fragility of these networks, here we propose a strategy to exchange only a small number of power lines or cables without increasing the total length of the links and the number of links of each node. These small local changes not only mitigate the efficiency of malicious attacks, but at the same time preserve the functionality of the system. In Fig. 1 *C* and *D* the robustness of the original networks are given by the areas under the dashed curves, whereas the areas under the solid lines correspond to the robustness of the improved networks. Therefore, the green areas in Fig. 1 *C* and *D* demonstrate the significant improvement of the resilience of the network for any fraction q of attack. This means that terrorists would cause less damage or they would have to attack more power stations, and hackers would have to attack more PoP to significantly damage the system.

Introducing the Unique Robustness Measure. Next, we describe in detail our methodology. Usually robustness is measured by the value of q_c, the critical fraction of attacks at which the network completely collapses (24). This measure ignores situations in which the network suffers a big damage without completely collapsing. We thus propose here a measure that considers the size of the largest component during all possible malicious attacks. Malicious raids often consist of a certain fraction q of hits and we want to assure that our process of reconstructing networks will keep the infrastructure as operative as possible, even before collapsing. Our unique robustness measure R, is thus defined as

$$R = \frac{1}{N}\sum_{Q=1}^{N} s(Q), \qquad [1]$$

where N is the number of nodes in the network and $s(Q)$ is the fraction of nodes in the largest connected cluster after removing $Q = qN$ nodes. The normalization factor $1/N$ ensures that the robustness of networks with different sizes can be compared. The range of possible R values is between $1/N$ and 0.5, where these limits correspond, respectively, to a star network and a fully connected graph.

Constraints for Improving Networks. For a given network, the robustness could be enhanced in many ways. Adding links without any restrictions until the network is fully connected would be an

---

Author contributions: C.M.S., A.A.M., J.S.A., S.H., and H.J.H. designed research, performed research, contributed new reagents/analytic tools, analyzed data, and wrote the paper.

The authors declare no conflict of interest.

*This Direct Submission article had a prearranged editor.

[1] To whom correspondence should be addressed. E-mail: schnechr@ethz.ch.

This article contains supporting information online at www.pnas.org/lookup/suppl/doi:10.1073/pnas.1009440108/-/DCSupplemental.

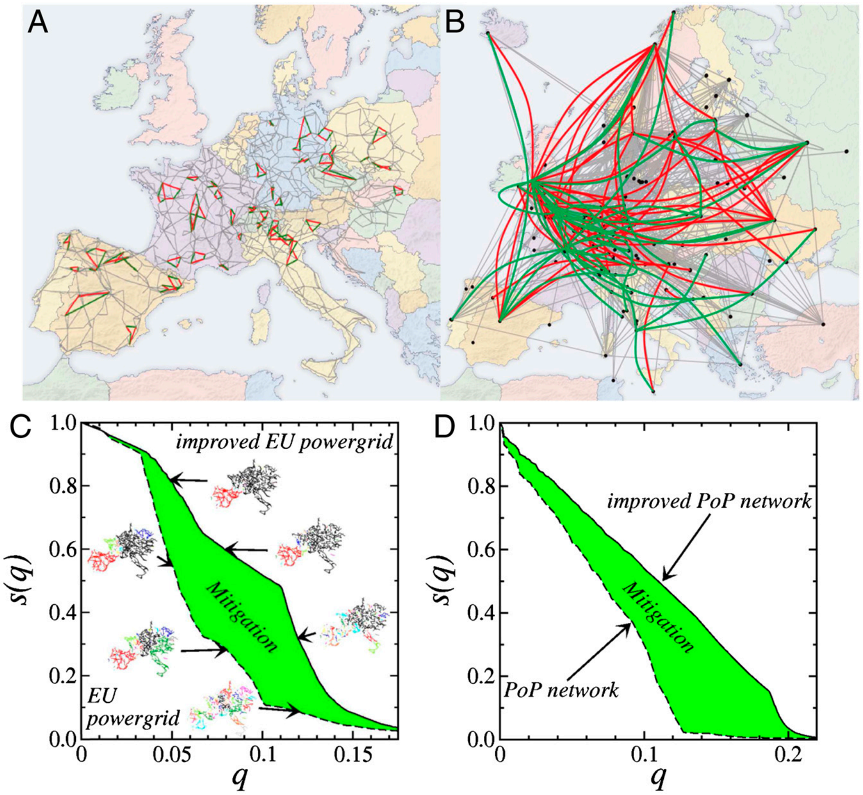

Fig. 1. Mitigation of malicious attacks on the power supply system in Europe and the global Internet at the level of service providers. In (*A*) we show the EU power grid with $N = 1{,}254$ generators and $M = 1{,}811$ power lines (22) and in (*B*) the Internet with $N = 1{,}098$ service providers and $M = 6{,}089$ connection among them, where only the European part is shown (29). The red edges correspond to the 5% connections that we suggest to replace by the green ones. A detailed description of the chosen edges is given in *SI Text*. The network fragmentation under a malicious attack is shown for (*C*) EU power generators and for (*D*) PoP. The dashed lines in (*C*) and (*D*) corresponds to the size of the largest component in each original system and the solid lines to typical redesigned networks after changing 5% of the connections. The green areas give the mitigation of malicious attack, which correspond to improving robustness by 45% for the EU power grid and 55% for the PoP.

obvious one. However, for practical purposes, this option can be useless because, for example, the installation of power lines between each pair of power plants would skyrocket costs and transmission losses. By associating costs to each link of the network, we must seek for a reconstruction solution that minimizes the total cost of the changes. We also assume that changing the degree of a node can be particularly more expensive than changing edges. These two assumptions suggest keeping invariant the number of links and the degree of each node. Under these constraints, we propose the following algorithm to mitigate malicious attacks. In the original network we swap the connections of two randomly chosen edges, that is, the edges e_{ij} and e_{kl}, which connect node i with node j, and node k with node l, respectively, become e_{ik} and e_{jl} (25), only if the robustness of the network is increased; i.e., $R_{\mathrm{new}} > R_{\mathrm{old}}$. Note that a change of the network usually leads to an adjustment in the attack sequence. We then repeat this procedure with another randomly chosen pair of edges until no further substantial improvement is achieved for a given large number of consecutive swapping trials. In Fig. S1, we show numerical tests indicating that the algorithm can indeed yield close to optimal robustness. As described so far, our algorithm can be used to improve a network against malicious attacks while conserving the number of links per node. Nevertheless, for real networks with economical constraints, this conservation of degree is not enough because the cost, like the total length of links, can not be exceedingly large and also the number of changes should remain small. Therefore, for reconstructing the EU power grid and the worldwide PoP, we use an additional condition that the swap of two links is only accepted if the total length (geographically calculated) of edges does not increase and the robustness is increased by more than a certain value.

Results

Improving Existing Infrastructures. Fig. 2*A* shows that, despite these strong constraints, the robustness R can be increased by 55% for PoP and 45% for the EU grid with only 5.5% of link changes

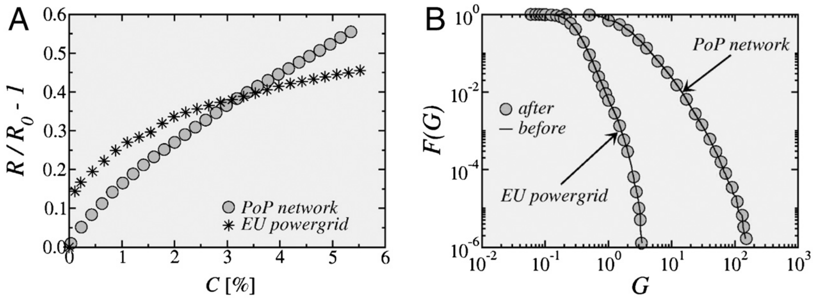

Fig. 2. Demonstration that small changes have a large impact on the robustness whereas the functionality of the networks remains. (*A*) Improvement of robustness R as a function of the fraction of changed links for both networks, where R_0 is the original robustness. In the case of the EU power grid, we find that changing only two connections increases the robustness by 15%. When changing 2% of the links, the robustness of the EU power grid improves by 35% and the Internet by 25%. (*B*) The cumulative conductance distribution $F(G)$ versus the conductance G for both networks before and after the changes. Conductances between two nodes are measured for all pairs of nodes, assuming that each link in the network has unitary conductance. Both curves are nearly identical, which means that the transport properties; i.e., the functionalities of the improved networks are very close to the original ones.

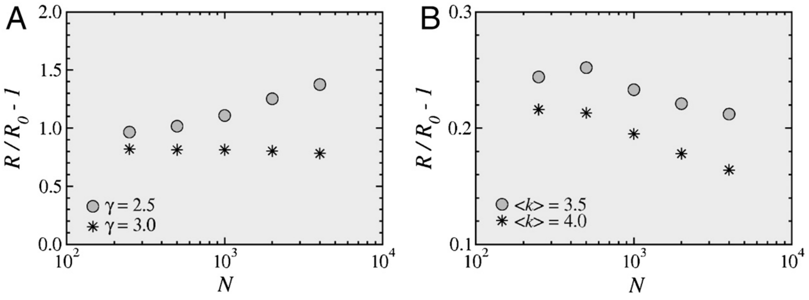

Fig. 3. Validation that one can design robust networks regardless of the degree distribution and the system size. The relative robustness improvement $R/R_0 - 1$ vs network size N for (*A*) scale-free networks with degree exponent $\gamma = 2.5$ and 3 and (*B*) Erdős-Rényi networks with $\langle k \rangle = 3.5$ and 4. Starting from a given network, we swap two randomly chosen connections, that is, e_{ij}, which connects node i with node j, and e_{kl} become e_{ik} and e_{jl}, only if the robustness of the network is increased. This procedure is repeated until during the last 10,000 attempts no further improvement could be achieved. Note that the swapping keeps the degree of each node unchanged. Results are averaged over at least five independent initial networks. We do not show error bars, because they are smaller than the symbol sizes.

and by 34% and 27%, respectively, with only 2%. Interestingly, although the robustness is clearly improved, we observe that the percolation threshold q_c remains practically the same for both networks, justifying our unique definition for the measure R as a robustness criterion. More strikingly, the conductance distribution (26), which is a useful measure for the functionality of the network, also does not change (see Fig. 2*B*). This suggests that our optimized network is not only more robust against malicious attacks, but also does not increase the total length of connections without any loss of functionality.

Designing Robust Networks. The success of this method in reconstructing real networks to improve robustness at low cost and small effort leads us to the following question: Can we apply our algorithm to design new highly robust networks against malicious attacks? In this case, because we build the network from the beginning, the number of changes should not represent any limitation, because we are dealing with only a computational problem. For designing, the only constraint that remains is the invariance of the degree distribution. Here we study both artificial scale-free (27) and Erdős–Rényi networks (28). In Fig. 3 we show how the robustness depends on the system size for designed scale-free networks with degree distribution $P(k) \sim k^{-\gamma}$, with $\gamma = 2.5$ and 3, and Erdős–Rényi networks with average degree $\langle k \rangle = 3.5$ and 4. One can see that our method is also very efficient in designing robust networks.

Whereas the most robust network structure for a given degree distribution is virtually impossible to determine, our study reveals that all networks investigated can be improved significantly (see Figs. S2 and S3). Moreover, as shown in Fig. 4*A*, the robust networks we obtain clearly share a common and unique "onion-like" structure consisting of a core of highly connected nodes hierarchically surrounded by rings of nodes with decreasing degree. To quantitatively test our observation, we calculate the maximal number of nodes S_k with degree k that are connected through nodes with a degree smaller or equal to k. As shown in Fig. 4*B*, paths between nodes of equal degree, which are not passing through nodes with higher degree, emerge in the robust networks. Although at a first glance onion-like networks might look similar to high assortative networks, the later ones are different and can be significantly more fragile (see Fig. S3). We also find that onion-like networks are also robust against other kinds of targeted attacks such on high betweenness nodes (24) (see Fig. S4). The last topological properties we study are the average shortest path length between two nodes, l, and the diameter, d, corresponding to the maximal distance between any pair of nodes (7). Counter intuitively, l and d do not decrease after the optimization, but slightly increase. Nevertheless, it seems that both values grow not faster than logarithmically with the system size N (see Fig. S5).

Discussion

In summary, we have introduced a unique measure for robustness of networks and used this measure to develop a method that significantly improves, with low cost, their robustness against malicious attacks. Our approach has been found to be successfully useful as demonstrated on two real network systems, the European power grid of stations and the Internet. Our results show that with a reasonably economical effort, significant gains can be

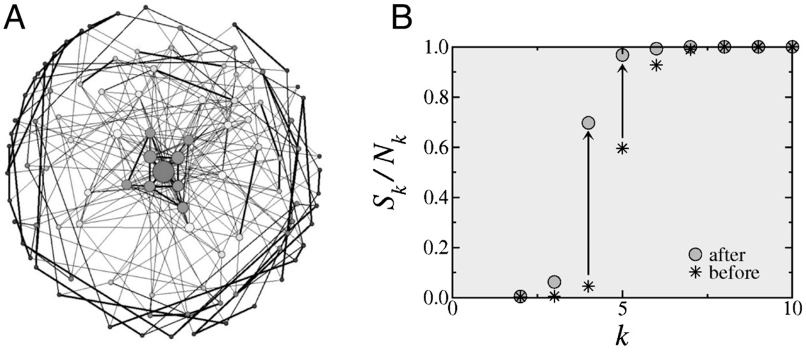

Fig. 4. Visualization of the novel onion-like topology of robust networks. (*A*) The onion-like topology of a robust scale-free network with $N = 100$ nodes, $M = 300$ edges and a degree distribution $P(k) \sim k^{-2.5}$. The sizes of the nodes are proportional to their degree, and nodes with similar degree have the same color. Edges between nodes with equal degree and the fully connected core are highlighted. In onion-like networks nearly each pair of nodes with equal degree k is connected by a path that does not contain nodes of higher degree. (*B*) Fraction of nodes with degree k that are connected through nodes with a degree smaller or equal to k for scale-free networks with $\gamma = 2.5$ and $N = 4{,}000$.

achieved for their robustness while conserving the nodes degrees and the total length of power lines or cables. In the case of designing scale-free networks, a unique onion-like topology characterizing robust networks is revealed. This insight enables to design robust networks with a prescribed degree distribution. The applications of our results are imminent on one hand to guide the improvement of existing networks but also serve on the other hand to design future infrastructures with improved robustness.

ACKNOWLEDGMENTS. We thank T. Mihaljev for useful discussions, and Y. Shavitt and N. Zilberman for providing the point of presence Internet data. We acknowledge financial support from the ETH Competence Center "Coping with Crises in Complex Socio-Economic Systems" (CCSS) through ETH Research Grant CH1-01-08-2. S.H. acknowledges support from the Israel Science Foundation, the Office of Naval Research, the Defence Threat Reduction Agency, and the Epiwork EU project. A.A.M. and J.S.A thank the Brazilian agencies Conselho Nacional de Desenvolvimento Científico e Tecnológico, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, Fundação Cearense de Apoio ao Desenvolvimento Científico, and Financiadora de Estudos e Projetos for financial support.

1. Barabási A-L, Albert R (1999) Emergence of scaling in random networks. *Science* 286:509–512.
2. Watts DJ (1999) *Small Worlds: The Dynamics of Networks Between Order and Randomness* (Princeton Univ Press, Princeton).
3. Albert R, Jeong H, Barabási A-L (2000) Error and attack tolerance of complex networks. *Nature* 406:378–382.
4. Pastor-Satorras R, Vespignani A (2001) Epidemic spreading in scale-free networks. *Phys Rev Lett* 86:3200–3203.
5. Cohen R, Erez K, ben-Avraham D, Havlin S (2001) Breakdown of the Internet under intentional attack. *Phys Rev Lett* 86:3682–3685.
6. Lloyd AL, May RM (2001) How viruses spread among computers and people. *Science* 292:1316–1317.
7. Albert R, Barabási A-L (2002) Statistical mechanics of complex networks. *Rev Mod Phys* 74:47–97.
8. Pastor-Satorras R, Vespignani A (2002) Immunization of complex networks. *Phys Rev E* 65:036104–036112.
9. Caldarelli G, Capocci A, De Los Rios P, Munoz MA (2002) Scale-free networks from varying vertex intrinsic fitness. *Phys Rev Lett* 89:258702–258705.
10. Cohen R, Havlin S, ben-Avraham D (2003) Efficient immunization strategies for computer networks and populations. *Phys Rev Lett* 91:247901–247905.
11. Dorogovtsev SN, Mendes JFF (2003) *Evolution of Networks: From Biological Nets to the Internet and WWW* (Oxford University Press, New York).
12. Newman MEJ (2003) The structure and function of complex networks. *SIAM Rev* 45:167–256.
13. Albert R, Albert I, Nakarado GL (2004) Structural vulnerability of the North American power grid. *Phys Rev E* 69:025103(R).
14. Valente AXCN, Sarkar A, Stone HA (2004) Two-peak and three-peak optimal complex networks. *Phys Rev Lett* 92:118702–118706.
15. Caldarelli G (2007) *Scale-Free Networks: Complex Webs in Nature and Technology (Oxford Finance)* (Oxford University Press, New York).
16. Moreira AA, Andrade JS, Herrmann HJ, Indekeu JO (2009) How to make a fragile network robust and vice versa. *Phys Rev Lett* 102:018701–018705.
17. Hooyberghs H, et al. (2010) Biased percolation on scale-free networks. *Phys Rev E* 81:011102–011117.
18. Frank H, Frisch IT (1970) Analysis and design of survivable networks. *IEEE T Commun Techn* 18:501–519.
19. Latora V, Marchiori M (2005) Efficient behavior of small-world networks. *Phys Rev Lett* 87:198701.
20. Sydney A, Scoglio C, Youssef M, Schumm P (2010) Characterizing the robustness of complex networks. *IJITST*, 2 pp:291–320.
21. Fiedler M (1973) Algebraic connectivity of graphs. *Czech Math J* 23:298–305.
22. Zhou Q, Bialek JW (2005) Approximate model of European interconnected system as a benchmark system to study effects of cross-border trades. *IEEE T Power Syst* 20:782–788.
23. Shavitt Y, Zilberman N (2010) A structural approach for PoP geo-location. *Conference on Computer Communications Workshops* (INFOCOM IEEE, San Diego), pp 1–6.
24. Holme P, Kim BJ, Yoon CN, Han SK (2002) Attack vulnerability of complex networks. *Phys Rev E* 65:056109–056123.
25. Maslov S, Sneppen K (2002) Specificity and stability in topology of proteins networks. *Science* 296:910–913.
26. Lopez E, Buldyrev SV, Havlin S, Stanley HE (2005) Anomalous transport in scale-free networks. *Phys Rev Lett* 94:248701–248705.
27. Molloy M, Reed B (1995) A critical point for random graphs with a given degree sequence. *Random Struct Algor* 6:161–179.
28. Erdős P, Rényi A (1960) On the evolution of random graphs. *Inst Hung Acad Sci* 5:17–61.
29. Batageli V, Mrvar A (1998) Pajek - Program for large network analysis. *Connections*, 21 pp:47–57.