**Statphys24 invited talk**

# Onion-like Network Topology Enhances Robustness against Malicious Attacks

**Hans J. Herrmann**[1,2], **Christian M. Schneider**[1], **André A. Moreira**[2], **José S. Andrade Jr.**[1,2] **and Shlomo Havlin**[3]

[1] Computational Physics, IfB, ETH Zurich, Schafmattstrasse 6, 8093 Zurich, Switzerland

[2] Departamento de Física, Universidade Federal do Ceará, 60451-970 Fortaleza, Ceará, Brazil

[3] Minerva Center and Department of Physics, Bar-Ilan University, 52900 Ramat-Gan, Israel

**Abstract.** We develop a method to generate robust networks against malicious attacks, as well as to substantially improve the robustness of a given network by swapping edges and keeping the degree distribution fixed. The method, based on persistence of the size of the largest cluster during attacks, was applied to several types of networks with broad degree distributions including a real network, the Internet. We find that our method can improve the robustness significantly. Our results show that robust networks have a novel "onion-like" topology consisting of a core of highly connected nodes hierarchically surrounded by rings of nodes with decreasing degree.

PACS numbers: 64.60.ah, 64.60.aq, 89.75.Da, 89.75.Fb, 89.75.Hc

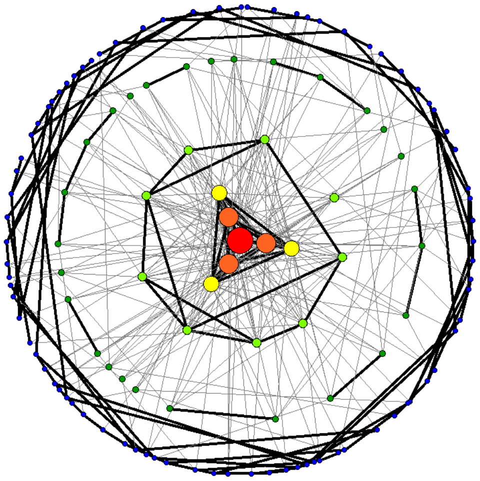

**Figure 1.** (Colors online) The onion-like topology of a robust network with $N = 124$ nodes and $M = 366$ edges obtained from the Apollonian network [24]. The size of the nodes is proportional to their degree. Edges between nodes with equal degree and the fully connected core are highlighted. In onion-like networks between nearly each pair of nodes of equal $k$ there is a path that does not contain nodes with higher degree.

## 1. Introduction

The security of real networks, like power supply networks [1], optical communication networks [2], computer networks or spy networks, is an important issue. Networks are considered to be secure if their function is not affected by the removal of nodes, which can be either random or targeted. Many networks are remarkably resistant against random failure, but a malicious attack is targeted to disrupt the network removing only a small fraction of nodes [3, 4, 5] or edges [3, 6]. A simple solution to avoid the disruption and increase the security is to add edges between nodes, but additional edges also increase the costs significantly. In this Letter we show that for a given degree distribution the most robust networks have an “onion-like“ topology (See Fig. 1)

## 2. Designing robust networks

A network is robust when as many as possible elements of the system remain globally connected even after a fraction of nodes or edges has been removed. Only few types of networks are robust against both random and malicious attacks [7, 8]. Based on a new measure for robustness which considers the size of the largest connected cluster during the entire attack process, an optimization process is used [9]. The optimization process significantly improves the robustness against malicious attack while keeping the node degrees constant. As a form of malicious attack we choose the high degree adaptive attack (HDA), which corresponds to the failure of the most stressed nodes in physical networks [10]. We investigate how properties of the networks change during our optimization process. We discover that, as illustrated in Fig. 1, the topology of robust networks converges, independent of the initial structure, to an onion-like structure, where high degree nodes are connected to each other, hierarchically surrounded by rings of nodes of decreasing degree. To confirm the generality of our results, we consider different types of networks as initial state for our optimization procedure. We study scale-free network models such as the Barabasi-Albert network [3], the Apollonian network [11, 12] and the scale-free configuration model [13] as well as the bimodal network, which is not scale-free and is initially extraordinarily robust [7, 8]. We also study the network of the Internet at the level of autonomous system (AS) obtained from DIMES project [14]. In either case we observe that the robustness against HDA can be increased significantly and all optimized networks exhibit the novel type of "onion-like" topology.

There are several ways to define the robustness of a network [10, 15]. Adapted from percolation theory, we associate the robustness with the average size of the largest connected cluster during the removal of nodes. The robustness measure $R$ sums the fractions of nodes in the largest connected cluster $s(Q)$ after removing $Q$ ‡ nodes

$$R = \frac{1}{N+1}\sum_{Q=0}^{N} s(Q) \tag{1}$$

where $N$ is the number of nodes in the network [9]. The robustness $R$, Eq. (1), which corresponds to the integral of the curves in Fig. 2, not only measures after how many removals the network fall apart (which is the common measure in percolation theory), but also considers the size of the largest connected cluster for each number of removed nodes. The range of $R$ is $[0, 0.5]$, where $R = 0$ corresponds to an original network of isolated nodes and $R = 0.5$ to the most robust network, which is a fully connected network during the entire attack. Previous work has dealt with finding the degree distribution for which the networks are most robust [7, 8]. Others have studied the effect of the interaction strength of the edges [16] and the dependence of the robustness on different topological properties, especially on the assortativity $r$ [15, 17]. These studies have focused on the percolation threshold $q_c$ without considering the size of the largest connected cluster. As shown in Fig. 2a, high assortative and onion-like networks have similar $q_c \approx 0.3$, but onion-like networks have a significantly higher $R$. This new robustness measure suggests a different perspective to characterize robustness.

We introduce the following algorithm, based on Monte Carlo method, to improve the robustness by changing the edges while keeping the degree distribution. We swap the connections of two randomly chosen edges, that is, $e_{ij}$, which connects node $i$ with node $j$, and $e_{kl}$ become $e_{ik}$ and $e_{jl}$ [18]. Only if the robustness after the swap is increased, i.e., $R_{\text{new}} > R_{\text{old}}$ the swap is accepted. Then we repeat this procedure with another randomly chosen pair of edges §.

We improve the networks against one typical attack strategy, the high degree adaptive (HDA) attack [10], but this method can be applied to any type of attack or combination

‡ The sum is divided into $N + 1$ equal intervals.

§ We repeat this procedure until the improvement during the last 10000 tested swaps is less than 1%.

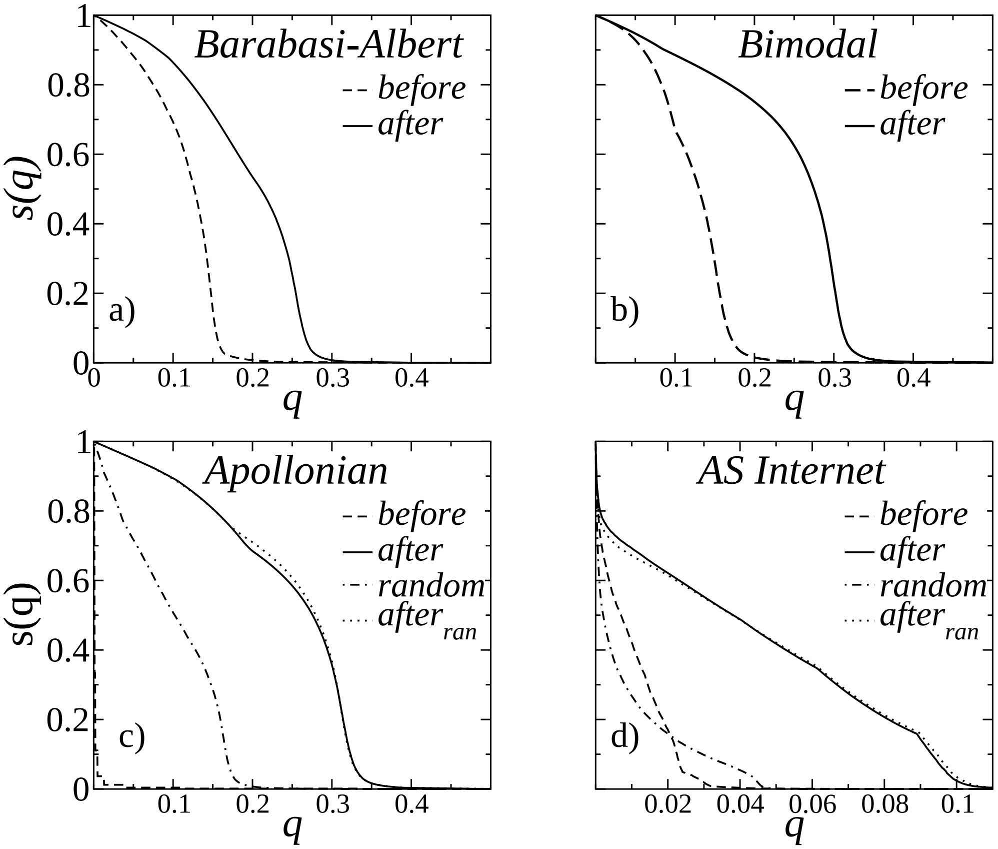

**Figure 2.** The fraction $s(q)$ of sites belonging to the largest connected cluster versus the fraction $q = Q/N$ of removed nodes using HDA attacks for a) BA networks with $N = 4096$ and $M = 8189$ (dotted line for BA networks with high assortativity), b) BM networks with $N = 4000, M = 8000, k_1 = 3, k_2 = 13$, c) AP networks with $N = 3283$ and $M = 9843$ (dotted lines for random starting configurations) and d) the AS with $N = 18124$ and $M = 37357$ (dotted lines for random starting configurations).

of attacks. In HDA one removes from the network sequentially the nodes with the highest degree. After each removal the degrees are recalculated to find the current highest degree node. If more than one node has the highest degree, one of them is chosen randomly and removed ‖. This attack strategy is more effective than removing the nodes which had highest degree in the beginning without recalculating the degrees [10]. Other attack strategies can be implemented based on the load of nodes and edges [10], on graph partition [19] or on inverse targeting immunization [20]. However, these strategies rely on global information while HDA needs only the local information about the node degree.

We use our method to improve the robustness against malicious attacks on several different types of networks. Figure 2 shows the fraction of nodes belonging to the largest connected cluster $s(q)$ before and after applying our method for Barabasi-Albert (BA) [3], Bimodal (BM)[7, 8], Apollonian (AP)[11, 12] networks and the Internet at the level

‖ Because of the random selection, $R$ is an estimation of the expectation of the robustness. Therefore a swap can be accepted, even if the robustness is decreased.

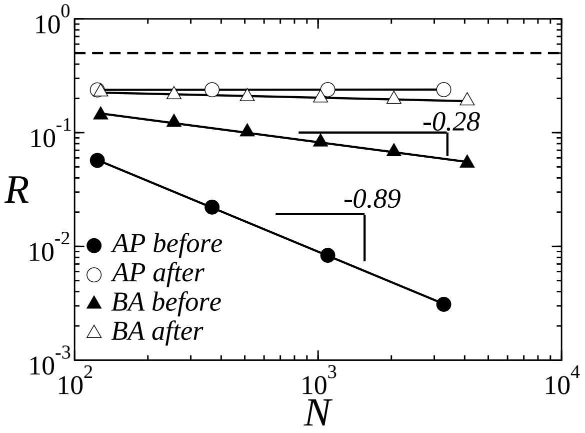

**Figure 3.** The robustness $R$ versus system size $N$ for AP and BA networks before and after applying the optimization procedure. The robustness seems to scale like a power law with $N$. The dashed line is the upper bound for the robustness.

of autonomous systems (AS)[14]. All results for the model networks are averaged over five different realizations. Most of the results for networks, which are created with the scale-free configuration model with an exponent $\gamma = 2.5$ (SF)[13], are similar to BA networks and are not discussed further here.

## 3. Numerical results

As shown in Fig.2, the networks become significantly more robust after the optimization. The largest cluster vanishes after removing twice as many high degree nodes in BA and BM networks after optimization. The improvement is even more pronounced in the AS and AP networks. To test the efficiency of our optimization process we performed a randomization of the initial networks keeping the node degrees fixed, before starting the optimization process. The enhanced robustness for these randomized networks (dotted lines in Fig.2c and 2d) is almost identical to those obtained from the original condition. This suggests that our algorithm is efficient in finding the optimal structure for a network with a given degree distribution independent on the initial state of the network.

In Fig.3 we plot the robustness $R$ as a function of the size $N$ of the network before and after our improvement. The robustness of the original networks decreases as a power-law, $R \sim N^{-\alpha}$ with $\alpha = 0.89 \pm 0.01$ for AP and $\alpha = 0.28 \pm 0.01$ for BA, while the robustness of the improved networks remains high and almost constant. This result shows that the improvement of the robustness increases significantly for larger networks. In many cases the modification of edges causes costs. To reduce these costs, the fraction of swapped edges $c$ should be small. In order to minimize this cost, we modify our condition for accepting a swap. It will be accepted, only if $R_{\text{new}} > R_{\text{old}} + \delta_T$, where $\delta_T$ is a threshold. Our aim is to get the highest robustness for a given fraction $c$ of swapped edges. Instead of calculating the robustness for many different values of $\delta_T$, we compute the envelope $R_E(c)$, which is the maximal possible robustness $R$ one can

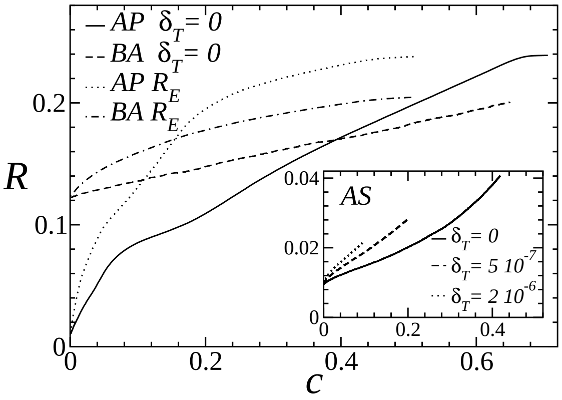

**Figure 4.** The robustness $R$ versus the relative number of swapped edges $c$ for AP with $N = 1096$ and BA with $N = 1024$ with $\delta_T = 0$ and their envelopes $R_E$. The inset shows the results for the AS network for different thresholds.

obtain for a fixed $c$. We start our optimization process with a large $\delta_T$ and reduce it during the process, if all swaps are rejected ¶. As shown in Fig.4, it is possible to reduce the number of swaps significantly while reaching the same robustness. For example, the fraction of swaps $c$ in the BA network can be reduced by up to $c = 0.2$ while reaching the same robustness.

By swapping the edges, we change network's topology. In Fig.1 we show an example of the topology after applying our algorithm to a small AP network. The network displays an "onion-like" topology. That is, the network is formed by a fully connected core of high degree nodes, surrounded by successive layers of nodes with decreasing degrees.

To test and quantitatively support our observations, we focus on four properties which characterize the topology: The average degree of the nearest neighbors of a $k$-degree node, the clustering coefficient, the onion structure and the average shortest path length. In the following we discuss the results for $\delta_T = 0$ and show examples for different network types. The topological properties are qualitative independent of the system sizes $N$ and the threshold $\delta_T$.

The average degree of the nearest neighbors of a $k$-degree node, $\overline{k}_{nn}$, is a measure for degree-degree correlations [21] and is defined as

$$\overline{k}_{nn}(k) = \sum_i k'_i \frac{E_{kk'_i}}{kN_k} \tag{2}$$

where $k'_i$ is the degree of node $i$ and $N_k$ is the number of nodes with degree $k$. $E_{kk'_i}$ counts the connections between the node $i$ and nodes with degree $k$. As shown in Fig.5a, $\overline{k}_{nn}$ is higher for high degree and lower for low degree in the robust networks compared to the original ones. This means that our algorithm tend to connect nodes of similar degree.

¶ At the beginning $\delta_T$ is set so high that nearly no swap is accepted. If the increase of $R$ during the last 1000 iteration steps is less than 1%, $\delta_T$ is reduced by 10%. The iteration stops, when $R$ is enhanced by less than 1% during the last 10000 iterations. With this algorithm we approximately calculate the envelope of all thresholds.

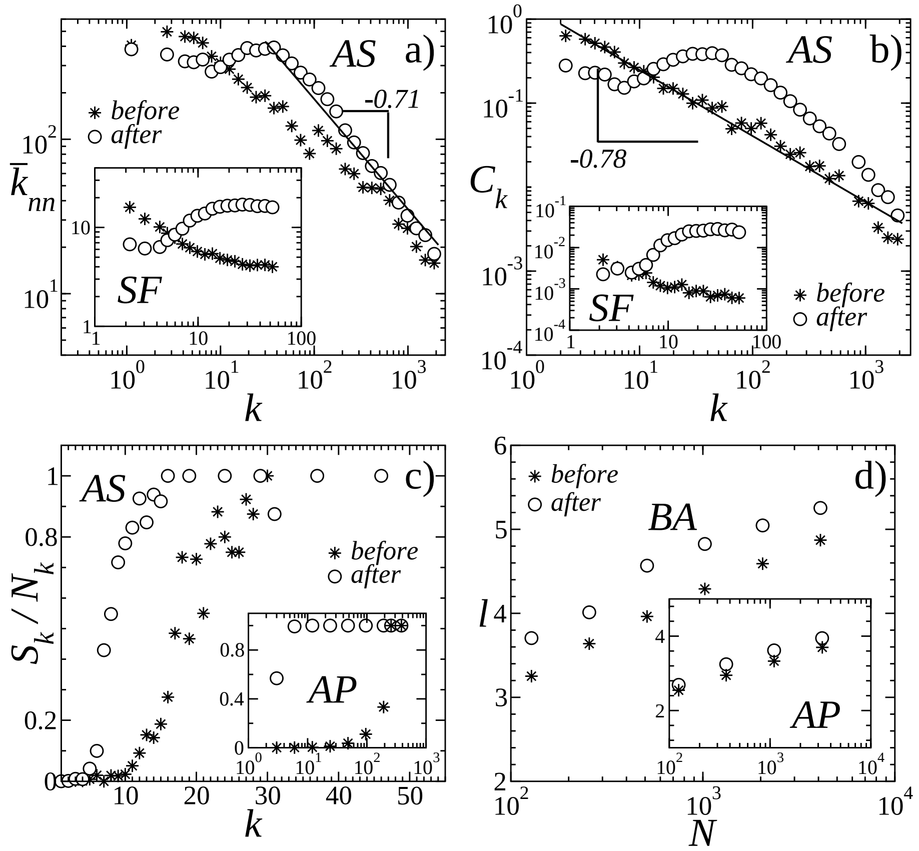

**Figure 5.** Dependence on the degree $k$ of a) the average degree of the nearest neighbors of a $k$-degree node, $\overline{k}_{nn}$, for AS and SF (inset); b) the cluster coefficient $C_k$ for AS and SF (inset); and c) the maximal fraction of nodes with degree $k$, which are connected through nodes with a degree smaller or equal to $k$. In d) we plot the average shortest path length $l$ versus the system size $N$ for BA and AP (inset).

Next we study the average clustering coefficient $C_k$ [22] of the nodes with connectivity $k$:

$$C_k = \frac{2E_k}{k(k-1)N_k} \tag{3}$$

where $E_k$ sums up the number of edges between the neighbors of each node with degree $k$. Fig.5b shows the behavior for $C_k$, which is similar to $\overline{k}_{nn}$. Both results confirm that nodes with high degree form a highly connected core. The decreasing tail for $\overline{k}_{nn}$ and $C_k$ for large $k$ in the case of the AS network arise from the low number of nodes with high degree.

Next we try to demonstrate further that the optimized network evolves to a hierarchical onion-like structure. To do this we calculate the maximal number of nodes $S_k$ with degree $k$, which are connected through nodes with a degree smaller or equal to $k$. As shown in Fig.5c, paths between nodes with equal degree without passing through nodes with higher degree emerge in the robust networks. This supports our assumption that the highly connected nodes of robust networks form a core hierarchically surrounded by rings of nodes of decreasing degree.

The last topological property we analyze is the average shortest path length $l$ between two nodes [3]. Although $l$ increases after the optimization, the average shortest path length is still comparable with the length before the optimization, as shown for BA and AP networks in Fig.5d. Also, the results shown in Fig.5d indicate that $l$ increases not faster than logarithmically with the system size $N$, thus demonstrating that the optimized networks have the small-world property [23].

## 4. Conclusion

In summary we have shown that a new measure for robustness of networks against malicious attacks, which focuses on the evolution of the size of the largest connected cluster during the attack, outperforms the common robustness measure. We have also developed a method that increase the robustness of networks against high degree adaptive attack while keeping the degree of the network nodes unchanged. Even if the number of links swaps is limited, the networks can be made significantly more robust. We found that the optimized networks evolve to a special structure with a core of high degree nodes surrounded by rings of nodes with decreasing degree. This novel onion-like topology implies that almost all nodes remain connected after removing the hubs in the core. Our results could be used to design robust optical networks with broad degree [2] and to improve existing networks without changing many edges. This could be applied to a power supply system to increase its robustness against acts of terrorism or to reduce the cascade failures in the case of a breakdown of the most stressed nodes. Applying our method to the AS Internet, malicious hackers would have to attack many more hubs to interrupt the system.

## Acknowledgments

We thank T. Mihaljev for useful discussions. 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 and the Epiwork EU project. A.A.M. and J.S.A would like to thank CNPq, CAPES, FUNCAP, and FINEP for financial support.

## References

[1] Albert R, Albert I and Nakarado G L, 2004, *Phys. Rev. E* **69**, 025103(R)
[2] Jahnke L, Kantelhardt J W, Berkovits R and Havlin S, 2008, *Phys. Rev. Lett* **101**, 175702
[3] Albert R, Jeong H and Barabási A-L, 2000, *Nature* **406**, 378
[4] Cohen R, Erez K, ben-Avraham D and Havlin S, 2000,*Phys. Rev. Lett* **85**, 4626
[5] Callaway D S, Newman M E J, Strogatz S H and Watts D J, 2000, *Phys. Rev. Lett* **85**, 5468
[6] Cohen R, Erez K, ben-Avraham D and Havlin S, 2001, *Phys. Rev. Lett* **86**, 3682
[7] Valente A X C N, Sarkar A and Stone H A, 2004, *Phys. Rev. Lett* **92**, 118702

[8] Tanizawa T, Paul G, Cohen R, Havlin S and Stanley H E, 2005, *Phys. Rev. E* **71**, 047101

[9] Schneider C M, Moreira A A, Andrade J S, Havlin S and Herrmann H J, 2010, *PNAS* accepted

[10] Holme P, Kim B J, Yoon C N and Han S K, 2002, *Phys. Rev. E* **65**, 056109

[11] Andrade J S, Herrmann H J, Andrade R F and da Silva L R, 2005, *Phys. Rev. Lett* **94**, 018702

[12] Doye J P K and Massen C P, 2005, *Phys. Rev. E* **71**, 016128

[13] Molloy M and Reed B, 1995, *Random Struct. Algorithms* **6**, 161

[14] www.netdimes.org

[15] Holme P and Zhao J, 2007, *Phys. Rev. E* **75**, 046111

[16] Moreira A A, Andrade J S, Herrmann H J, Indekeu J O, 2009, *Phys. Rev. Lett* **102**, 018701

[17] Newman M E J, 2002, *Phys. Rev. Lett* **89**, 208701

[18] Maslov S and Sneppen K, 2002, *Science* **296**, 910-913

[19] Chen Y, Paul G, Havlin S, Liljeros F and Stanley H E, 2008, *Phys. Rev. Lett* **101**, 058701

[20] Schneider C M, Mihaljev T and Herrmann H J, 2010, in preparation

[21] Boguñá M and Pastor-Satorras R, 2003, *Phys. Rev. E* **68**, 036112

[22] Albert R and Barabási A-L, 2002, *Rev. Mod. Phys.* **74**, 47

[23] Watts D J and Strogatz S H, 1998, *Nature* **393**, 440

[24] Batageli V and Mrvar A, 2008, *http://vlado.fmf.uni-lj.si/pub/networks/pajek/* **V 1.23**