SCIENTIFIC REPORTS

OPEN

SUBJECT AREAS:
COMPLEX NETWORKS
PHASE TRANSITIONS AND CRITICAL PHENOMENA

Received
27 June 2014

Accepted
19 December 2014

Published
13 March 2015

Mandala Networks: ultra-small-world and highly sparse graphs

Cesar I. N. Sampaio Filho[1], André A. Moreira[1], Roberto F. S. Andrade[2], Hans J. Herrmann[1,3] & José S. Andrade, Jr.[1,3]

[1]Departamento de Física, Universidade Federal do Ceará, 60451-970 Fortaleza, Ceará, Brazil, [2]Instituto de Física, Universidade Federal da Bahia, 40210-340 Salvador, Bahia, Brazil, [3]Computational Physics for Engineering Materials, IfB, ETH Zurich, Schafmattstrasse 6, 8093 Zurich, Switzerland.

Correspondence and requests for materials should be addressed to J.S.A. (soares@fisica.ufc.br)

The increasing demands in security and reliability of infrastructures call for the optimal design of their embedded complex networks topologies. The following question then arises: what is the optimal layout to fulfill best all the demands? Here we present a general solution for this problem with scale-free networks, like the Internet and airline networks. Precisely, we disclose a way to systematically construct networks which are robust against random failures. Furthermore, as the size of the network increases, its shortest path becomes asymptotically invariant and the density of links goes to zero, making it ultra-small world and highly sparse, respectively. The first property is ideal for communication and navigation purposes, while the second is interesting economically. Finally, we show that some simple changes on the original network formulation can lead to an improved topology against malicious attacks.

The tremendous increase in complexity of infrastructural networks, like the Internet and those related with transportation and energy supply, is mandatorily accompanied by requirements of higher standards of system reliability, security and robustness. This trend can only be sustained if these complex networks have the right structure. Under this framework, the scale-free property, present in many real networks, determines important aspects related with their functionality[1–5]. However, while scale-free networks are usually quite robust against random failures, they typically break down rapidly under malicious attacks[6–11]. Numerical studies have recently revealed that this weakness can be mitigated if their structure becomes onion-like, which means that nodes of equal degree are connected among each other and to nodes of higher degree[12,13]. Since then, the properties of onion-like structures have been extensively investigated[14–23]. Based on this insight, here we will address the challenge of providing a paradigm for complex networks with better topology. More precisely, we show that it is possible to design a family of scale-free networks which are robust to random failures and considering some modifications, we can improve the resilience against malicious attacks. Additionally, these networks also exhibit other improved properties, like a finite shortest path and extreme sparseness in the thermodynamic limit, which substantially increases communication and reduces costs. Thus these new networks become potential candidates for the design and implementation of complex infrastructural networks.

In the deterministic network model introduced here, the nodes belonging to a given shell have intra-shell and inter-shell connections, and the most connected nodes (hubs) are localized in the innermost shells. The network is recurrently expanded in such a way that every new generation corresponds to the addition of a new shell. Examples of these networks with four shells are shown in Figs. 1(a) and (b). Here we coin the name *mandala network* for this new family of graphs. In the first case, thereafter called network A, the first generation consists of a nucleus with three central nodes forming a complete graph (first shell). From each node in this nucleus, two new nodes emerge to form a connected ring of six nodes, composing the second shell of the second generation network. Following this iterative process, the third shell in the third generation network has an additional connected ring with twelve nodes, which, at this point, must also be linked to their respective ancestral nodes in the first and second shells. The same rules then apply for all new shells present in higher generation networks. This design therefore imposes that nodes at the same shell have the same degree. More precisely, the degree k_{ig} of a node at the *i-th* shell in the *g-th* network generation is given by,

$$k_{ig} = 2^{g-i+1} + (i-1). \quad (1)$$

Defining n_i as the number of nodes in the *i-th* shell, by construction, we have that $n_{i+1} = 2n_i$. From this relation, the number of nodes in the network is given by $N=\sum_{i=1}^{g} n_i$, where the summation is over the total number g of shells.

In fact, the network described so far in Fig. 1(a) is a particular case resulting from the recursive method proposed here to generate an ensemble of scale-free networks. For example, in Fig. 1(b) we show another example of mandala network, thereafter named network *B*. Precisely, the method depends on a set of three parameters, (n_1, b, λ), namely, the number of nodes in the first generation, n_1, the number of new nodes added to each node in the more external shell, b, and the scale factor, λ, for node degree in successive generations. Therefore, Eq. (1) can be written in a more general form as, $k_{ig} = b\lambda^{g-i} + (i-1)$ and $n_{i+1} = bn_i$. For instance, the networks *A* and *B* are completely defined by the sets (3, 2, 2) and (4, 4, 2), respectively.

Results

Scale-free networks. Any network generated by this method has discrete degree spectrum. In order to characterize the scale-free dependence, we consider the cumulative degree distribution, $P(k)=\sum_{k'\geq k} n(k')/N$. Taking into account that in each shell all nodes have the same degree, the cumulative distribution can be written as, $P\left(k_{ig}\right)=\sum_{j=1}^{i} n_j/N$. Applying Eq. (1) and the relation $n_{j+1} = bn_j$, it can be shown that the cumulative distribution decays in the form, $P(k_{ig}) \sim 1/k_{ig}$. In Fig. 2, we show a logarithmic plot of the cumulative degree distribution for networks *A* and *B*. In both cases, we have the same scale-free dependence.

At this point, an explanation about the exponent of the degree distribution $[p(k)]$ is useful[24–26]. Since our network has a discrete degree distribution, in order to calculate the standard definition of $p(k)$, it becomes necessary to consider binned intervals between consecutive degrees. Thus, the degree distribution is calculated as, $p(k_{ig}) \equiv n_i/N\Delta k_{ig}$, where $\Delta k_{ig} = k_{ig} - k_{(i+1)g}$ is the width of the interval. In this way, as $\Delta k_{ig} \sim k_{ig}$, it follows that $p\left(k_{ig}\right)\sim 1\Big/k_{ig}^2$.

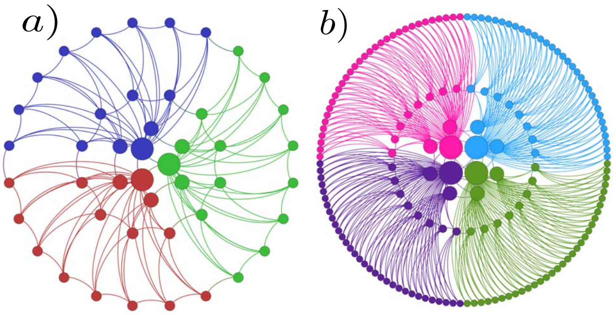

Figure 1 | (a) Representation of the mandala network of type *A*, generated with parameters $b = 2$, $n_1 = 3$ and $\lambda = 2$. The nodes correspond to circles whose areas are proportional to degree, and nodes in the same community have the same color. The first generation consists of a complete graph with three nodes defining the nucleus of the network. To each one of these nodes, two new nodes are connected to form a connected circular ring of six nodes, corresponding to the second shell. Next, the most external nodes generate two new nodes forming a circular ring with twelve nodes (third shell). Every node in the same community is connected with all its ancestral ones. (b) Network of type *B*, generated with parameters $b = 4$, $n_1 = 4$ and $\lambda = 2$.

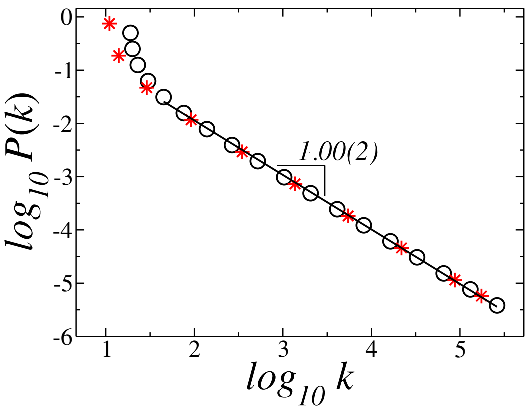

Figure 2 | Logarithmic plot of the cumulative degree distribution for the networks *A* (black circles) and *B* (red stars). The solid line represents the least-squares fit to data in the scaling regions of a power law, $P(k) \sim k^{-\beta}$, with $\beta = 1.00 \pm 0.02$, which confirms our analytical result.

Ultra-small-world networks. Another important property of the mandala networks relates to the mean shortest path length $\langle\ell\rangle=\sum_{ij}^{N}\ell_{ij}/[N(N-1)]$, where ℓ_{ij} is the shortest distance between any two nodes i and j in the network, and the summation goes over all possible node pairs in the system. In our case, this expression can be written in a more convenient form as,

$$\langle\ell\rangle=\frac{1}{N(N-1)}\sum_{j=1}^{g} n_j\phi_j, \tag{2}$$

where $\phi_j=\sum_{k=1}^{N}\ell_{jk}$ is the sum of the shortest path lengths connecting a node in the *j-th* shell with all other nodes in the network, n_j is the number of nodes in the *j-th* shell, and the summation goes over the number of shells. Using the symmetry of the network *A*, for example, it is possible to show that $\phi_j = \alpha_j N - \xi_j$ (see the section Methods), where ξ_j has different values for different shells, and α_i is given by 5/3, 29/12, 5/2, 31/12, 63/24, for $i = 1, 2, 3, 4,$ and 5, respectively, so that $\alpha \rightarrow 8/3$, for $i \rightarrow \infty$. Taking into account the linear dependence of ϕ_j with N and considering the relations for n_j, Eq. (2) reduces to

$$\langle\ell\rangle=\alpha+\frac{\mathcal{O}(N)}{N^2}, \tag{3}$$

which leads to $\langle\ell\rangle \rightarrow 8/3$ in the thermodynamic limit, $N \rightarrow \infty$. We show in Fig. 3 a semi-log plot of the mean shortest path length as a function of the number of nodes. The asymptotic convergence confirms our analytical result and therefore indicates that our network has an ultra-small-world behavior, namely $\langle\ell\rangle$ becomes independent of N. One should note, however, that this result is still different from the case of a complete graph, for which $\langle\ell\rangle = 1$, corresponding to the mean-field limit. Applying a similar sequence of calculations to the network *B*, it can be readily shown that the mean shortest path length for this topology also converges to a constant in the limit of large system sizes, but now equal to 11/4.

Highly sparse graphs. Next, we define the density d of connections as the ratio between the number of existing connections and the maximal number of possible connections for an undirected network with N nodes, $d=\sum_i n_i k_{ig}/[N(N-1)]$. Considering the expression for k_{ig} given by Eq. (1), we can rewrite the definition of d in the following way:

$$d=\frac{1}{N(N-1)}\left[\sum_{i}^{g} n_i 2^{g-i+1}+\sum_{i}^{g} n_i(i-1)\right]. \tag{4}$$

Expressing both summations in Eq. (4) in terms of the number of nodes in the network, $N=\sum_{i}^{g} n_i$, and considering the limit of a very large number of generations, we obtain,

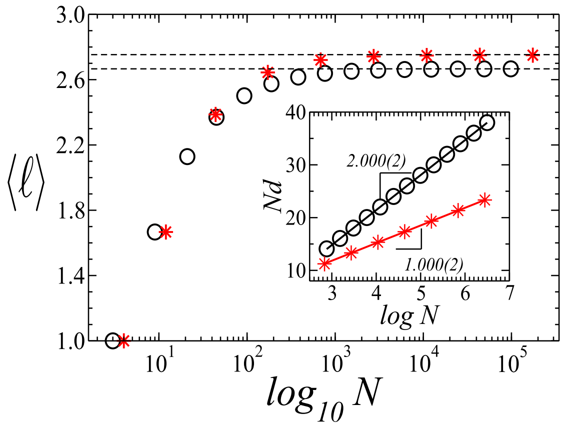

Figure 3 | Semi-log plot showing the dependence of the mean shortest path length $\langle \ell \rangle$ on the number of nodes N, for the networks A (black circles) and B (red stars). As depicted, the mean shortest-path lengths of A and B converge to the values 8/3 (top dashed line) and 11/4 (bottom dashed line), respectively, in the limit of a large number of nodes. Therefore, both networks can be considered as ultra-small worlds. The inset shows the semi-log plot of the density of connections d as a function of the number of nodes N in log-linear scale. Our analytical results reveal that $d \sim \frac{1}{N} \log N$ for network A (black circles) and for network B (red stars). The solid lines are the best fits to the numerically generated data sets, confirming these predicted behaviors. Hence both networks are highly sparse.

$$d \sim \frac{1}{N} \log N. \tag{5}$$

The inset of Fig. 3 shows the dependence of the density of connections on the number of nodes for networks of type A, confirming the asymptotic behavior predicted by Eq. (5). In the case of network B, where the number of new nodes generated is twice that of network A, the density of connections decays faster. Indeed, applying the same approach and considering $b = 4$, it is possible to show for network B that $d = (\log N)/N$. As a consequence, we conclude that our networks, despite of their ultra-small-world property, are extremely sparse when compared to the behavior of a complete graph, $d = 1$, and has only logarithmic correction to $d \sim 1/N$ that is valid for the Erdös-Rényi network at the percolation threshold. It is worth noticing that mandala networks are reminiscent of the expander graphs[27], since both models share similar properties as high sparsity and high connectedness. However, the mandala networks do not have self-loops or multiple edges with the same endpoints. Moreover, in the case of expander graphs, the maximal degree is limited, while in the mandala networks are scale-free.

Robustness. The framework of percolation is usually considered for the analysis of the robustness of complex networks[7,22,28–34]. In this context, robustness is typically quantified by the critical fraction q_c of removed nodes that leads to a total collapse of the network[6,9,10,12]. Nevertheless, as previously reported[12–14,16], this approach does not account for situations in which the system can suffer a big damage without breaking down completely. The size of the giant component, the largest connected cluster in the system, during the removal process of nodes has been recently introduced[12] as a refined measure to robustness,

$$R = \frac{1}{N+1} \sum_{Q=1}^{N} s, \tag{6}$$

where s is the fraction of nodes belonging to the giant component after removing $Q = qN$ nodes, q is the fraction of nodes removed, and R is in the range [0, 1/2]. The limit $R = 0$ corresponds to a system of isolated nodes, while $R = 1/2$ to the most robust network, which is the case of a completely connected graph. Here we check the robustness of our complex network model when subjected to mechanisms of random failures and two strategies of malicious attacks, namely, targeted by degree and targeted by betweenness[6–10].

In the main plot of Fig. 4, we show the fraction $s(q)$ of nodes belonging to the giant component during a random removal process as a function of the fraction of removed nodes q, for different values of the size N of networks A and B and averaged over 200 samples. Our results indicate that both networks A and B are robust, regardless of the system size N considered. This is corroborated in the inset of Fig. 4, where we plot the robustness measure R as a function of N for networks A and B. Both versions of the mandala network present a rather robust behavior, as compared to other models and real networks[12,13], with $R \approx 0.45$ and $R \approx 0.43$, for types A and B, respectively.

Unfortunately, as originally defined, our model network does not present a resilient behavior when subjected to malicious strategies of attack. We first consider attacks whose targets are the surviving nodes with the highest degree. In our network, since nodes at the same shell have the same degree, we start by choosing a node randomly with equal probability from the set of nodes with the highest degree (first shell). Due to the hierarchical structure of the network, a node from the second shell will only be removed after all nodes from the first shell disappear. This removal sequence remains valid till the targeted attack reaches the second-last shell. At this point, the random removal of a node in this shell can cause the simultaneous disconnection of other nodes from the giant cluster in the same, as well as in the outermost shell. As shown in Fig. 5, this strategy of attack leads to a drastic collapse of the structure when we remove less than 40% of the nodes.

In order to improve the robustness of the mandala model to malicious attacks, we propose the following two types of modification on the original network structure. First, we can randomly rewire each edge of the last shell, maintaining invariant the density of connections. The results in Fig. 5 show that robustness increases to $R = 0.36$, as compared to the value $R \approx 0.30$ of the original network. Second, as depicted in Fig. 5, we can systematically increase the number of

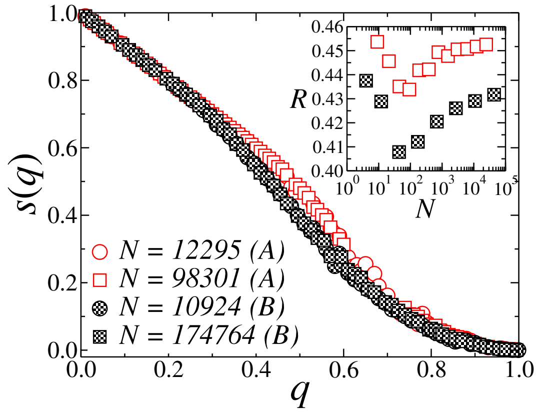

Figure 4 | Fraction $s(q)$ of nodes belonging to the giant component as a function of the fraction of randomly removed nodes q. Our results exhibit high robustness for both A and B networks, that are also shown to be practically independent of the network size for the different numbers of nodes N considered. The inset shows the robustness measure R as a function of N for networks A (opened symbols) and B (closed symbols) subjected to random failures. Both versions are rather robust to random attacks as compared to other models and real networks[12], with $R \approx 0.45$ and $R \approx 0.43$, for types A and B, respectively. All results correspond to averages over 200 samples.

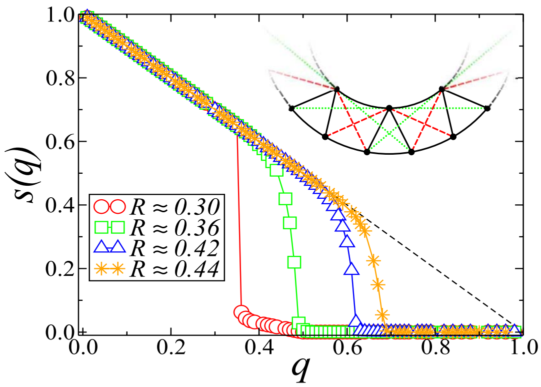

Figure 5 | Fraction $s(q)$ of nodes belonging to the giant component of network A as a function of the fraction of removed nodes q for attacks targeted by degree. The circles correspond to the original network and the rectangles to the case with rewiring process in the last shell. The triangles and stars correspond to the cases where the network has, respectively, $\kappa = 2$ and $\kappa = 4$ new edges per node, being also subjected to a rewiring processes in the last shell. The diagram inside shows the way additional edges are included between successive shells. Its black lines are the edges of the original network, and the dashed red and dotted green lines correspond to the cases where we add $\kappa = 2$ and $\kappa = 4$ new edges per node, respectively. The dashed line in the main plot corresponds to the limit of the ultra-robust network, and the inset box shows the corresponding robustness measures R for all cases considered. In all simulations, we used a single network of size $N = 49149$.

connections between successive shells. As shown in Fig. 5, this change can promote a substantial increase in the resilience, depending on the number of additional connections per node, κ. In any case, it is important to notice that for all new versions considered, the obtained networks maintain their high-sparsity and ultra-small-world properties, since we just add a number $\mathcal{O}(N)$ of new links.

Another important type of targeted attack is to remove nodes sequentially according to their betweenness centrality, in a descending order. The original version of the mandala network also displays a fragile behavior when subjected to this type of process (see Fig. 6), collapsing before 10% of removal with $R \approx 0.027$. Again, as Fig. 6 also shows, a rewiring process applied to the last shell can significantly improve the resilience of the mandala network, $R = 0.32$. This value is even larger than the one obtained for a Barabási-Albert network ($\gamma = 3$) having approximately the same density of connections (see Fig. 6).

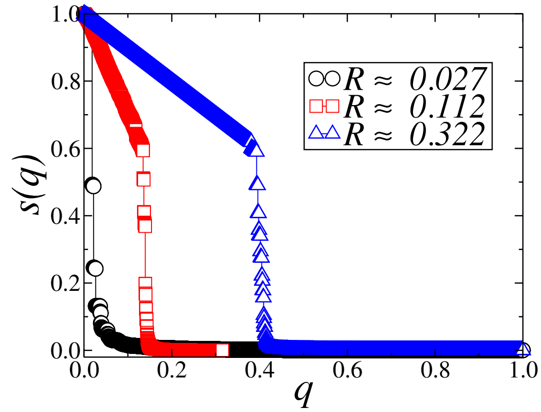

Figure 6 | Fraction $s(q)$ of nodes belonging to the giant component of network A as a function of the fraction of removed nodes q, for attacks targeted by betweenness centrality. The circles and triangles correspond to, respectively, the original network A and the case with rewiring process in the last shell. The rectangles are the results for the Barabási-Albert model. The inset box shows the corresponding robustness measures R for the networks considered. In all simulations, we used a single network of size $N = 6138$ and approximately the same density of connections of the original mandala network.

The Ising model. In small-world networks, the fact that the diameter of the graph does not grow faster than log N implies an infinite dimensionality. Mean-field theories therefore can successfully describe their critical behavior[1,35–39]. In order to investigate how collective ordering emerges in mandala networks, for which the shortest-path length is independent on N, we consider Ising spins σ_i associated to their nodes and ferromagnetic interactions J between them on the edges. Adopting the reduced Hamiltonian, $\mathcal{H}/k_bT = -J\sum_{ij}\sigma_i\sigma_j$, we perform Monte Carlo (MC) simulations on networks of type A for different system sizes N and temperature T values. In particular, we analyse the finite-size scaling properties of the model at the $T_c = 0$. The results in Fig. 7 show that the divergence of the maximum of the susceptibility with N, measured from the peak of the susceptibility, has the form, $T_c(N) \sim N^{1/\bar{\nu}}$, with a critical exponent, $1/\bar{\nu} = 0.50 \pm 0.01$.

Discussion

In summary, we have presented a recursive method to generate an ensemble of complex networks defined by a set of three parameters, namely (n_1, b, λ).

We have shown analytically and confirmed through numerical simulation that the networks originated from our model have scale-free topologies and are ultra-small, i.e., the average shortest-path lengths of sufficiently large networks become independent of their number of nodes. Our results also show that, as compared to a complete graph, which is ultra-small, these networks are highly sparse, with the density of edges going to zero with system size. Although mandala networks are robust against random failures, they are fragile against malicious attacks targeted by degree and betweenness centralities. However, simple corrections can be applied to the original model, improving significantly its robustness against both types of malicious attacks. Finally, we have verified that the critical temperature of the Ising model on the mandala network topology diverges with system size according to a power-law dependence, described by an exponent $1/\bar{\nu} = 0.50 \pm 0.01$. We expect to generalize this last result to other universality classes, for example, considering directed percolation and self-organized models on our deterministic networks.

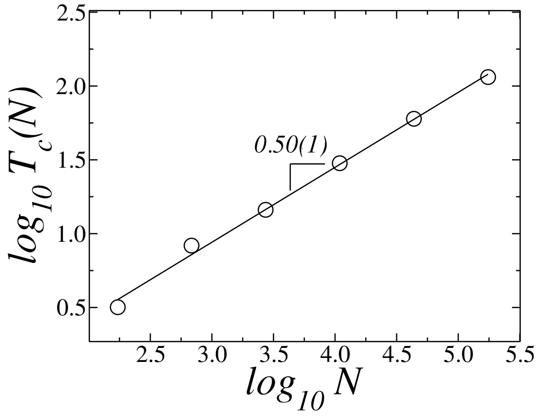

Figure 7 | Log-log plot showing the finite-size scaling analysis for the critical temperature of the Ising model implemented on the network model A. The maximum of the susceptibility diverges according to a power-law dependence, $T_c(N) \sim N^{1/\bar{\nu}}$, with $1/\bar{\nu} = 0.50 \pm 0.01$.

Methods

The mean shortest path length. Consider the definition of the shortest path length:

$$\langle \ell \rangle = \frac{1}{N(N-1)} \sum_{i=1}^{N} \sum_{j=1}^{N} \ell_{ij}, \tag{7}$$

and let us define $\phi_i = \sum_j \ell_{ij}$ as the summation of the shortest paths from the node i to all nodes in the network. Therefore, Equation (7) can be written as,

$$\langle \ell \rangle = \frac{1}{N(N-1)} \sum_{i=1}^{N} \phi_i. \tag{8}$$

From the symmetry of the network, nodes in the same shell have the same value of ϕ. Thus, we can interchange the summation in terms of the number of nodes to a summation in terms of the number of shells,

$$\langle \ell \rangle = \frac{1}{N(N-1)} \sum_{j=1}^{g} n_j \phi_j, \tag{9}$$

where n_j represents the number of nodes in the j-th shell and ϕ_j is now interpreted as the summation over the shortest paths from a node in the j-th shell to all nodes in the network.

To determine ϕ_j we choose a node, called *root node*, in the j-th shell and calculate its shortest path to other nodes, considering shell by shell. Here we will consider a detailed calculation for three first shells. For the first shell, considering the node 1 as root we obtain,

$$\begin{aligned}\phi = {} & [\ell_{12} + \ell_{13}]_{sh1} + [\ell_{14} + \ell_{15} + \ell_{16} + \ell_{17} + \ell_{18} + \ell_{19}]_{sh2} + \\ & [\ell_{110} + \ell_{111} + \ell_{112} + \ell_{113} + \cdots + \ell_{121}]_{sh3} + \cdots\end{aligned} \tag{10}$$

The first bracket is equal to $(n_1 - 1)$, since all nodes in the first shell are at a distance equal to one for the root node. In the second shell, we have $\frac{1}{3}n_2$ nodes at a distance equal to one and $\frac{2}{3}n_2$ nodes at a distance two of the root node. In this way, for the j-th outermost shells, we have $\frac{1}{3}n_j$ nodes at a distance equal to one and $\frac{2}{3}n_j$ nodes at a distance two of the root node. Using these results in Equation (10), it follows that,

$$\begin{aligned}\phi = {} & [n_1 - 1]_{sh1} + \left[\frac{1}{3}n_2 \times 1 + \frac{2}{3}n_2 \times 2\right]_{sh2} + \left[\frac{1}{3}n_3 \times 1 + \frac{2}{3}n_3 \times 2\right]_{sh3} \\ & + \cdots + \left[\frac{1}{3}n_g \times 1 + \frac{2}{3}n_g \times 2\right]_{shg}\end{aligned} \tag{11}$$

$$\phi = (n_1 - 1) + \frac{5}{3}\left[n_2 + n_3 + \cdots + n_g\right]. \tag{12}$$

Therefore, the value of ϕ for any node in the first shell is given by,

$$\phi_1 = \frac{5N}{3} - n_1, \tag{13}$$

where we consider $N = \sum_j n_j$. A similar approach can be applied to others shell. Choosing now the root node in the second shell, we obtain,

$$\begin{aligned}\phi = {} & \left[\frac{5}{3}n_1\right]_{sh1} + \left[\frac{3}{2}n_2\right]_{sh2} + \left[\frac{2}{12}n_3 \times 1 + \frac{3}{12}n_3 \times 2 + \frac{7}{12}n_3 \times 3\right]_{sh3} \\ & + \left[\frac{2}{12}n_4 \times 1 + \frac{3}{12}n_4 \times 2 + \frac{7}{12}n_4 \times 3\right]_{sh4} + \cdots \\ & + \left[\frac{2}{12}n_g \times 1 + \frac{3}{12}n_g \times 2 + \frac{7}{12}n_g \times 3\right]_{shg},\end{aligned} \tag{14}$$

and ordering the identical terms results in,

$$\phi = \frac{5}{3}n_1 + \frac{3}{2}n_2 + \frac{29}{12}\left[n_3 + n_4 + \cdots + n_g\right]. \tag{15}$$

The value of ϕ for nodes in the second shell is then given by,

$$\phi_2 = \frac{29N}{12} - \frac{31}{12}n_1. \tag{16}$$

Finally, using a similar sequence of calculation, for the i-th shell, we obtain that, $\phi_i = \alpha_i N - \xi_i$, with α_i equal to 5/3, 29/12, 5/2, 31/12, 63/24, 127/48, and 255/96 for the seven first shells, respectively. Therefore, we have $\alpha_i \to \frac{8}{3}$ for $i \to \infty$.

The Ising model. The Monte Carlo simulations of the Ising model on the mandala networks were performed using the Metropolis algorithm, starting from different initial spin configurations. In order to study the critical behavior of the system, we considered the magnetization M_L and the susceptibility χ_L, which are defined by

$$M_N(T) = \left\langle \langle m \rangle_{time} \right\rangle_{sample}, \tag{17}$$

$$\chi_N(T) = N\left[\left\langle \langle m^2 \rangle_{time} - \langle m \rangle^2_{time} \right\rangle_{sample}\right], \tag{18}$$

where $\langle m \rangle = \left| \frac{1}{N} \sum_{i=1}^{N} \sigma_i \right|$, T is the temperature and N is the total number of nodes in the network. The symbols $\langle \cdots \rangle_{time}$ and $\langle \cdots \rangle_{sample}$, respectively, denote time averages taken in the stationary state and configurational averages taken over 100 independent samples. Time is measured in Monte Carlo steps (MCS), and 1 MCS corresponds to N attempts of changing the states of the spins. In our simulations, the initial 10^5 MCS were discarded to guarantee that the system reached the steady state, after which the time averages were estimated using the next 6×10^5 MCS. The value of temperature where χ_N has a maximum is identified as $T_c(N)$ for N = 172, 684, 2732, 10924, 43692, and 174764.

1. Albert, R. & Barabási, A.-L. Statistical mechanics of complex networks. *Rev. Mod. Phys.* **74**, 031109 (2002).
2. Newman, M. The structure and function of complex networks. *SIAM Review* **45**, 167 (2003).
3. López, E., Buldyrev, S. V., Havlin, S. & Stanley, H. E. Anomalous transport in scale-free networks. *Phys. Rev. Lett.* **94**, 248701 (2005).
4. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M. & Hwang, D.-U. Complex networks: Structure and dynamics. *Phys. Rep.* **424**, 175 (2006).
5. Barabási, A.-L. Scale-free networks: A decade and beyond . *Science* **325**, 412 (2009).
6. Albert, R., Jeong, H. & Barabási, A.-L. Error and attack tolerance of complex networks, *Nature* **406**, 378 (2000).
7. Callaway, D. S., Newman, M. E. J., Strogatz, S. H. & Watts, D. J. Network Robustness and Fragility: Percolation on Random Graphs, *Phys. Rev. Lett.* **85**, 5468 (2000).
8. Cohen, R., Erez, K., ben Avraham, D. & Havlin, S. Resilience of the Internet to Random Breakdowns, *Phys. Rev. Lett.* **85**, 4626 (2000).
9. Cohen, R., Erez, K., ben Avraham, D. & Havlin, S. Breakdown of the Internet under Intentional Attack, *Phys. Rev. Lett.* **86**, 3682 (2001).
10. Holme, P., Holme, B. J., Yoon, C. N. & Han, S. K. Attack vulnerability of complex networks, *Phys. Rev. E* **65**, 056109 (2002).
11. Tanizawa, T., Paul, G., Cohen, R., Havlin, S. & Stanley, H. E. Optimization of network robustness to waves of targeted and random attacks, *Phys. Rev. E* **71**, 047101 (2005).
12. Schneider, C. M., Moreira, A. A., Andrade, J. S., Havlin, S. & Herrmann, H. J. Mitigation of malicious attacks on networks, *Proc. Natl. Acad. Sci.* **108**, 3838 (2011).
13. Herrmann, H. J., Schneider, C. H., Moreira, A. A., Andrade, J. S. & Havlin, S. Onion-like network topology enhances robustness against malicious attacks, *J. Stat. Mech.: Theory Exp.* **01**, 01027 (2011).
14. Wu, Z.-X. & Holme, P. Onion structure and network robustness, *Phys. Rev. E* **84**, 026106 (2011).
15. Valdez, L. D., Buono, C., Braunstein, L. A. & Macri, P. A. Effect of degree correlations above the first shell on the percolation transition, *Europhys. Lett.* **96**, 38001 (2011).
16. Schneider, C. H., Mihaljev, T. & Herrmann, H. J. Inverse targeting An effective immunization strategy, *Europhys. Lett.* **98**, 46002 (2012).
17. Tanizawa, T., Havlin, S. & Stanley, H. E. Robustness of Onionlike Correlated Networks against Targeted Attacks, *Phys. Rev. E* **85**, 046109 (2012).
18. Zeng, A. & Liu, W. Enhancing network robustness against malicious attacks, *Phys. Rev. E* **85**, 066130 (2012).
19. Helbing, D. Globally networked risks and how to respond, *Nature* **497**, 51 (2013).
20. Dong, G. *et al.* Robustness of network of networks under targeted attack, *Phys. Rev. E* **87**, 052804 (2013).
21. Skarpalezos, L., Kittas, A., Argyrakis, P., Cohen, R. & Havlin, S. Anomalous biased diffusion in networks, *Phys. Rev. E* **88**, 012817 (2013).
22. Wang, B., Gao, L., Gao, Y. & Deng, Y. Maintain the structural controllability under malicious attacks on directed networks, *Europhys. Lett.* **101**, 58003 (2013).
23. Louzada, V. H. P., Daolio, F., Herrmann, H. J. & Tomassini, M. Smart rewiring for network robustness, *J. Complex Netw.* **1**, 150 (2013).
24. Andrade, J. S., Herrmann, H. J., Andrade, R. F. S. & da Silva, L. R. Apollonian Networks: Simultaneously Scale-Free, Small World, Euclidean, Space Filling, and with Matching Graphs, *Phys. Rev. Lett.* **102**, 079901 (2009).
25. Guo, J.-L. & Wang, L.-N. *Physics Procedia* **3**, 1791 (2010).
26. Mungan, M. Comment on Apollonian Networks: Simultaneously Scale-Free, Small World, Euclidean, Space Filling, and with Matching, *Phys. Rev. Lett.* **106**, 029802 (2011).
27. Hoory, S., Linial, N. & Wigderson, A. Expander graphs and their applications. *Bull. Amer. Math. Soc.* **43**, 439 (2006).

28. Newman, M. E. J. & Ziff, R. M. Fast Monte Carlo algorithm for site or bond percolation, *Phys. Rev. E* **64**, 016706 (2001).
29. Cohen, R., Havlin, S. & ben Avraham, D. Efficient Immunization Strategies for Computer Networks and Populations, *Phys. Rev. Lett.* **91**, 247901 (2003).
30. Moreira, A. A., Andrade, J. S., Herrmann, H. J. & Indekeu, J. O. How to Make a Fragile Network Robust and Vice Versa, *Phys. Rev. Lett.* **102**, 018701 (2009).
31. Hooyberghs, H. *et al.* Biased percolation on scale-free networks, *Phys. Rev. E* **81**, 011102 (2010).
32. Newman, M. E. J. Communities, modules and large-scale structure in networks, *Nature Phys*. **8**, 25 (2011).
33. Peixoto, T. P. & Bornholdt, S. Evolution of Robust Network Topologies: Emergence of Central Backbones, *Phys. Rev. Lett.* **109**, 118703 (2012).
34. Taylor, D. & Restrepo, J. G. A network-specific approach to percolation in complex networks with bidirectional links, *Europhys. Lett.* **98**, 16007 (2012).
35. Newman, M. E. J. & Watts, D. J. Scaling and percolation in the small-world network model, *Phys. Rev. E* **60**, 7332 (1999).
36. Giuraniuc, C. V. *et al.* Trading Interactions for Topology in Scale-Free Networks, *Phys. Rev. Lett.* **95**, 098701 (2005).
37. Dorogovtsev, S. N., Goltsev, A. V. & Mendes, J. F. F. Critical phenomena in complex networks, *Rev. Mod. Phys.* **80**, 1275 (2008).
38. Castellano, C. & Pastor-Satorras, R. Routes to Thermodynamic Limit on Scale-Free Networks, *Phys. Rev. Lett.* **100**, 148701 (2008).
39. Ferreira, S. C., Ferreira, R. S., Castellano, C. & Pastor-Satorras, R. Quasi-stationary simulations of the contact process on quenched networks, *Phys. Rev. E* **84**, 066102 (2011).

Acknowledgments

We thank the Brazilian agencies CNPq, CAPES, FUNCAP, and FAPESB, the National Institute of Science and Technology for Complex Systems (INCT-SC Brazil), to the ETH Risk Center (Switzerland), and the European Research Council through Grant FlowCSS No. FP7-319968 for financial support.

Author contributions

The authors C.S.F., A.M., R.A., H.J.H. and J.S.J. contributed equally.

Additional information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Sampaio Filho, C.I.N., Moreira, A.A., Andrade, R.F.S., Herrmann, H.J. & Andrade, J.S. Mandala Networks: ultra-small-world and highly sparse graphs. *Sci. Rep.* **5**, 9082; DOI:10.1038/srep09082 (2015).