Available online at www.sciencedirect.com

ScienceDirect

Cellular Immunology 244 (2006) 80–83

Cellular Immunology

www.elsevier.com/locate/ycimm

Evolution of robust and efficient system topologies

Sergiu Netotea [a], Sándor Pongor [a,b,*]

[a] Bioinformatics Group, Biological Research Centre, Hungarian Academy of Sciences, Temesvári krt. 62, H-6701 Szeged, Hungary
[b] Protein Structure and Bioinformatics Group, International Centre for Genetic Engineering and Biotechnology, Padriciano 99, I-34012 Trieste, Italy

Received 3 December 2006; accepted 11 December 2006
Available online 12 April 2007

Abstract

Mutation/selection algorithms were applied to increase the efficiency and the robustness of sparse random networks. Selection for better efficiency leads to the well-known star topology, while selection for robustness only results in a relatively dense core and a small periphery. Concomitant selection for both efficiency and robustness leads to networks with intermittent center/periphery values. Networks evolving under multiple attack regimes develop distinct topologies with larger cores, and are characterized by parameter distributions different from those developing under single-attack regimes.

Keywords: Complex networks; Evolution of biological networks; Network modules

1. Introduction

The emergence of self organized network structures is one of the key aspects of molecular and cellular interactions, including those between the molecular and cellular components of the immune system. In order to remain stable in time and resistant to attack, biological networks must evolve in a particular way. One of the fundamental models proposed for network evolution is that of Barabási's that suggests a link between the growth of a network, and its topology as well as robustness [1]. Other models, including the one discussed here, rearrange a given size network and look at the resulting topologies [2–6]. Rearrangement ("rewiring") models follow the traditions of evolutionary modeling, i.e. they optimize a fitness function that combines various factors into one numerical index. Naturally, there are many ways to formulate and combine the components of the fitness function and testing the possibilities makes the process computationally expensive. Here we describe another approach in which all parameters are treated essentially as constraints: a mutation is selected if all of its parameters exceed or at least reach the corresponding values of the previous state, so there are no tunable parameters. In a broad sense, this approach bears on Kimura's neutralist theory evolution; moreover it is computationally efficient so it allows one to study a wide range of phenomena.

Our main goal was to study the evolution of robust yet efficient network topologies and to see if selecting mutations only for efficiency or only for attack tolerance (robustness) will influence network topology. Our approach was inspired by the study of Venkatasubramanian and associates who showed that selection of efficient and robust networks leads to certain patterns [3], as well as by our previous work on the attack tolerance of sparse networks [7]. Here we show that concomitant selection for efficiency and robustness influences the fundamental topological properties of the network, and that evolution under multiple attacks leads to distinct topologies.

2. Methods

The two fundamental network properties we deal with are efficiency and robustness. The global efficiency [8] of a network is defined as:

* Corresponding author. Address: Bioinformatics Group, Biological Research Centre, Hungarian Academy of Sciences, Temesvári krt. 62, H-6701 Szeged, Hungary. Fax: +39 0 40 226 555.
E-mail address: pongor@icgeb.org (S. Pongor).

0008-8749/$ - see front matter
doi:10.1016/j.cellimm.2006.12.007

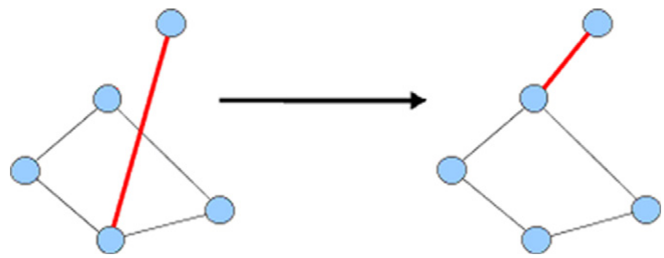

Fig. 1. A simple model of network evolution. At each step an edge is rewired at random. If the new topology is more fitted according to the selected fitness criteria, the new network is used for the next step.

$$E = \frac{1}{n(n+1)} \sum_{i \neq j} \frac{1}{d_{ij}}, \tag{1}$$

where n is the number of nodes, and d_{ij} is the shortest path between the nodes i and j. The robustness of a system can be described as a property, such as efficiency, calculated after attack (E_t) expressed as a fraction of the same property (E) of the original network.

$$R = \frac{E_t}{E} \tag{2}$$

for the attacks we used a strategy in which the node with the highest capability to mediate information between other nodes was removed. This capability is expressed by the betweenness centrality expressed as:

$$C_B(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{3}$$

where $\sigma_{st}(v)$ is the number of shortest paths between nodes s and t that pass through the node v, and σ_{st} is the total number of shortest paths between nodes s and t [9]. The robustness against multiple attacks was assessed by maximal damage strategy [10], by successively removing the five most central nodes in terms of C_B, with recalculation of the C_B values after each attack. So the value of E_t in Eq. (2) was calculated after five attacks. Finally, we used a simple measure, periphery %, defined as the % of the nodes with degree = 1.

For modeling the evolution of a network we start with a random network with a given number of nodes and edges and then change one end-position of a randomly chosen edge.

A mutation is accepted if the target property (E, R or both) is equal or better than before the mutation. This

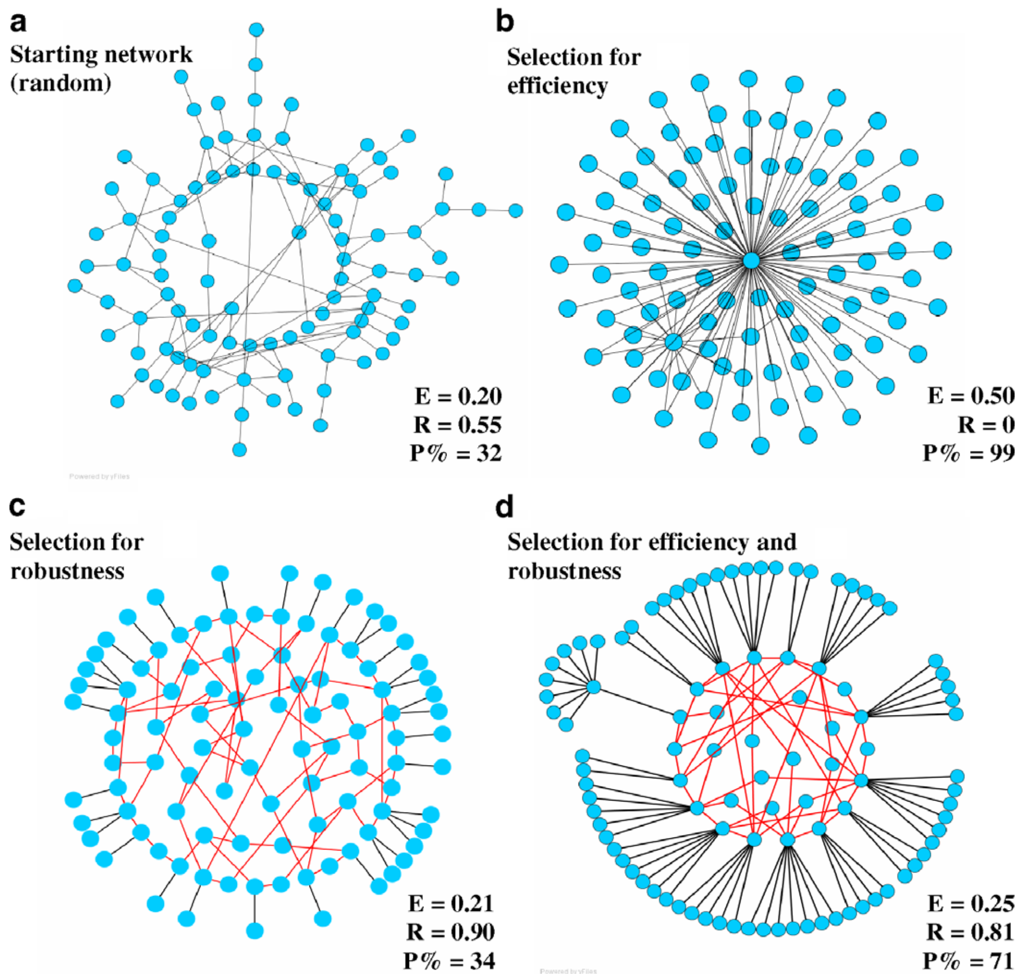

Fig. 2. Example of network topologies. A random network of 100 nodes and 120 edges (a) was subjected to selection under various regimes (b–d) E, efficiency; R, robustness; P, periphery. Note that the parameter P% of (d) is between (b) and (c).

Table 1
Comparison of network parameters

Parameter	Initial random graph	Criterion of selection			
		5 attack R	$E+5$ attack R	$E+1$ attack R	E
Efficiency	0.22	0.21	0.23	0.28	0.50
R (5 attacks)	0.47	0.88	0.89	0.55	0.00
R (1 attack)	0.91	0.98	0.98	0.99	0.04
Periphery%	31	31	44	68	77
Avg. nn (degree)	3.22	3.76	4.62	7.88	86.86
Diameter	14.10	15.00	11.70	8.50	2.00
Radius	7.60	8.30	6.80	4.60	1.00

The values are the average of 20 simulations. R, robustness; E, efficiency; nn, nearest neighbor (also see [11]).

method is straightforward but it may lead to local maxima in the search space of network topologies, so we used a genetic algorithm that has better convergence to global maxima. Our algorithm can be outlined as follows:

1. Start with a population of random graphs encoded as a chromosome describing each graph topology.
2. A number of graphs "individuals" are selected for crossover and mutation. Crossover is done by exchanging a number of relevant subgraphs. The mutation means rewiring an edge at random. The crossover and mutation rates are set heuristically to insure better convergence.
3. A new individual is accepted if the graph passes the efficiency/robustness criteria.

Steps 2 and 3 are repeated until the appearance rate of the most fitted individuals significantly decreases.

This procedure reproducibly converges to the same or better optima as purely random mutation and selection, so in spite of the size of the topological space we are confident about the quality of the final optima (Fig. 1).

3. Results and discussion

We modeled the evolution of sparse graphs with 100 nodes and 120 edges, which roughly corresponds to the node/edge ratio of gene-regulation networks. Some typical structures are shown in Fig. 2. Evolving the network using an efficiency-only rule leads to the well-known star topology where the center is formed by one (or a few) nodes and all other nodes are peripheral (A). Evolution under a robustness-only regime results in a large core and a small periphery, with the nodes apparently preserving the small degrees seen in the initial network. Evolution under both efficiency and robustness constraints leads to the formation of a strong center and a larger periphery. It thus appears that robustness strengthens the core, while efficiency increases the periphery.

We found little correlation between the properties mentioned above; on the other hand the kind of attack strategy used had a tangible effect on the distribution of some network parameters (Table 1). Selection against multiple attacks resulted in an altered degree distribution as compared to selection against single attack (Fig. 3).

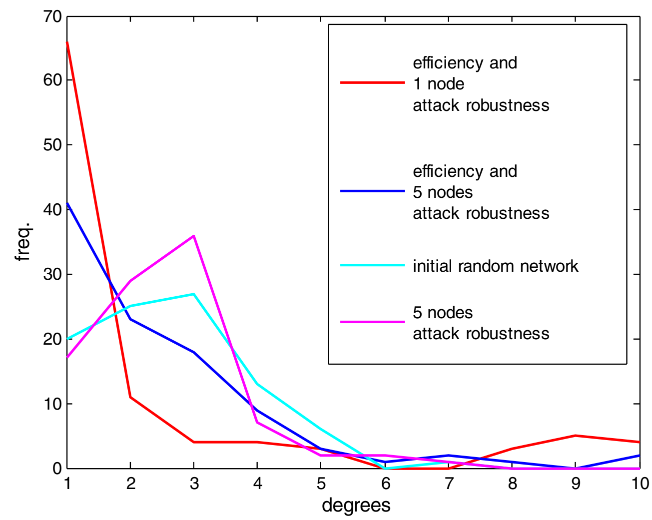

Fig. 3. Degree distribution of networks evolved under single and multiple attacks regimes. The labels denote the criterion of selection used.

We observed circular patterns similar to those described by Venkatasubramanian and associates [3], however the data did not allow us to conclusively associate them with any of the factors studied here (data not shown).

We conclude that the topology of the networks changes when the networks adapt to an environment where both efficiency and robustness are required, and the presence of multiple attacks bring about further topology changes as compared to single attacks.

Acknowledgment

Work at ICGEB was supported in part by grants from the Ministero dell'Università e della Ricerca (D.D. 2187, FIRB 2003, art. 8).

References

[1] A.-L. Barabási, R. Albert, Emergence of scaling in random networks, Science 286 (1999) 509–512.

[2] R.F. Cancho, R. Solé, Optimization in complex networks, SFI Working Paper 01-11-068.
[3] V. Venkatasubramanian, S. Katare, P.R. Patkar, Fang-ping Mu, Spontaneous emergence of complex optimal networks through evolutionary adaptation, Comput. Chem. Eng. 28 (9) (2004) 1789–1798.
[4] K.A. Lehmann, M. Kaufmann, Evolutionary algorithms for the selforganized evolution of networks, GECCO'05, June 25–29, 2005, Washington, DC, USA.
[5] D. Newth, J. Ash, Evolving cascading failure resilience in complex networks, The 8th Asia Pacific Symposium on Intelligent and Evolutionary Systems 6th–7th December 2004. Cairns, Australia.
[6] F. Schweitzer, W. Ebeling, H. Rosé, O. Weiss, Optimization using evolutionary strategies, in: Parallel Problem Solving from Nature—PPSN IVLecture Notes in Computer Science, 1141, Springer, Berlin, 1996, pp. 940–949.
[7] P. Csermely, V. Ágoston, S. Pongor, The efficiency of multi-target drugs: the network approach might help drug design, Trends Pharmacol. Sci. 26 (2005) 178–182.
[8] V. Latora, M. Marchiori, Economic small-world behavior in weighted networks, Eur. Phys. J. B 32 (2003) 249–263.
[9] U. Brandes, A faster algorithm for betweenness centrality, J. Math. Sociol. 25 (2) (2001) 163–177.
[10] V. Ágoston, P. Csermely, S. Pongor, Multiple weak hits confuse complex systems: a transcriptional regulatory network as an example, Phys. Rev. E 71 (2005) 051909.
[11] R. Diestel, Graph Theory, third ed., Springer-Verlag, Heidelberg, 2005.