Attacks and Cascades in Complex Networks

Ying-Cheng Lai[1], Adilson E. Motter[2], and Takashi Nishikawa[3]

[1] Department of Mathematics and Statistics, Department of Electrical Engineering, Arizona State University, Tempe, AZ 85287, USA
[2] Max Planck Institute for the Physics of Complex Systems, Nöthnitzer Strasse 38, 01187 Dresden, Germany
[3] Department of Mathematics, Southern Methodist University, Dallas, TX 75275, USA

Abstract. This paper reviews two problems in the security of complex networks: *cascades of overload failures on nodes* and *range-based attacks on links*. Cascading failures have been reported for numerous networks and refer to the subsequent failure of other parts of the network induced by the failure of or attacks on only a few nodes. We investigate a mechanism leading to cascades of overload failures in complex networks by constructing a simple model incorporating the flow of physical quantities in the network. The second problem is motivated by the fact that most existing works on security of complex networks consider attacks on nodes rather than on links. We address attacks on links. Our investigation leads to the finding that many scale-free networks are more sensitive to attacks on short-range than on long-range links. Besides its importance concerning network security, our result has the unexpected implication that the small-world phenomenon in these scale-free networks is mainly due to short-range links.

1 Introduction

Complex networks [1] such as the Internet, the electrical power grid, and the transportation network, are an essential part of a modern society. The security of such a network under random or intentional attacks is of great concern. Recently, an interdisciplinary field among information science and engineering, statistical and nonlinear physics, applied mathematics, and social science has emerged, bringing novel concepts and approaches to the study of complex networks [2–5]. Issues such as the characterization of the network architecture, dynamics on complex networks, and the effect of attacks on network operation have begun to be addressed. A central point of this review is that the flow of information and other physical quantities in the network can be critically important for network security. This *dynamical* aspect of the security problem, despite its highly practical relevance, has been only partially understood in the context of complex networks. Here we shall review some of our initial results in this direction.

Most large natural and man-made networks are sparse and evolve in time. Two important properties displayed by many of these networks are the small-world [6] and scale-free [7] properties. Small-world networks are characterized by the clustering coefficient C and the average network distance L. The former is the probability that any two nodes are connected to each other, given that they are both connected to a common node. The latter measures the average minimal

Y.-C. Lai, A.E. Motter, and T. Nishikawa, Attacks and Cascades in Complex Networks, Lect. Notes Phys. **650**, 299–310 (2004)
http://www.springerlink.com/

number of links connecting any two nodes in the network. Many regular networks have high clustering coefficients and large network distances. Random networks, on the other hand, have small network distances and low clustering coefficients [8]. Small-world networks fall somewhere in between these two extremes as they have large clustering coefficients and small average network distances [6,9]. A small-world network is then locally similar to a regular network but globally similar to a random network. The scale-free property, on the other hand, is defined by an algebraic behavior in the probability distribution $P(k)$ of the number k of links at a node. Barabási and Albert [7] have presented a model which generates a class of scale-free networks. Their model incorporates two basic features in the evolution of the network: growth and preferential attachment. The former means that the number of nodes in the network increases with time and the latter stipulates that the probability for a new node to be connected to an existing node depends on the number of links that this node already has. A number of other models of scale-free networks have been proposed (see, for example, [10]).

Most existing works on the security of scale-free networks consider attacks on nodes rather than on links ([11,12] are among the few exceptions). We believe that attacks on links are as important for the network security as those on nodes, and therefore deserve a careful investigation. As we argue, studying the effect of attacks on links can provide an understanding to the fundamental question of why scale-free networks are typically highly efficient. Roughly, the efficiency of a scale-free network is determined by the average network distance between nodes. It has been assumed that long-range connections are responsible for the small average network distance observed in complex networks. In the Watts-Strogatz model of small-world networks, the small network distances are due to links connecting nodes that would otherwise be separated by a long distance, i.e. long-range links [6]. The range of a link l_{ij} connecting nodes i and j is defined to be the shortest distance between i and j when l_{ij} is removed [9]. The intuition is then that scale-free networks are much more sensitive to attacks on long-range than those on short-range links. We show that in fact, for many scale-free networks, the opposite is true. Thus, the small-world phenomenon in these scale-free networks is caused by short-range links.

This review is organized as follows. In Sect. 2, we will present an example of complex network that may be of broad interest: the conceptual network of English words. The topology of this network was recently studied by us [13] and we hope this example can serve to illustrate the interdisciplinary nature of research on complex networks, and how quantitative characterizations can be useful for a discipline that has traditionally been qualitative. In Sect. 3, we present a simple model to address the issue of attack-induced cascades in complex networks [14]. Ranged-based attacks on links and the origin of the small-world phenomenon in scale-free networks [15] are detailed in Sect. 4. A brief discussion is presented in Sect. 5.

2 Conceptual Network of Language

A language can be regarded as a network where words correspond to nodes of the network. We define two words in a language to be connected if they express similar concepts. The resulting network of connections among many thousands of words is potentially relevant not only for the study of the languages themselves, but also for cognitive science. This issue has recently been studied quantitatively [13] by mapping out the conceptual network of English language. In particular it has been shown that this network exhibits the small-world property.

To construct the network [13], we define the connections according to the entries of a Thesaurus dictionary. Such a dictionary gives for every entry a list of words that are conceptually similar to the entry word. For instance, for the word "nature" it lists "character", "world", "universe" etc. We define a network where each *entry* word is a node, and two nodes are connected if one of the corresponding words is listed as conceptually similar the other one, as depicted in Fig. 1. In our study we used online English Thesaurus that is available at [16], which has over 30,000 entries. The resulting network has an average of about 60 connections per node.

Despite being sparse, the conceptual network is expected to be highly clustered, because there are many sets of related words that are densely interconnected. Indeed, the numerical computation of the clustering coefficient C yields a number more than 250 times larger than the corresponding value for a random network with the same parameters (see Table I). On the other hand, because the network is sparsely connected and only words expressing similar concepts are linked, one might naively conclude that the average network distance L should be large. However, our numerical computation yields $L = 3.2$, which is very close to the value of about 2.5 of the corresponding random network (see Table I). This means that two words in the 30,000-words dictionary are connected by only *three degrees of separation*, on average. This surprisingly small L is due to words that correspond to two or more very different concepts and work as shortcuts, connecting regions of the network that would otherwise be separated by many links. In fact, less than 1 percent of the words require more than 4 steps to be reached from other words, on average. Words that require many links to be

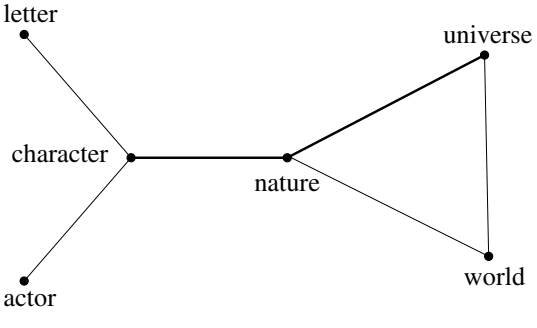

Fig. 1. Small part of the conceptual network of the English language.

Table 1. Comparison between the conceptual network defined by the Thesaurus dictionary and a random network with the same parameters. N is the total number of nodes (entry words) in the largest connected component, $\bar{k}$ is the average number of links per node, C is the clustering coefficient, and L is the average network distance.

	N	$\bar{k}$	C	L
Actual configuration	30,244	59.9	0.53	3.16
Random configuration	30,244	59.9	0.002	2.5

reached are usually very specialized, such as "appendectomy" which requires a path of length eight to be connected with "quadrillion"[4].

Therefore, the conceptual network English language is highly clustered and at the same time has a very small average network distance, *i.e.*, it is a *small-world network*. Although we have focused on a particular language (English) we expect similar results to hold of other languages as well because high clustering comes from the existence of concepts shared by more than two words and short average network distance comes from the existence of words that share meanings with otherwise unrelated words. Both features are seemingly present in many languages.

This result is potentially relevant for cognitive science. From the standpoint of retrieval of information in an associative memory, the small-world property of the network represents a maximization of efficiency. On the one hand, similar pieces of information are stored together; on the other hand, even very different pieces of information are never separated by more than a few links. The former makes searching by association possible, while the latter guarantees a fast search [17]. It is thus tempting to speculate that associative memory may have arisen partly because of a maximization of efficiency in the retrieval of information by natural selection.

For more details we refer to [13]. Different aspects of language networks have been addressed by other authors [18–22,3,23,24].

3 Attack-Induced Cascades in Complex Networks

A convenient way to address the security of a complex network is to examine how the size of the largest connected component, which is a measure of the efficiency of communication (or information flow) within the network, is reduced under random or intentional attacks. Scale-free networks are known to be sensitive to the removal of highly connected nodes [25–29]. However, the existence of a giant connected component in the network does not depend on the presence of highly connected nodes and can be present even after the removal of a significant number of nodes [29,30]. Previous studies on network security address mainly static properties. Our concern is that network architecture represents only one aspect

[4] *quadrillion* → *googol* → *infinity* → *holiness* → *purity* → *sterility* → *birth control* → *vasectomy* → *appendectomy*

of the security problem. An important question for many real-world situations is how attacks affect the functions of a network when the flow of information or other physical quantity in the network are taken into consideration. In particular, the removal of nodes changes the balance of flows and may trigger a cascading failure [31–34], as the one that happened on August 10, 1996 in the western U.S. power grid [35,36]. A simple model has been recently introduced [14] for cascades of *overload* failures in complex networks. We show that for networks where loads can redistribute among the nodes, intentional attacks on highly loaded nodes can trigger a large-scale cascade of overload failures.

Our model is defined as follows [14]. Suppose that at each time step one unit of the relevant quantity is exchanged between every pair of nodes in the network and is transmitted along the shortest paths connecting them. The load at a node is then simply the betweenness centrality [37–39], i.e. total number of shortest paths passing through the node. The capacity of a node is the maximum load that the node can handle. Since capacity is costly, it is natural to assume that the capacity C_i of node i is proportional to the initial load L_i on that node,

$$C_i = (1 + \alpha)L_i, \quad i = 1, 2, ...N, \tag{1}$$

where $\alpha \geq 0$ is the tolerance parameter, and N is the initial number of nodes. When all the nodes are connected, the entire network operates insofar as $\alpha \geq 0$. But the removal of nodes in general changes the distribution of loads. The load at a particular node can then change. If it increases and becomes larger than the capacity, the corresponding node fails. Any failure leads to a new redistribution of loads and, as a result, subsequent failures can occur. Because of the global redistribution of load, new failures may be driven by events happening far away. This cascading process can stop after a few steps but it can also propagate and shutdown a considerable fraction of the network[5]. But under what conditions can such a global cascade happen?

Our result is that global cascades occur if the network exhibits a *highly heterogeneous distribution of loads* and the removed nodes are among those with *higher load*. Otherwise, cascades are not expected. In order to understand this result, consider the removal of a single node. If the node has small load, its removal will not cause major changes in the balance of loads. However, when the load at the node is large, its removal is likely to affect significantly the loads at other nodes and possibly starts a sequence of overload failures. In networks with some degree of randomness, the distribution of loads is highly correlated with the distribution of links. In particular, networks with heterogeneous distribution of links, such as scale-free networks, are expected to be heterogeneous with respect to load as well, so that nodes with larger number of links will have higher load [38,40], on average. This results reveals another aspect of the robust-yet-fragile property of heterogeneous networks, which was first observed for the attack on *several* nodes [25]. In the case of cascades, a large damage can be caused by the attack on one or very few nodes.

[5] A different model and mechanism for overload breakdown due to networks growth has been considered in [39].

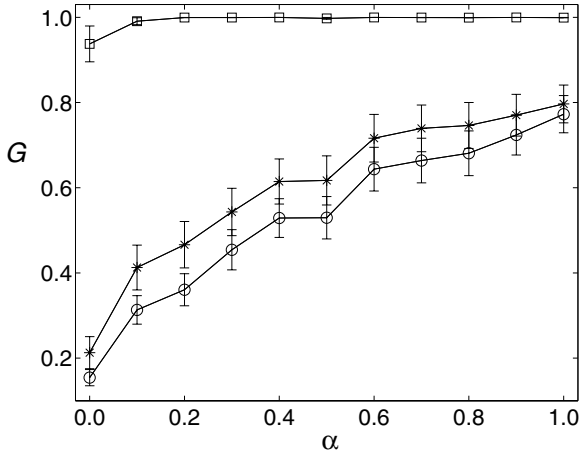

Fig. 2. Cascading failure in scale-free networks with scaling exponent $\gamma = 3$, as triggered by the removal of one node chosen at random (squares), or among those with largest connectivities (stars) or highest loads (circles). Each curve corresponds to the average over 5 triggers and 10 realizations of the network. The error bars represent the standard deviation. The number of nodes in the largest component is $5000 \leq N \leq 5100$.

We simulate cascades triggered by random failures and by intentional attacks. In the case of failures, we choose a trigger at random among all the nodes of the network. In the case of attacks, the targeted node is selected from those with highest loads or largest connectivities. We consider heterogeneous networks with scale-free distribution of links and compare them with an equivalent homogeneous configuration. To generate the networks, we start with a list of integers representing the connectivities of the nodes, i.e. the number of end-links of each node [41,15]. Next, we pick up pairs of end-links at random and connect them to form a link and repeat this process until the last pair is connected, prohibiting self- and repeated links. Let N denote the number of nodes in the largest connected component of the resulting network. The damage caused by a cascade is quantified in terms of the relative size G of the largest connected component $G = N'/N$, where N' are the number of nodes in the largest component after the cascade.

Figure 2 shows results for scale-free networks with scaling exponent $\gamma = 3$. On average, G remains close to unity in the case of random breakdowns but is significantly reduced under intentional attacks, even for α unrealistically large. This result is in agreement with intuition, because in the case of random breakdown the trigger is probably one of the many nodes with small load, while in the case of intentional attack it is a node with very large load. The damage is larger for smaller values of α, and the attack of nodes with highest loads is more destructive than the attack of nodes with largest connectivities. Figure 3 shows the corresponding results for a homogeneous network with the same number of nodes and exactly 3 links per node. In the inset we display results for scale-free

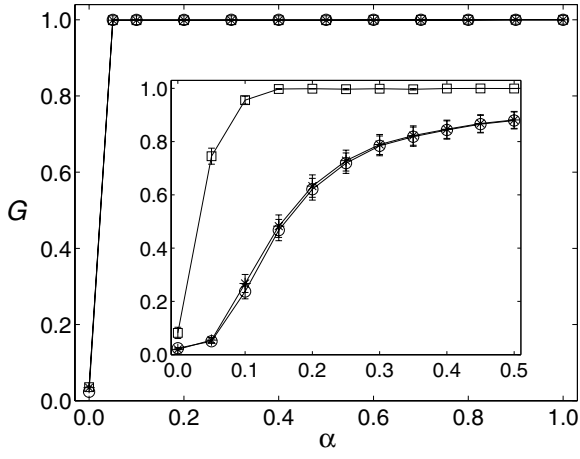

Fig. 3. Cascading failures in homogeneous networks with degree $k = 3$ and $N = 5000$. Inset: the same for scale-free networks with $\gamma = 3$, $N = 5000$, and $k \geq 2$ (different from the networks in Fig. 1, here each node has 2 or more links). The resulting average connectivity is $\langle k \rangle \approx 3.1$. The legends and other parameters are the same as in Fig. 1.

networks with about the same average number of links per node. The homogeneous network does not experience cascading failures due either to random breakdown or to intentional attacks for α as small as 0.05. For the scale-free (heterogeneous) network, cascades triggered by the attack on a key node can drastically reduce the size of the the largest connected component, as shown in the inset. Therefore, networks with homogeneous distribution of load appear to be more robust against attacks than the heterogeneous ones. This conclusion does not rely on the particular properties of these models, as the same was also observed for other classes of networks.

These findings are expected to be important for real-world networks. Indeed, many infrastructure networks have heterogeneous distribution of load and as such are expected to undergo large-scale cascades if some vital nodes are attacked, but rarely in the case of random breakdown. For details see [14].

4 Range-Based Attacks on Links in Complex Networks

The Watts and Strogatz [6] model of small-world networks identifies the small shortest paths observed in locally structured, sparse networks as being due to long-range connections, while short-range links are responsible for high clustering. This observation matches with the known results for the Erdös-Rényi model of random networks [42], where almost all links are long-range connections and the average network distance increases only logarithmically with the number N of nodes [8]. In most regular networks, on the other hand, all the links have small range and the average shortest path increases with a power of N. All these models display a relatively homogeneous distribution of connectivities. Many

real networks having very small average network distance have been identified as scale-free [7,3]. Scale-free networks are heterogeneous as their connectivity can vary significantly from node to node and a considerable number of links can be associated with a few highly connected nodes.

A recent paper [15], which we shall review here, has studied the contribution of short-range links to the shortness of the node-to-node distances in scale-free networks, by analyzing the impact of attacks on short-range links versus those on long-range links. Our results contrast with the tacit assumption that long-range connections are responsible for the small average network distance exhibited by these networks. Our findings are based on the observation that the average network distance is a global quantity which is mainly determined by links with large load.

Our attack strategy is as follows [15]. We measure the *efficiency* of the network as links are successively removed according to their ranges: (*i*) for short-range attacks, links with shorter ranges are removed first; (*ii*) for long-range attacks, links with longer ranges are removed first. The efficiency is measured by the shortest paths between pairs of nodes. A convenient quantity to characterize the efficiency is [43]

$$E = \frac{2}{N(N-1)} \sum \frac{1}{d_{ij}}, \tag{2}$$

where d_{ij} is the length of the shortest path between nodes i and j and the sum is over all $N(N-1)/2$ pairs of nodes. The network is more efficient when it has small shortest paths, which according to our definition corresponds to large E.

To be specific we consider the network model described in the previous section, where the nodes are connected randomly for a given scale-free distribution with scaling exponent γ, and self- and repeated links are prohibited. In order to have nontrivial networks in the limits of small and large γ, we bound the connectivity so that $k_{min} \leq k_i \leq k_{max}$ for $i = 1, 2, \ldots, N$, where k_{min} and k_{max} are constant integers. For $\gamma \to \infty$, the network is homogeneous as all the nodes have the same connectivity k_{min}. The distribution of connectivities becomes increasingly more heterogeneous as γ is decreased.

In randomly generated networks, nodes with larger connectivity are expected to be on average closer to each other than those with smaller connectivity [15]. More specifically, the distance d_{ij} between nodes i and j is expected to be highly correlated with the product of the connectivities k_i and k_j. This suggests that the range is also correlated with the product of the connectivities so that short-range links tend to link together highly connected nodes, while long-range links tend to connect nodes with very few links. Moreover, links between nodes with large connectivities are expected to be passed through by a large number of shortest paths (see [12]). That is, on average these links should possess a higher load [12] than those connected to nodes with few links, where the load of a link is defined as the number of shortest paths passing through the link [37,38]. These have been confirmed numerically, as shown in Fig. 4 for $\gamma = 3$. As a result, high load should be associated mainly with short-range links. Since links with higher load are expected to contribute more to the shortness of the paths between nodes,

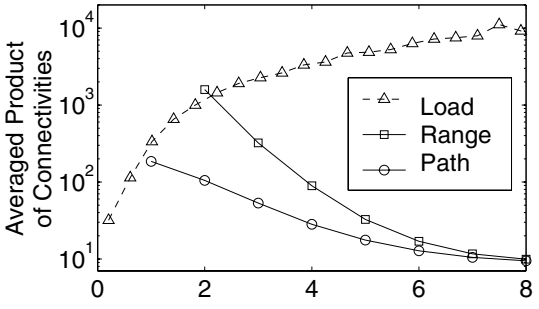

Fig. 4. Averaged product of connectivities as a function of the shortest path, range, and load for $\gamma = 3$, where the load is binned and normalized by 10^4. Each curve corresponds to the average over 10 realizations for $N = 5000$, $k_{min} = 3$, and $k_{max} = 500$.

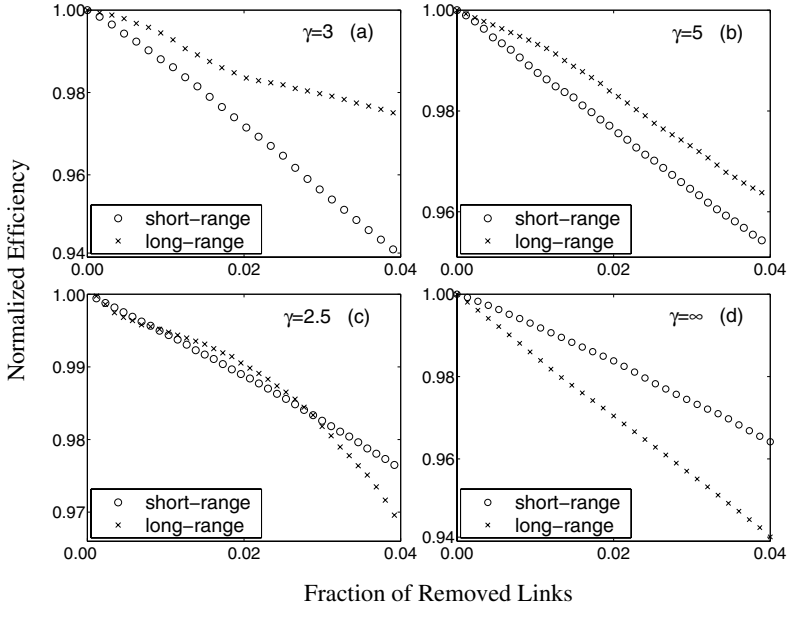

Fig. 5. Efficiency for short- and long-range attacks (normalized by the initial value) as a function of the fraction of removed links. All the parameters other than γ are the same as in Fig. 5.

such a correlation between load and range implies that attacks on short-range links are more destructive than those on long-range links.

In Fig. 5 we show the efficiency for both short- and long-range attacks, for different values of γ. Short-range attacks are clearly more destructive than long-range ones for intermediate values of γ, as shown in Figs. 5(a) and 5(b) for $\gamma = 3$ and $\gamma = 5$, respectively. The corresponding relation between the average load and range, plotted in Fig. 6 for $\gamma = 3$, confirms that higher load on links with shorter range is the mechanism underlying this phenomenon. Long-range attacks become

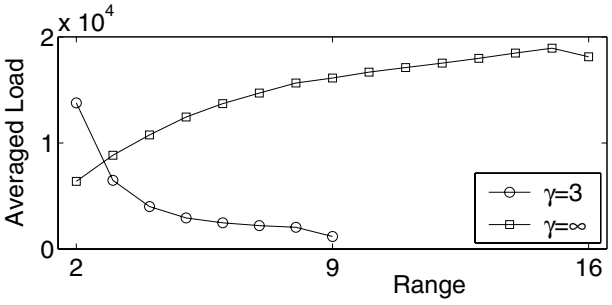

Fig. 6. Averaged load as a function of the range for $\gamma = 3$ and $\gamma = \infty$. All the parameters other than γ are the same as in Fig. 4.

more destructive only for networks with sufficiently small or large values of γ. In Figs. 5(c) and 5(d) we show the results for $\gamma = 2.5$ and $\gamma = \infty$, respectively. The exchange of the roles of attacks on short- and long-range links for networks with small values of γ is a model dependent effect due to the appearance of a densely connected subnetwork of nodes with large connectivity. For networks with large values of γ, switching of the roles of short- and long-range attacks is caused by the homogenization of the network and similar behavior has been observed in growing models of scale-free networks as well [15]. In a homogeneous network all the nodes have approximately the same connectivity. Therefore, links with higher load are precisely those between distant nodes, i.e., those with larger range, as shown in Fig. 6 for $\gamma = \infty$. Incidentally, the long-range attack is also more destructive in other homogeneous models, such as the Watts-Strogatz model and the Erdös-Rényi random model [15].

We have also considered growing models of scale-free networks [7,44]. In all the cases, short-range attack has been observed to be the most effective for scale-free networks with scaling exponent around $\gamma = 3$ [15].

5 Discussion

In this paper, we have reviewed two problems concerning attacks on and security of complex networks. The study of attacks on complex networks is important in order to identify the vulnerabilities of real-world networks, which can be used either for protection (e.g., of infrastructures) or for destruction (e.g., in the control of epidemic diseases). Additionally, it can provide guidance in designing more robust artificial networks (e.g., communication networks).

Our result on cascades in complex networks indicates that while the scale-free property makes many natural and man-made networks quite robust against to random failure of nodes, the presence of a few nodes with very large load may make the network vulnerable to a cascade of overload failures capable of disrupting the network into small fragments. Such a global cascade represents a

serious threat because it may be triggered by relatively small events and prevents an efficient communication between most nodes in the network.

We have also shown that for a wide interval of the scaling exponent around $\gamma = 3$, fairly random scale-free networks are more vulnerable to short-range attacks than long-range ones. This property results from a higher concentration of load on short-range links. Our findings have the important implication that short-range links are more important than long-range links for an efficient communication between nodes, which is the opposite to what one might expect from other classes of small-world networks. This result is potentially relevant for the spread of sexual diseases, which has been argued to take place in a scale-free network [45]. Although we have focused on scale-free networks, similar results are expected to hold for other classes of heterogeneous networks.

More details about the content of this review can be found in [13–15].

Acknowledgements

This work was supported by NSF under Grant No. ITR-0312131 and by AFOSR under Grant No. F49620-01-1-0317.

References

1. S. H. Strogatz, Nature (London) **410**, 268 (2001).
2. L. A. N. Amaral, A. Scala, M. Barthélémy, and H. E. Stanley, Proc. Natl. Acad. Sci. U.S.A. **97**, 11149 (2000).
3. R. Albert and A.-L. Barabási, Rev. Mod. Phys. **74**, 47 (2002).
4. S. N. Dorogovtsev and J. F. F. Mendes, Adv. Phys. **51**, 1079 (2002).
5. M. E. J. Newman, SIAM Rev. **45**, 167 (2003).
6. D. J. Watts and S. H. Strogatz, Nature (London) **393**, 440 (1998).
7. A.-L. Barabási and R. Albert, Science **286**, 509 (1999).
8. B. Bollobás, *Random Graphs* (Academic Press, London, 1985).
9. D. J. Watts, *Small Worlds: The Dynamics of Networks between Order and Randomness* (Princeton University Press, Princeton, 1999).
10. K. Klemn and V. M. Eguíluz, Phys. Rev. E **65**, 057102 (2002).
11. M. Girvan and M. E. J. Newman, Proc. Natl. Acad. Sci. U.S.A. **99**, 8271 (2002).
12. P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, Phys. Rev. E **65**, 056109 (2002).
13. A. E. Motter, A. P. S. de Moura, Y.-C. Lai, and P. Dasgupta, Phys. Rev. E **65**, 065102 (2002).
14. A. E. Motter and Y.-C. Lai, Phys. Rev. E **66**, 065102 (2002).
15. A. E. Motter, T. Nishikawa, and Y.-C. Lai, Phys. Rev. E **66**, 065103 (2002).
16. ftp://ibiblio.org/pub/docs/books/gutenberg/etext02/mthes10.zip
17. A. P. S. de Moura, A. E. Motter, and C. Grebogi, Phys. Rev. E **68**, 036106 (2003).
18. M. Steyvers and J. B. Tenenbaum, cond-mat/0110012 (2001).
19. R. F. I. Cancho and R. V. Solé, Proc. Royal Soc. London B **268**, 2261 (2001).
20. S. N. Dorogovtsev and J. F. F. Mendes, Proc. Royal Soc. London B **268**, 2603 (2001).
21. O. Kinouchi, A. S. Martinez, G. F. Lima, G. M. Lourenço, and S. Risau-Gusman, Physica A **315**, 665 (2002).

22. M. Sigman and G. A. Cecchi, Proc. Natl. Acad. Sci. U.S.A. **99**, 1742 (2002).
23. L. F. Costa, cond-mat/0309266 (2003).
24. P. Allegrini, P. Grigolini, and L. Palatella, cond-mat/0310648 (2003).
25. R. Albert, H. Jeong, and A.-L. Barabási, Nature (London) **406**, 378 (2000).
26. R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **85**, 4626 (2000).
27. D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).
28. R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **86**, 3682 (2001).
29. A. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata, A. Tomkins, and J. Wiener, Comput. Netw. **33**, 309 (2000).
30. A. P. S. de Moura, Y.-C. Lai, and A. E. Motter, Phys. Rev. E **68**, 017102 (2003).
31. D. J. Watts, Proc. Natl. Acad. Sci. USA **99**, 5766 (2002).
32. Y. Moreno, J. B. Gómez, and A. F. Pacheco, Europhys. Lett. **58**, 630 (2002).
33. K.-I. Goh, D.-S. Lee, B. Kahng, and D. Kim, Phys. Rev. Lett. **91**, 148701 (2003).
34. Y. Moreno, R. Pastor-Satorras, A. Vázquez, and A. Vespignani, Europhys. Lett. **62**, 292 (2003).
35. B. A. Carreras, D. E. Newman, I. Dolrou, and A. B. Poole, in: *Proceedings of Hawaii International Conference on System Sciences*, January 4-7, 2000, Maui, Hawaii.
36. M. L. Sachtjen, B. A. Carreras, and V. E. Lynch, Phys. Rev. E **61**, 4877 (2000).
37. M. E. J. Newman, Phys. Rev. E **64**, 016132 (2001).
38. K.-I. Goh, B. Kahng, and D. Kim, Phys. Rev. Lett. **87**, 278701 (2001).
39. P. Holme and B. J. Kim, Phys. Rev. E **65**, 066109 (2002).
40. M. Barthélemy, Phys. Rev. Lett. **91**, 189803 (2003).
41. M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. E **64**, 026118 (2001).
42. P. Erdös and A. Rényi, Publ. Math. Inst. Hung. Acad. Sci. **5** , 17 (1960).
43. V. Latora and M. Marchiori, Phys. Rev. Lett. **87**, 198701 (2001).
44. S. N. Dorogovtsev and J. F. F. Mendes, Phys. Rev. E **62**, 1842 (2000).
45. F. Liljeros, C. R. Edling, L. A. N. Amaral, H. E. Stanley, and Y. Aberg, Nature (London) **411**, 907 (2001).