New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
8 December 2014

ACCEPTED FOR PUBLICATION
26 January 2015

PUBLISHED
18 February 2015

PAPER

Percolation of localized attack on complex networks

Shuai Shao[1], **Xuqing Huang**[1], **H Eugene Stanley**[1] **and Shlomo Havlin**[1,2]

[1] Center for Polymer Studies and Department of Physics, Boston University, Boston, MA 02215, USA
[2] Department of Physics, Bar-Ilan University, Ramat-Gan 52900, Israel

E-mail: sshao@bu.edu

Keywords: localized attack, complex network, percolation theory, robustness of network, Erdos–Renyi network, scale-free network, generating function

Supplementary material for this article is available online

Abstract

The robustness of complex networks against node failure and malicious attack has been of interest for decades, while most of the research has focused on random attack or hub-targeted attack. In many real-world scenarios, however, attacks are neither random nor hub-targeted, but localized, where a group of neighboring nodes in a network are attacked and fail. In this paper we develop a percolation framework to analytically and numerically study the robustness of complex networks against such localized attack. In particular, we investigate this robustness in Erdős–Rényi networks, random-regular networks, and scale-free networks. Our results provide insight into how to better protect networks, enhance cybersecurity, and facilitate the design of more robust infrastructures.

The functioning of complex networks such as the internet, airline routes, and social networks is crucially dependent upon the interconnections between network nodes. These interconnections are such that when some nodes in the network fail, others connected through them to the network will also be disabled and the entire network may collapse. In order to understand network robustness and design resilient complex systems, one needs to know whether a complex network can continue to function after a fraction of its nodes have been removed either through node failure or malicious attack [1–21]. This question is dealt within percolation theory [21–24] in which the percolation phase transition occurs at some critical occupation probability p_c. Above p_c, a giant component, defined as a cluster whose size is proportional to that of the entire network, exists; below p_c the giant component is absent and the entire network collapses. Only nodes in the giant component continue to function after the node-removal process.

The robustness of complex networks under attack is dependent upon the structure of the underlying network and the nature of the attack. Previous research has focused on two types of initial attack: random attack and hub-targeted attack. In a random attack each node in the network is attacked with the same probability [1–3, 8, 10, 21]. In a hub-targeted attack the probability that high-degree nodes will be attacked is higher than that for low-degree nodes [1, 3, 4, 7, 12]. An important feature of the network structure is its degree distribution, $P(k)$, which describes the probability that a node has a specific degree k. Networks with different degree distributions behave very differently under different types of attack. For instance, the internet, which shows a power law degree distribution, is extremely robust against random attack but vulnerable to hub-targeted attack [1, 4].

However these two types of attack—random attack and hub-targeted attack—do not adequately describe many real-world scenarios in which complex networks suffer from damage that is localized, i.e., a node is affected, then its neighbors, and then their neighbors, and so on (see figure 1). Examples include the effects of earthquakes, floods, or military attacks on infrastructure networks and the effects of a computer virus or malware on computer networks. Recent occurrences of the latter include attacks carried out by cybercriminals who create a 'botnet', a cluster of neighboring 'zombie computers' in a computer network and, by using them, are able to damage the entire network. An understanding of the effect of this kind of attack on the functioning of a network is still lacking.

Here we will analyze the robustness of complex networks sustaining this kind of localized attack in order to determine how much damage a network can sustain before it collapses, i.e., to find the percolation threshold p_c.

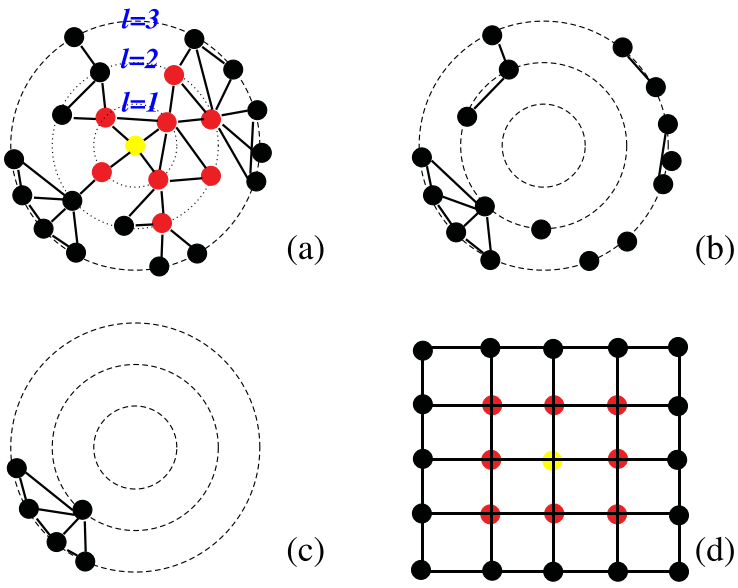

Figure 1. Schematic illustration of the localized attack process. (a) A fraction $1 - p$ of the nodes are chosen to be removed, starting from the root node, its nearest neighbors, next nearest neighbors, and so on (yellow represents the root node, red the other nodes to be removed). (b) Remove the chosen nodes and the links. An attacked 'hole' centered around the root node is formed. (c) Only nodes in the giant component (largest cluster) keep functioning and are left in the network. (d) Localized attack on regular lattice (here, square lattice). For a regular lattice with $N \to \infty$, one needs to attack all nodes in order to collapse the network, i.e., $p_c \to 0$.

We also want to predict the fraction of nodes that keep functioning after an initial attack of a fraction of $1 - p$ nodes, i.e., the relative size of the giant component (the order parameter), P_∞. Note that localized attack has been studied only on specific network structures [25] or on interdependent spatially embedded networks [26], but a general theoretical formalism for studying localized attacks on complex networks is currently missing.

Here we develop a mathematical framework for studying localized attacks on complex networks with arbitrary degree distribution and we find exact solutions for percolation properties such as the critical threshold p_c and the relative size of the giant component P_∞. In particular, we apply our framework to study and compare the robustness of three types of random networks, (i) Erdős–Rényi (ER) networks with a Poissonian degree distribution ($P(k) = e^{-\langle k\rangle}\langle k\rangle^k/k!$) [27], (ii) random-regular (RR) networks with a Kronecker delta degree distribution ($P(k) = \delta_{k,k_0}$), and (iii) scale-free (SF) networks with a power law degree distribution ($P(k) \sim k^{-\lambda}$) [5]. We find that the effect of a localized attack on an ER network is identical to that of a random attack. For an RR network, we find that the p_c of a localized attack is always smaller (i.e., more robust) than that of a random attack. However, the robustness of a SF network against localized attack is found to be critically dependent upon the power law exponent λ. Surprisingly, a critical exponent λ_c exists such that when $\lambda < \lambda_c$, for localized attack the network is significantly more vulnerable compared to random attack, with p_c being larger. While for $\lambda > \lambda_c$, the opposite is true.

Consider a random network with a degree distribution $P(k)$, which indicates the probability that a node in the network has k neighbors. The generating function of the degree distribution is defined as $G_0(x) = \sum_{k=0}^{\infty} P(k)x^k$ [28, 29]. We start from a randomly chosen 'root' node. All nodes in the random network are listed in ascending order of their distances from this root node (see figure 1(a)). The shell l is defined as the set of nodes that are at distance l from the root node [30–32]. Within the same shell, all nodes are at the same distance from the root node and are positioned randomly.

We initiate the localized attack process by removing the root node, then the nodes in the first shell, and so on. We remove nodes in the ascending order of their distances from the root node. Within the same shell we remove nodes randomly and, after nodes in shell l are fully removed, we begin removing nodes in shell $l + 1$. We continue the localized attack process until a fraction $1 - p$ of nodes in the entire network are removed. Thus a 'hole' of attacked nodes forms around the root node. The remaining p fraction of nodes in the network are those at greater distances from the root node (see figure 1(b)). After the initial removal of $1 - p$ fraction of the network nodes and all links connected to them, the remaining network fragments into connected clusters. As in percolation theory [22, 23], only nodes in the giant component (the largest cluster) are still functional. Nodes belonging to other small clusters are considered non-functional and are also removed (see figure 1(c)). Note that

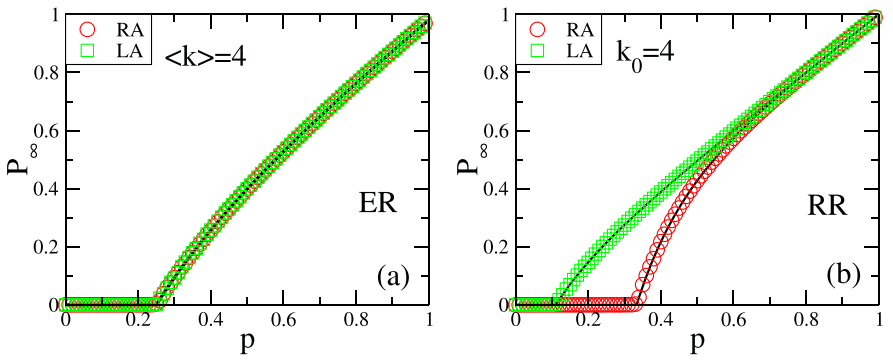

Figure 2. Percolation transitions for (a) an ER network and (b) an RR network under localized attack (LA) and random attack (RA), with network size $N = 10^6$, average degree $\langle k\rangle = 4$ in ER network, and $k_0 = 4$ in RR network. Theoretical results (solid lines) and simulations (symbols) agree well with each other. Note that the effect of localized attack and random attack on an ER network (see (a)) are identical (here, $p_c = 1/\langle k\rangle = 0.25$), while an RR network (see (b)) is more robust against localized attack compared to random attack. The value of p_c fits very well the prediction of equation (4).

for localized attack on a regular lattice, as the number of network nodes $N \to \infty$, $p_c \to 0$, i.e., one has to attack order of N nodes in the regular lattice in order to collapse the lattice (see figure 1(d)).

We find that the generating function of the degree distribution of the remaining network after the localized attack is (see supplementary information)

$$G_0^p(x) = \frac{1}{G_0(f)} G_0\left[f + \frac{G_0'(f)}{G_0'(1)}(x-1)\right], \tag{1}$$

where p is the fraction of unremoved nodes and $f \equiv G_0^{-1}(p)$. The critical probability p_c where the network collapses and the size of the giant component $P_\infty(p)$ for $p > p_c$ can be derived analytically from equation (1). The generating function of the cluster sizes in the remaining network is $H_0^p(x) = xG_0^p(H_1^p(x))$, where $H_1^p(x)$ satisfies the transcendental equation $H_1^p(x) = xG_1^p(H_1^p(x))$ and $G_1^p(x) = G_0^{'p}(x)/G_0^{'p}(1)$ [28]. By combining equation (1) and the criterion for the network to collapse [2, 3], $G_1^{'p}(1) = 1$, we find that p_c satisfies

$$G_0''\left(G_0^{-1}\left(p_c\right)\right) = G_0'(1). \tag{2}$$

The size of the giant component $S(p)$ as a fraction of the remaining network satisfies

$$S(p) = 1 - G_0^p\left(H_1^p(1)\right), \tag{3}$$

where $H_1^p(1)$ satisfies $H_1^p(1) = G_1^p(H_1^p(1))$. The relative size of the giant component as a fraction of the original network is $P_\infty(p) = pS(p)$.

We apply the above mathematical framework to three types of complex networks: ER networks, RR networks, and SF networks, and compare the results of a localized attack with those of a random attack.

For an ER network with an average degree $\langle k\rangle$, the degree distribution follows a Poissonian distribution $P(k) = e^{-\langle k\rangle}\langle k\rangle^k/k!$ and the corresponding generating function of degree distribution is $G_0(x) = e^{\langle k\rangle(x-1)}$. From equation (1) we have $G_0^p(x) = e^{p\langle k\rangle(x-1)}$, which is the same as the generating function of the degree distribution for the remaining network after a random attack. Thus the effect of a localized attack is exactly the same as that of a random attack on an ER network (see figure 2(a)), and the critical threshold is $p_c = 1/\langle k\rangle$. The size of the giant component $P_\infty(p)$ satisfies $P_\infty(p) = p(1 - e^{-\langle k\rangle P_\infty(p)})$. In an RR network each node is connected to k_0 other nodes randomly and the generating function of the degree distribution is $G_0(x) = x^{k_0}$. Using equation (2) we find that the critical threshold for a localized attack on an RR network is

$$p_c = \left(k_0 - 1\right)^{-\frac{k_0}{k_0-2}}. \tag{4}$$

Note that for an RR network under random attack the critical threshold is $p_c = (k_0 - 1)^{-1}$. Thus, for $k_0 > 2$, p_c under localized attack is always smaller than p_c under random attack (see figure 2(b)). This means that an RR network is more resilient against localized attack than against random attack. When $k_0 \gg 1$, random and localized attacks have the same critical threshold ($p_c = 1/(k_0 - 1)$), since in this limit every node is a neighbor of the root node and there is no difference between random and localized attacks. Since $\lim_{k_0\to 2} p_c = e^{-2} \approx 0.135$

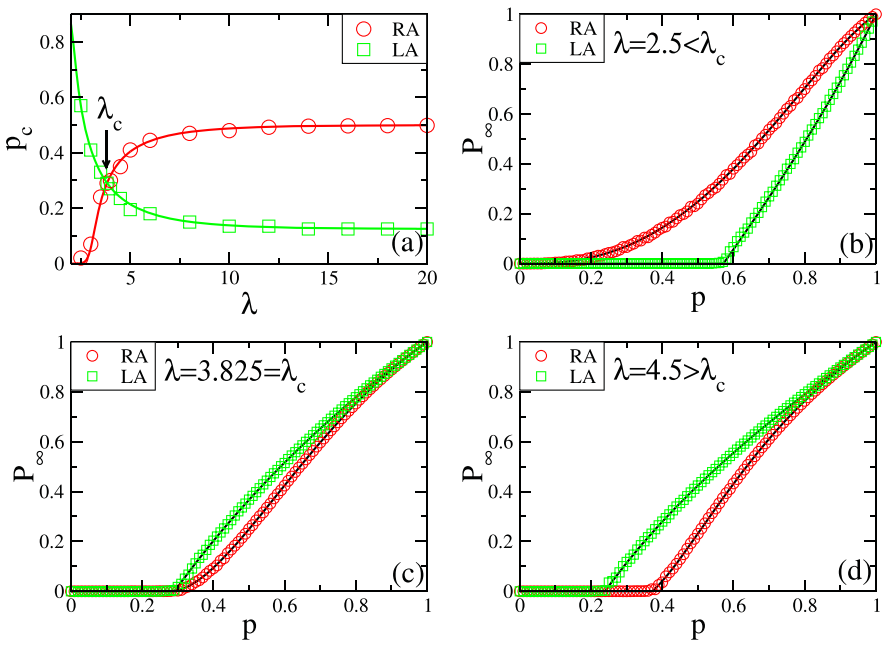

Figure 3. Percolation properties for a SF network under localized attack (LA) and random attack (RA). Solid lines are from theory (equation (1)) and symbols represent simulation results with $N = 10^6$, $m = 2$, and $\langle k\rangle = 3$. (a) Critical threshold p_c as a function of degree exponent λ. When $\lambda \to \infty$, the SF network converges to an RR network with $k_0 = \langle k\rangle = 3$, so p_c (RA) $\to 1/(k_0 - 1) = 0.5$ and p_c (LA) $\to (k_0 - 1)^{-\frac{1}{k_0-2}} = 0.125$, as confirmed in simulations. Note that for $2 < \lambda \leqslant 3$, $p_c \to 0$ in the thermodynamic limit ($N \to \infty$) for random attack [2]. (b) When $\lambda < \lambda_c$, the SF network is more vulnerable to localized attack compared to random attack. (c) When $\lambda = \lambda_c$, p_c for localized attack and for random attack are equal. (d) When $\lambda > \lambda_c$, the SF network is more robust against localized attack compared to random attack.

and $\lim_{k_0\to\infty} p_c = 0$, one can see that p_c for a localized attack on an RR network is always within the range $(0,\ e^{-2})$ for all $k_0 > 2$. For $p > p_c$, from equation (3), the relative size of the giant component $P_\infty(p)$ satisfies

$$\left(p - P_\infty(p)\right)^{\frac{1}{k_0}} - p^{\frac{1}{k_0}} = \left(p - P_\infty(p)\right)^{\frac{k_0-1}{k_0}} - p^{\frac{k_0-1}{k_0}}. \tag{5}$$

For a SF network the degree distribution is $P(k) \sim k^{-\lambda}$ $(m \leqslant k \leqslant M)$, where m and M are the lower and upper bounds of the degree, respectively, and λ is the power law exponent. The critical threshold p_c and the size of the giant component $P_\infty(p)$ are solved numerically by using the theoretical framework developed in equation (1) (see figure 3). We find that the degree heterogeneity plays an important role in the robustness of SF networks against localized attack. The critical threshold p_c and the size of the giant component $P_\infty(p)$ for the percolation transition of the SF network under localized attack depends on λ. We find that in a SF network there is a critical value λ_c below which a localized attack is significantly more severe than a random attack, but when $\lambda > \lambda_c$ a random attack is more severe. Indeed, as seen in figure 3(a), for $\lambda < \lambda_c$, p_c for a localized attack is significantly higher than for a random attack. As λ increases and the network becomes less heterogeneous, p_c decreases and the network becomes more robust against localized attacks. The specific value of λ_c depends on other parameters, such as m, M, and $\langle k\rangle$. In figures 3(b)–(d), we plot the size of the giant component $P_\infty(p)$ as a function of p and compare the results of a localized attack with those of a random attack. One intuitive explanation for the dependence of network robustness on λ is that, on the one hand, there is a higher probability that higher degree nodes will be within the attacked hole, which accelerates the fragmentation of the SF network; on the other, only nodes on the surface of the attacked hole are connected to the remaining network and contribute to its breakdown, which mitigates the fragmentation process. The total impact of the localized attack is the result of the competition between these two effects. As λ increases and the SF network becomes less heterogeneous, the first effect becomes less dominant and the network becomes more robust. Our analytical analysis shows that for an ER network these two effects always compensate each other and yield equal effects from both localized attack and random attack. For an RR network, on the other hand, the degrees are all the same and therefore only the second effect exists, and the underlying network becomes more robust against localized attack than against random attack.

We also investigate the robustness of real-world networks against localized attack and random attack using a peer-to-peer computer network [33] and a global airline route network [34]. The real-world data proves the feasibility of our model, as shown in supplementary information.

To conclude, we have developed a mathematical framework for studying the percolation of localized attacks on complex networks with an arbitrary degree distribution. Using generating function methods, we have solved exactly for the percolation properties of random networks under localized node removal. Our results show that the effects of localized attack and random attack on an ER network are identical. While a RR network is more robust against localized attack than against random attack, the robustness of a SF network depends on the heterogeneity of the degree distribution. When $\lambda < \lambda_c$, the SF network is found to be significantly more vulnerable with respect to localized attack compared to random attack. When $\lambda > \lambda_c$, the opposite is true. Our results can provide insight into understanding the robustness of complex systems and facilitate the design of resilient infrastructures.

Acknowledgments

We wish to thank ONR (Grant N00014-09-1-0380, Grant N00014-12-1-0548, Grant N62909-14-1-N019), DTRA (Grant HDTRA-1-10-1-0014, Grant HDTRA-1-09-1-0035), NSF (Grant CMMI 1125290), the European MULTIPLEX, CONGAS and LINC projects, DFG, the Next Generation Infrastructure (Bsik) and the Israel Science Foundation for financial support. We also thank the FOC program of the European Union for support.

References

[1] Albert R, Jeong H and Barabási A L 2000 *Nature* **406** 6794
Albert R, Jeong H and Barabási A L 2000 *Nature* **406** 378
[2] Cohen R, Erez K, ben-Avraham D and Havlin S 2000 *Phys. Rev. Lett.* **85** 4626
[3] Callaway D S, Newman M E J, Strogatz S H and Watts D J 2000 *Phys. Rev. Lett.* **85** 5468
[4] Cohen R, Erez K, ben-Avraham D and Havlin S 2001 *Phys. Rev. Lett.* **86** 3682
[5] Barabási A L and Albert R 2002 *Rev. Mod. Phys.* **74** 47
[6] Derényi I *et al* 2005 *Phys. Rev. Lett.* **94** 160202
[7] Gallos L *et al* 2005 *Phys. Rev. Lett.* **94** 188701
[8] Newman M E J 2010 *Networks: an Introduction* (Oxford: Oxford University Press)
[9] Bashan A, Parshani R and Havlin S 2011 *Phys. Rev.* E **83** 051127
[10] Buldyrev S V *et al* 2010 *Nature* **464** 1025
[11] Parshani R, Buldyrev S V and Havlin S 2010 *Phys. Rev. Lett.* **105** 048701
[12] Huang X, Gao J, Buldyrev S V, Havlin S and Stanley H E 2011 *Phys. Rev.* E **83** 065101
[13] Bashan A, Bartsch R P, Kantelhardt J W, Havlin S and Ivanov P C 2012 *Nat. Commun.* **3** 702
[14] Gao J, Buldyrev S V, Havlin S and Stanley H E 2011 *Phys. Rev. Lett.* **107** 195701
[15] Gao J, Buldyrev S V, Stanley H E and Havlin S 2012 *Nat. Phys.* **8** 40
[16] Gao J, Buldyrev S V, Stanley H E, Xu X and Havlin S 2013 *Phys. Rev.* E **88** 062816
[17] Brummitt C D, D'Souza R M and Leicht E A 2012 *Proc. Natl Acad. Sci.* **109** 680
[18] Baxter G J, Dorogovtsev S N, Goltsev A V and Mendes J F F 2012 *Phys. Rev. Lett.* **109** 248701
[19] Peixoto T P and Bornholdt S 2012 *Phys. Rev. Lett.* **109** 118703
[20] Shang Y, Luo W and Xu S 2011 *Phys. Rev.* E **84** 031113
[21] Cohen R and Havlin S 2010 *Complex Networks, Structure, Robustness and Function* (Cambridge: Cambridge University Press)
[22] Bunde A and Havlin S 1991 *Fractals and Disordered Systems* (Berlin: Springer)
[23] Stauffer D and Aharony A 1994 *Introduction to Percolation Theory* (Boca Raton, FL: CRC Press)
[24] Coniglio A 1982 *J. Phys. A: Math. Gen.* **15** 3829
[25] Neumayer S, Zussman G, Cohen R and Modiano E 2009 *INFOCOM IEEE* 1566–74
[26] Berezin Y, Bashan A, Danziger M M, Li D and Havlin S 2013 arXiv: 1310.0996
[27] Bollobás B 1985 *Random Graphs* (London: Academic)
[28] Newman M E J, Strogatz S H and Watts D J 2001 *Phys. Rev.* E **64** 026118
[29] Molly M and Reed B 1995 *Random Struct. Algorithms* **6** 161
[30] Kalisky T, Cohen R, Mokryn O, Dolev D, Shavitt Y and Havlin S 2006 *Phys. Rev.* E **74** 066108
[31] Shao J, Buldyrev S V, Braunstein L A, Havlin S and Stanley H E 2009 *Phys. Rev.* E **80** 036105
[32] Newman M E J 2002 *Phys. Rev.* E **66** 016128
[33] Stanford Large Network Collection, Internet peer-to-peer network data. http://snap.stanford.edu/data/.
[34] Openflight.org, Airport network data. http://openflight.org/data.html.