SCIENTIFIC REPORTS

OPEN

SUBJECT AREAS:

COMPLEX NETWORKS

PHASE TRANSITIONS AND CRITICAL PHENOMENA

Received
10 November 2014

Accepted
3 February 2015

Published
11 March 2015

Correspondence and requests for materials should be addressed to Y.B. (bereziny@gmail.com)

Localized attacks on spatially embedded networks with dependencies

Yehiel Berezin[1], Amir Bashan[2], Michael M. Danziger[1], Daqing Li[3,4] & Shlomo Havlin[1]

[1]Department of Physics, Bar Ilan University, Ramat Gan 52900, Israel, [2]Channing Division of Network Medicine, Brigham and Women's Hospital and Harvard Medical School, Boston, MA, USA, [3]School of Reliability and Systems Engineering, Beihang University - Beijing 100191, China, [4]Science and Technology on Reliability and Environmental Engineering Laboratory - Beijing 100191, China.

Many real world complex systems such as critical infrastructure networks are embedded in space and their components may depend on one another to function. They are also susceptible to geographically localized damage caused by malicious attacks or natural disasters. Here, we study a general model of spatially embedded networks with dependencies under localized attacks. We develop a theoretical and numerical approach to describe and predict the effects of localized attacks on spatially embedded systems with dependencies. Surprisingly, we find that a *localized* attack can cause substantially more damage than an equivalent *random* attack. Furthermore, we find that for a broad range of parameters, systems which appear stable are in fact metastable. Though robust to random failures—even of *finite* fraction—if subjected to a localized attack larger than a critical size which is independent of the system size (i.e., a *zero* fraction), a cascading failure emerges which leads to complete system collapse. Our results demonstrate the potential high risk of localized attacks on spatially embedded network systems with dependencies and may be useful for designing more resilient systems.

Many modern critical infrastructures are embedded in two dimensional space[1–5]. Examples include ground transportation systems like road and railway networks, electrical power networks, gas and oil pipelines, water supply, the internet and communication lines. The main feature of these spatial networks is that their links represent real physical connections (connectivity links), where link length is relatively short compared to the system size. With the ongoing technological development, these systems have become more and more integrated and interdependent (via dependency links) upon each other. These dependencies lead to substantially increased vulnerability of spatial as well as non-spatial networks to random failures and even first order transitions which are characterized by the emergence of cascading failures[6–21]. However, failures in spatially embedded systems are often not random but geographically localized. These "localized attacks" can be caused by natural disasters (e.g., the 2011 Tōhoku earthquake and tsunami) or malicious attacks (e.g., weapons of mass destruction). The resilience of a complex system with dependencies under attack of this sort, which we call "localized attack," has not been addressed before.

Even though different infrastructure systems have their own specific function and dynamics, they share a 2D spatial embedding that implies a fundamental restriction on their structure due the length limitation of connectivity and dependency links. Therefore we study here the general vulnerability of spatially embedded systems under localized attacks. We find here that localized attacks on spatially embedded systems with dependencies are significantly more damaging than random failures (see Fig. 1a), in marked contrast to single networks.

Furthermore, we discover a metastable phase which spans a broad range of parameters and is qualitatively different from the stable and unstable phases known to percolation theory. In metastable systems, there exists a critical damage size with radius r_h^c, above which localized damage will spread and destroy the entire system and below which the damage will remain in place (see Fig. 1a and 1c). This critical size is determined solely by intensive system quantities and thus, in marked contrast to random failures, it does not scale with system size and constitutes a *zero-fraction* of the system in the limit of large systems ($N \rightarrow \infty$) (Fig. 1d).

To our knowledge, this is the first study to consider geographically localized attacks from the perspective of percolation theory. Previous research using percolation theory has studied the effects of attacks targeting nodes with special topological properties such as degree but not geographically correlated attacks[22–25]. Geographic localized attacks have been utilized to identify the most vulnerable parts of specific infrastructure networks[26–28] but have not been studied in a general percolation framework. Cascading failures have been studied as the outcome of specific dynamic models: load-shedding[29], binary decisions with fractional

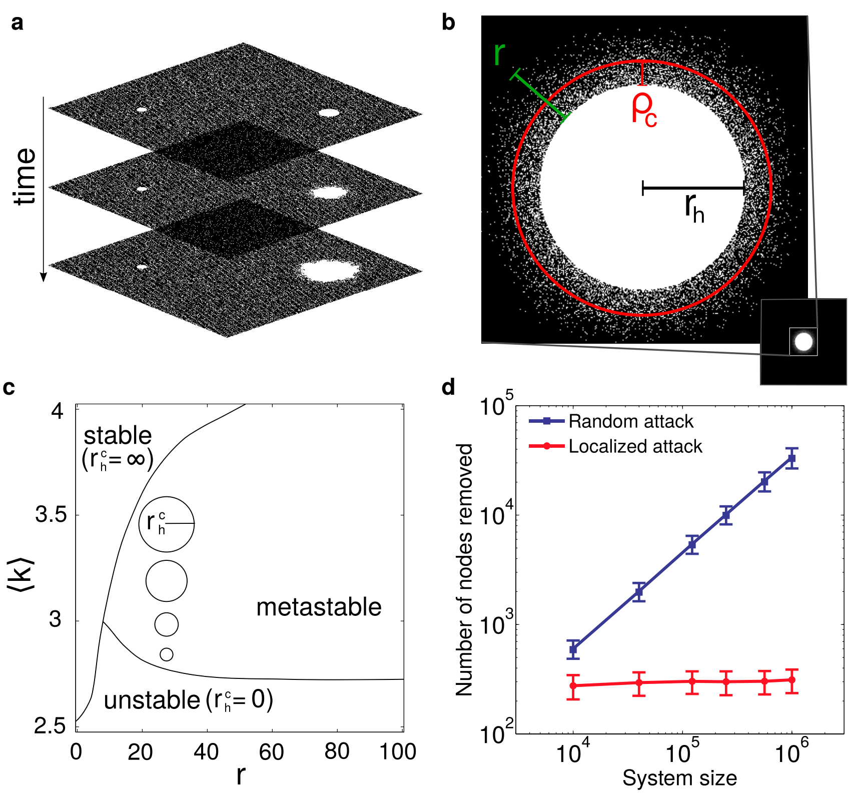

Figure 1 | The effect of a localized attack on a system with dependencies. (a), Propagation of local damage in a system of two interdependent diluted lattices with spatially constrained dependency links between the lattices (only one lattice shown here). The hole on the right is above the critical size r_h^c and spreads throughout the system while the hole on the left is below r_h^c and remains essentially the same size. (b), A localized circular failure of radius r_h in a lattice with dependency links of length up to r. Outside the hole, the survival probability of a node increases with the distance ρ from the edge. The parameter ρ_c denotes the distance from the edge of the hole at which the occupation probability is equal to the percolation threshold of a lattice without dependencies $p_c \approx 0.5927$[36]. (c), Phase diagram of a lattice with dependencies or two interdependent lattices. Depending on the average degree $\langle k \rangle$ and dependency length r, the system is either stable, unstable or metastable. The circles illustrate the increase (when $\langle k \rangle$ increases) of the critical attack size (r_h^c) that leads to system collapse in the metastable region. (d), As the system size grows, the minimal number of nodes which cause the system to collapse increases linearly for random attacks but stays constant ($\approx$300) for localized attacks. This figure was obtained for a system of interdependent lattices diluted to $\langle k \rangle \approx 2.9$ and $r = 15$ (in the metastable phase-see c), with 1000 runs for each data point.

thresholds[30], and betweenness-based loads[31,32]. Recently, it was shown that a new kind of cascading failure emerges from percolation on interdependent networks[12–19,33]. However, these studies considered random attacks only. The unique cascading failures that we describe here have not been observed before. Indeed, they can only arise when the more realistic features of spatial embedding, dependencies and localized attacks are considered together.

Though many of the models for complex systems with dependencies assume dependencies between networks, it has been shown that similar effects are present in a single network composed of connectivity and dependency links[34–37]. Here, we treat dependency as a general property and examine cascading failures triggered by localized attacks within a single network as well as between networks.

When considering spatially embedded networks, the dimension of a network is a fundamental quantity to characterize its structure and basic physical properties[39]. On the basis of universality principles, all single network models with links of a characteristic length, embedded in a space of the same dimension, have the same percolation behavior[38]. Therefore, any 2D network with a characteristic link length belongs to the same universality class as regular lattices. When dependency links are introduced, the critical behavior is additionally determined by the length of the dependency link[17]. For tractability, the theory presented in this work is based on 2D lattices. However, the effects of localized attacks on systems with dependencies are expected to be the same for any system embedded in 2D space as illustrated with the European power grid[40] in Sup. Fig. 2 and synthetic power grids[41,42] in Supplementary Figs. 1–4.

We model spatially embedded systems via square lattices diluted to degree $2.5 \leq \langle k \rangle \leq 4$. The dependencies between nodes are constrained to be less than a distance r (in lattice units) and can be taken across networks or within a single network. See *Methods* for details of system construction.

The localized geographical attack is modeled by the removal of all nodes within a distance r_h from a random location in the system (see Fig. 1a–b). This triggers a cascade in which the nodes that depend on the removed nodes fail, triggering further losses as more nodes get cut off from the largest connected component. This percolative damage triggers further damage due to the dependencies between the nodes. This process is continued iteratively until no more nodes fail. At the end of this cascade, the system is categorized as functional or non-functional depending on whether a largest connected component of the order of the system size N remains or not.

Results

We discover that the k–r plane can be divided into three distinct phases as shown in Fig. 1c. In the stable phase, no matter how large r_h is (as long as it is finite) the damage will remain localized and the system will stay intact. In the unstable phase, the system spontaneously collapses even with $r_h = 0$ (no localized attack). In this phase, low $\langle k \rangle$ and dependencies lead to the spontaneous emergence of holes which overwhelm the system. Between these phases, the system is metastable. If a hole smaller than r_h^c is removed, the system remains intact. However, if a hole of size $\geq r_h^c$ is removed, it will trigger a cascade which destroys the entire system. This cascade is characterized by the spread of damage from the initial localized attack throughout the system (Fig. 1a, b). This metastability is analogous to the well known supercooling property of water in which water can be cooled well below its freezing point and remain in the liquid state until a disturbance triggers crystallization of a critical size and it turns to ice[44].

For a system in the metastable phase under *random* attack, the number of nodes required to trigger system collapse increases linearly with the system size (See Fig. 1d). Therefore, as $N \rightarrow \infty$, metastable systems are robust to the removal of $O(N)$ nodes, as long as they are removed randomly. However, if the attack is *localized*, the number of nodes required remains constant (Fig. 1d) and even a zero fraction removed can trigger a cascading failure which destroys the system. Thus increasing the size of the system does not increase its resilience with respect to localized attacks. We find similar results for both interdependent networks and single networks composed of connectivity and dependency links. The results presented in the main text were obtained from interdependent networks and comparison to single networks with connectivity and dependency links is shown in Supplementary Fig. 1.

Predicting the value of r_h^c for a given system is an important question which is treated below theoretically and numerically, with good agreement.

Simulations. We find that r_h^c is entirely determined by the average degree $\langle k\rangle$ and the maximal dependency link length r. These are intensive system quantities and therefore r_h^c does not grow with system size (Fig. 1d). Figs. 2c and 2d show how the critical damage size r_h^c changes with respect to $\langle k\rangle$ and r for a system of size $L \times L = 1000 \times 1000$. In Fig. 2c we can see that the metastable region covers a wider range of $\langle k\rangle$ values when r increases. In the metastable phase, for every r, r_h^c increases with $\langle k\rangle$ and jumps up dramatically at a certain $\langle k\rangle$ value which represents the end of the metastable phase and the beginning of the stable phase. Furthermore, we see that this jump occurs at larger $\langle k\rangle$ values for larger r values (Fig. 2c). In Fig. 2d, we see that above a certain minimum value, r_h^c has an approximately linear dependence on r in the metastable region. This is due to the fact that a larger r means that a given node's dependency link can be located farther away. Thus the secondary damage from the localized attack is more dispersed and a larger attack size is required to initiate a cascade. Furthermore, we find that the critical damage size r_h^c takes a minimal value and the system is most susceptible to small local attacks when r is near the stable phase. Extensive numerical simulations of r_h^c over a high resolution grid of parameters $\langle k\rangle$ and r is shown in Fig. 2a and the theoretical prediction which is in good agreement is given in Fig. 2b. The theoretical description of the effect of $\langle k\rangle$ and r on r_h^c is presented below.

Theory. Since the metastable region spreads over a wide range of realistic values of r and $\langle k\rangle$, it is of great interest to understand how this transition takes place and to develop a theory to predict the value of $r_h^c(r,\langle k\rangle)$. To do so, we first consider in detail the chain of events triggered by the geographically localized damage. When a hole of r_h is removed from the system, it can directly disable nodes up to a distance r from its edge due to the existence of dependency links of length $\leq r$ (see Fig. 1b). The probability that a given node was dependent on one of the removed nodes is highest at the edge of the hole and monotonously decreases with the distance from the edge, until it equals zero at distance r. To calculate this decrease, we need to calculate the probability that a node i depends on a node which was removed in the localized attack (cf. Fig. 1b). This probability is determined by the area of intersection of two circles: the localized attack (with radius r_h) and the circle of maximal dependence (with radius r and center i). Taking ρ as the distance from the edge of the hole, the gradient of occupation probability following an attack can be evaluated as

$$p(\rho,r,r_h,\langle k\rangle)=p_s(\langle k\rangle)\frac{I(r_h,r,\rho)}{\pi r^2} \tag{1}$$

where $p_s(\langle k\rangle)$ is the occupation concentration before the attack and $I(r_h,\, r,\, \rho)$ is the standard formula for the area of intersection of two circles of radius r and r_h with centers located a distance $\rho + r_h$ from each other. This probability describes a lattice concentration gradient in the form of an annulus of width r surrounding the removed hole, see Fig. 1b. For a given set of system parameters $(r,\, r_h,\, \langle k\rangle)$ we can set $p(\rho)$ on the LHS of Eq. (1) to p_c of the lattice and solve for ρ. If a solution in the region of interest $(0 < \rho < r)$ exists, it corresponds to a distance ρ_c at which the lattice concentration will be equal to its critical value. The existence of such a point is a necessary but not sufficient condition for the hole to propagate. Below p_c, the network forms clusters with a characteristic size $\xi_<(p)$, which diverges at p_c, where $\xi_<(p)$ is the connectedness correlation length for $p < p_c$[38,45]. Hence the sufficient condition for damage propagation is that the critical region $0 < \rho < \rho_c$ be wide enough for clusters of size $\xi_<(p)$ to form and break away.

The value of $\xi_<(p)$ is determined by the underlying topology and can thus be calculated from the percolation problem on a lattice without dependencies using an appropriate estimation for p in the $0 < \rho < \rho_c$ region. From Eq. (1), $p(\rho)$ increases monotonically over this region and an accurate evaluation solution for $\xi_<$ would require treating the full gradient percolation problem[46]. In this work, for simplicity we assume $p=\bar{p}$ which is the average of $p(\rho)$ over the region of interest. Additionally, the removal of the hole causes secondary damage due to dependencies in the annulus and the concentration of the gradient is decreased by a factor of $g(r)$ which we calculate numerically and find to vary monotonically from 0.85 to 0.89 as a function of r. We can thereby estimate $\bar{p}\approx g(r)\int_0^{\rho_c} p(\rho)d\rho$. We evaluate $\xi_<$ following[38] as:

$$\xi_<^2=\frac{1}{N_p}\sum_{(i,j)}\left|\mathbf{r}_i-\mathbf{r}_j\right|^2 \tag{2}$$

where $(i,\, j)$ refers to nodes i and j which are in the same connected component, r_i is the coordinate and, N_p is the total number of such pairs of nodes. In order for the hole to propagate, the clusters which are of typical size $\xi_<$, need to be smaller than ρ_c. Therefore, the critical hole size (r_h^c) for any system is obtained from the self-consistent solution of

$$\xi_< = \rho_c \tag{3}$$

where both sides are functions of r, r_h and p_s. Using these considerations, we can predict r_h^c for every set of $(k,\, r)$ parameters as shown in Fig. 2b. These theoretical results are in close agreement with the numerical simulations (Fig. 2a) for the value of r_h^c as well as its lack of scaling with system size (Fig. 1d). Though the above method for calculating r_h^c is accurate only for systems of diluted lattices, the effects of local attacks on more realistic topologies are the same as shown on the UCTE European power grid[40] and on synthetic power grids[41] in Supplementary Figs. 2–4.

Discussion

Everything about the scenario described above is local: nodes can have dependency links only up to length r, the connectivity links are tied to an underlying lattice structure with characteristic length of one unit in the model or are limited by length-cost in the real world system and the attack is restricted to a hole of finite radius r_h. However, for a wide range of system parameters, this leads to a catastrophic cascade which destroys the entire system.

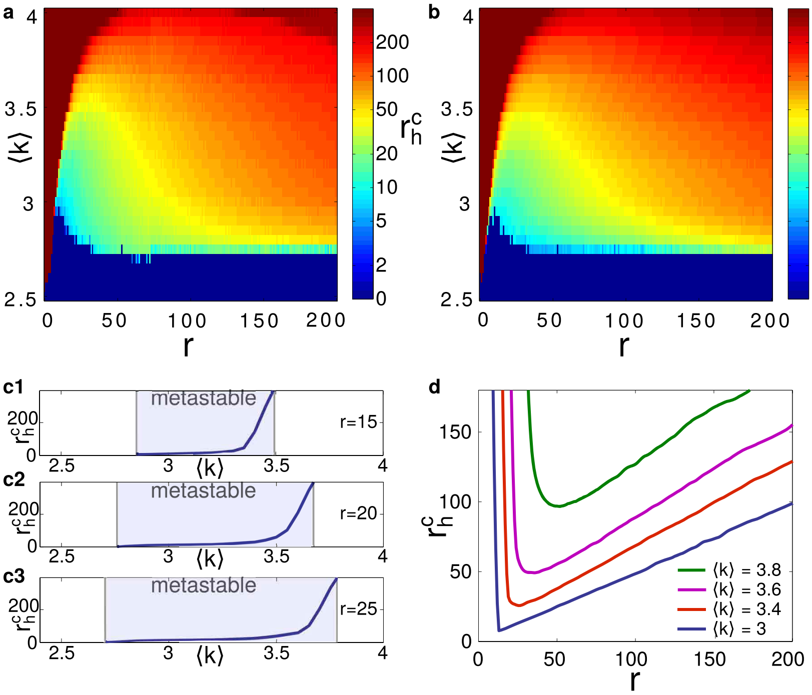

Figure 2 | Dependence of the critical attack size r_h^c on the average degree $\langle k\rangle$ and the system dependency length *r*. (a, b), The value of r_h^c as a function of the dependency length *r* and average degree $\langle k\rangle$ represented as a log-scaled colormap. (a), Simulation results. We use a binary search algorithm to find the critical radius size, ie, the minimal r_h for which the local attack spreads through the entire system. (b), Analytical results. The critical size is calculated as the smallest value of r_h for which Eq. (3) has a self-consistent solution. For a numerical comparison between the simulation and analytical results in the metastable phase, see Supplementary Fig. 5. (c1, c2, c3), Critical attack size r_h^c as a function of average degree $\langle k\rangle$ for three *r* values, determined by simulations. The curves represent moving along vertical lines from bottom to top in (a) (cf. the circles in Fig. 1c). The shaded region represents the metastable region of $\langle k\rangle$ for each *r*. The area to the left of the shaded region is unstable and to the right is stable. (d), Critical attack size r_h^c as a function of system dependency length *r* for several $\langle k\rangle$ values, determined by simulations. The minimum of each curve represents the dependency length for which the system is most vulnerable to localized attacks. The numerical results in this figure were generated using a system of two interdependent diluted lattices. For comparison with a single diluted lattice composed of both, connectivity and dependency links, see Supplementary Information Fig. 1.

It is instructive to compare this process to a single spatially embedded network without dependencies. If a hole of any finite size is created in a lattice or other spatially embedded network, it will have no effect on the overall system robustness. Only the trivial case of r_h approaching the system size L leads to system collapse. A similar argument holds with respect to dependency links which are not restricted in length. If a hole of size r_h (mass $\sim r_h^2$) is removed from one network, it will lead to *random* removal of a fraction $\sim r_h^2/N$ in the other network. Therefore, in the limit of large systems, the numerator remains constant while the denominator tends to infinity and we find that here too the localized attack will have negligible impact. Only when the dependency links are of limited length does this unique phenomenon arise.

Surprisingly, the localization of dependency opens the door for the spreading phenomenon which amplifies the local damage and leads to total system collapse. When a hole of radius r_h is removed from the system, the nodes that depended on them must be within a distance r of the hole. Thus the secondary damage is highly concentrated around the edge of the hole, leading to the creation of a damage front which propagates outwards, step by step. This is why the amount of damage caused per node removed is substantially higher when the damage is localized as compared with random removal (Fig. 1d). If $r \to \infty$ or $r \to 0$, this weakness would not exist because the secondary damage would spread everywhere uniformly or remain in place, respectively.

Paradoxically, the highly localized topology of embedded interdependent networks enables relatively small localized attacks to cause catastrophic global damage. These results have profound implications for the role of network topology in the design of resilient infrastructures.

We note that after the submission of this manuscript, an analytical framework to study localized attacks on non-embedded networks was developed by Shao et al.[43]

Methods

On the basis of universality principles, the theoretical analysis and specific predictions for r_h^c presented in this work are based on a lattice model. To make the model more realistic while maintaining its solvability, we have diluted the lattices from the standard square lattice ($k = 4$) to lower values of $\langle k\rangle$. The range of $\langle k\rangle$ values studied here is based on empirical studies of power grids which have found a mean degree of $2.5 \le \langle k\rangle \le 3$[42]. This dilution is carried out by removing a given fraction of nodes from the system and allowing the percolative process to reach a steady state, including the effects of the dependencies. This dilution process is equivalent to the percolation problem on interdependent spatially embedded networks[17].

Dependencies can be constructed between networks or within a network. We model dependencies between spatially embedded networks by overlaying two diluted square lattices A and B of size $L \times L$ with periodic boundary conditions on the same Cartesian plane. Each node in network A is dependent upon a node in network B (and vice versa) which is chosen at random from all of the nodes within a radius r. If a node in A is dependent on a node in B, the failure of the node in B will cause the node in A to fail immediately and vice versa. These dependency relationships are taken to be mutual to prevent a single failure from propagating through the entire system[16]. The numerical results in this paper were generated in this manner. The lattice size was $L = 1000$ ($N = 10^6$), $\langle k\rangle$ was sampled in intervals of 0.05 and r sampled in intervals of one lattice unit.

We obtain the same results via constructing dependencies between nodes on a single network in the following way. For each node i, a random node j within a radius r from i is selected and the two nodes are taken to be mutually interdependent. The exposition of the theory above describes the effects of dependencies of either type. The numerical results are essentially the same, see Supplementary Fig. 1 for a detailed comparison.

1. Barthélemy, M. Spatial networks. *Phys. Rep.* **499**, 1–101 (2011).
2. Rinaldi, S., Peerenboom, J. & Kelly, T. Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE* **21**, 11–25 (2001).

3. Peerenboom, J. & Fischer, R. Analyzing Cross-Sector Interdependencies. Paper presented at *HICSS 2007:40th Annual Hawaii International Conference on System Sciences, 2007, Hawaii*. doi:10.1109/HICSS.2007.78.
4. Rosato, V. *et al.* Modelling interdependent infrastructures using interacting dynamical models. *Int. J. of Crit. Infrastruc.* **4**, 63 (2008).
5. Helbing, D. Globally networked risks and how to respond. *Nature* **497**, 51–59 (2013).
6. Albert, R., Jeong, H. & Barabási, A.-L. Error and attack tolerance of complex networks. *Nature* **406**, 378–382 (2000).
7. Ben-Naim, E., Frauenfelder, H. & Toroczkai, Z. *Complex networks*, vol. **650** (Springer, 2004).
8. Caldarelli, G. & Vespignani, A. *Large Scale Structure and Dynamics of Complex Networks: From Information Technology to Finance and Natural Science (Complex Systems and Interdisciplinary Science)* (World Scientific Publishing Company, 2007).
9. Dorogovtsev, S. N., Goltsev, A. V. & Mendes, J. F. F. Critical phenomena in complex networks. *Rev. Mod. Phys.* **80**, 1275–1335 (2008).
10. Newman, M. *Networks: an introduction* (OUP Oxford, 2010).
11. Cohen, R. & Havlin, S. *Complex Networks: Structure, Robustness and Function* (Cambridge University Press, 2010).
12. Buldyrev, S. V. *et al.* Catastrophic cascade of failures in interdependent networks. *Nature* **464**, 1025–1028 (2010).
13. Leicht, E. A. & D'Souza, R. M. Percolation on interacting networks. *ArXiv e-prints* (2009) 0907.0894.
14. Vespignani, A. Complex networks: The fragility of interdependency. *Nature* **464**, 984–985 (2010).
15. Baxter, G. J. *et al.* Avalanche Collapse of Interdependent Networks. *Phys. Rev. Lett.* **109**, 248701 (2012).
16. Gao, J. *et al.* Networks formed from interdependent networks. *Nature Phys.* **8**, 40–48 (2012).
17. Li, W. *et al.* Cascading Failures in Interdependent Lattice Networks: The Critical Role of the Length of Dependency Links. *Phys. Rev. Lett.* **108**, 228702 (2012).
18. Bashan, A. *et al.* The extreme vulnerability of interdependent spatially embedded networks. *Nature Phys.* **9**, 667–672 (2013).
19. Zhao, K. & Bianconi, G. Percolation on interacting, antagonistic networks. *J. Stat. Mech. Theor. Exp.* **2013**, P05005 (2013).
20. Radicchi, F. & Arenas, A. Abrupt transition in the structural formation of interconnected networks. *Nature Phys.* **9**, 717–720 (2013).
21. Reis, S. D. S. *et al.* Avoiding catastrophic failure in correlated networks of networks. *Nature Phys.* **10**, 762–767 (2014).
22. Cohen, R. *et al.* Resilience of the Internet to Random Breakdowns. *Phys. Rev. Lett.* **85**, 4626–4628 (2000).
23. Callaway, D. S. *et al.* Are randomly grown graphs really random? *Phys. Rev. E* **64**, 041902 (2001).
24. Gallos, L. K. *et al.* Stability and Topology of Scale-Free Networks under Attack and Defense Strategies. *Phys. Rev. Lett.* **94**, 188701 (2005).
25. Schneider, C. M. *et al.* Mitigation of malicious attacks on networks. *Proc. Natl. Acad. Sci. U.S.A.* **108**, 3838–3841 (2011).
26. Neumayer, S. *et al.* Assessing the impact of geographically correlated network failures. Paper presented at *Military Communications Conference, 2008, San Diego*. doi:10.1109/MILCOM.2008.4753111 (2008).
27. Agarwal, P. K. *et al.* The resilience of WDM networks to probabilistic geographical failures. *Networking, IEEE/ACM Transactions on* **21**, 1525–1538 (2013).
28. Neumayer, S. *et al.* Assessing the vulnerability of the fiber infrastructure to disasters. *Networking, IEEE/ACM Transactions on* **19**, 1610–1623 (2011).
29. Dobson, I. *et al.* An initial model for complex dynamics in electric power system blackouts. Paper presented at *2001 47th Hawaii International Conference on System Sciences, Hawaii* doi:10.1109/HICSS.2001.926274.
30. Watts, D. J. A simple model of global cascades on random networks. *Proc. Natl. Acad. Sci. U.S.A.* **99**, 5766–5771 (2002).
31. Motter, A. E. & Lai, Y.-C. Cascade-based attacks on complex networks. *Phys. Rev. E* **66**, 065102 (2002).
32. Crucitti, P., Latora, V. & Marchiori, M. Model for cascading failures in complex networks. *Phys. Rev. E* **69**, 045104 (2004).
33. Cellai, D. *et al.* Percolation in multiplex networks with overlap. *Phys. Rev. E* **88**, 052811 (2013).
34. Parshani, R., Buldyrev, S. V. & Havlin, S. Critical effect of dependency groups on the function of networks. *Proc. Natl. Acad. Sci. U.S.A.* **108**, 1007–1010 (2011).
35. Zhao, J.-H., Zhou, H.-J. & Liu, Y.-Y. Inducing effect on the percolation transition in complex networks. *Nature Comm.* **4** (2013).
36. Bashan, A., Parshani, R. & Havlin, S. Percolation in networks composed of connectivity and dependency links. *Physical Review E.* **83** (5), 051127.
37. Bashan, A. & Havlin, S. The combined effect of connectivity and dependency links on percolation of networks. *Journal of Statistical Physics.* **145** (3), 686–695.
38. Bunde, A. & Havlin, S. *Fractals and disordered systems* (Springer-Verlag New York, Inc., 1991).
39. Li, D. *et al.* Dimension of spatially embedded networks. *Nature Phys.* **7**, 481–484 (2011).
40. Zhou, Q. & Bialek, J. Approximate model of european interconnected system as a benchmark system to study effects of cross-border trades. *Power Systems, IEEE Transactions on* **20**, 782–788 (2005).
41. Deka, D. & Vishwanath, S. Generative growth model for power grids. Paper presented at *2013 International Conference on Signal-Image Technology & Internet-Based Systems*, Kyoto, Japan. doi:10.1109/SITIS.2013.97.
42. Hines, P. *et al.* The Topological and Electrical Structure of Power Grids. Paper presented at *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, doi:10.1109/HICSS.2010.398.
43. Shao, S. *et al.* Percolation of localized attack on complex networks. arXiv:1412.3124.
44. Debenedetti, P. G. & Stanley, H. E. Supercooled and Glassy Water. *Phys. Today* **56**, 40 (2003).
45. Coniglio, A. Cluster structure near the percolation threshold. *J. Phys. A: Math. Gen.* **15**, 3829 (1982).
46. Sapoval, B., Rosso, M. & Gouyet, J. F. The fractal nature of a diffusion front and the relation to percolation. *J. Physique Lett.* **46**, 149–156 (1985).

Acknowledgments

We acknowledge the LINC (no. 289447 funded by the EC's Marie-Curie ITN program (FP7-PEOPLE-2011-ITN)) and MULTIPLEX (EU-FET project 317532) projects, the Deutsche Forschungsgemeinschaft (DFG), the Israel Science Foundation, ONR and DTRA for financial support. Daqing Li acknowledges support from the National Natural Science Foundation of China (61104144) and National Basic Research Program of China (2012CB725404).

Author contributions

Y.B., A.B., M.M.D., D.L. and S.H. conceived and designed the research. Y.B. carried out the numerical simulations. Y.B., A.B. and M.M.D. developed the theory and wrote the paper with contributions from all other authors. The authors declare no competing financial interests.

Additional information

Supplementary information accompanies this paper at http://www.nature.com/scientificreports

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

How to cite this article: Berezin, Y., Bashan, A., Danziger, M.M., Li, D. & Havlin, S. Localized attacks on spatially embedded networks with dependencies. *Sci. Rep.* **5**, 8934; DOI:10.1038/srep08934 (2015).