

SCIENTIFIC REPORTS



OPEN

Predicting the Lifetime of Dynamic Networks Experiencing Persistent Random Attacks

Boris Podobnik^{1,2,3,4}, Tomislav Lipic^{2,5}, Davor Horvatic⁶, Antonio Majdandzic², Steven R. Bishop⁷ & H. Eugene Stanley²

Received: 10 February 2015

Accepted: 11 August 2015

Published: 21 September 2015

Estimating the critical points at which complex systems abruptly flip from one state to another is one of the remaining challenges in network science. Due to lack of knowledge about the underlying stochastic processes controlling critical transitions, it is widely considered difficult to determine the location of critical points for real-world networks, and it is even more difficult to predict the time at which these potentially catastrophic failures occur. We analyse a class of decaying dynamic networks experiencing persistent failures in which the magnitude of the overall failure is quantified by the probability that a potentially permanent internal failure will occur. When the fraction of active neighbours is reduced to a critical threshold, cascading failures can trigger a total network failure. For this class of network we find that the time to network failure, which is equivalent to network lifetime, is inversely dependent upon the magnitude of the failure and logarithmically dependent on the threshold. We analyse how permanent failures affect network robustness using network lifetime as a measure. These findings provide new methodological insight into system dynamics and, in particular, of the dynamic processes of networks. We illustrate the network model by selected examples from biology, and social science.

Many real-world complex systems are largely robust to outside attacks and spontaneous fluctuations that cause either temporary or permanent localised breakdowns^{1–9}. However, the majority of them ultimately collapse and thus have a finite lifetime. The collapse commonly occurs when the system reaches a critical point and the system abruptly shifts from one phase to another^{10–16}. Examples of real-world complex systems that experience sudden collapse are numerous, e.g., the spread of disease in living organisms¹⁷, the spread of political dissent in a human society, or the spread of a product sales pattern in economics.

In recent years network science has been utilized to describe complex systems^{18–32}, and many dynamic network models have been proposed^{33–40} to explain the complicated dynamics that occur in real-world networks. Thus far, most network research has separated the analysis of (a) empirical indicators of critical transitions^{11–16,41} from the analysis of (b) network robustness^{1,2,9,42–45}. The studies in group (a) have focused on a phenomenon known as critical slowing down, where the correlations and variance of the fluctuations increase as the system approaches a critical point^{14,46}. The research in (b) focuses on quantifying vulnerability of different networks under different types of random failures and deliberate attacks.

Most of the existing studies measure the structural robustness of the network by employing the theoretical framework of statistical physics and percolation theory to analyse the impact of a node or link removal on the structural integrity of the network which is commonly assessed by evaluating the size

¹University of Rijeka, Faculty of Civil Engineering, Rijeka, 51000, Croatia. ²Boston University, Center for Polymer Studies, Department of Physics, 590 Commonwealth Avenue, Boston, Massachusetts 02215, USA. ³Zagreb School of Economics and Management, Zagreb, 10000, Croatia. ⁴University of Ljubljana, Faculty of Economics, Ljubljana, 1000, Slovenia. ⁵Rudjer Boskovic Institute, Centre for Informatics and Computing, Zagreb, 10000, Croatia. ⁶University of Zagreb, Physics Department, Zagreb, 10000, Croatia. ⁷University College London, Department of Mathematics, Gower Street, London, WC1E 6BT, UK. Correspondence and requests for materials should be addressed to B.P. (email: bp@phy.hr)

of the giant component. In this regard, network robustness is quantified by the percolation threshold, which is the fraction of the nodes (or links) needed to remove for the network to fall apart (i.e. the giant component to vanish).

Recent studies try to estimate percolation thresholds in different types of real networks for the site and bond percolation models^{44,45}. However, measuring structural network robustness by static percolation thresholds assumes an underlying network with static nodes and links where the failure of a node (or link) is equivalent to a permanent loss of its functionalities. Since in many real-world scenarios the functionality of nodes and links vary over time, theoretical frameworks for quantitative analysis of global, self-healing and targeted recovery processes occurring in different complex networks were also recently proposed^{40,47,48}.

Motivated by the fact that ultimately many real networks collapse and thus have a finite lifetime, here we incorporate both (a) and (b) within a common theoretical framework based on decaying dynamical networks. We focus on networks in which nodes flip between two intrinsic states and also have the ability to control the state of their neighbours. Examples of these networks range from cascading processes in interdependent networks^{29,30}, epidemic spreading in scale-free networks¹⁷, dynamic networks able to spontaneously recover⁴⁰ to the glassy dynamics of kinetically constrained models⁴⁹. Among these networks of particular interest is a broad class of complex systems characterized by both a gradually declining trend³⁷ and a sudden collapse⁵⁰.

We find that introducing permanent failure in the presence of a stochastic contiguous spreading process produces networks that are continuously decaying only up to a specific, critical point—the network lifetime (t_c)—when the network abruptly collapses. We find that this critical point is logarithmically dependent upon the threshold and inversely dependent on the size of the outside attack. In practise when comparing different empirical complex systems, the value of t_c may serve as an indicator of system's dynamical risk. Using $1/t_c$ then the larger the parameter value t_c , the smaller the dynamical risk.

Results

Thus far no single network model has been able to explain the process of finite-time decline with the possibility of spontaneous collapse, how ageing or continuous ongoing time-dependent attacks affect network robustness, how long a network can continue to function before it collapses, or how to predict the time of network collapse (t_c) prior to its occurrence.

1. The function of a node n_i is dependent upon its nearest neighbours. Generally speaking, a network is robust if its nodes are able to function even when a large fraction of its nearest neighbours have failed. Here this fraction is denoted by T_n . If at time t the fraction of active neighbours of node n_i is smaller than or equal to T_n , then at time $t + 1$ node n_i will become externally inactive with a probability r . We use a fractional threshold^{51,52}, which is more appropriate than the absolute threshold^{40,53} when networks have heterogeneous degrees.
2. Each node can internally fail, independently of other nodes, with a probability p quantifying the magnitude of the attack. This is related to the static network case when robustness is studied under simultaneous random or targeted attacks^{1,2,9,36,54,55}.
3. Although we assume that a node can recover from an internal failure after a finite period of time (τ), internal failure always carries the potential risk of being permanent, an event we define by a probability $1 - q$. Thus, when a network is influenced by ongoing time-dependent attacks, not every node will be able to recover. A node can be considered active only if it is both internally and externally active⁴⁰. For a more complicated network this will include adding the introduction of link failures or the addition of new nodes (see Methods and Model extensions).

Reference⁴⁰ shows that when the assumptions (i)–(iii) are applied, then when the network model has no permanent failures the local node recoveries (modelled by τ) and the stochastic contiguous spreading (modelled by a probability r) lead to the spontaneous emergence of macroscopic “phase-flipping” phenomena, corresponding e.g. to flipping between “good” (up phase) and “bad” (down phase) years in economics^{51,52}. It has also been shown that when the size of the network is increased, the average time spent in the down phase is greater than the average time spent in the up phase. This result has a serious consequence when applied to model world economy and globalization—the model predicts that recession time increases with an increase in the number of countries in the world economy. Reference⁵¹ shows that when the (i)–(iii) network model has no permanent failures, there are substantial changes in the autocorrelation and variance of fluctuations—characteristic of critical slowing¹⁴—as the system approaches a critical point.

In seminal studies of the stability of large complex systems, Gardner and Ashby⁵⁶ (numerically) and May⁵⁷ (analytically) examined how such systems maintain stability up to some critical level of connectedness and then suddenly, as the level of connectedness increases, become unstable. In contrast, our focus is on the reverse process in which a continuous decrease in the number of functioning nodes and links between them over time decreases network complexity. We describe the level of network functionality in terms of the fraction of the total number of nodes that are continuing to function⁴⁰ and the fraction

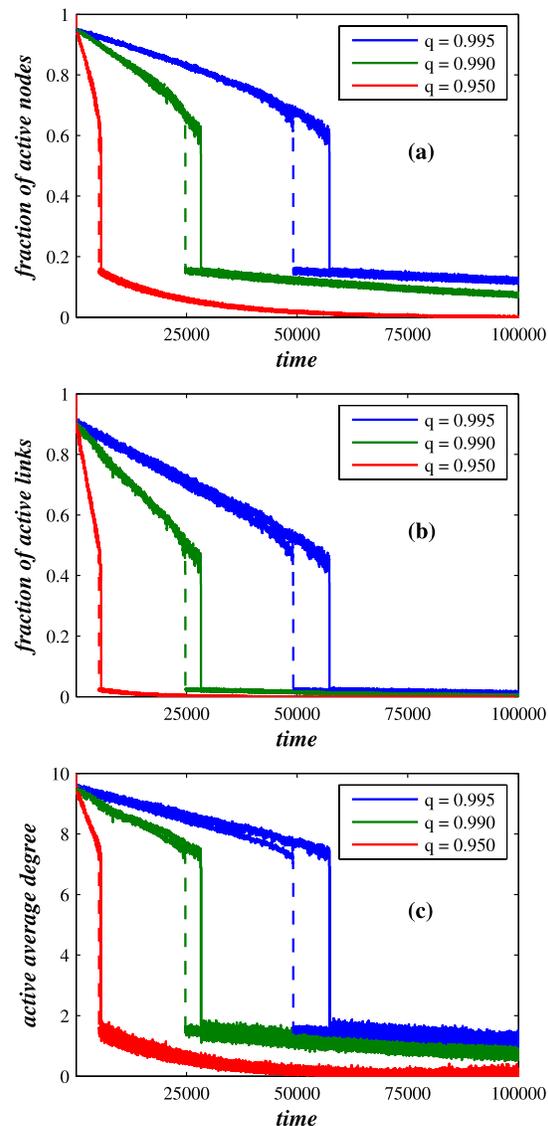


Figure 1. Comparison between BA (solid line) and ER (dashed line) decaying dynamic networks, when $\langle k \rangle = 10$. Under the same level of attack, quantified by equal p , the BA decaying network exhibits the higher level of robustness than the ER decaying network, where robustness is quantified by larger t_c . For (a) the fractions of active nodes and (b) links and (c) the active average degree as a function of time, the BA decaying networks are more robust than the ER networks. By active average degree we mean the average degree calculated for nodes that are active both internally or externally. Here the robustness is defined in a dynamic way—the more robust a network is, the longer it lasts. For both networks we use $p = 0.001$, $r = 0.8$, $T_h = 0.5$, and $\tau = 50$.

of active links, f_l^{51} . In this dynamical network framework, in contrast to static networks, the network functionality is not only limited to the size of giant component.

The dynamic approach used to quantify the robustness of a network under time-dependent attacks can also be used to address the ageing process of networks. In this case the probability p serves as an internal network property⁴⁰. Over time not every internally-failed node can recover, e.g., at the cell level in biology there may be a defective apoptotic process⁵⁸.

To determine how T_h and q affect network functionality, we first generate three random Erdős Renyi (ER) networks and three scale-free networks (Barabasi-Albert BA model), each with initial $N(t=0) = 10,000$ nodes and an average degree $\langle k \rangle = 10$. Then, each network is placed under persistent attack, quantified by p , where we allow nodes in the inactive phase to permanently fail with a probability $1 - q$. For varying values of q for each decaying network, Fig. 1 shows the fraction of active nodes f_a , the fraction of active links f_b , and the average degree, each as a function of time. In Fig. 1 T_h is fixed but the values of q varied, and we see that the network decays continuously until at some specific time (t_c)

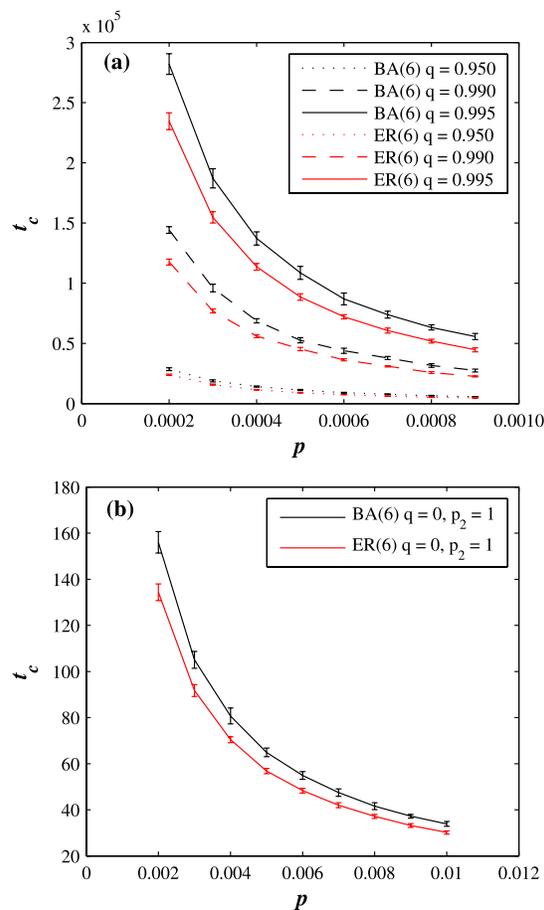


Figure 2. Robustness of BA and ER decaying networks for different values of q , where t_c serves as the measure of robustness. We show t_c versus p for (a) $q = 0.995, 0.99, 0.95$. The BA decaying networks exhibit higher level of robustness than the ER decaying networks. We use $r = 0.8$ and $\langle k \rangle = 6$. (b) For BA and ER decaying dynamic networks when a node cannot recover ($q = 0$), for $\langle k \rangle = 6$ the larger time t_c (the larger robustness) we obtain for BA decaying network than for ER decaying network. Here, the larger the time t_c , the longer the network lifetime, and the more robust the network.

it abruptly and spontaneously collapses; a collapse brought on by a sudden large increase in the number of inactive links and nodes. This sudden collapse does not require any parameter other than q . As expected, the more rapid variation of the exponential decay, the sooner the network will collapse. When we compare the fractions of active nodes and links we see that, when the network collapse occurs, the fraction of active links decreases substantially more than the fraction of active nodes, where the fraction of active links is approximately $1 - r$.

Our analysis addresses both how long a dynamic network will function before collapse, and how robust it will be under long-term continuous attack, i.e., the larger the network lifetime t_c , the more robust the network. This study of robustness of dynamic networks under continuous attack is highly relevant to both researchers and practitioners. For example, it can be used in military science for determining how a military network can remain robust under persistent enemy attack, or a goal in finance is determining how a financial system can remain robust when a fraction of its banks fails over time. References^{1,2} reported that scale-free networks are more robust than ER networks to multiple random and simultaneous attacks.

We next compare the robustness of decaying BA and ER networks, and our definition of network robustness is dynamic, i.e., the more robust a network is, the longer it will last. Figure 1 compares the robustness of decaying BA and ER networks under continuous long-term attack, measured by p , as a function of time. We use the same parameters for both types of network. Using network lifetime to quantify dynamic network robustness, Fig. 1 shows that, even when nodes and links fail, BA networks are generally more robust than ER networks. A dynamic BA network is typically able to survive longer with higher values of t_c than an ER network before it exhibits an abrupt drop in the fraction of its active nodes and links and its average degree. Figure 1(c) shows that, for the q values displayed, the average degree of a dynamic BA network lasts longer (i.e., t_c is larger) than the average degree of a dynamic ER network.

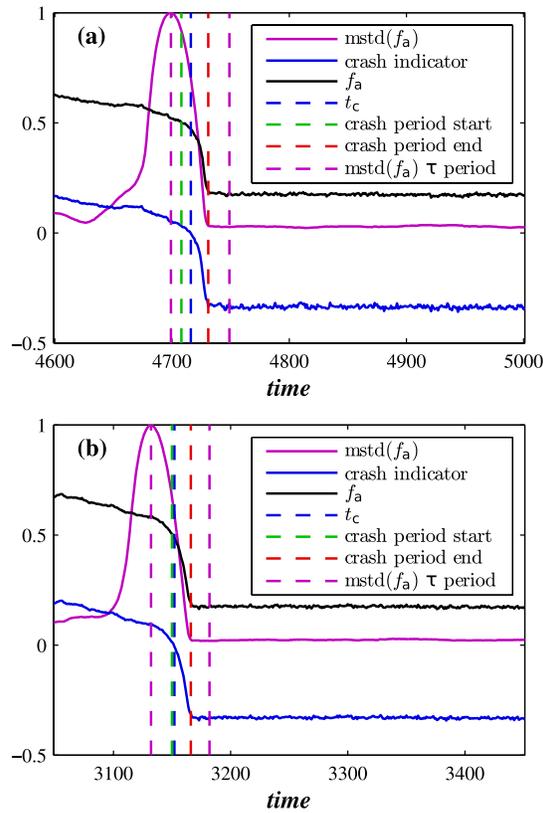


Figure 3. Indicators of network crash. Shown are two indicators together with the fraction of active nodes f_a obtained for (a) BA and (b) ER decaying network when $q = 0.99$ and $\langle k \rangle = 6$. We show indicator I (mstd), moving standard deviation of fraction of active nodes (forward method) with window size $\tau = 50$ (the same τ as in recovery process), and indicator II (crash indicator), the average fraction of active neighbours in excess of threshold T_h . When the average fraction of active neighbouring nodes drops below the threshold T_h for the first time (t_c), cascading failures trigger a network crash. We use $p = 0.003$, $T_h = 0.5$, and $r = 0.8$.

To determine whether this difference in robustness is general or sample-dependent, we compare decaying BA and ER networks for different q values. For fixed T_h and r , and varying values of q , Fig. 2(a) shows the relationship between t_c , whose precise definition will be explained in Fig. 3, and p . The BA decaying networks generally exhibit a higher level of robustness than the ER decaying networks¹. We find a similar dependence between t_c and p for varying network degrees.

The dynamic approach taken here also allows the non-trivial possibility that, following an attack, nodes can remain permanently damaged, corresponding to the $q = 0$ case in which no recovery is allowed. This allows us to compare our results with studies in which robustness is analysed in static networks under either simultaneous random or targeted attack^{1,2,9,36,54,55}. Note that when $q = 0$, the period τ becomes irrelevant. For a fixed $T_h = 0.5$ and $\langle k \rangle = 6$, Fig. 2(b) shows how the time t_c is affected by the level of outside attack, quantified by p . Again as in Fig. 2(a), the larger the level of outside attack, the smaller the network lifetime. Because no recovery is allowed for this case, the lifetime values in Fig. 2(b) are much smaller than those in Fig. 2(a). When $q = 0$, decaying BA networks exhibit a significantly higher level of robustness than decaying ER networks, and the times t_c calculated for BA networks are consistently larger than those calculated for ER networks—the dependence between t_c and p follows a hyperbolic function.

In a complex dynamic system, thresholds and critical points control the transition process between different states⁵⁹. A phase transition occurs when a system reaches a system threshold. Using this perspective, the network decline and collapse numerically described above can also be treated analytically. Note that at time $t - \tau$, attacks on a network that has $N(t - \tau)$ active and inactive living nodes will cause $pN(t - \tau)$ nodes to switch to the internally inactive phase. The change in the number of living, or active, nodes is proportional to the probability that a node that internally failed at $t - \tau$ will not recover, $1 - q$, thus

$$dN(t - \tau) = -(1 - q)pN(t - \tau)dt. \tag{1}$$

The number of living nodes remaining is determined by an exponential decay $N(t) = N(0)\exp(-(1 - q)pt)$ with a decay rate of $\lambda = (1 - q)p$, where $N(t)/N(0)$ is the average fraction of living nodes

equivalent to the average fraction of living neighbours of each node. For simplicity, let us assume that all nodes have the same initial degree k , remembering that node n_i will be active if the number of its active neighbours is larger than $m = T_h k$. For a network with degree distribution f_k at time t , the fraction of n_i 's failed neighbouring nodes $N_f(t)/N(t)$ among $N(t)$ living nodes previously estimated as $k(t) = k \exp(-(1 - q)pt)$, can be approximated using the probabilities of internal and external failures, p and $E[m, k(t)]$,

$$a' \equiv a'[p^*, r, m, k(t)] = p^* + r(1 - p^*) \sum_k f_k E[m, k(t)], \tag{2}$$

where $E[m, k(t)] = \sum_{j=0}^m \binom{k(t)}{k(t) - j} a'^{k(t)-j} (1 - a')^j$ and $p^* = 1 - \exp(-p\tau)^{40}$. In the above figures we consider the ratio between the living active and the initial number of nodes $N_a(t)/N(0)$, which is equivalent to

$$f_a \equiv \frac{N_a(t)}{N(t)} \frac{N(t)}{N(0)} = (1 - a') \exp[-(1 - q)pt]. \tag{3}$$

Here $\exp[-(1 - q)pt]$ is due to the continuous decline of the network, and $1 - a'$ indicates the sudden network crash occurring when the fraction of living nodes $k(t)/k$ approaches the threshold $T_h = m/k$. At this limit, from Eqs. (2) and (3) we see that $E[m, k(t)] \rightarrow 1$ and the probability of external failure dominates p .

Although predictive power is important in any scientific endeavour, it is widely assumed that predicting critical transitions is extremely difficult because any change in the dynamic state of a system immediately prior to reaching the critical point will be slight¹¹. Unlike early-warning indicators that utilize recent system outputs to detect impending system collapse, we use past data to estimate network parameters, from which we generate numerical simulations that describe the network state at any future time, including the time of network failure t_c . Thus we are able to accurately predict the time of network failure.

Figure 3 shows the predictive power of this dynamic approach when applied to both ER and BA networks which are in the process of decaying. It shows the fraction of active nodes for time scales that include the network crash and also two important values: (I) the standard deviation of the fraction of active nodes calculated using moving boxes similar to the approach proposed in Reference¹¹ and (II) the average fraction of active neighbours—active both internally and externally—above the threshold T_h . Equations (2) and (3) provide a theoretical explanation for II, predicting that when the fraction of currently living nodes approaches the threshold that controls the external failures, the probability of critical transition increases and cascading failures trigger a network crash. Note that just prior to a network crash, indicator I increases substantially and thus is an indicator of the impending failure and a predictor of the time t_c , i.e., it predicts when network failure will occur. Reference¹¹ suggests that as a dynamic system approaches a critical threshold its state at any given moment increasingly resembles its previous state, implying an increase in variance and autocorrelation as reported for dynamic networks in Reference⁵¹. We find that this predictive power holds for both BA and ER decaying networks for a wide variety of parameters. In Fig. 3 the values of II shift from positive to negative and the time when this occurs can also be used as a predictor of the time of network collapse t_c . In addition to the two numerical indicators, we also suggest an analytic formula for t_c , obtained by equating $(1 - a') \exp[-(1 - q)pt]$ in Eq. (3) with T_h , so that

$$t_c = -\ln(T_h/(1 - a'))/p(1 - q). \tag{4}$$

In the decaying network approach, the proportional threshold T_h controls both node-level crashes and “macro” network-level crashes, which makes T_h a breakdown threshold. For a general set of network parameters, the time of network failure is the ratio between the closeness of the fraction of active nodes to the threshold, $-\ln(T_h)$, and the rapidity of their approach to the threshold, $p(1 - q)$. In Fig. 3(a,b) we see that t_c typically corresponds to the beginning of the network failure period. Additionally, for varying values of q in Fig. 4 we find that the fraction of active nodes decreases during a network failure in both decaying BA and ER networks for $T_h - r$.

Figures 1 through 4 describe how t_c is affected by T_h , p , and q . Figure 3(a,b) show that during a network crash the fraction of active neighbouring nodes approaches the threshold. We also find that the time series of the fraction of active neighbours of each node above the threshold T_h substantially changes over time. Figure 5(a,b) display the average representing our indicator II, calculated for each network in Fig. 3(a,b), and also the higher moments, variance, skewness, and kurtosis. For different times prior, during, and after the network failure, Fig. 6 shows the distribution of the fraction of active neighbours of each node above the threshold T_h . Just prior to network failure, skewness, kurtosis, and the distribution substantially change.

In estimating the time of a future network crash, we calculate network parameters from its creation at time $t = 0$ to some time t during which the fraction of active nodes f_a decreases from 1 to some value f' . When we numerically generate the network we thus record the time t at which f_a reaches f' . Then the

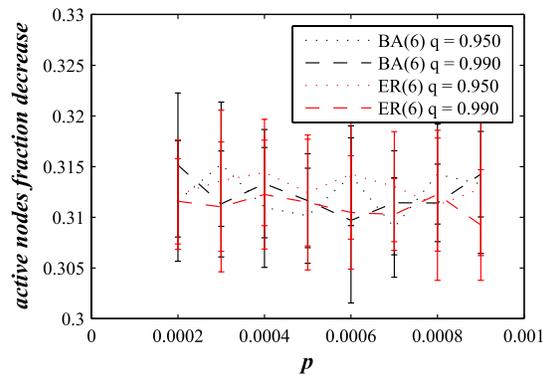


Figure 4. For the varying q values, for both decaying ER and decaying BA network we show the size of the decrease of f_a during the network crash, equal to $T_h - r$.

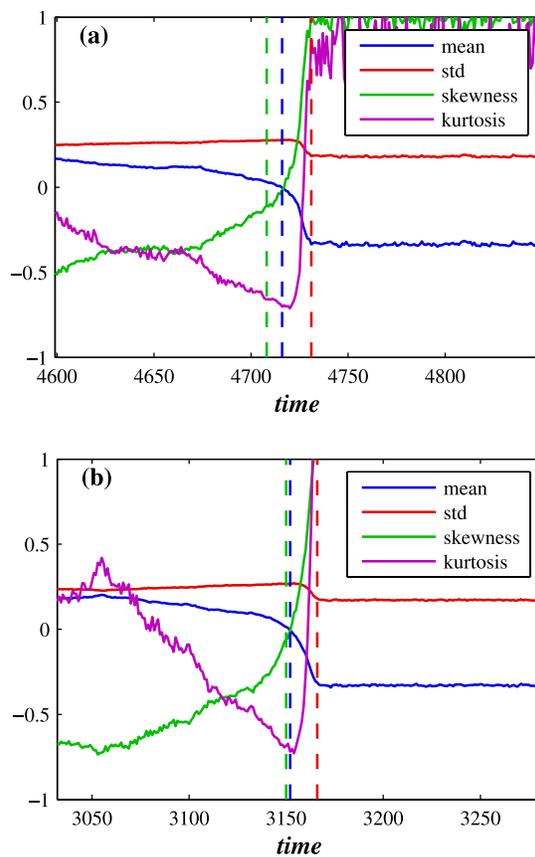


Figure 5. Statistics of the fraction of active neighbours in excess of threshold T_h for (a) decaying BA and (b) decaying ER network with $\langle k \rangle = 6$. We show how the first four moments change over time just before, during, and just after the crash. Just before the network crash, skewness and kurtosis dramatically and abruptly increase.

true prediction of future network collapse is not t_c but $t_c - t$, i.e., t_c represents the entire lifetime of the network, and our interest is in estimating the lifetime remaining after t .

Decay with the Stochastic Threshold. It is known in the field of finance that increasing the number of links between banks reduces the systemic risk and the risk of financial contagion⁶⁰. Until now we assumed that the threshold T_h quantifying network robustness was the same for each node. Such assumption is not appropriate in the real-world of finance because not every bank is equally robust. We therefore assume that the robustness of each node is locally defined. For example, suppose two banks, X and Y,

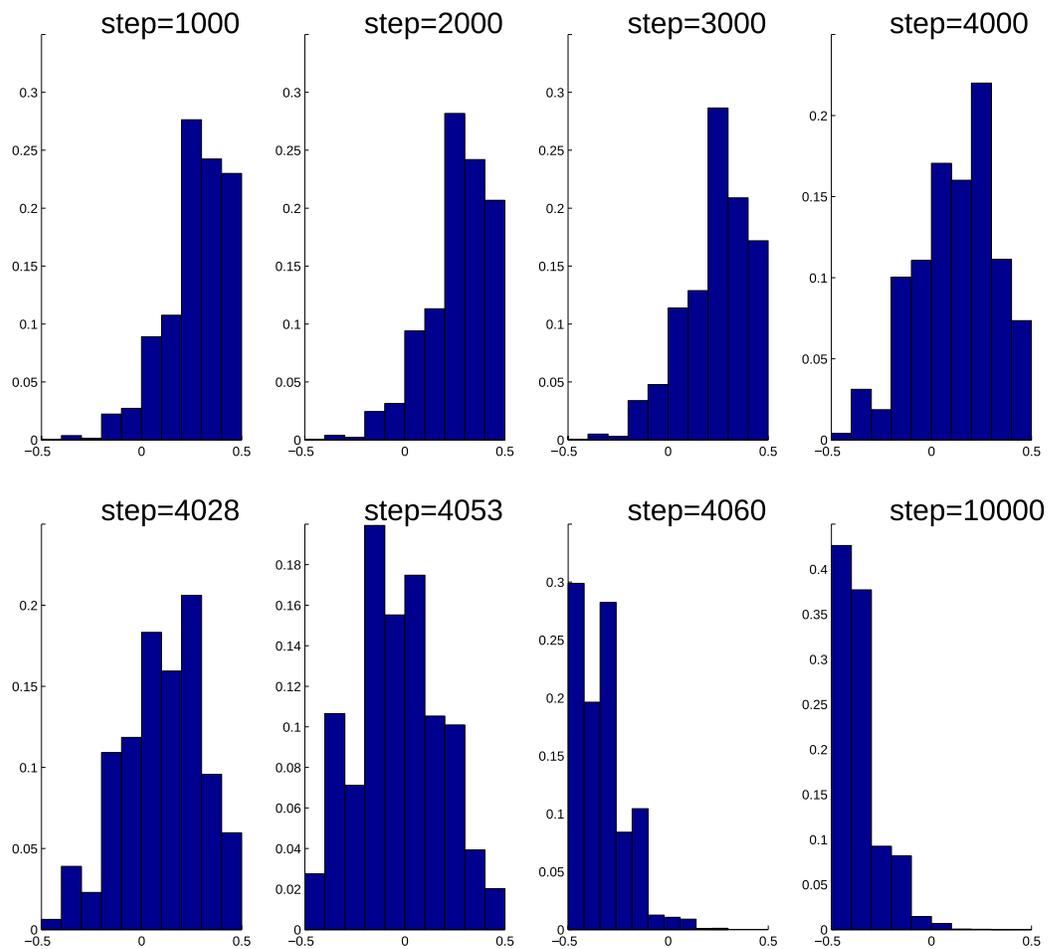


Figure 6. Distribution of the fraction of active neighbours in excess of threshold T_h substantially changes during the network failure.

have an equal debt of 10B\$ but different assets of 15B\$ and 12B\$, respectively, and each allocates 3B\$ to three neighbouring banks. If the criterion of bank solvency is that assets must be larger than debts, X can survive even when all neighbouring banks fail, but Y cannot survive if more than one neighbouring bank fails. Therefore X is more robust than Y.

We next assume that the robustness of each node is randomly chosen from a Gaussian distribution with a mean 0.5 and a varying standard deviation. Figure 7 shows standard deviations equal to (a) 0, (b) 0.1 and (c) 0.2. In all three cases we find that the estimate for t_c of Eq. (4), where now T_h corresponds to the mean of the Gaussian, correctly predicts the time of network breakdown. However we find that the standard deviation of the fraction of active nodes rapidly changes as the uncertainty of the threshold increases. In the smaller T_h uncertainty shown in Fig. 7(a,b), the standard deviation of the fraction of active nodes is characterized by one unique large bump. In contrast, when the standard deviation in T_h changes from 0 to 0.2, we find that the unique bump disappears and is replaced by many smaller flash fluctuations, because different nodes in the network are characterized by different robustness thresholds and thus do not collapse simultaneously. We conclude that heterogeneity in node robustness may create a more robust network, and allows us to devise a strategy for preventing a partially dissolving network from collapsing completely.

Note that Fig. 7 suggests that the average fraction of active neighbours in excess of threshold T_h slowly decreases over time, with a functional dependence approximated by a linear dependence, $I_0 - \alpha t$, where each node i has its own threshold T_{hi} . α represents a slope of the linear dependence that is comparable to $p(1 - q)$ [see Eq. (3)], and I_0 is intercept. Each node collapses when approximately $I_0 - \alpha t = T_{hi}$. Then, for two nodes having thresholds T_{h1} and T_{h2} , we obtain

$$\alpha(t_2 - t_1) = T_{h1} - T_{h2}. \tag{5}$$

The more robust the node, the longer it survives. The larger the uncertainty in T_h , the larger the difference in the time of collapse. If $T_{h1} = T_{h2}$ as in Fig. 7(a), we obtain a virtually simultaneous collapse of

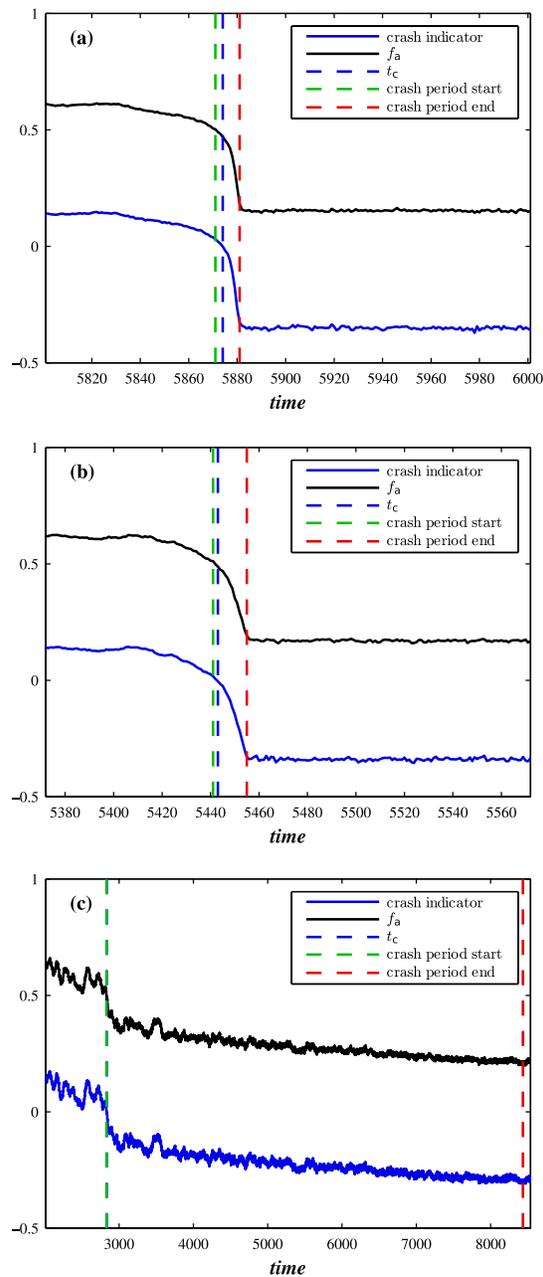


Figure 7. The effect of varying threshold T_h on a network crash. Shown are the fraction of active nodes f_a and indicator II (crash indicator), the average fraction of active neighbours in excess of threshold T_h . We use the BA network with $\langle k \rangle = 10$ and $p = 0.003$, $r = 0.8$, $q = 0.99$, and the varying threshold T_h taken from a Gaussian distribution $G(\mu = 0.5, \sigma)$ where (a) $\sigma = 0$, (b) $\sigma = 0.1$, and (c) $\sigma = 0.2$.

all nodes. We may speculate that if $t_2 - t_1$ is larger than the average relaxation time during the cascade process when T_h is homogeneous, there will be no unique large bump in the standard deviation of the fraction of active nodes, but two separate smaller bumps as in Fig. 7(c). In Fig. 7 we also find that when the standard deviation of T_h increases, the relaxation time of the cascade process also increases.

When applying forecasting theories in practice, the effort of the modelling procedure must be to approximate the empirical system. Often we must also assume that the model parameters, commonly obtained by fitting past data, do not change during a period of forecasting. Thus, if the financial system of a country, modelled by a set of parameters, approaches a financial breakdown and the government intervenes, the model parameters must be changed. To this end, in Fig. 8 the average fraction of active neighbours in excess of threshold T_h slowly decreases over time and just before the network collapse at $t = t_c$ the government intervenes by decreasing the threshold T_h to all nodes causing an abrupt jump in the fraction of active nodes. As one may expect this government measure just postpones the network

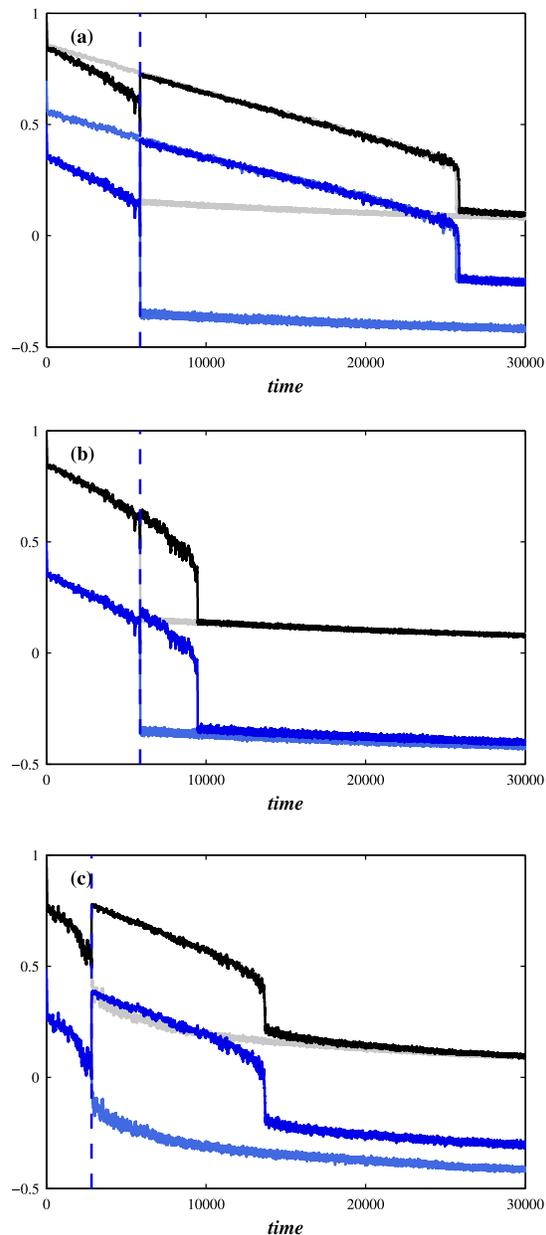


Figure 8. By decreasing the threshold T_h , and thus increasing the robustness just before the network collapse, the fraction of active nodes rises abruptly, and the network becomes more stable. Shown are the fraction of active nodes (black) and crash indicator (blue) for the BA network with $\langle k \rangle = 10$ where at t_c the constant threshold T_h is decreased by 0.2 (a) for each node and (b) only for the 1,000 nodes with the largest degree. (c) For the same network, but with a varying threshold taken from a Gaussian distribution $G(\mu=0.5, \sigma=0.2)$, the treatment of decreasing the threshold T_h by 0.2 for nodes which T_h is greater than 0.5 is made at $t=t_c$. We use $p=0.003$ and $r=0.8$. Light colours indicate the fraction of active nodes and crash indicator without the treatment.

collapse for some future time as seen in Fig. 8(a). Clearly this modelling procedure seems reasonable for countries where the policy of constant increase in indebtedness eventually must lead to a bankruptcy. Different government policies are shown in Fig. 8(b,c). In Fig. 8(b) the government, following “too big to fail policy”, intervenes at $t=t_c$ by decreasing the threshold T_h for only 100 largest nodes. Similarly in Fig. 8(c) this time when the threshold is a stochastic variable taken from a Gaussian $N(0.5, \sigma=0.2)$ at $t=t_c$ the government decreases the threshold T_h for only nodes with threshold larger than 0.5 (the less robust nodes).

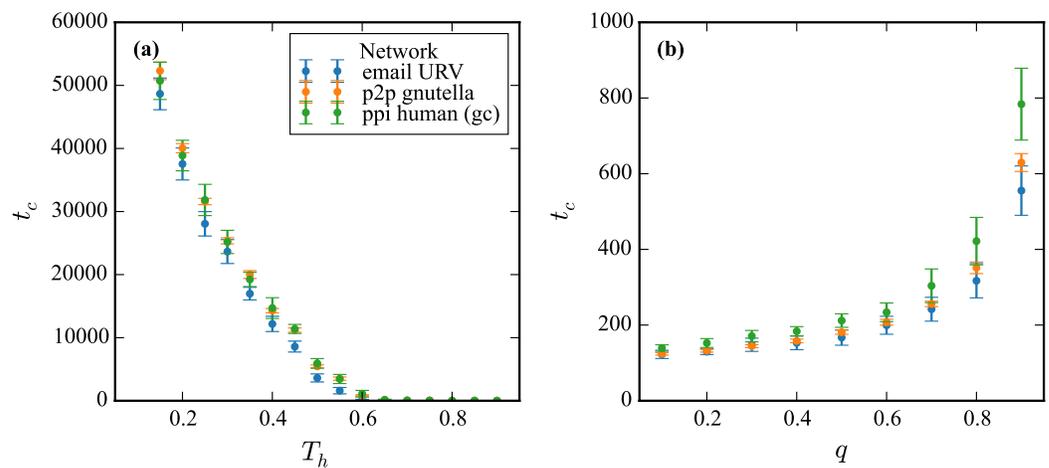


Figure 9. The dependence of t_c on (a) T_h and (b) q for three selected real networks. We use model with fixed parameters $p = 0.003$ and $r = 0.8$, and in (a) $q = 0.99$ while in (b) $T_h = 0.5$. The dependence is in agreement with the results of Eq. (4).

Characterizing t_c dependence on real network structure. As the robustness of a network largely depends on the network's structure, in addition to the analysis of ER and BA random network models, we also analyse dynamics of the decaying dynamic network model on a variety of real networks topologies. We consider a collection of 24 real-world networks of technical (man-made), biological and social systems with different structural properties (e.g. number of nodes, degree distributions, absorptivity, clustering coefficient and diameter) in order to show how they characterize dynamical robustness measure t_c of the model.

For technical systems representatives we include physical infrastructure networks (US Power Grid⁶¹, Euro Road⁶², Open Flights⁶³ and US Airports⁶³), and computer networks⁶⁴ that include networks of autonomous systems of the Internet from CAIDA and Route Views projects (AS-733, Oregon1, Oregon2) together with peer-to-peer file sharing network Gnutella. Protein-protein interaction maps for the human⁶⁵, plant⁶⁶, worm⁶¹ and yeast⁶⁷ interactome network from CCSB Intercome Database are chosen as representatives for biological systems. Finally, social systems representatives include scientific collaboration networks⁶⁸ (CondMat, HepTh, NetScience), interaction networks in online social networking platforms⁶⁹ (ego-Facebook, ego-Twitter, ego-gPlus) and personal communication networks (PGP⁷⁰ and email URV⁷¹), political blogosphere (Blogs⁷²) and connections between board of directors in public companies in Norway (Boards⁷³).

In Supplementary Table S1 we provide the complete list of the analysed real networks with their structural properties. All networks were acquired from a variety of online freely available data sources specified also in the table. All originally weighted and/or directed networks were reduced to their unweighted and undirected projections without multiple links. Additionally, for networks with self-loops we analyse their structures with and without self-loops, while for disconnected networks, we also analyse their giant components resulting the analysis of overall 38 topological structures with different structural properties.

For all of these topological structures we report the averaged t_c over 20 realizations of the model dynamics with $p = 0.003$, $q = 0.99$, $r = 0.8$ and $T_h = 0.5$ in Supplementary Table S2. Supplementary Figure S3–S12. show a realization of the chosen model dynamics of the fraction of active nodes for which t_c in the table was calculated. In order to easier compare t_c results for the set of real networks with varying structural properties, in Supplementary Figure S1. For the same model we report, the t_c dependence on the average degree of the two BA random networks with different size. Similarly, in Supplementary Figure S2, for BA random network with tunable clustering⁷⁴ we report how t_c depends on average clustering coefficient and transitivity.

For three selected real networks (email personal communication network at URV, peer-to-peer file sharing network Gnutella and the human protein-protein interactome network) in Fig. 9 we show the dependence of t_c on (a) T_h and (b) q . The dependence is in agreement with the results of Eq. (4).

Discussion

In both the natural and social sciences a wide range of real-world complex networks have a finite lifetime characterized by abrupt shifts between phases. One of the differences between the behaviour of natural systems and social systems near a critical point is that the sudden random change commonly occurs at a fixed point in natural systems⁷⁵. In contrast, in social sciences even a critical point is a random variable and, although there is an expectation that some radical change is imminently probable, it is generally assumed that it is not possible to predict the exact time of its occurrence. We have explored the predictive power for a particular class of dynamic non-equilibrium decaying networks. In

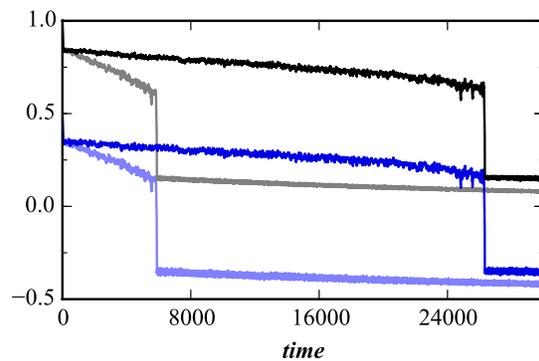


Figure 10. Allowing that new nodes are added while the network decays, when the average fraction of active neighbours in excess of threshold T_h reaches zero, the network abruptly drops. We use the BA network with $\langle k \rangle = 10$ and $p = 0.003$, $r = 0.8$, $p' = 0.00002$, and the constant threshold $T_h = 0.5$. Shown are the fraction of active nodes (black) and crash indicator (blue). Light colours indicate the fraction of active nodes and crash indicator without adding new nodes.

our network model the proportional threshold T_h responsible for node-level crashes is the parameter that also controls “macro” network-level crashes. Our dynamic network study includes cases in which nodes can recover ($q \neq 0$) or remain in a failed state ($q = 0$) after a failure caused by the ageing process or by severe hostile time-dependent attacks. Model extensions are included in the Methods section. How successful our network model might be when applied in practice depends first on how capable we are in estimating model parameters, especially the critical threshold⁷⁶ and second, how good our network is as a proxy for a real-world complex system. In practice the second issue is common when real-world stochastic systems, composed of large number of units, such as financial systems, are modelled using such theoretical stochastic processes as multivariate autoregression. In addition, real-world networks are not isolated, but interact with other networks²⁹. Due to interdependencies between different networks, a shock to a particular network may change both its own parameters and the parameters of all the other networks in the system. Because the time to the network breakdown is strongly dependent upon network parameters, it is clear that any change in network parameters will also affect our prediction of the timing of network collapse.

Methods and Model Extensions

Adding new nodes. The model for network growth can be extended such that nodes can be created as well as destroyed. We assume that, at each time t , among $N(t)$ living nodes, each living node can create a new node with a probability p' . Figure 10 shows that the average fraction of active nodes suddenly drops when the average fraction of active neighbours in excess of threshold T_h reaches zero.

The phase-flipping with decay. Reference⁴⁰ reports that introducing both dynamic recovery and stochastic contiguous spreading leads to spontaneous collective network phase-flipping phenomena which critical behaviour of the system is characterized by first-order phase transition and hysteresis. For the $q = 1$ case, we set the network parameter to enable phase-flipping between two stable states. Figure 11 shows that when the decay mechanism is included ($q \neq 1$) with a decreasing parameter q , the fraction of living nodes gradually disappears over time and also the occurrence of phase-flipping phenomena and the collective network mode.

Introducing link failures. We assume that in decaying networks both links and nodes can fail at any time t . We also assume that any link ℓ can independently (internally) fail with a probability p_ℓ . We define a link to be “healthy” (active) if it is active both internally, controlled by p_ℓ , and externally, controlled by p in (ii). Defining a dynamic network includes determining which part of the parameter space is characteristic of a stable network regime and which is characteristic of an unstable network regime. Our dynamic network is defined by the three probability parameters, p , r , and p_ℓ . We provide analytical results for the hysteresis behaviour in parameter space for the case when nodes always recover after an inactive period ($q = 1$), here enclosed by manifolds comprising spinodals that separate the regions of stability and instability. For an active node i with k_i neighbours, the link between n_i and another node n_j thus fails either due to an internal link failure (X) with probability p_ℓ or an external node failure n_j (Y) equal to a —in the latter case and according to definition, when n_j fails, all of its links have failed. Thus, assuming X and Y are independent, the link is active with probability $(1 - a')(1 - p_\ell)$ and accordingly

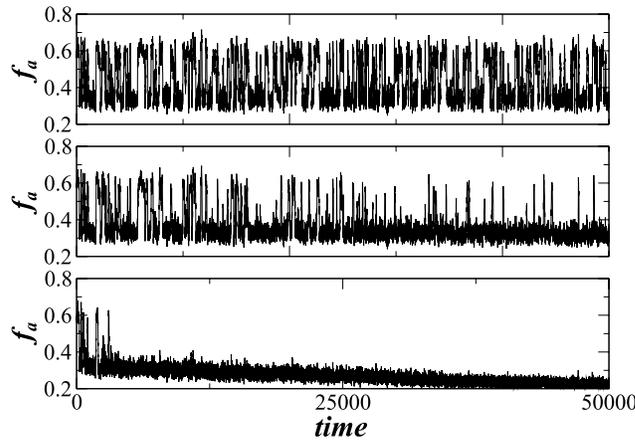


Figure 11. Phase-flipping with decay mechanism for the decaying BA network with parameters $T_h=0.50$, $\tau=50$, the average degree $\langle k \rangle=3$, 1000 nodes. With decreasing q , from 0.999995, 0.9999, and 0.999 (from top to bottom) we show that the average f_a decays with time where the smaller q , the faster the decay.

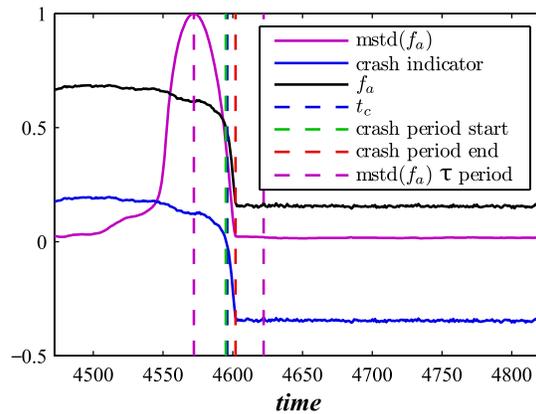


Figure 12. Indicators for network crash, similar as in Fig. 4 but now we include internal link failures. Shown are 3 indicators obtained for an ER decaying network when $q=0.99$, $T_h=0.99$, $r=0.8$, $p=0.003$, and $p_\ell=0.003$.

inactive with probability $1 - (1 - a')(1 - p_\ell) = a' + p_\ell - a'p_\ell \equiv a'_\ell$. Similar to the case in (i), when the links fail internally we define node n_i to be active only when there are more than m active links—not nodes, as in (i). Thus by

$$E(k, m, a'_\ell) \equiv \sum_{j=0}^m a_\ell'^{k-j} (1 - a'_\ell)^j \binom{k}{k-j} \tag{6}$$

we define the probability that the neighbourhood of node n_i is critically damaged with more than m broken links. Finally, we derive the probability that a randomly chosen node n_i with degree k is inactive, which is equal to the fraction of inactive nodes,

$$a'_k \equiv a' = p^* + r(1 - p^*)E(k, m, a'_\ell). \tag{7}$$

Here we apply the probability formula $P(X \cup Y) = P(X) + P(Y) - P(X)P(Y)$ for two independent events. Note that this equation is derived under the assumption that internal failures affect external failures and thus the notion that external and internal failures are independent is only approximately true. Figure 12 presents an ER decaying network and shows the predictive power for the case in which internal link failures are taken into consideration.

Equation (7) assumes that all nodes have the same degree, and thus for simplicity we here analyse random networks that are regular. Figure 13 shows the mean-field (MFT) prediction for the position of spinodals (merging at a critical point) in parameter space (p^*, r) for fixed values of p_ℓ obtained from Eq.

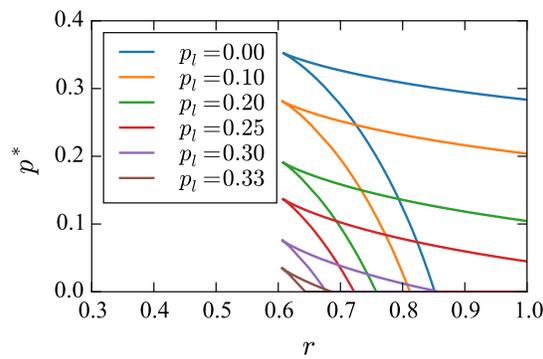


Figure 13. For $q=1$ case, we show the phase diagram with outline of the hysteresis region in model parameter space (p^*, r) for fixed values of p_l obtained from Eq. (7), where $p^* = 1 - \exp(-p\tau)$. Hysteresis region is bounded with two spinodal lines merging at a critical point. We use $k=10$ and $m=4$.

(7), where $p^* = 1 - \exp(-p\tau)$ ⁴⁰. In parameter space, the hysteresis region is enclosed by comprising spinodals.

References

- Albert, R., Jeong, H. & Barabási, A.-L. Error and attack tolerance of complex networks. *Nature* **406**, 378–382 (2000).
- Cohen, R., Erez, K., Ben-Avraham, D. & Havlin, S. Resilience of the internet to random breakdowns. *Phys. Rev. Lett.* **85**, 4626 (2000).
- Callaway, D. S., Newman, M. E., Strogatz, S. H. & Watts, D. J. Network robustness and fragility: Percolation on random graphs. *Phys. Rev. Lett.* **85**, 5468 (2000).
- Newman, M. E. Spread of epidemic disease on networks. *Phys. Rev. E* **66**, 016128 (2002).
- Gallos, L. K., Cohen, R., Argyrakis, P., Bunde, A. & Havlin, S. Stability and topology of scale-free networks under attack and defense strategies. *Phys. Rev. Lett.* **94**, 188701 (2005).
- Serrano, M. Á. & Boguná, M. Percolation and epidemic thresholds in clustered networks. *Phys. Rev. Lett.* **97**, 088701 (2006).
- Newman, M. & Ghoshal, G. Bicomponents and the robustness of networks to failure. *Phys. Rev. Lett.* **100**, 138701 (2008).
- Moreira, A. A., Andrade, Jr J. S., Herrmann, H. J. & Indekeu, J. O. How to make a fragile network robust and vice versa. *Phys. Rev. Lett.* **102**, 018701 (2009).
- Gao, J., Buldyrev, S. V., Havlin, S. & Stanley, H. E. Robustness of a network of networks. *Phys. Rev. Lett.* **107**, 195701 (2011).
- May, R. M. Thresholds and breakpoints in ecosystems with a multiplicity of stable states. *Nature* **269**, 471–477 (1977).
- Scheffer, M. *et al.* Early-warning signals for critical transitions. *Nature* **461**, 53–59 (2009).
- Barnosky, A. D. *et al.* Approaching a state shift in earth's biosphere. *Nature* **486**, 52–58 (2012).
- Boettiger, C. & Hastings, A. Tipping points: From patterns to predictions. *Nature* **493**, 157–158 (2013).
- Scheffer, M. Complex systems: foreseeing tipping points. *Nature* **467**, 411–412 (2010).
- Veraart, A. J. *et al.* Recovery rates reflect distance to a tipping point in a living system. *Nature* **481**, 357–359 (2012).
- Scheffer, M. *et al.* Anticipating critical transitions. *Science* **338**, 344–348 (2012).
- Pastor-Satorras, R. & Vespignani, A. Epidemic spreading in scale-free networks. *Phys. Rev. Lett.* **86**, 3200 (2001).
- Watts, D. J. & Strogatz, S. H. Collective dynamics of 'small-world' networks. *Nature* **393**, 440–442 (1998).
- Barabási, A.-L. & Albert, R. Emergence of scaling in random networks. *Science* **286**, 509–512 (1999).
- Huberman, B. A. & Adamic, L. A. Internet: growth dynamics of the world-wide web. *Nature* **401**, 131–131 (1999).
- Bhalla, U. S. & Iyengar, R. Emergent properties of networks of biological signaling pathways. *Science* **283**, 381–387 (1999).
- Krapivsky, P. L., Redner, S. & Leyvraz, F. Connectivity of growing random networks. *Phys. Rev. Lett.* **85**, 4629 (2000).
- Dorogovtsev, S. N., Mendes, J. F. F. & Samukhin, A. N. Structure of growing networks with preferential linking. *Phys. Rev. Lett.* **85**, 4633 (2000).
- Albert, R. & Barabási, A.-L. Statistical mechanics of complex networks. *Rev. Mod. Phys.* **74**, 47 (2002).
- Garlaschelli, D., Caldarelli, G. & Pietronero, L. Universal scaling relations in food webs. *Nature* **423**, 165–168 (2003).
- Montoya, J. M., Pimm, S. L. & Solé, R. V. Ecological networks and their fragility. *Nature* **442**, 259–264 (2006).
- Arenas, A., Díaz-Guilera, A., Kurths, J., Moreno, Y. & Zhou, C. Synchronization in complex networks. *Phys. Rep.* **469**, 93–153 (2008).
- Miura, W., Takayasu, H. & Takayasu, M. Effect of coagulation of nodes in an evolving complex network. *Phys. Rev. Lett.* **108**, 168701 (2012).
- Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E. & Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **464**, 1025–1028 (2010).
- Brummitt, C. D., D'Souza, R. M. & Leicht, E. Suppressing cascades of load in interdependent networks. *Proc. Natl. Acad. Sci. USA* **109**, E680–E689 (2012).
- Radicchi, F. & Arenas, A. Abrupt transition in the structural formation of interconnected networks. *Nature Phys.* **9**, 717–720 (2013).
- Scholtes, I. *et al.* Causality-driven slow-down and speed-up of diffusion in non-markovian temporal networks. *Nat. Commun.* **5**, 5024 (2014).
- Jain, S. & Krishna, S. Crashes, recoveries, and "core shifts" in a model of evolving networks. *Phys. Rev. E* **65**, 026103_1–026103_4 (2002).
- Perra, N. *et al.* Random walks and search in time-varying networks. *Phys. Rev. Lett.* **109**, 238701 (2012).
- Kolar, M., Song, L., Ahmed, A. & Xing, E. P. Estimating time-varying networks. *Ann. Appl. Stat.* **4**, 94–123 (2010).
- Holme, P. & Saramäki, J. Temporal networks. *Phys. Rep.* **519**, 97–125 (2012).
- Saavedra, S., Reed-Tsochas, F. & Uzzi, B. Asymmetric disassembly and robustness in declining networks. *Proc. Natl. Acad. Sci. USA* **105**, 16466–16471 (2008).
- Ghoshal, G., Chi, L. & Barabási, A.-L. Uncovering the role of elementary processes in network evolution. *Sci. Rep.* **3**, 2920 (2013).

39. Aguirre, J., Papo, D. & Buldú, J. M. Successful strategies for competing networks. *Nature Phys.* **9**, 230–234 (2013).
40. Majdandzic, A. *et al.* Spontaneous recovery in dynamical networks. *Nature Phys.* **10**, 34–38 (2014).
41. Dai, L., Korolev, K. S. & Gore, J. Slower recovery in space before collapse of connected populations. *Nature* **496**, 355–358 (2013).
42. Karrer, B., Newman, M. E. J. & Zdeborová, L. Percolation on sparse networks. *Phys. Rev. Lett.* **113**, 208702 (2014).
43. Hamilton, K. E. & Pryadko, L. P. Tight lower bound for percolation threshold on an infinite graph. *Phys. Rev. Lett.* **113**, 208701 (2014).
44. Radicchi, F. Predicting percolation thresholds in networks. *Phys. Rev. E* **91**, 010801 (2015).
45. Radicchi, F. Percolation in real interdependent networks. *Nature Phys.* **11**, 597–602 (2015).
46. Quax, R., Kandhai, D. & Sloot, P. M. Information dissipation as an early-warning signal for the Lehman brothers collapse in financial time series. *Sci. Rep.* **3**, 1898 (2013).
47. Gong, M., Ma, L., Cai, Q. & Jiao, L. Enhancing robustness of coupled networks under targeted recoveries. *Sci. Rep.* **5**, 8439 (2015).
48. Shang, Y. Impact of self-healing capability on network robustness. *Phys. Rev. E* **91**, 042804 (2015).
49. Ritort, F. & Sollich, P. Glassy dynamics of kinetically constrained models. *Adv. Phys.* **52**, 219–342 (2003).
50. Scheffer, M. & Carpenter, S. R. Catastrophic regime shifts in ecosystems: linking theory to observation. *Trends Ecol. Evol.* **18**, 648–656 (2003).
51. Podobnik, B. *et al.* Network risk and forecasting power in phase-flipping dynamical networks. *Phys. Rev. E* **89**, 042807 (2014).
52. Podobnik, B. *et al.* Systemic risk in dynamical networks with stochastic failure criterion. *Europhys. Lett.* **106**, 68003 (2014).
53. Watts, D. J. A simple model of global cascades on random networks. *Proc. Natl. Acad. Sci. USA* **99**, 5766–5771 (2002).
54. Holme, P., Kim, B. J., Yoon, C. N. & Han, S. K. Attack vulnerability of complex networks. *Phys. Rev. E* **65**, 056109 (2002).
55. Song, C., Havlin, S. & Makse, H. A. Origins of fractality in the growth of complex networks. *Nature Phys.* **2**, 275–281 (2006).
56. Gardner, M. R. & Ashby, W. R. Connectance of large dynamic (cybernetic) systems: critical values for stability. *Nature* **228**, 784 (1970).
57. May, R. M. Will a large complex system be stable? *Nature* **238**, 413–414 (1972).
58. Zmasek, C. M., Zhang, Q., Ye, Y. & Godzik, A. Surprising complexity of the ancestral apoptosis network. *Genome Biol.* **8**, R226 (2007).
59. May, R. M., Levin, S. A. & Sugihara, G. Complex systems: Ecology for bankers. *Nature* **451**, 893–895 (2008).
60. Allen, F. & Gale, D. Financial contagion. *J. Polit. Econ.* **108**, 1–33 (2000).
61. Watts, D. J. & Strogatz, S. H. Collective dynamics of ‘small-world’ networks. *Nature* **393**, 440–442 (1998).
62. Subelj, L. & Bajec, M. Robust network community detection using balanced propagation. *Eur. Phys. J. B* **81**, 353–362 (2011).
63. Opsahl, T., Agneessens, F. & Skvoretz, J. Node centrality in weighted networks: Generalizing degree and shortest paths. *Soc. Networks* **32**, 245–251 (2010).
64. Leskovec, J., Kleinberg, J. & Faloutsos, C. Graph evolution: Densification and shrinking diameters. *ACM Trans. Knowl. Discov. Data* **1**, 2 (2007).
65. Rolland, T. *et al.* A proteome-scale map of the human interactome network. *Cell* **159**, 1212–1226 (2014).
66. Dreze, M. *et al.* Evidence for network evolution in an Arabidopsis interactome map. *Science* **333**, 601–607 (2011).
67. Yu, H. *et al.* High-quality binary protein interaction map of the yeast interactome network. *Science* **322**, 104–110 (2008).
68. Newman, M. E. The structure of scientific collaboration networks. *Proc. Natl. Acad. Sci. USA* **98**, 404–409 (2001).
69. Leskovec, J. & McAuley, J. J. Learning to discover social circles in ego networks. *Adv. Neural Inf. Process. Syst.* **25**, 539–547 (2012).
70. Boguñá, M., Pastor-Satorras, R., Diaz-Guilera, A. & Arenas, A. Models of social networks based on social distance attachment. *Phys. Rev. E* **70**, 056122 (2004).
71. Guimerá, R., Danon, L., Diaz-Guilera, A., Giralt, F. & Arenas, A. Self-similar community structure in a network of human interactions. *Phys. Rev. E* **68**, 065103 (2003).
72. Adamic, L. A. & Glance, N. The political blogosphere and the 2004 U.S. election: Divided they blog. Paper presented at the 3rd international workshop on Link discovery (LinkKDD ’05), 36–43. New York, NY, USA: ACM Press. (10.1145/1134271.1134277) (2005-08-21).
73. Seierstad, C. & Opsahl, T. For the few not the many? The effects of affirmative action on presence, prominence, and social capital of women directors in Norway. *Scand. J. Manag.* **27**, 44–54 (2011).
74. Holme, P. & Kim, B. J. Growing scale-free networks with tunable clustering. *Phys. Rev. E* **65**, 026107 (2002).
75. Helbing, D. Globally networked risks and how to respond. *Nature* **497**, 51–59 (2013).
76. Zhao, J.-H., Zhou, H.-J. & Liu, Y.-Y. Inducing effect on the percolation transition in complex networks. *Nat. Commun.* **4**, 2412 (2013).

Acknowledgements

We are grateful to Javier Martin Buldú and Jacobo Aguirre for useful comments and discussion. BP work was partially supported by the University of Rijeka. S.R.B. acknowledges the financial support of the Engineering and Physical Sciences Research Council under the grant ENFOLDing - Explaining, Modelling, and Forecasting Global Dynamics, reference EP/H02185X/1. The Boston University work was supported by ONR Grant N00014-14-1-0738, DTRA Grant HDTRA1-14-1-0017 and NSF Grant CMMI 1125290.

Author Contributions

B.P., T.L., D.H., A.M., S.R.B. and H.E.S. conceived and designed the research. B.P., T.L. and D.H. carried out the numerical simulations, analysed the results and developed the theory. All authors discussed the results and contributed to the text of the manuscript.

Additional Information

Supplementary information accompanies this paper at <http://www.nature.com/srep>

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

How to cite this article: Podobnik, B. *et al.* Predicting the Lifetime of Dynamic Networks Experiencing Persistent Random Attacks. *Sci. Rep.* **5**, 14286; doi: 10.1038/srep14286 (2015).



This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>