Damage isolation via strategic self-destruction: A case study in 2D random networks

This article has been downloaded from IOPscience. Please scroll down to see the full text article.
2009 EPL 86 24002
(http://iopscience.iop.org/0295-5075/86/2/24002)

View the table of contents for this issue, or go to the journal homepage for more

Download details:
IP Address: 67.20.205.9
The article was downloaded on 16/06/2010 at 20:07

Please note that terms and conditions apply.
Damage isolation via strategic self-destruction: A case study in 2D random networks

TAEHYONG KIM\(^1\), WOO-CHANG HWANG\(^1\), AIDONG ZHANG\(^1\), MURALI RAMANATHAN\(^{1,2}\) and SURAJIT SEN\(^3(a)\)

\(^1\) Department of Computer Science and Engineering, State University of New York - Buffalo, NY 14260, USA
\(^2\) Departments of Pharmaceutical Sciences and Neurology, State University of New York - Buffalo, NY 14260, USA
\(^3\) Department of Physics, State University of New York - Buffalo, NY 14260, USA

received 21 October 2008; accepted in final form 17 March 2009
published online 8 May 2009

PACS 46.65.+g – Random phenomena and media
PACS 05.40.-a – Fluctuation phenomena, random processes, noise, and Brownian motion
PACS 64.60.aq – Networks

Abstract – We study the nucleation, spreading, and control of irreversible diffusive damage in a 2D fixed-radius random network. The control is achieved via strategic self-destruction. Our studies suggest that rapidly activated aggressive and encompassing self-destruction may provide optimum long-term survival of the network. When the damaged area is sufficiently small, strategic self-destruction may be too dependent on local geometry and the details of the dynamics and hence non-trivial to estimate. Our results reveal broad insights into how it may be possible to combat and control the spreading of problematic effects across fixed-radius random networks.

Introduction. – The spread of killer epidemics in a network of population centers [1,2], that of a progressive, degenerative disease in a biological system [3], of power grid failure across a wide area network [4,5], etc., are a few problems of strong current interest. All these problems feature damage nucleation and diffusion in a complex system characterized by many sensitive parameters such as the structure of the network, information transfer, and response rates of the system, the rate of damage progression, and the degree of damage. We ask the question as to whether it is possible to offer a drastic and causal response to mitigate damage progression in these systems by strategically “killing off” parts of the system to insure the overall system survival. In particular, we ask how much strategic self-destruction is appropriate for damage control.

Unlike in previously studied statistical physics inspired analyses of models of damage spreading with attention to the phases in which damage is slow, fast, etc. [6–11], here we consider issues associated with a scenario describing the system’s response to damage. We introduce parameters that allow us to investigate the details of the growing damage process and of the ramifications of different levels of system response to such damage.

Our work concerns generic random networks [12–15] where the nodes within a predetermined range are connected, i.e., the so-called fixed-radius random networks [16,17]. These networks show strong dependence on the radius of connectivity and have been considered, e.g., in the context of communication technologies, spreading of diseases [18], and the outbreak of the recent avian flu virus in South Korea [19]. Extensive simulations suggest that sufficiently prompt and aggressive self-defense that is launched across regions that are significantly larger than the length scale of the damaged region(s) may offer the best option for prolonging the survival of the system [20].

In what follows, we describe the details of the system and of the models of damage progression and self-destruction investigated here and then present the results. We show that strategic self-destruction can efficiently contain damage progression if done promptly and decisively. Our study suggests that when the damaged area is small enough, network geometry and process details may strongly dictate the level of needed self-destruction. We propose a simple phenomenological picture to describe our work. We close with a brief discussion of the relevance of this work to the broader contexts alluded to above.

The model. – We consider static networks in 2D composed of randomly distributed nodes or points on a

\(^{(a)}\)E-mail: sen@nsm.buffalo.edu
unit square. Any two nodes are connected by edges or bonds if the distance between them is not greater than a preset length 0 \leq \delta < 1, where \delta = 0 means there can be no edges and \delta = 1 implies all possible edges are present. Thus, \delta defines the degree of linkages, and hence the community structure represented by the network, and serves as a measure of the size of the affected area. We typically set \delta = 0.05, i.e., 1/20 of the edge length of the unit cell. Our exploratory studies (not shown here) suggest that in fixed-radius random networks for 0.05 < \delta < 0.1, it may become too difficult to carry out partial self-destruction to contain diffusive damage. For \delta > 0.1, we find that diffusive damage spreads too aggressively throughout the system to be easily contained by any process unless the system response rates are remarkably fast.

Edges are not allowed to intersect in our studies, i.e., new nodes cannot be created via edge intersections. Let \( q_i(\delta) \) denote the coordination number of node \( i \). Once the edges have been defined, we assign a weight 0 \leq w_{jk} \leq 1 to characterize the state of fitness of an edge between nodes \( j \) and \( k \), where 0 and 1 define death and best health, respectively. The damage at any node \( i \) at the iteration step denoted via time \( t \) can then be written as \( u_i(t_k) \equiv [1 - \sum_{k=1}^N w_{ik}|q_i|] \geq 0 \). Observe that \( u_i(0) = 0 \) (healthy) and a dead node will have \( u_i(t \to \infty) \to 1 \). The dependence of the site averaged \( u_i \) as a function of time, as \( t \to \infty \) and on the system response will be our central focus here. As we shall see below, our systems converge in time quickly to the final values of affected areas and hence we believe that the asymptotic behavior in \( t \) for our studies can be safely extracted.

We probe damage spreading away from the boundaries and hence choose to investigate damage nucleation at the center of the network. Let \( \delta \) be the radius of the center that characterizes the localized region where damage begins. We mainly focus on \( r_0 > \delta \) to ensure consideration of scenarios where significant damage can occur. As we shall see, \( r_0 \) introduces a length scale in which the system must respond via self-destruction to prolong survival and is hence an important parameter. In most of our studies, \( r_0 = 0.1 \). We include some analyses of damage progression when \( r_0 < \delta \), which confirm that damage is very minimal under such circumstances.

To make the simplest model of aggression [21], we let all the functional edges within radius \( r(t) \) that are activated by the aggressor have their weights reduced by unity (i.e., “killed”) with probability \( p_a \). The spatial extent of aggression can then be written as \( r(t + \Delta t) = r_0(1 + f_a(t))r(t) \) for \( t > 0 \), where \( f_a(t) \) is the ratio of the actual number of damaged-to-active edges and \( p_a(t) = f_a(t) \). In modeling aggression, we set 1/3 of the edges emanating from any node to be damaged within \( r(t) \), which from a computing standpoint means that there is an intrinsic fluctuation in \( f_a \) as a function of \( t \). The reason for the choice of \( p_a = 1/3 \) in most of our calculations is as follows: We have explored the consequences of damage occurring at many rates and find that when 0 < \( p_a < 0.3 \), the amount of damage grows slowly, whereas roughly between 0.3 < \( p_a < 0.7 \) the damage is significant and fairly constant and for 0.7 < \( p_a < 1 \) the amount of damage grows so strongly that effective containment seems too challenging. It hence makes sense to consider scenarios where the damage growth is strong but not a “runaway” process and hence our choice of \( p_a \). In each time step, the model entails three sequential processes: i) aggressor damage (controlled by \( r_0, p_a(t) \)), ii) alarm generation and propagation, and iii) defensive action. We discuss ii) and iii) below.

When a node \( i \)'s damage \( u_i(t) > \tau_a \), \( \tau_a \) being the alarm activation threshold, alarm signals are transmitted to all the neighbors of \( i \) within \( \delta \). The magnitude of the alarm signal arriving at any node \( i \) via an edge is assumed to be proportional to the weight of the edge itself. We typically consider 0 < \( \tau_a < 0.5 \), although some higher values of \( \tau_a \) have been explored. The probability of edge destruction at an alarm activated edge is denoted by \( p_d \). Typically, we set \( p_d = 1 \). Hence, for \( \tau_a = 0.5 \), about half the edges connected to a node are destroyed. As \( \tau_a \to 0 \) or 1, the alarm generation rate becomes progressively sensitive or insensitive, respectively, to the degree of damage. The alarm at any given node is transmitted via the live edges to the neighbors.

The sum of all the alarm signals received at any node is denoted by \( a_i(t) \). The maximum value of \( a_i \) achieved at the end of a time step completes step ii) and initiates step iii). When \( a_i(t) > \tau_d \), the defense activation threshold, defensive damage commences and sets the edge weights in some chosen radius \( \phi \) surrounding the node \( i \) to zero. Of course, nodes with edges damaged by a defensive process do not generate any alarm signals. Edges killed are not resurrected and contribute to the total number of dead edges. Observe that when \( \tau_a, \tau_d \to 0 \), the aggression and defensive damage can become nearly simultaneous. However, such a scenario is unlikely in most cases of damage progression and controlled self-destruction and is hence not much emphasized here.

All alarm signals are set to zero upon the completion of the defensive damage process. Calculations of the next time step begin at this point and \( t \) is incremented by unity. No memory of alarm generation at any node is carried forward. The goal of our study is to explore the parameter space of this problem and find \( \phi = \phi_{\text{min}} \), if it exists, for which the total edge death is minimized (for a biological perspective on damage control and even repair see [22]).

The ability to effectively control the damage in the network for 0.3 < \( p_a < 0.7 \) (the range we focus on in this study) via controlled self-destruction with \( p_d = 1 \) can be sensitive to the magnitudes of \( \tau_a \) and \( \tau_d \). In what follows, we investigate the behavior of \( \phi \) and search for \( \phi_{\text{min}} \) for which successful containment of damage via partial self-destruction is possible in the parameter regimes of interest. We henceforth characterize the damage via

\[
U(t) \equiv \left\{ \frac{1}{N_e} \sum_j \sum_{i=1}^N u_i(t_j) \right\}.
\]
Damage isolation via self-destruction

Fig. 1: (a) Snapshot of a fixed-radius random network in which damage (black) has been contained by aggressive self-destruction (dark gray) leaving the rest of the network healthy. (b) Average fraction of damaged edges linked to some site \( i \) vs. time step, dashed (defensive) and gray (aggressive) damage. (c) Spatially averaged fraction of damaged edges vs. time for low, intermediate, and optimum values of \( \phi \). (d) Spatially averaged fraction of damaged edges at late times plotted against \( \phi \) shows that for \( \phi > 0.22 \), the defensive damage dominates. See the text for details.

and via \( U(t \to \infty) = \left( \frac{1}{N_e} \sum_i \frac{u_i(t \to \infty)}{N_e} \right) \), where \( N_e \) is the total number of edges and \( \langle \cdots \rangle \) means averaged over typically \( 10^3 \) independent runs on the same random network.

Results. – We recall that the fixed-radius random networks tend to be more interesting when they are weakly connected. In our studies, we typically consider networks with \( 10^3 \) nodes. Our simulations reveal that for \( \delta = 0.05 \) and \( 0.1 \), the number of nodes as a function of the coordination number behaves as a Gaussian about some mean (as a consequence of the central limit theorem [23]). For \( \delta = 0.05 \), this mean is 7.52, and for \( \delta = 0.1 \), this mean is 28.77. Our calculations suggest that the coordination number grows as \( \delta^2 \) in this 2D network, whereas the edge lengths increase as \( \delta \). As one would expect, if \( \delta \) is large, any damage can spread rapidly and can quickly become unmanageable. As alluded to above, this is what we see in our simulations, which suggest that damage control is virtually impossible when \( \delta \to 0.1 \) or more, unless unrealistically fast response times to mitigate damage spreading are invoked. For this reason, we set \( \delta = 0.05 \) in most of the results discussed below.

To begin with, let \( \tau_a = \tau_d = 0.5 \), \( p_a = 1/3 \) and \( p_d = 1.0 \). For these parameters, we explore whether the damage can be contained provided \( \phi \) is optimal. The damage characteristics arising from aggressive and defensive processes contribute to \( U(t) \). As we note below and in fig. 1, if the chosen radius across which self-destruction is done, \( \phi \), is too small or too large, then damage from offensive and defensive processes can be high, respectively. Figure 1(a) shows an example of a network where the damage (shown via dark bonds) is contained via optimal self-destruction (gray bonds). In fig. 1(b), we describe the average on-site damage incurred across a time step, which can be written as \( \langle u(t) - u(t-1) \rangle \) vs. time \( t \). The notation \( \langle \cdots \rangle \) implies that the data shown is obtained by averaging over \( 10^3 \) independent simulations on the same network. In this chosen case, the initial damage is high, but thanks to partial self-destruction the damage is rapidly controlled and is eventually contained. In figs. 1(b) and (c) and in most of our simulations, we find that the asymptotic behavior in \( t \) sets in by \( t \sim 50 \). It is noteworthy that the high initial damage is successfully curbed by self-destruction for \( \phi = 0.22 \) in the calculation shown. Figure 1(c) reveals the cumulative damage in time, showing that when \( \phi = 0.02 \), the entire network is eventually damaged and that for sustaining minor damage \( \phi \) must be sufficiently large. However, increasing \( \phi \) indefinitely is not suitable either as that enhances the damage due to the defensive processes. Figure 1(d) shows that for \( U(t \to \infty) = 0 \) is the least when \( \phi = 0.22 \) for the chosen parameters. In figs. 1(b)–(d), the data shown was obtained by averaging the results over \( 10^3 \) runs on the same network.

The dependence of the damage at late times, \( U(t \to \infty) \), on the key model parameters is addressed in fig. 2. In fig. 2(a) (like in fig. 1(d)), we show the behavior of \( U(\infty) \) as different values of \( \phi \) are chosen to control the damage with \( r_0 = 0.1 \). The behavior is for various values of \( \tau_a \) for \( \tau_d = 0.5 \) and for two cases where \( \tau_a = \tau_d = 0.1, 0.2 \). Except when \( \tau_a, \tau_d \rightarrow 0 \), we find that for chosen \( \tau_a, \tau_d \) a \( \phi_{\text{min}} \neq 0 \) exists. Almost identical behavior emerges if \( \tau_a \) is held fixed in the same way. In fig. 2(b), we present the dependence of \( U(t \to \infty) \) on \( r_0 \) at \( \phi_{\text{min}} = 0.22 \). Observe that at late times, as shown in fig. 1(a) and (d), damage from defense is higher. Further, damage from defense grows more rapidly than that from aggression. Hence, to minimize self-destruction, appropriate choice of \( \phi \) is important.

To further highlight the importance of \( \phi \) in the context of self-destruction in fig. 2(c), we show that for small enough \( r_0 \) (such as for \( r_0 < 0.1 \)), if \( \phi \) is optimal, then damage is most efficiently controlled. To see this point note that our calculations show that the damage for \( \phi = 0.22 \) is less than that for \( \phi = 0.32 \) or 0.12 for \( r_0 < 0.1 \). This optimal \( \phi \) may be fragile in nature, dependent strongly on the local network geometry and on the details of damage progression and alarm activation level. However, what is reassuring and expected is that for \( r_0 \gg 0.1 \), damage from \( \phi = 0.32 \) is the least, thus suggesting that aggressive control with \( \phi/r_0 > 2 \) may be needed to contain the damage. We shall return to a discussion of fig. 2(c) below.

Finally, in fig. 2(d) we show the behavior of \( U(\infty) \) as \( p_a \) and \( p_d \) are varied for \( \tau_a = \tau_d = 0.5 \), \( p_a = 1/3 \), \( p_d = 1.0 \) and \( \phi_{\text{min}} = 0.22 \). The results justify why in these models the
If we focus on the total damage characterized by $U(\infty)$ as a function of the strategic self-destruction radius $\phi$, then we can construct a description of the processes that take place. For example, when $\phi \to 0$, defensive processes would be practically absent and hence $U(\infty) \to 1$ (i.e., all edges are dead) whereas, when $\phi \to L/2$, again $U(\infty)$ would be large but the magnitude will depend on $p_a$, $\tau_a$, and $\tau_d$ because defensive processes will cause too much destruction. Hence, the behavior we wish to see is whether the defensive processes would be able to isolate the damage and would thus be able to minimize $U(\infty)$ as a function of $\phi$ at $\phi = \phi_{\text{min}}$ (see fig. 2(c)).

To model the cases when the defensive process can isolate the damage spreading and hence stop the system from getting destroyed, we assume that the defensive process decimates the damage as a function of $\phi$. Since self-destruction of edges as a function of $\phi$ depends on the alarm, and stochastic processes control where the alarm will be activated, we assume $U(\infty)|_{\text{damage}} \sim \exp(-\alpha_1 \phi^2)$, where $\alpha_1$ fixes how rapidly $U(\infty)$ decays with increasing $\phi$. Edge death caused via self-destruction, $U(\infty)|_{\text{self-destruction}}$, sets in at low values of $\phi$ and would maximize at some network and parameter value of $\phi = \phi_{\text{min}}$ and begin to decay for $\phi > \phi_{\text{min}}$. We assume $\phi_{\text{min}}$ would start to decay once $U(\infty)|_{\text{damage}}$ is sufficiently low. The joint behavior of

$$U(\infty)|_{\text{damage}} + C_1 U(\infty)|_{\text{self-destruction}} \text{ in } \phi,$$

where $C_1 \leq 1$ is a constant, should then describe the basic processes captured within our simulation model. Observe that for $C_1 > 1$, damage from self-destruction would exceed 1 at $\phi = \phi_{\text{min}}$, which would be unphysical. Hence, we require $C_1 < 1$. It turns out, however, that the edge death process has its subtleties. Edge deaths due to damage for increasing $\phi$ do not completely vanish but rather, for all practical purposes, end up making a very small contribution for all $\phi > 0$. Hence, as more and more area is being decimated with increasing $\phi$, $U(\infty)|_{\text{self-destruction}}$ must remain a weakly increasing function of $\phi$ for sufficiently large $\phi$. The behavior of $U(\infty)$ vs. $\phi$ shown in figs. 1(d) and 2(a) suggests $\alpha_1$ depends on how rapidly the system responds to damage and hence on $\tau_a$ and $\tau_d$ for acceptable $p_a$ and in turn controls the magnitude of $\phi_{\text{min}}$, where $\phi_{\text{min}}$ is not too much larger than $r_0$. It may be noted here that simulations suggest that for the fixed-radius random network for $\delta = 0.05$, $\phi_{\text{min}} \approx 2r_0$ as shown in fig. 2(c) for $r_0 > 0.1$ or so.

**Phenomenological analysis.** – It is challenging to develop a simple theoretical picture to describe the complex processes addressed simulataneously in this work. However, having noted that we are considering the problem on a fixed-radius random network the findings may be summarized as follows. We observe that for $\delta \sim 0.05$, a length-scale $\sim L/10$, $L$ being the length of the lattice, would be affected. Containment of the affected region typically requires an area that encompasses the region with a diameter that is much larger, e.g., $\sim L/5$, and hence for $\delta > 0.05$, unless the self-destruction commences almost immediately after damage has occurred, containment would tantamount to completely self-destruction. Runaway damage may easily happen if network connectivity is significantly higher than that considered here. If we focus on the total damage characterized by $U(\infty)$ as a function of the strategic self-destruction radius $\phi$, workable scenarios typically should involve a slow enough damage diffusion rate and a fast enough response, which is what we have focused on here. Observe that the studies are not too sensitive to changes in $p_a$ for $p_a < 0.7$. Not surprisingly, damage increases sharply for $p_a > 0.7$ or so and is the least when $p_d = 1$, which justifies the reason behind our choice of $p_d$ in most of the calculations reported here.

**Summary and conclusion.** – To summarize, we contend that this study of damage progression and containment via self-destruction on 2D fixed-radius random networks shows that the system possesses strong parameter sensitivities. The networks of interest seem to be those with $0.5 < \delta < 0.1$. For damaged area radius $\phi > \delta$, significant damage is possible. If the “kill
probability” $p_a < 0.3$ (roughly 1/3 of the edges/node) and the self-destruction probability $p_d = 1$, then damage control may be possible provided the alarm activation threshold (i.e., how fast the system responds) $\tau_a$ and the defense activation threshold $\tau_d$ are sufficiently low and the defensive damage length scale $\phi$ exceeds $r_0$ by a factor of 2 or more. For $0.3 < p_a < 0.7$, damage control may still be possible under prompt alarm and aggressive self-destruction conditions. However, for $p_a > 0.7$, we found that it was not possible to control the damage progression using reasonable parameters. Our studies suggest that more sensitive alarm activation to initiate defensive damage can help curb the overall damage. However, in real systems, such a rapid response to damage progression can be impractical. We have presented a brief phenomenological analysis of our studies to provide a broad framework for future theoretical formulation of this and related problems. The simple study presented here can potentially be of interest in the context of modeling processes such as the spreading of dangerous infections and epidemics in populated areas (see [19] for a study of the evolution and the hypothetical containment of Avian Influenza outbreak in South Korea in 2008) using this model and in modeling disease progression in living systems such as a generic model of progression of central nervous system diseases that is based upon the ideas presented here [21].

***

This work has been partially supported by grants from the Kapoor Foundation, National Science Foundation, National Institutes of Health, National Multiple Sclerosis Society, and the Army Research Office - Short Term Innovative Research program.

REFERENCES