Abstract

We study the cascading traffic jamming on a two-dimensional random geometric graph using the Motter and Lai model. The traffic jam is caused by a localized attack incapacitating a circular region or a line of a certain size, as well as a dispersed attack on an equal number of randomly selected nodes. We investigate if there is a critical size of the attack above which the network becomes completely jammed due to cascading jamming, and how this critical size depends on the average degree $\langle k \rangle$ of the graph, on the number of nodes $N$ in the system, and the tolerance parameter $\alpha$ of the Motter and Lai model.
Cascading traffic jamming in a two-dimensional Motter and Lai model.

Gabriel Cwilich\textsuperscript{1}, and Sergey V. Buldyrev\textsuperscript{1}

\textsuperscript{1} Department of Physics, Yeshiva University, 500 West 185th Street, New York, New York 10033

April 20, 2022

1 Introduction

The Motter and Lai model [1, 2] is a generic model of overload spreading. It can be used to model street traffic [3, 4], internet traffic [1] and power grids [5, 6, 7, 8]. In the Motter and Lai model, the betweenness of a node is defined as the number of the shortest paths connecting any pair of nodes in the network that pass through (but do not end in) this node. After the network is constructed, the initial betweenness $b_i^{(o)}$ of each node $i$ is calculated. A node can withstand a maximum betweenness of $L_i \equiv (1 + \alpha) b_i^{(o)}$, where $\alpha$, the tolerance, is a global parameter of the system. When modeling traffic, a node should be understood as an intersection of several streets or roads, which becomes gridlocked if the amount of cars trying to cross it in a unit time exceeds a limit set by the tolerance. Previously, cascading failures in the Motter and Lai Model were studied in randomly connected networks not embedded in space [5, 6], and on a square lattice where the shortest path was defined by minimizing the sum of the normally distributed weights of the links, which may be interpreted as the traveling times between pairs of sites [3]. In the latter work a square of a given size is deleted from the lattice. As a result, the new shortest paths trying to avoid the damaged area concentrate in the perimeter of the deleted square and, depending on the tolerance, the size of the square and the size of the lattice, the nodes on the perimeter may become overloaded and can be deleted from the system as unusable. As a result, at the next stage of the cascade the nodes in the vicinity of the unusable nodes may become overloaded and the traffic jam will spread around the initially damaged area roughly as circles whose radii grow approximately linearly with time, defined as the number of stages in the cascade. The speed of growth increases as the tolerance $\alpha$ decreases. Also the speed increases linearly with the size of the system. Among the important questions not addressed so far, are the following. What is the minimal radius of the initially damaged area for which a cascade starts to propagate? What is the distribution of this minimal radius for different central nodes, and how does it depend on the tolerance $\alpha$ and the size of the system? In this paper we will address these questions for more realistic graphs than the square lattice, namely the random geometric graphs [9].

2 The model

We create a random geometric graph [9] on a unit square with periodic boundaries by placing $N$ nodes with random coordinates $(x, y)$, each one uniformly distributed in the interval $(0, 1)$. Next we select a radius $r = \sqrt{\langle k \rangle / (\pi N)}$, where $\langle k \rangle$ is the desired average degree of the graph, and connect all pairs of nodes whose mutual distance is less or equal than $r$. By construction, this graph has a Poissonian degree distribution with average degree $\langle k \rangle$. The percolation threshold for this graph is $\langle k \rangle = k_c = 4.512$ [9]. We use values of $\langle k \rangle$ larger than or equal to 5 to ensure that the majority of nodes belong to the giant component of the graph. Since only the giant component plays a role in the overall traffic on the graph, we delete all the nodes in the finite clusters before unleashing the initial attack on the system. We define the length of a path as the sum of the Euclidean lengths of all its links. We calculate the initial betweenness of each node $i$ of the graph, $b_i$, and set its maximal load as $L_i = b_i (1 + \alpha)$.

We produce three types of attacks on the graph (Fig. 1): i) a circular attack in which we delete the $n_d$ nodes that have the shortest path lengths to a randomly selected node called the center of the attack; ii) a linear attack, in which we delete $n_d$ nodes selected from a vertical stripe of width $r$ around the center of the attack, in such a way that the standard deviation in the vertical direction from the center of the attack of the deleted nodes is minimal; and iii) a random attack in which we delete $n_d$ nodes selected at random throughout the system.

At stage $t = 1$, immediately after the initial attack, the betweenness of all nodes is recomputed and all the nodes whose new betweenness exceeds $L_i$ are deleted. This process is repeated for $t > 1$ until the betweenness of any remaining node $i$ does not exceed $L_i$. For each realization of the network and of the initial attack we compute the
total number of cascading stages \( N_t \), the number of survived nodes at the end of the cascade \( N_f \), and the number of nodes in the largest connected cluster at the end of the cascade \( N_c \). In addition, for each stage \( t \) of the cascade we compute the number of nodes deleted at that stage, \( F(t) \), and also their average shortest path distance \( r(t) \) from the central node of the attack, for the case of a circular or linear attacks. For random attack this last quantity is not defined.

3 Results

3.1 Circular attacks

We find that for a given value of the parameters \( \alpha, n_d, (k) \) and \( N \), some attacks result in the eventual overload of a large fraction of the nodes; in those cases the giant component of the functional nodes disintegrates and constitutes a small fraction of functional nodes at the end of the cascade (Fig. 1c). Other attacks do not lead to large cascading failures (Fig. 1b). The number of stages in those cascades is small and almost the entire graph and its giant component survive at the end of them. As a consequence, there is a wide region in the parameter space in which the distribution of the cascade lengths, the distribution of the number of functional nodes at the end of the cascade, and the distribution of the size of the giant component at the end of the cascade are bimodal, with two peaks for large and small cascades and nothing in between. In terms of the cumulative distribution, the bimodality manifests itself by a large plateau of the size of the giant component at the end of the cascade are bimodal, with two peaks for large and small cascades. The existence of the plateau suggests that once a cascade reaches a certain number of failed nodes, it propagates further with probability 100%. This number can be estimated from the 20% of the total number of nodes in the system. We find that for a given value of the parameters \( \alpha, n_d, (k) \) and \( N \), the critical attack size \( n_{dc} \) is practically independent of \( \alpha \). Indeed Fig. 4 shows that for smaller values of the tolerance \( \alpha \) the plateau in the cumulative distribution may not be as well defined as in Fig. 2. In this case \( P_t \) can be still defined as the value at which the slope of the cumulative distribution reaches its minimum (or the minimum in the probability density).

Another question we want to explore is how the probability \( P_t \) of large cascades depends on \( n_d \), the size of the attack (Fig. 3). For small \( n_d \), \( P_t \) increases with \( n_d \) with a rate which decreases with \( \alpha \). For small tolerance \( \alpha \leq 2 \), \( P_t \) reaches 100% (for the case of \( \alpha = 1 \), it does it at \( n_d \approx 80 \) in our example of \( N = 10000 \) and \( (k) = 8 \)). After this, \( P_t \) stays at 100% until it starts to decrease for very large values of \( n_d \). For larger values of the tolerance \( \alpha \), \( P_t \) increases with \( n_d \) until it reaches a maximum, \( P_{t_{\text{max}}} \) at the “most efficient” attack size \( n_{d_{\text{max}}} \), a quantity which is practically independent of \( \alpha \). As \( N \) exceed \( n_{d_{\text{max}}} \), \( P_t \) starts to decrease to zero again. For \( N = 10000 \) and \( (k) = 8 \), \( n_{d_{\text{max}}} = 270 \pm 20 \). As \( \alpha \) increases, \( P_{t_{\text{max}}} \) decreases monotonically.

Figure 7 shows that as \( n_d \) approaches \( n_{d_{\text{max}}} \) the system becomes more vulnerable for larger system sizes, since for any \( n_d \) and \( \alpha \), \( P_t \) increases with \( N \), the size of the system. This is particularly clear in the case of attacks of sizes \( n_d > n_{d_{\text{max}}} \). The explanation of this phenomenon is the following. Once \( n_d \) becomes comparable with \( N \), the amount of origins and destinations for the traffic becomes \( N - n_d \) and the typical betweenness of nodes becomes roughly proportional to \( (N - n_d)^2 \) instead of \( N^2 \); accordingly, when the ratio of these quantities \( (1 - n_d/N)^2 \) becomes sufficiently smaller than unity, not a single node will be overloaded and no cascades will be observed. From the point of view of real traffic this corresponds to the situation when the area destroyed in the attack is comparable to the size of the entire city. In this case the drivers inside the destroyed area cannot drive, while those drives whose destinations are inside this area cancel their trip. This takes a lot of drivers from the roads and the overall traffic becomes less intense.

Indeed Fig. 4 shows that for smaller \( N \) both \( P_{t_{\text{max}}} \) and \( n_{d_{\text{max}}} \) become smaller. Accordingly, one can hypothesize that for \( N \to \infty \), \( P_t \) will become almost independent of the system size and will increase approximately linearly with \( \ln[n_d/f(\alpha, (k))] \), where \( f(\alpha, (k)) \) is an increasing function of \( \alpha \) and a decreasing function of \( (k) \). By definition, \( n_{dc} \) is
the value at which \( P_1 = 0.5 \) and, thus, \( \ln(n_{dc}) = \text{const} + f(\alpha, \langle k \rangle) \). To verify this relation, and to find the properties of the function \( f(\alpha, \langle k \rangle) \) we plot \( \ln(n_{dc}) \) as function of \( \alpha \) for different values of \( \langle k \rangle \) for large enough sizes \( N \) of the system so that the dependence on \( N \) can be neglected. This is illustrated in Fig. 5. One can see an approximate linear behavior: \( f(\alpha, \langle k \rangle) \approx a(\langle k \rangle)\alpha + b(\langle k \rangle) \), where \( a(\langle k \rangle) \) and \( b(\langle k \rangle) \) are functions of \( \langle k \rangle \). While the dependence \( b(\langle k \rangle) \) is weak, \( a(\langle k \rangle) \) diverges when \( k \to k_c = 4.512 \) as a power law, indicating that it is a function of a correlation length, \( \xi \), of the percolation phase transition \([10]\), which diverges for \( k \to k_c \). This can be explained qualitatively by considering the shortest paths which cross the initial circle of attack of radius \( R \) along a certain direction. The number of such independent paths is \( R/\xi \). After the attack, all these paths will be rerouted through a node on the perimeter of the circle, and hence its load will increase by factor \( R/\xi \). So for this node to be overloaded, and the damage done by the initial attack start to spread, \( R \) must satisfy a condition \( R > (1 + \alpha)\xi \). Thus \( n_{dc} \), the size of a critical attack, should be a monotonic function of the product of \( \alpha \) and \( \xi \). Quantitatively, however, this simple scaling equation is incorrect and requires improvements which we leave out for future studies. From Fig. 5 one can conclude that for the same tolerance \( \alpha \) the system becomes more vulnerable for larger \( \langle k \rangle \) since \( n_{dc} \) is a decreasing function of \( \langle k \rangle \).

3.2 Localized vs. Random Attacks

In random networks not embedded in space [5] the critical fraction of nodes \( 1 - p = n_{dc}/N \) increases linearly with \( \alpha \) for small values of the tolerance, and practically does not depend on \( N \). Also, it has been found there that random attacks are more efficient than localized ones [5].

Here we will examine if these facts are also true for the Motter and Lai model on a two-dimensional geometric graph. Figure 6 compares the fraction of large cascades \( P_1 \) as function of the size of the initial attack \( n_d \) for \( \alpha = 2 \), \( \langle k \rangle = 8 \) and \( N = 10000, 20000 \) and 40000. We can see that in the left region of the curves (where the vulnerability still increases with the size of the attack) for increasing system sizes, \( P_1 \) decreases with \( N \) for fixed \( \alpha \) and \( n_d \), i.e. the larger networks are less vulnerable than smaller ones; and this is true for all three types of attacks, not only for the circular ones. Therefore, \( n_{dc} \) increases with increasing \( N \). Still, \( 1 - p_c = n_{dc}/N \) the fractional size of the attack, decreases when \( N \) increases, similarly to the case of random networks. There the \( 1 - p_c \) decreased linearly with \( \ln N \) with a very small slope. However, in case of the embedded networks studied here, \( 1 - p_c \) decreases with \( N \) approximately as a power law \( N^{-0.75} \) for all types of attacks. Also, one can see that a random attack is less efficient (or damaging) than a circular one and that the circular attack is, in turn, less efficient than the linear one. The fact that a linear attack is more efficient than a circular one is easy to explain. The idea is that the overload happens, as discussed, when the linear size \( R \) of the attack is greater than \( (1 + \alpha)\xi \), and for a linear attack this requires fewer attacked nodes \( n_d \) than for the circular attack of the same linear size. Random attacks were more efficient in terms of destroying a network than localized attacks in random networks not embedded in space; this has been explained by taking into account that random attack eliminated more links than localized attacks. Why this is not the case in the networks under study here is not clear, However a similar effect is observed in interdependent networks embedded in space [11] [12] [13]. This is not a trivial observation, and requires further study.

3.3 Temporal and Spatial Propagation of the Cascade

In a localized attack on a random network not embedded in space [5], the nodes which are closest to the initial attack have a smaller probability of being overloaded during the first stages of the attack compared with nodes far from the attacked region, while another work [3] has demonstrated that for the networks on a square lattice immediately after the initial attack the overloaded nodes are concentrated near the perimeter of the attack, while at later stages they spread around the area of the initial attack as concentric circles. To examine which of these two scenarios is correct for circular attacks on a random geometric graph, we compute histograms of the distances from the central node of the attack of the overloaded nodes at the different stages \( t \) of the cascade [Fig. 7(a)] for \( N = 10000, \alpha = 2 \) and \( n_d = 64 \). The distance of a node from the central node is computed as the length of the shortest path connecting these two nodes. Because in our model all the nodes are located in the unit square, these distance are distributed between 0 and 1. Also, the smallest bin of the distribution in all cases is depleted, because the nodes deleted during the initial attack are all concentrated near the central node. For \( t = 1 \) the distribution has a sharp peak close to the origin. As \( t \) increases, the peak widens and shifts towards the larger distances.

Whether the cascade will spread over the entire system or stop is decided during its first few stages, when the number of failed nodes at each stage, \( F(t) \), slightly decreases with \( t \) [Fig. 7(b)]. After this, if the cascade survives, \( F(t) \) starts to grow faster than linearly. \( F(t) \) presents a characteristic maximum near the middle stages of the cascade. The number of nodes in this maximum grows as \( N \), the same as observed for the \( \zeta \) model on lattice graphs [3], while the width of the peak stays constant with the size of the system; these two facts indicate that the total fraction of the overloaded nodes at the end of the cascade is independent of the system size.
The average distance of the nodes overloaded at stage \( t \) increases linearly with \( t \) at the beginning, while the size of the overloaded area is much smaller than the size of the system [Fig. 7(c)]. For small \( t \) many cascades propagate slowly, being on a brink of extinction, especially for \( n_d < n_{dc} \). After this initial latent period of the cascade, after \( F(t) \) reaches its minimum and before it reaches its maximum (which happens when the size of the overloaded area becomes comparable to the system size), the velocity of the cascade propagation is approximately constant. The average velocity in this regime is a slightly decreasing function of the size of the system \( N \). This is due to the fact that the linear size of the system in our simulations does not depend on \( N \), and the stage \( t_{\text{max}} \) when \( F(t) \) reached its maximum is practically independent on \( N \), while the total number of nodes overloaded by this time is proportional to \( N \). Accordingly, the overloaded nodes are distributed in the same number of growing fingering shapes corresponding to different stages of the cascade, which for larger \( N \) contain larger number of nodes. Thus one can expect that the velocity of the cascade spatial propagation would depend very mildly on \( N \). In contrast with that, one can expect that the velocity \( v \) of propagation of the cascade should decrease when the tolerance \( \alpha \) increases. Indeed, we found (Fig. 7(d)), that \( v \approx v_0(\langle k \rangle)\alpha^{-0.6} \) for the networks with different average degrees. The prefactor \( v_0(\langle k \rangle) \) diverges as \( (\langle k \rangle - \langle k_c \rangle)^{-0.43} \) as a function of the correlation length.

Figure 1 shows that the nodes deleted at each stage of the cascade follow some shortest “roads” avoiding the previously overloaded area. Thus, the fastest growth occurs near the tips of the previously overloaded area and, hence, the growth of the overloaded area somewhat resembles viscous fingering [14]. It is not surprising that for the linear and the circular attacks this growth mechanism is similar. What is unexpected is that for the random attack, after a first few stages when the overloads are randomly distributed over the entire system, these overloads become concentrated near fixed centers, after which the growth of the overloaded area starts to resemble the viscous fingering of the circular attacks around these centers (Fig. 8). Obviously, the type of instability in the Motter and Lai model differs from the Saffman-Taylor instability [14], but it is definitely not the circular growth observed in [3] for a lattice model and resembles the equipotential lines of a dipole.

4 Conclusion

We investigate the Motter and Lai model on a two-dimensional random geometric graph with average degree \( \langle k \rangle \) for the case of circular, linear and random initial attacks. We find that the distribution of the sizes of the cascades is bimodal, consisting of very small cascades and very large cascades which destroy a finite fraction of the entire system, and nothing in between. We define the critical size of the attack \( n_{dc} \) as the number of initially deleted nodes at which the probability of large cascades \( P_L \) is 50%. We find the following qualitative properties of the system.

(i) The random attacks are less efficient than circular attacks which are, in turn, less efficient than linear attacks.

(ii) The larger systems are less vulnerable than smaller systems for the same \( \alpha \) and \( \langle k \rangle \) if \( n_d \ll N \).

(iii) In a marked difference with the networks not embedded in space, the critical size of the attack \( n_{dc} \) is not proportional to \( N \) as it is for the not embedded networks, but only mildly increases with \( N \).

(iv) The densely connected graphs with large average degree \( \langle k \rangle \) are more vulnerable than the graphs with smaller average degree.

(v) The critical size of the attack, \( n_{dc} \), increases exponentially with the tolerance \( \alpha \).

(vi) For large enough \( \alpha \), there is a most efficient attack size at which \( P_L \) reaches a maximum. The height of this maximum, \( P_{t_{\text{max}}} \), increases with the system size \( N \), until it reaches 100%.

(vii) At the beginning of a localized attack the overloads are concentrated near the area initially attacked.

(viii) At later stages of the cascade, the growth of the overloaded region is not circular but resembles viscous fingering around a few centers for the case of a random attack, or around the central node in the case of a localized attack (both for circular or linear attacks).

(ix) The spatial speed of the propagation of the cascade, for the case of circular and linear attacks, is practically independent of \( N \), but it is inverse proportional to a power of the tolerance \( \alpha \), and proportional to a power of a correlation length.

(x) Near the critical attack size \( n_{dc} \), the cascades have an initial latent period during which the number of overloaded links at each step fluctuates near zero and the cascade may spontaneously stop.

All these qualitative relations require further detailed investigation in order to determine accurate scaling laws behind them.
5 Acknowledgements

This research is supported by the Defense Threat Reduction Agency grant HDTRA1-19-1-0016 and by Binational Science Foundation Grant No. 2020255. We also acknowledge the partial support of this research through the Dr. Bernard W. Gamson Computational Science Center at Yeshiva College. We thank A. Bashan, D. Vaknin and S. Havlin for useful comments.

References

[1] A. E. Motter and Y.C. Lai, Cascade-based attacks on complex networks, Phys. Rev. E 66, 065102 (2002).
[2] A. E. Motter, Cascade Control and Defense in Complex Networks, Phys. Rev. Lett. 93, 098701 (2004).
[3] J. Zhao, D. Li, H. Sanhedrai, R. Cohen and S. Havlin, Spatio-temporal propagation of cascading overload failures in spatially embedded networks, Nature Communications 7, 10094 (2016).
[4] I. A. Perez, D. Vaknin, C. E. La Rocca, S.V. Buldyrev, L. A. Braunstein and S. Havlin, Cascading failures in isotropic and anisotropic spatial networks induced by localized attacks and overloads, New Journal of Physics (in press, 2022); arXiv preprint arXiv:2112.11308 (2021).
[5] Y. Kornbluth, G. Barach, Y. Tuchman, B. Kadish, G. Cwilich, and S. V. Buldyrev, Network overload due to massive attacks, Phys.Rev. E 97, 052309 (2018).
[6] Y. Kornbluth, G. Cwilich, S. V. Buldyrev, S. Soltan, and G. Zussman, Distribution of blackouts in the power grid and the Motter and Lai model, Phys. Rev. E 103, 032309 (2021).
[7] Y. Yang T. Nishikawa and E. Motter, Small vulnerable sets determine large network cascades in power grids, Science 358, eaan3184 (2017).
[8] M. Anghel, K. A. Werley and A. E. Motter, Stochastic model for power grid dynamics, Proceedings of the 40th Annual Hawaii International Conference on System Sciences HICSS-07, Waikoloa, Big Island, HI, USA, vol. 1, p. 113 (2007).
[9] P. Balister, A. Sarkar and B. Bollobas, Percolation, Connectivity, Coverage and Colouring of Random Geometric Graphs, Handbook of Large-Scale Random Networks, editors B. Bollobas, R. Kozma, D. Miklos, pp 117-142, (Springer-Verlag Budapest, 2008).
[10] D. Stauffer and A. Aharony, Introduction to Percolation Theory, Taylor and Francis, (Philadelphia, 1994).
[11] Y. Berezin, A. Bashan, M. M. Danziger, D. Li and S. Havlin, Localized attacks on spatially embedded networks with dependencies, Sci. Rep. 5, 8934, (2015).
[12] W. Li, A. Bashan, S. V. Buldyrev, H. E. Stanley, and S. Havlin, Cascading Failures in Interdependent Lattice Networks: The Critical Role of the Length of Dependency Links, Phys. Rev. Lett. 108, 228702 (2012).
[13] D. Vaknin, M.M. Danziger and S. Havlin, Spreading of localized attacks in spatial multiplex networks, New J. Phys. 19, 073037, (2017).
[14] Philip Geoffrey Saffman and Geoffrey Ingram Taylor, The penetration of a fluid into a porous medium or Hele-Shaw cell containing a more viscous liquid, Proc. Royal Soc A. 245, 1242 (1958).
Figure 1: (a) Circular attack on a geometric graph with $N = 10000$, $(k) = 8$ and $\alpha = 2$. The white circles represent the nodes attacked initially ($n_d = 64$). The red circles are the nodes overloaded at the first stage of the cascade. (b) The end of the cascade of the attack shown in (a). Different colors in rainbow order (red, orange, yellow, green, cyan, blue, violet) show the stages of the cascade from 1 to 37. (c) Circular attack on $n_d = 64$ nodes in a different graph, also of $(k) = 8$ which ends after 7 stages without damaging the giant component. (d) Linear attack on the same graph with $n_d = 16$ at the end of the cascade at stage 40. The color code is the same as in panel (b). (e) Stage 1 of the cascade after a random attack with $n_d = 64$. (f) Final stage 37 of this random attack. The color code is the same as in panel (b). One can see that the overloads on the first stage are spread uniformly but at later stages (yellow and green) they are concentrated near three centers, resembling the patterns in panels (b) and (d).
Figure 2:  (a) Cumulative distribution of $N_f/N$, the fraction of nodes not overloaded at the end of the cascades for different attack size $n_d$, for $N = 20000$, $\langle k \rangle = 8$, and $\alpha = 2$. (b) Cumulative distribution for the fraction of nodes in the giant component, $N_c/N$. (c) Cumulative distribution for the number of stages in the cascades $N_t$ for the same set of parameters. The distributions are produced from 1000 independent realizations of the network with a randomly selected central node. The lines corresponding to large $n_d$ for which the fraction of large cascades starts to decrease with increasing $n_d$ are shown in red.
Figure 3: The fraction of large cascades, $P_L$, as function of the attack size $n_d$ for different tolerances $\alpha$, for $N = 10000$ and $\langle k \rangle = 8$. The lines corresponding to large $\alpha$ exhibit a maximum at the most efficient attack size $n_{\text{dmax}}$ at which $P_L < 1$. The horizontal line $P_L = 0.5$ shows the crossing which defines the critical attack size $n_d = n_{dc}$. For small $\alpha$, $P_L$ reaches unity at a certain $n_d > n_{dc}$, and stays at this value until $n_d$ becomes comparable with the system size $N$. 
Figure 4: The percent of large cascades as function of the attack size $n_d$ for different tolerances $\alpha$ and different system sizes $N$. Different values of $\alpha$ are indicated by different colors, while different $N$ are indicated by different symbols. One can conjecture that even for $\alpha = 3$ (green lines) for larger $N > 20000$, $P_L$ would reach unity. Also one can see, on the left side of the curves that for large $N$, $P_L$ becomes a slowly varying function of $N$, which might converge to a fixed limit when $N \to \infty$. 
Figure 5: The behavior of $n_{dc}$ as function of $\alpha$ for different values of $\langle k \rangle$. Inset: the dependence of $n_{dc}$ as function of $\langle k \rangle - 4.512$ for $\alpha = 0.6$ as an example of the power law behavior of the size of the 50% risk attack as function of the distance to the percolation critical point. The slope is approximately equal to 1.2.
Figure 6: Comparison of $P_\ell$ as function of $n_d$ for linear, circular and random attack for different system size $N$, for $\langle k \rangle = 8$ and $\alpha = 2$. 
Figure 7: Propagation of the overload cascades around the circular attack. (a) The PDF of the distances of the overloaded nodes to the central node of the attack, at stages $t$ of the cascade, for $n_d = 64$, $N = 10000$, $\alpha = 2.0$ and $\langle k \rangle = 8$. (b) The number $F(t)$ of nodes overloaded at stage $t$ of the cascade for different system sizes $N$ and for different sizes of the attack ($n_d$). Note that each curve is scaled to the size of the corresponding system. (c) The dependence of the average distance from the central node of the nodes overloaded at stage $t$ of the cascade as function of $t$. The circles indicate the most probable distance of the overloaded nodes from the central node at stage $t$, i.e. the position of the peak of the PDFs in panel (a). In (b) and (c) $\langle k \rangle = 8$ and $\alpha = 2$. (d) Dependence of the velocity of the cascade, (defined as the slope of initial linear part of the graph in panel(c)), with the tolerance $\alpha$, for different values of $\langle k \rangle$. $N = 10000$ and $n_d = 64$. 
Figure 8: A snapshot of a system of $N = 40000$ nodes at stage $t = 19$ of the cascade of overloads, following a random initial attack with $n_d = 128, \alpha = 2.0$ and $\langle k \rangle = 8$. 