Threat Networks and Threatened Networks: Interdisciplinary Approaches to Stabilization and Immunization

H. Eugene Stanley[1] and Shlomo Havlin[1,2]

[1] *Center for Polymer Studies and Department of Physics*

Boston University, Boston, MA 02215, USA

[2] *Minerva Center and Department of Physics, Bar-Ilan University, Ramat Gan, Israel*

(goolsby.tex last revised: 25 April 2003)

I. THE GOAL

Our scientific goal is to uncover common principles governing the behavior of a range of social networks. Our practical goal is to use this understanding to develop specific strategies to destroy threat networks, and in parallel to develop specific strategies to defend threatened social networks against attack. There is evidence that progress toward achieving both goals can be achieved using new approaches from modern statistical physics to social network structure and dynamics that our group has contributed to.

II. THE "RESEARCH GROUP"

H. E. Stanley, University Professor and Professor of Physics, leads a research group focused on a range of interdisciplinary problems concerned both with scale-invariant social networks and with social networks lacking scale invariance (see, e.g., Ref. [1]). A significant fraction of his recent papers are on the subject of interdisciplinary approaches to the understanding of real-world networks, with special emphasis on social networks. He served as Ph.D. thesis advisor to A.-L. Barabási, the leader in the modern theory of networks. He has been identified by Science Citation Index for being among the 100 most-cited physicists worldwide. He received national recognition as recipient of this year's NSF Director's Award, and he has been invited to speak on new developments in understanding the structure and dynamics of social networks.

An important member of our research group, whose work is key to the success of this project, is Professor S. Havlin, Director of the Minerva Center, Bar-Ilan University, Israel. He is acknowledged to be among the top 10 workers in the modern theory of networks, and figures prominently in the recent book on modern networks by A.-L. Barabási [2]. In particular, Professor Havlin has pioneered mechanisms to attack threat networks and immunize social networks against attack.

III. TOPICS INVESTIGATED

Populations, which can be viewed as networks of social acquaintances, are vulnerable to disease epidemics initiated by terrorist organizations. Any random immunization of people against such an attack is problematic because it must encompass almost the entire population in order to successfully stop the spreading damage [3–7]. Other types of social networks are organizations, such as military or security agencies, where working relations are represented by links. To be effective, those organizations must be stable and allow fast data flow in the network. We propose to address these problems — using concepts and tools of both social sciences and statistical and nonlinear physics — by designing more stable social network structures, enabling them to resist random and intentional attacks. Further, we will develop efficient strategies for immunizing population networks. For this purpose we will need to better understand the topological structures of existing social networks, and to improve our understanding of transport in such systems.

Our methods in statistical physics are based on relatively new concepts, such as correlated site-bond percolation theory, which has been pioneered by our research group [8–10]. The applications of percolation theory range from predicting the amount of oil that can be extracted from an underground reservoir, to understanding the network formation mechanism involved in the hardening of a boiled egg. The use of percolation theory by our interdisciplinary team has already proven valuable in the study of social networks. We have generalized percolation theory in order to analyze the structure and stability of general networks under random failures [11] and intentional attacks [12]. Based on this generalization, we propose to study a novel approach for designing new social networks that are more resilient to intentional attacks. We also will develop methods based on our percolation approach [13] that will enable us to more effectively immunize populations against different types of epidemics.

IV. RECENT ADVANCES OF OUR GROUP AND OTHER GROUPS

A. Scale-Free Social Networks

Very recent analysis of social networks, as well as many other networks (such as trust networks and sexual networks), reveals that some of these networks display the important property of being scale-free [1,4,14], i.e., there is a very wide distribution of the number of links per vertex. Most vertices have a small number of connections. However, there are a small number of vertices that have a very large number of connections, and there are vertices in the full range between these extremes. Further, it seems that there is a possible explanation for this scale free behavior [15], and that the results for sexual networks extend to other social networks [16].

Our group is studying the structure of a wide range of social network types [17], and is building mathematical models of large social networks [13]. In studies we have conducted about the stability of scale-free social network we have proven that these networks are optimally resilient to random failure of individuals [11]. Even if almost all elements of a network malfunction, a large fraction of the individuals will be left connected, and will allow interactions between a large fraction of the population. This situation is unlike that of homogeneous networks, in which such a failure will break the entire network into small unconnected islands. On the other hand, a deliberate attack on the most connected elements in the network, which will put them out of action, will lead to failure of the entire network after only a small fraction of nodes have been targeted [12]. Further, studies show that search can be conducted in such heterogeneous network in a much more efficient way than in a homogeneous network [18].

A deep connection exists between (a) the stability of a network and (b) the propagation of disease. Heterogeneous networks are prone to the rapid spreading of epidemics. If the individuals to be immunized are chosen randomly, spreading is unavoidable, even if almost all individuals in the network are immunized. However, if the individuals to be immunized are chosen using "smart" strategies, it becomes possible to reduce the number of infected individuals to almost zero. Using models, it is possible to forecast the consequences of epidemic outbursts and to try to control them. It is established that random immunization of a large fraction of the population fails to prevent epidemics of diseases that spread upon contact between infected individuals; for example, Malaria requires 99% of the population to be immunized in order to stop epidemic spreading [6,7]. On the other hand, targeted immunization of the most-connected individuals requires global knowledge of the topology of the social network in question, rendering 99% immunization impractical. We proposed recently an effective strategy, based on the immunization of a small fraction of *acquaintances* of randomly-selected individuals, that prevents epidemics without requiring global knowledge of the social network [19].

Our group's work on social networks has attracted sufficient attention in the social science community that the authors of these studies have already been invited to present their work at international conferences, and have been invited by Oxford University Press to prepare a monograph on social networks. This work is very tentative, and more work is needed before it can be applied to destroying threat networks.

B. Traffic Flow on Networks

We will adapt to social network analysis recent results on traffic flow. In 1994 Leland et al. [20] found that Ethernet LAN traffic is self-similar, so that "bursts" occur on every time scale. These findings show that long-range correlations in the interval times of arriving packets and extreme variability (or infinite limit of the variance). Paxson and Floyd [21] have found evidence for self-similarity of Wide Area Network (WAN) Traffic, and showed the failure of Poisson modeling in this case. New empirical findings challenge the validity of the traditional queuing models, and new models have since been proposed. In contrast to the above measurements, Takayasu et al. [22,23] have measured a $1/f$ power spectrum only at the critical point of a phase transition, and it is still not clear whether the flow is always self-similar in such networks. They found finite correlation times in the fluctuations of network traffic, and identified phase transitions between "sparse" and "jam" phases of the network.

The empirical phenomena mentioned above can influence the design of control schemes for traffic. However, the empirical description of the traffic is not yet complete. As we have demonstrated recently in the case of vehicular traffic [24], a careful nonlinear statistical analysis of measured data may lead to the finding of several congested phases. One of our goals is to clarify this issue, and one method that we will use in the analysis of measured time series is Detrended Fluctuation Analysis (DFA). DFA was developed by our group [25] and has been successfully applied by us and others to many systems, e.g., to DNA sequences, the analysis of climate changes, heart rate variability, and economics. One of the advantages of this method is its ability to detect long-range correlations in the records in the presence of trends and other nonstationarities.

V. DESCRIPTION OF THE ONGOING WORK

A. Preliminary Results of Our Group

We have developed a method that classifies complex real-world networks according to their statistical topological properties [17]. By studying a wide range of different types of networks, we find evidence for the occurrence of three classes of small-world networks:

(a) scale-free networks,

(b) broad-scale networks, characterized by a connectivity distribution that has a power-law regime followed by a sharp cut-off;

(c) single-scale networks, characterized by a connectivity distribution with a fast-decaying tail.

We have also developed a percolation approach for general networks and obtained surprising results for scale-free networks [11–13]. The network is fully resilient to random failure of sites and is extremely vulnerable to intentional attack. Our analytical approach will enable us to study realistic social networks—e.g., where known correlations between individuals are included—where the measured clustering property and the real geographical distance, measured experimentally, will be taken into account. We have already preliminary findings showing that the geographical effect has a strong influence on the stability and transport of the network [26,27].

B. Structural and Transport Properties of Networks

We also plan to study several topological properties of networks—e.g., clustering and correlations. Some preliminary results already exist, such as the work on clustering in trust networks [28]. The clustering coefficient [29,30], which quantifies the extent to which nodes adjacent to a given node are linked, seems not to be affected when the network collapses.

This is relevant to terrorist organizations that are comprised of small strongly-connected cells that are connected to each other by a few, highly-connected individuals [31]. The clustering was found to also be important in electric power networks, e.g., the power grid in the Western States in which the clustering coefficient is significantly larger than that of random networks. A useful method to quantify correlations (by measuring assortative tendencies, i.e., the tendency of high-degree vertices to associate preferentially with other high-degree vertices) was suggested recently by Newman [32].

We plan to extend these studies to other real social networks and to study also the degree distribution for sites at a given distance from the most-connected site. We will also study the effect of geographical distance in real networks. This information is important for evaluating the stability and the immunization threshold. We will also analyze the transport properties of data flow in social networks. We will apply DFA analysis and multifractal analysis [33] to better understand transport in complex social networks. We plan to develop structural and transport modeling that will enable better understanding of the structure and transport in such networks.

C. Optimizing the Stability of Threatened Networks

We will use the analytical approach we developed to calculate the percolation threshold for a given network [11,12], in order to design topologies that improve the stability of scale-free networks under both random failures and intentional attacks. This will be done by calculating the percolation threshold while keeping the average number of links for an individual in the network constant (for safety and security reasons) and then varying parameters such as the form of the degree distribution, the type of correlations, and the clustering coefficients. We will also test the effect of geographical distances on the stability of scale free networks. This will enable us to propose ways to design more stable networks and to improve the stability of existing networks.

D. Additional Work

Random immunization fails to prevent epidemics of diseases that spread in populations upon contact between infected individuals [6,7]; the same is true for immunization of computers against viruses [34]. Unless almost the entire system is immunized, the virus continues to spread through the population or computer network. To deal with this problem, we have developed an analytical method that can accurately determine, for various scenarios, the threshold needed to stop spreading epidemics [13]. Among these possible scenarios are (i) immunizing people who are acquaintances of an infected individual, (ii) immunizing only those people who are acquaintances of at least two infected individuals, or (iii) immunizing only those people who are acquaintances of highly-connected infected individuals.

Our recent results on social networks are complemented by analogous strategies for protecting other threatened networks, such as communication networks. For example, we have already demonstrated that, in scale-free uncorrelated networks, if we immunize the neighbors of randomly-chosen sites, the critical threshold can be reduced by a factor of five [19]. This result has dramatic practical implications.

Our analytical approach will enable us to study efficient immunization strategies in more realistic networks where, e.g., correlations, clustering effects, and geographical topology are taken into account. The immunization approach will also help to develop methods to disintegrate targeted organizations, since by removing the nodes that are most relevant for immunity, the targeted network will collapse.

VI. EXPECTED CONTRIBUTIONS

(a) We will improve the tentative explanation [15] of scale-free social networks, and develop a better understanding of the range of social networks that are scale-free [16].

(b) We will develop a better understanding of the topological structures of threatened social networks.

(c) We will develop new algorithms to improve the stability and safety of threatened networks. We will design networks for optimal resistance to epidemics, malfunctions and attacks. We will design efficient and secure algorithms organizational data flow.

(d) We will design efficient methods for effective “immunization” that will greatly reduce spreading in threatened networks—the same mathematics describes spread of infectious agents in social networks, or “viruses” in communication networks. Those methods will also help to identify weaknesses and thereby protect threatened networks.

VII. SPECIAL FEATURES OF OUR RESEARCH GROUP

Many of the primary methods to be used in this work have been developed by our research group. These include the analytical percolation approach to general networks [11–13], the efficient immunization theory [19,13], and the DFA method [25]. We also were among the first to identify scale-free networks in certain social systems and sexual networks [14–16], and we developed an approach for classifying network topologies [17].

REFERENCES

[1] H. E. Stanley, “Power Laws and Universality,” Nature **378**, 554 (1995).

[2] A.-L. Barabási, *Linked: The New Science of Networks* (Perseus Publishing, Cambridge, 2002).

[3] R. Albert, H. Jeong and A.-L. Barabási, “Attack and Error Tolerance of Complex Networks,” *Nature* **406**, 378–382 (2000).

[4] R. Albert and A.-L. Barabási, “Statistical Mechanics of Complex Networks,” *Rev. Mod. Phys.* **74**, 47–97 (2002).

[5] S. N. Dorogovtsev and J. F. F. Mendes, “Evolution of Networks,” *Adv. in Phys.* **51**, 1079–1187 (2002).

[6] R. M. Anderson, and R. M. May, *Infectious Diseases of Humans* (Oxford University Press, Oxford, 1991).

[7] A. L. Lloyd and R. M. May, “How Viruses Spread among Computers and People,” *Science* **292**, 1316–1317 (2001).

[8] H. E. Stanley, J. S. Andrade, S. Havlin et al., “Percolation Phenomena: A Broad-Brush Introduction with Some Recent Applications to Porous Media, Liquid Water, and City Growth,” Physica A **266**, 5–16 (1999).

[9] A. Bunde and S. Havlin, eds., *Fractals and Disordered Systems* (Springer, New York, 1996).

[10] D. ben-Avraham and S. Havlin, *Diffusion and Reactions in Fractals and Disordered Systems* (Cambridge University Press, Cambridge, 2000).

[11] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, “Resilience of the Internet to Random Breakdown,” Phys. Rev. Lett. **85**, 4626 (2000).

[12] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, “Breakdown of the Internet under

Intentional Attack," Phys. Rev. Lett. **86**, 3682 (2001).

[13] R. Cohen, S. Havlin, and D. ben-Avraham, "Structural Properties of Scale-Free Networks" in *Handbook of Graphs and Networks: From the Genome to the Internet*, edited by S. Bornholdt and H. G. Schuster (Wiley-VCH, Berlin, in press, 2002).

[14] F. Liljeros, C. R. Edling, L. A. N. Amaral, H. E. Stanley, and Y. Åberg, "The Web of Human Sexual Contacts," Nature **411**, 907–908 (2001) cond-mat/0106507.

[15] L. A. N. Amaral, C. R. Edling, F. Liljeros, and H. E. Stanley, "Mechanisms for the Formation of a Web of Sexual Contacts" (preprint).

[16] F. Liljeros, L. A. N. Amaral, and H. E. Stanley, "Scale-Invariance in the Growth of Voluntary Organizations" (preprint).

[17] L. A. N. Amaral, A. Scala, M. Barthélémy, and H. E. Stanley, "Classes of Behavior of Small-World Networks," Proc. National Academy of Sciences **97**, 11149–11152 (2000).

[18] L. A. Adamic, R. M. Lukose, A. R. Punyani, and B. A. Huberman, "Search in Power Law Networks," Phys. Rev. E **64**, 046135 (2001).

[19] R. Cohen, D. ben-Avraham, and S. Havlin, "Efficient Immunization of Populations and Computers," cond-mat/0207387 (2002).

[20] W. E. Leland, M. S. Taqqu, W. Willinger, and D. V. Wilson, "On the Self-Similar Nature of Ethernet Traffic (Extended Version)," IEEE/ACM Trans. Netw. **2**, 1 (1994).

[21] V. Paxson and S. Floyd, "Wide Area Traffic: The failure of Poisson Modeling," IEEE/ACM Trans. Netw. **3**, 226 (1995).

[22] K. Fukuda, H. Takayasu, and M. Takayasu, "Spatial and Temporal Behavior of Congestion in Internet Traffic," Fractals **7**, 23 (1999).

[23] M. Takayasu, H. Takayasu, and K. Fukuda, "Dynamic Phase Transition Observed in Internet Traffic Flow," Physica A **277**, 248 (2000); *Ibid.*, "Application of Statistical

Physics to Internet Traffic," Physica A **274**, 140 (1999).

[24] E. Tomer, L. Safonov, and S. Havlin, "Presence of Many Stable Nonhomogeneous States in an Inertial Car-Following Model," Phys. Rev. Lett. **84**, 382 (2000).

[25] C. K. Peng, S. Havlin, H. E. Stanley, and A. L. Goldberger, "Quantification of Scaling Exponents and Crossover Phenomena in Nonstationary Heartbeat Time Series" [*Proc. NATO Dynamical Disease Conference*], edited by L. Glass, Chaos **5**, 82–87 (1995).

[26] A. F. Rosenfeld et al., "Scale-Free networks on Lattices," cond-mat/0205613 (2002).

[27] R. Cohen and S. Havlin, "Ultra Small World in Scale-Free Networks," cond-mat/0205476 (2002).

[28] X. Guardiola et al., "Macro- and Microstructure of Trust networks," cond-mat/020640 (2002).

[29] D. J. Watts and S. H. Strogatz, "Collective Dynamics of 'Small-World' Networks," Nature **393**, 440–442 (1998).

[30] D. J. Watts, *Small Worlds: The Dynamics of Networks between Order and Randomness* (Princeton University Press, Princeton, 1999).

[31] V. E. Krebs, "Mapping Networks of Terrorist Cells," Connections **24**, 43–52 (2002).

[32] M. E. J. Newman, "Assortative Mixing in Networks," cond-mat/0205405 (2002).

[33] P. Ch. Ivanov, L. A. Nunes Amaral, A. L. Goldberger, S. Havlin, M. G. Rosenblum, Z. Struzik, and H. E. Stanley, "Multifractality in Human Heartbeat Dynamics," Nature **399**, 461 (1999).

[34] R. Pastor-Sattoras and A. Vespignani, "Epidemic Dyanamics and Endemic States in Compex Networks," Phys. Rev. E **63**, 066117 (2001).