The robustness of interdependent transportation networks under targeted attack

PENG ZHANG1, BAISONG CHENG1, ZHUANG ZHAO1, DAQING LI2−3(a), GUANGQUAN LU4(b), YUNPENG WANG4 and JINGHUA XIAO1

1 School of Science, Beijing University of Posts and Telecommunications - Beijing 100876, China
2 School of Reliability and Systems Engineering, Beihang University - Beijing 100191, China
3 Science and Technology on Reliability and Environmental Engineering Laboratory - Beijing 100191, China
4 Beijing Key Laboratory for Cooperative Vehicle Infrastructure Systems and Safety Control, Beihang University Beijing 100191, China

received 16 July 2013; accepted in final form 13 September 2013
published online 7 October 2013

PACS 89.75.Fb – Structures and organization in complex systems
PACS 05.10.-a – Computational methods in statistical physics and nonlinear dynamics
PACS 89.40.-a – Transportation

Abstract – The modern world is built on the robustness of interdependent infrastructures, which can be characterized as complex networks. Recently, a framework for the analysis of interdependent networks has been developed to explain the mechanism of robustness in interdependent networks. Here, we extend this interdependent network model by considering flows in the networks, and we study the system’s robustness under different attack strategies. In our model, nodes may fail because of either overload or loss of interdependency. Considering the interaction between these two failure mechanisms, it is shown that interdependent scale-free networks show extreme vulnerability. The robustness of interdependent scale-free networks is found in our simulations to be much smaller than that of the single scale-free networks or the interdependent scale-free networks without flows.

Introduction. – Over the past decade, network theory has become one of the major tools that are used to study complex systems and has been proven useful in the description and analysis of complex systems in various fields [1–12]. As one of the most fundamental questions in this field, the robustness of networks has been studied intensively, which has aided in providing efficient solutions to protect real networks against faults or attacks [13–17]. However, most of these studies have been based on the assumption that networks are isolated, neglecting the interdependency among them. Recently, Buldyrev et al. have presented a theory of interdependent networks. In their work, a mutual percolation model is proposed to study the vulnerability of network of networks wherein the links between the networks are interdependency links [18]. This has initiated a series of studies concerning various interdependent networks. Parshani et al. have proposed a theoretical framework for studying the case of partially interdependent networks by defining the coupling strength $q$. Their findings have shown that reducing the coupling strength leads to a change from the first- to second-order percolation transition [19]. Gao et al. have generalized the theory on network of networks, showing that the percolation theory of a single network is a limiting case of this generalization [20–22].

Interdependency does exist among various networks in the form of transferring flows; such networks include airlines, urban road networks, the Internet and power grids [23–29]. The failure of some network components, either because of random breakdown or intentional attacks, could change the balance of the flows, thereby causing overloads and triggering cascading failures, which are likely to cause catastrophes [13–15,30–33]. Motter et al. have presented a model to consider a cascade of overload failures in single networks [13,14]. In this study, we generalize their model to interdependent networks and analyze the robustness of such networks against cascading failures.
caused by both overloads and loss of interdependency under random or intentional attack strategies. First, we study the robustness of interdependent scale-free (SF) networks under various types of attacks and explore in detail the dependence of the robustness on the scaling exponent $\gamma$ of the degree distributions, $P(k) \sim k^{-\gamma}$. Second, we study how interdependent Erdős-Rényi (ER) networks respond to different attack strategies. We lastly perform a study to investigate the effect of the interdependency $q$ on the robustness of coupled networks.

**The model.** In our model, we assume for simplicity that the coupled networks $A$ and $B$ are of the same size, $N_A = N_B = N$, and the same degree distribution, $P_A(k) = P_B(k)$. $q$ quantifies the fraction of nodes having interdependency links to network $B$. Each node in network $A$ depends only on one node in network $B$ and vice versa, which establishes a one-to-one bidirectional dependent relation. The one-to-one bidirectional dependent links are established randomly to avoid any correlations among the two networks. In the iterative failure process, if node $A_i$ stops functioning because of attack or overload failure, node $B_i$, which depends on $A_i$, stops functioning as well, and vice versa. The load quantifies the amount of flows that a request is transmitted and is considered to depend on the total number of shortest paths passing through it [34–36]. The load of node $i$ can be denoted by

$$L(i) = \sum_{(v_1,v_2)} \frac{\sigma_{v_1,v_2}(i)}{\sigma_{v_1,v_2}}, \quad i = 1, 2, \ldots, N, \quad (1)$$

where $\sigma_{v_1,v_2}$ is the total number of shortest paths between node $v_1$ and $v_2$, and $\sigma_{v_1,v_2}(i)$ is the number of shortest paths between node $v_1$ and $v_2$ through node $i$.

Following ref. [13], the capacity of node $i$ is denoted by

$$C(i) = (1 + \alpha) \cdot L_0(i); \quad i = 1, 2, \ldots, N, \quad (2)$$

where $\alpha$ is the tolerance parameter, and $L_0(i)$ is the initial load of node $i$. A node fails when its load exceeds its capacity.

If we intentionally remove (“attack”) some nodes in network $A$, this action will initially induce cascading failure by redistributing loads among the nodes in network $A$. Here, we assume that only the nodes in the giant component remain functional. The failed nodes may disintegrate network $A$, and all nodes outside the giant component will cause their dependency counterparts in network $B$ to fail. These failed nodes in network $B$ will cause overloads, thereby causing more nodes to fail. This process will continue recursively until no further damage is produced, either by overloads or by interdependency losses.

In our model, the links between network $A$ and $B$ only reflect dependence relationships. It is different from that used in ref. [37], wherein the links between network $A$ and $B$ are used for traffic processes.

Various attack strategies have been studied in isolated networks with or without considering overloads in refs. [4,13,14,38–42]. Here we focus on three different attack strategies: i) remove the node with the highest load, ii) remove the node with the largest degree, and iii) remove a node randomly. We compare these three different strategies.

**Results.** Now we present numerical simulations of various attack strategies on interdependent ER networks (ER-ER) and interdependent SF networks (SF-SF) with flows. To generate SF-SF networks, we use the method described in ref. [7]. Using this method, we are able to compare SF networks with different scaling exponents $\gamma$ by fixing the average degree $\langle k \rangle$. The relative size of the largest connected component $G = N'/N$ is used to quantify the network robustness, where $N$ and $N'$ are the size of the largest component before and after cascading, respectively. Considering the computation cost of the overload calculation, the network size chosen for the simulation is $N_A = N_B = 5000$. We intentionally remove the one node with the highest load or the largest degree, and the results are compared to those of random removal. After the initial attack, nodes can fail in a domino-like process because of either overload inside one of networks or loss of interdependency between the two networks. Therefore, the cascading failure process is more complicated in interdependent networks when these two failure mechanisms interact and receive different feedback.

We begin the study with interdependent SF networks. It is shown in fig. 1 that intentional attack causes more damage to interdependent networks than does random removal. The interdependent SF network with $\gamma = 3$ is found to be more vulnerable than the other interdependent networks ($\gamma = 2.3$ and 4.7). Because of the correlation between degree and load [36], the attack based on the node degree is found in our study to be as harmful as the attack based on the node load. Therefore, in the following we will not specify the attack type (based on degree or load) when we refer to attack.
Network heterogeneity has been found to be one of the main causes of cascading failures [38]. The scaling exponent $\gamma$ of a SF network with degree distribution $P(k) \sim k^{-\gamma}$ can characterize the heterogeneity in the degree distribution. We present the robustness against attacks of interdependent SF networks with various $\gamma$ values in fig. 2. It is shown in fig. 2(a) that for $2.5 < \gamma < 3.7$ in the case of interdependent SF networks with average degree $\langle k \rangle \approx 4$, intentional attack on one node with the highest degree (load) will induce the total collapse of the entire interdependent network. Even random removal will cause network damage of over 60%. This demonstrates the extreme network vulnerability as a result of the interaction between the two failure mechanisms: overloads and interdependency losses. For $\langle k \rangle \approx 4$, we found that there exists a “valley” of $\gamma$ between 2.5 and 3.7 for which the interdependent network exhibits minimal robustness. Under random removal, the network also exhibited its minimal robustness near $\gamma = 3$. For larger tolerance $\alpha = 0.9$ in fig. 2(c), a similar pattern is also found, although the valley that corresponds to minimal network robustness is smaller in range, while $G$ is comparatively large because of larger system tolerance $\alpha$.

To determine whether this pattern depends on the average degree, we greatly increase the average degree $\langle k \rangle \approx 14$. With the discovery of a narrow “valley” of $\gamma$, it is suggested in fig. 2(b) and (d) that a larger fraction of interdependent SF networks can be preserved after attacks, indicating that the networks are more robust, for a large average degree. The large-degree effect can be interpreted as an increase in the redundancy of paths between pairs, which relieves the pressure of overloads. By comparing the results shown in fig. 2(a)–(d), the robustness of an interdependent network can be seen to depend significantly on the $\gamma$ values and the average degree $\langle k \rangle$ of the degree distribution $P(k) \sim k^{-\gamma}$.

By comparing the results for an interdependent network to those for a single network, this study will aid in identifying the effects of interaction between two failure mechanisms in interdependent networks. In single networks (coupling strength $q = 0$ in our model), shown in fig. 2(e) and (f), the intentional attack can cause much less damage than in the interdependent networks shown in fig. 2(a) and (b). The difference is also very significant for random removal, which causes almost no damage to the single network. Because it lacks the interaction of two failure mechanisms, the single network is more robust than the interdependent network.

For interdependent homogeneous (ER) networks, fig. 3 shows that when $\alpha = 0$, removing one node will break down the whole system, no matter which removal strategy is applied. When $\alpha = 0.1$, it is shown that targeted attacks can damage the largest connected component by more than 90%. As the tolerance $\alpha$ increases further (above 0.25), the removal strategies become less able to trigger a significant breakdown in the networks. It appears that the
robustness of interdependent ER networks changes more abruptly as $\alpha$ increases than does the robustness of interdependent SF networks, and the narrow betweenness distribution of the interdependent ER networks may be the primary cause of this difference. It also indicates that there exists a critical value of $\alpha$, $\alpha_c$. Using the method described in [43], the critical value $\alpha_c$, can be identified by the peak of the number of iterative (NOI) cascading failures. The inset of fig. 3 presents the NOI values as a function of $\alpha$, obtained from the simulation results. It can be found that the critical value $\alpha_c$ nears 0.15 for attacks and 0.1 for the random removal.

After discussing the process of cascading failures in fully interdependent ER networks and interdependent SF networks with flows, we perform simulations for the case of partial coupling strength $0 \leq q < 1$. In fig. 4, we present the numerical results of determining the largest component $G$ as a function of $\alpha$ in interdependent SF networks under random and intentional attack. It is shown that the network robustness is very sensitive to the interdependency between networks, where interdependency can decrease the network robustness. The single network (coupling strength $q = 0$) is more robust than interdependent networks. It again appears that the interaction between overloads and the loss of interdependency qualitatively changes the network robustness.

Conclusion. — Modern complex networks for transporting different flows are becoming more and more dependent on one another. In this study, we examine the robustness of interdependent networks with flows under random faults and intentional attacks. During the failure processes of the interdependent network, there are two possible failure mechanisms: overloads and loss of interdependency. These two mechanisms may amplify each other, or they may impede each other under certain conditions. For example, the nodes removed because of interdependency loss can relieve the pressure on the network flow and may even reduce the occurrence of overloads [14]. Because of this complicated interaction between overloads and interdependency loss, interdependent SF networks are found to have robustness properties that are distinct from those of interdependent networks without flows. For an interdependent SF network with degree distribution $P(k) \sim k^{-\gamma}$, the network robustness does not change monotonically with the scaling exponent $\gamma$; instead, a valley of minimal network robustness exists within a range of $\gamma$ values. In our simulations, the robustness of an interdependent SF network is found to be much smaller than that of a single SF network or that of an interdependent SF networks without flows. For interdependent ER networks, the robustness changes abruptly as the tolerance parameter $\alpha$ changes, possibly because of the narrow betweenness distribution. We believe that further study of the interaction between overloads and interdependency losses during cascading failures processes is an essential step towards fully understanding the robustness of interdependent transportation networks.

This work was supported by The National Basic Research Program of China (2012CB725404). DL would like to acknowledge the support from National Natural Science Foundation of China (Grant No. 61104144). PZ acknowledges the support from National Natural Science Foundation of China (NSFC) under Grant No. 11147119 and the Fundamental Research Funds for the Central Universities No. 2012RC0707.

REFERENCES

[1] Watts D. J. and Strogatz S. H., Nature, 393 (1998) 440.
[2] Barabási A.-L. and Albert R., Science, 286 (1999) 509.
[3] Albert R. and Barabási A.-L., Science, 74 (2002) 47.
[4] Cohen R., Erez K. K., ben-Avraham D. and Havlin S., Phys. Rev. Lett., 85 (2000) 4626.
[5] Dorogovtsev S. N. and Mendes J. F. F., Evolution of Networks: From Biological Nets to the Internet and WWW (Oxford University Press, New York) 2003.
[6] Caldarelli Guido and Vespignani Alessandro, Large Scale Structure and Dynamics of Complex Networks: From Information Technology to Finance and Natural Science (World Scientific Press, Singapore) 2007.
[7] Cohen R. and Havlin S., Complex Networks: Structure, Robustness and Function (Cambridge University Press, Cambridge) 2010.
[8] Newman M. E. J., Networks: An Introduction (Oxford University Press, New York) 2010.
[9] Schneider C. M., Moreira A. A., Andrade J. S. jr., Havlin S. and Herrmann H. J., Proc. Natl. Acad. Sci. U.S.A., 108 (2011) 9838.
The robustness of interdependent transportation networks under targeted attack

[10] Li G., Reis S. D. S., Moreira A. A., Havlin S., Stanley H. E. and Andrade J. S. Jr., Phys. Rev. Lett., 104 (2010) 018701.
[11] Li D., Kosmidis K., Bunde A. and Havlin S., Nat. Phys., 7 (2011) 481.
[12] Havlin S., Kenett D. Y., Ben-Jacob E., Bunde A., Herrmann H., Kantelhardt J. W., Kertész J., Kirkpatrick S., Portugali J. and Solomon S., Eur. Phys. J. ST, 214 (2012) 273.
[13] Motter A. E. and Lai Y., Phys. Rev. E, 66 (2002) 066102.
[14] Motter A. E., Phys. Rev. Lett., 93 (2004) 098701.
[15] Watts D. J., Proc. Natl. Acad. Sci. U.S.A., 99 (2002) 5766.
[16] Dobson I., Carreras B. A., Lynch V. E. and Newman D. E., Chaos, 17 (2007) 026103.
[17] Simonsen I., Buzna L., Peters K., Bornholdt S. and Helbing D., Phys. Rev. Lett., 100 (2008) 218701.
[18] Buldyrev S. V., Parshani R., Paul G., Stanley H. E. and Havlin S., Nature, 464 (2010) 1025.
[19] Parshani R., Buldyrev S. V. and Havlin S., Phys. Rev. Lett., 105 (2010) 048701.
[20] Gao Jianxi, Buldyrev Sergey V., Havlin Shlomo and Stanley H. Eugene, Phys. Rev. Lett., 107 (2011) 195701.
[21] Gao Jianxi, Buldyrev Sergey V., Stanley H. Eugene and Havlin Shlomo, Nat. Phys., 8 (2012) 40.
[22] Dong Gaogao, Gao Jianxi, Du Ruijin, Tian Lixin, Stanley H. Eugene and Havlin Shlomo, Phys. Rev. E, 87 (2013) 052804.
[23] Sachtjen M. L., Carreras B. A. and Lynch V. E., Phys. Rev. E, 61 (2000) 4877.
[24] Guimerà R., Arenas A., Díaz-Guilera A. and Giralt F., Phys. Rev. E, 66 (2002) 026704.
[25] Pastor-Satorras R., Vázquez A. and Vespignani A., Phys. Rev. Lett., 87 (2001) 258701.
[26] Willinger W., Govindan R., Jamin S., Paxson V. and Shenker S., Proc. Natl. Acad. Sci. U.S.A., 99 (2002) 2573.
[27] Goh K.-I., Kahng B. and Kim D., Phys. Rev. Lett., 88 (2002) 108701.
[28] Parshani R., Rozenblat C., Ietri D., Ducruet C. and Havlin S., EPL, 92 (2010) 68002.
[29] Rosato V., Issacharoff L., Tiriticco F., Meloni S., de Porcellinis S. and Setola R., Int. J. Crit. Infrastruct., 4 (2008) 63.
[30] Moreno Y., Gómez J. B. and Pacheco A. F., Europhys. Lett., 58 (2002) 630.
[31] Albert Réka, Albert István and Narakost M., Phys. Rev. E, 69 (2004) 025103.
[32] Wang Jian-Wei and Rong Li-Li, Safety Sci., 47 (2009) 1332.
[33] Zio Enrico and Sansavini Giovanni, IEEE Trans. Rel., 60 (2011) 94.
[34] Newman M. E. J., Phys. Rev. E, 64 (2001) 016132.
[35] Goh K.-I., Kahng B. and Kim D., Phys. Rev. Lett., 87 (2001) 278701.
[36] Holme P. and Kim B. J., Phys. Rev. E, 65 (2002) 066109.
[37] Tan Fei, Xia Yongxiang, Zhang Wenping and Jin Xinyu, EPL, 102 (2013) 28009.
[38] Albert R., Jeong H. and Barabási A.-L., Nature, 406 (2000) 378.
[39] Callaway D. S., Newman M. E. J., Strogatz S. H. and Watts D. J., Phys. Rev. Lett., 85 (2000) 5468.
[40] Cohen R., Erez K., Ben-Avraham D. and Havlin S., Phys. Rev. Lett., 86 (2001) 3682.
[41] Crucitti Paolo, Latora Vito and Marchiori Massimo, Phys. Rev. E, 69 (2004) 045104.
[42] Wang Xiao Fan and Xu Jian, Phys. Rev. E, 70 (2004) 056113.
[43] Parshani R., Buldyrev S. V. and Havlin S., Proc. Natl. Acad. Sci. U.S.A., 108 (2011) 1007.