Research Article

Vulnerability Analysis of Interdependent Scale-Free Networks with Complex Coupling

Chunjie Cao,[1,2] Zhiqiang Zhang,[2] Jingzhang Sun,[2] Xianpeng Wang,[1,2] and Mengxing Huang[1,2]

[1]*State Key Laboratory of Marine Resource Utilization in South China Sea, Hainan University, Haikou, China*
[2]*College of Information Science & Technology, Hainan University, Haikou, China*

Correspondence should be addressed to Zhiqiang Zhang; zhiqiang_zhang@hainu.edu.cn

Recent studies have shown that random nodes are vulnerable in interdependent networks with simple coupling. However, relationships in actual networks are interrelated and complex coupling. This paper analyzes the vulnerability of interdependent scale-free networks with complex coupling based on the BA model. The results indicate that these networks have the same vulnerability against the maximum node attack, the load of the maximum node attack, and the random node attack, which explain that the coupling relationship between network nodes is an important factor in network design.

1. Introduction

The small-world network model [1] (Watts and Strogatz, 1998) and the scale-free network model [2] (Barabasi and Albert, 1999) inspired research on complex networks. At present, research of complex networks penetrates into almost all fields such as computer networks, social networks, and biological networks. Based on the small-world network model and scale-free network model, researchers have improved the moment conditions. In the field of computer networks, researchers presented an algorithm for building a new small-world network model by combining the two archetypal small-world networks [3], which can better describe the real instant messaging chat network. In the research of the social networks, researchers established a navigable small-world network based on game-theory model [4] and used this to solve the problem of reciprocity and navigability in social networks. In terms of biological networks, researchers found that the FRC network topology is highly robust and revealed the critical role of the network integrity in the activation of adaptive immune responses [5]. Researchers continue to improve the complex network model and laid the foundation for the research of complex network theory.

Currently, network vulnerability analysis is a very important topic in the theoretical research of complex networks, which mainly studies the problem of vulnerability of complex networks under various attacks (such as deliberate attacks and random failures), especially the vulnerability of an interdependent network system. Recently, domestic and foreign scholars have carried out a series of researches on the impact of the complex network vulnerability and triggered cascading failures. In order to analyze constantly changing impact of component failure propagation on the system, Cheng et al. proposed an optimizing model based on game theory [6]. They found that the failure of components has a great negative impact on the physical network system and used a linear programming method to solve this problem. As for how to effectively model critical infrastructures with interdependent relationships, Rinaldi established the interdependent network system using dynamic simulation and identified the range of cascading security operation [7]. According to the complex relationship between the power system and the rapid processing data network, Cai et al. established an interdependent network model to analyze the complex effects caused by cascading failures [8]. The modern society relies on the complex network of critical infrastructure

systems (such as power networks, telecommunication networks, transportation networks, and water supply systems). Although urban communities rely on each independent infrastructure, recent disasters, such as hurricanes, large-scale power outages, and terrorist attacks, have shown that the most dangerous vulnerabilities were hidden between different interdependencies infrastructures. In a system, the failure of a subsystem is likely to result in the failure of the other, and then the failure of cascading is triggered. On September 28, 2003, a power plant in Italy's grids failed, which led to disabling of the corresponding Internet node. This also resulted in other power stations going offline. Eventually, this effect caused a blackout in the southern peninsula [9]. Regarding this event, Buldyrev et al. published the results of a study (April 2010, Nature) [10] showing that the coupled complex network system facing random faults is also fragile.

Buldyrev et al.'s conclusion reveals the effect of network dependence on network vulnerability. However, as Vespignani said, Buldyrev et al.'s model is simply coupled and ideal. It cannot reflect the complex dependency relationship of actual network systems [11]. This BA model based paper studies the network vulnerability of scale-free networks with complex dependency. Results show that the scale-free networks with complex dependencies are vulnerable against the node of the maximum degree, the node of the maximum load, and the random node attack, and when a single node is attacked, most nodes in the network are compromised. This presents a serious challenge to the complex network systems' design and optimization.

2. Network Model

In recent years, researchers have discovered many complex networks, including the Internet, WWW, and metabolic networks; all these networks' connection degree distribution functions have power laws [12–15]. There is no obvious feature length in these networks' nodes connectivity. These networks are called scale-free networks. Currently, researchers propose many optimized methods for the scale-free networks model by using sparse matrix vector multiplication to construct scale-free networks [16], using the internal weighted average method to calculate the configuration parameters of scale-free networks [17], and using boosting regression algorithm and Bayesian algorithm to construct prior information and establish the scale-free networks based on prior information [18]. Random scale-free networks are modeled with chain fault [19]. We add the strategy of multiscale networks to generate artificial neural networks when constructing scale-free networks, which is used to simulate the network performance of the multiscale [20].

2.1. BA Network Model. Barabasi and Albert proposed a scale-free network model (BA model) to describe two important features of actual networks.

(i) Growth characteristic: the network scale is expanding. As a large number of new articles are published every month, such as on the WWW, there are a lot of new web pages every day.
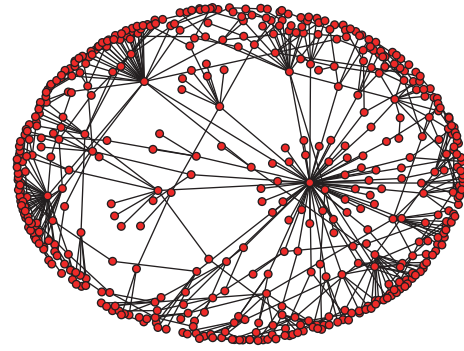

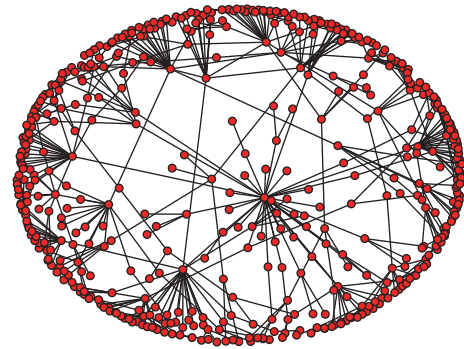FIGURE 1: Scale-free network A.

FIGURE 2: Scale-free network B.

(ii) Priority connection characteristic: the new node tends to connect with nodes with a higher degree. This phenomenon is called "the rich get richer effect" or "Matthew effect."

Based on the growth characteristic and priority connection characteristic, the algorithm for constructing the BA scale-free network model is as follows.
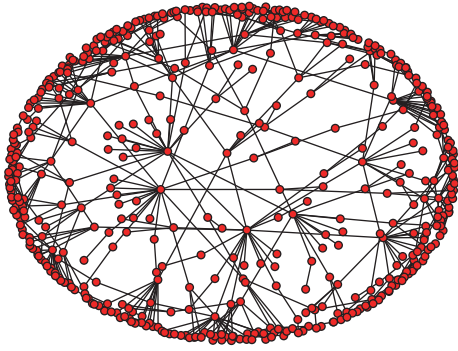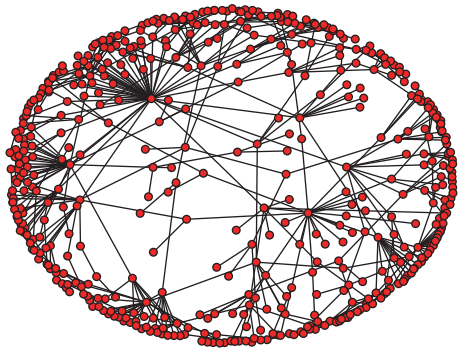
(iii) Growth: the network starts with m_0 nodes, with the addition of a new node and chain to the m existing nodes, where $m \leq m_0$.

(iv) Priority connection: define P_i as the probability of a new node connecting with node i. The relationship between P_i, degree k_i of node i, and degree k_j of node j is as follows:

$$P_i = \frac{k_i}{\sum_j k_j}. \tag{1}$$

(v) After t steps, the BA model construction algorithm generates a network with $N = t + m$ nodes and mt edges.

2.2. Complex Coupling Interdependent Scale-Free Network. Based on the BA scale-free network model constructing algorithm, altogether, at least $T = 100$ samples are made, each time generating two scale-free networks (A and B) with 1000 nodes, as shown in Figures 1-2, and randomly generating coupling coefficient matrixes (M_{AB} and M_{BA}) existing in between networks A and B, as shown in Figures 3-4. If $M_{AB}(i, j) = 1$, then nodes A_i and B_j will have a coupling relationship; that is, if node A_i loses, node B_j fails. If $M_{AB}(i, j) = 0$, then nodes A_i and B_j will have no coupling relationship; that is,

FIGURE 3: Coupling coefficient matrix M_{AB}.

FIGURE 4: Coupling coefficient matrix M_{BA}.

FIGURE 5: Maximum node attack.

FIGURE 6: Node of maximum load attack.

node A_i loses, while node B_j is validated. Coupling coefficient matrix depicts that the relationship of interdependence network nodes does not have to be a two-way direct coupling relationship. And this method also reflects the reality of actual networks. In the network model proposed by Buldyrev et al., interdependence network nodes have a two-way direct coupling relation. That is, if node A_i loses, node B_j fails, and there is no influence on other nodes. And if node B_j loses, node A_i also fails. However, in the actual network, coupling relationships among different network nodes are complex; node A_i possibly has a coupling relationship with node B_{j1} or may have a coupling relationship with node B_{j2}. And node B_j loss does not necessarily result in node A_i failure (e.g., Internet, WWW, and electric power networks). This is our improvement on Buldyrev et al.'s network model.

3. Vulnerability Analysis

In many real networks, a single or a few failed nodes or failed edges (this fault may happen randomly or may be due to a deliberate attack) can cause other nodes to break down through the coupling relationships between nodes and then cause a chain reaction, eventually causing the breakdown of a lot of nodes, even the entire network. This phenomenon is called cascading failure, sometimes called "avalanche" phenomenon. This phenomenon is a widespread problem in traffic networks, Internet networks, power networks, social and economic networks, and other real complex networks.
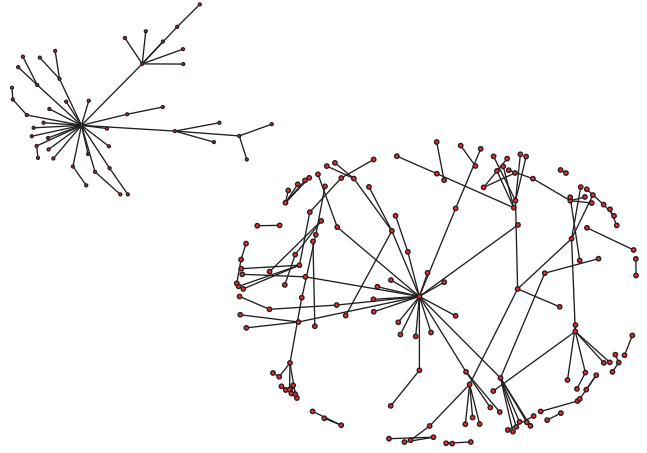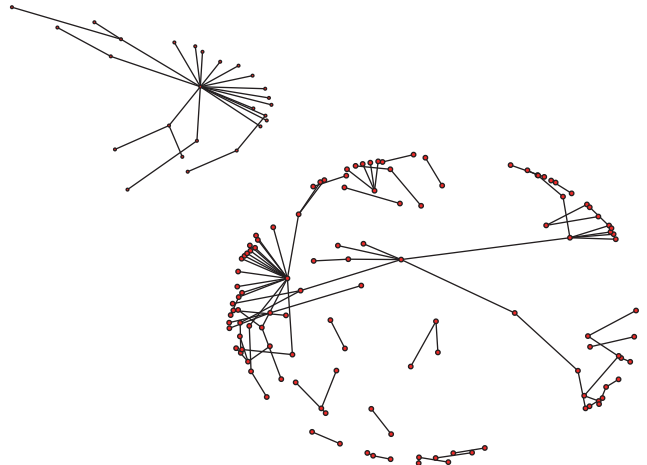
We perform an analysis based on the above network model and attack the node of maximum degree, the node of maximum load, and the random node in network A by using the maximum degree node attack, the maximum load node attack, and the random node attack, negate the effects of the node, and then observe the effect of connectedness of network B. The connectivity is analyzed through the quantity of nodes contained in the maximal connected subset (subgraph) in network B; as shown in Figures 5–7, the nodes of maximum degree and random nodes are easy to select and calculate, and selection of the maximum load node uses the betweenness of the node as a selection standard. Betweenness adopts the Floyd algorithm to calculate the shortest path between nodes of network A.

From a large amount of data analysis under three attack modes, we can see that nonscale networks maintained a similar network topology, and the scale of the largest connected subgraph is approximately equal. As shown in Figure 8, the straight line in the graph is the average value of the maximal connected subgraph under three attack methods. In this figure's bottom left corner is the probability distribution maximal connected subgraph under three attack methods.
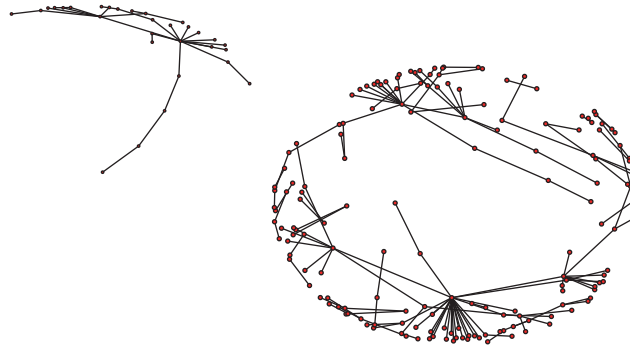
FIGURE 7: Random node attack.

- –▲– Random node attack
- –●– Maximum node attack
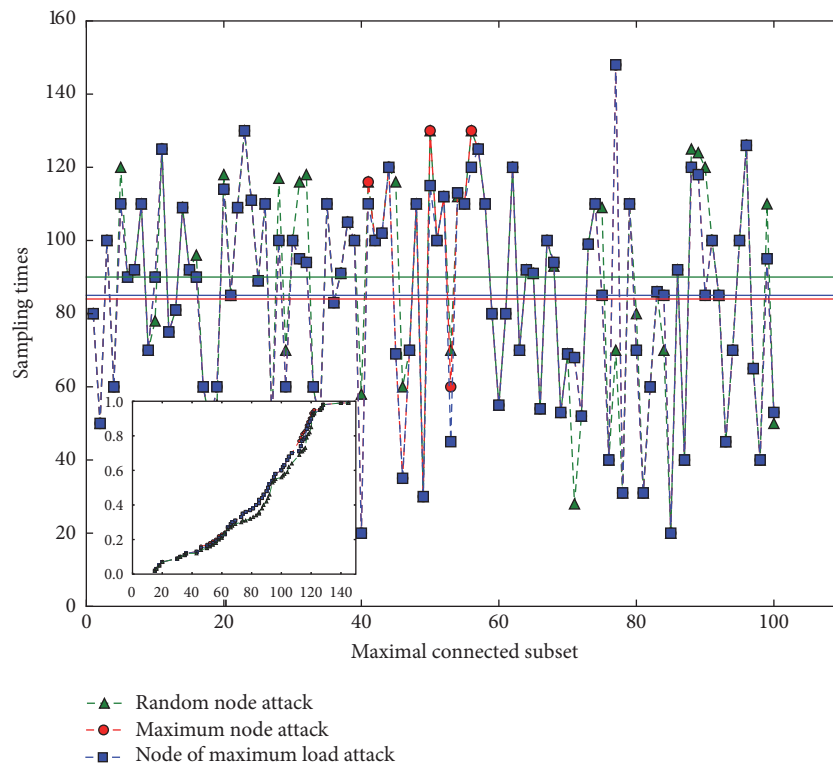- –■– Node of maximum load attack

FIGURE 8: Connected subset size contrast.

Statistical results show that the three attack methods have the same influence on the scale of the largest connected subgraph node of scale-free networks with complex coupling relationships. From the perspective of connectivity, the attack caused the decline of the network performance by 90%.

4. Conclusion

The model proposed by Buldyrev et al. is simply coupled and ideal. It cannot fully present the complicated dependence of the actual network system. This paper studies scale-free networks with complex dependency based on the BA model. Results show that the scale-free networks with complex dependencies are vulnerable against the node of the maximum degree, the node of the maximum load, and the

random node attack, and when a single node is attacked, most nodes in the network are compromised. This presents a serious challenge to the complex network systems' design and optimization. Therefore, the coupling between networks must be taken into account in the design of reliable systems.

Conflicts of Interest

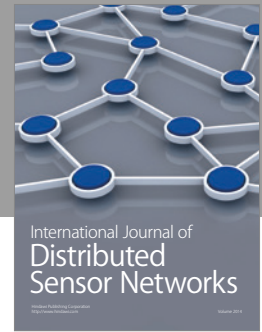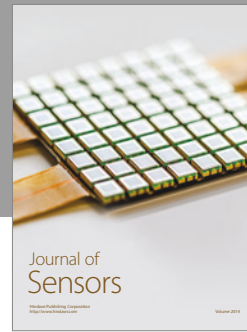The authors declare that they have no conflicts of interest.

Acknowledgments

References

[1] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[2] A.-L. Barabasi and R. Albert, "Emergence of scaling in random networks," *American Association for the Advancement of Science. Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[3] J. Guan, M. Tang, G. Huang, W. Zhu, S. Zhou, and G. Ji, "A new small-world network model for instant messaging chat network," in *Proceedings of the 11th Systems of Systems Engineering Conference (SoSE '16)*, June 2016.

[4] Z. Yang and W. Chen, "A game theoretic model for the formation of navigable small-world networks," in *Proceedings of the 24th International Conference on World Wide Web (WWW '15)*, pp. 1329–1339, May 2015.

[5] M. Novkovic, L. Onder, J. Cupovic et al., "Topological Small-World Organization of the Fibroblastic Reticular Cell Network Determines Lymph Node Functionality," *PLoS Biology*, vol. 14, no. 7, Article ID e1002515, 2016.

[6] M. X. Cheng, M. Crow, and Q. Ye, "A game theory approach to vulnerability analysis: Integrating power flows with topological analysis," *International Journal of Electrical Power and Energy Systems*, vol. 82, pp. 29–36, 2016.

[7] S. M. Rinaldi, "Modeling and simulating critical infrastructures and their interdependencies," in *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, IEEE, January 2004.

[8] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530–538, 2016.

[9] L. A. Nunes Amaral, A. Scala, M. Barthelemy et al., "Classes of behavior of small-world networks," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 97, no. 21, Article ID 0001458, pp. 11149–11152, 2000.

[10] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[11] A. Vespignani, "Complex networks: The fragility of interdependency," *Nature*, vol. 464, no. 7291, pp. 984-985, 2010.

[12] C. Petersen, J. G. Simonsen, and C. Lioma, "Power law distributions in information retrieval," *ACM Transactions on Information Systems*, vol. 34, no. 2, article 8, 2016.

[13] I. Dobson, J. Chen, J. S. Thorp, B. A. Carreras, and D. E. Newman, "Examining criticality of blackouts in power system models with cascading events," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS '02)*, January 2002.

[14] A. Medina, I. Matta, and J. Byers, "On the origin of power laws in internet topologies," *Computer Communication Review*, vol. 30, no. 2, pp. 18–28, 2000.

[15] G. J. Fakas, Z. Cai, and N. Mamoulis, "Diverse and proportional size-l object summaries for keyword search," in *Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD '15)*, pp. 363–375, June 2015.

[16] W. T. Tang, R. Zhao, M. Lu et al., "Optimizing and auto-tuning scale-free sparse matrix-vector multiplication on Intel Xeon Phi," in *Proceedings of the IEEE/ACM International Symposium on Code Generation and Optimization (CGO '15)*, pp. 136–145, February 2015.

[17] S. F. Muldoon, E. W. Bridgeford, and D. S. Bassett, "Small-world propensity and weighted brain networks," *Scientific Reports*, vol. 6, Article ID 22057, 2016.

[18] B. Yang, J. Xu, B. Liu, and Z. Wu, "Inferring gene regulatory networks with a scale-free property based informative prior," in *Proceedings of the 8th International Conference on BioMedical Engineering and Informatics (BMEI '15)*, pp. 542–547, October 2015.

[19] R.-R. Yin, B. Liu, H.-R. Liu, and Y.-Q. Li, "Research on invulnerability of the random scale-free network against cascading failure," *Physica A: Statistical Mechanics and its Applications*, vol. 444, pp. 458–465, 2015.

[20] A. Gutfraind, I. Safro, and L. A. Meyers, "Multiscale network generation," in *Proceedings of the 18th International Conference on Information Fusion (Fusion '15)*, pp. 158–165, July 2015.

Journal of
Engineering

The Scientific World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

International Journal of
Distributed
Sensor Networks

Advances in
Civil Engineering

Journal of
Control Science
and Engineering

Journal of
Robotics

Submit your manuscripts at
https://www.hindawi.com

Journal of
Electrical and Computer
Engineering

Advances in
OptoElectronics

VLSI Design

International Journal of
Navigation and
Observation

Modelling &
Simulation
in Engineering

International Journal of
Aerospace
Engineering

International Journal of
Chemical Engineering

International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components

Shock and Vibration

Advances in
Acoustics and Vibration