Robust Networks to Cascading Failures

Hoang Anh Q. Tran
Dept. of Computer Science
National Defense Academy of Japan
Yokosuka, Kanagawa, Japan
ed13004@nda.ac.jp

Akira Namatame
Dept. of Computer Science
National Defense Academy of Japan
Yokosuka, Kanagawa, Japan
nama@nda.ac.jp

***Abstract*—Nowadays, the ongoing progress of networking in essential utilities such as the Internet, the WWW, transportation networks, electrical power grid networks, etc., brings significant benefits to the quality of our life. However, networked systems hold a certain danger that a failure of a single node in the system may diffuse to all other nodes. This chain of failure is widely known as cascading failure. Examples of cascading failure include disease epidemics, traffic congestion, electrical power system blackouts, and so on. In these systems, if external shocks or excess loads at some nodes are propagated to other connected nodes due to failure, the domino effects often come with disastrous consequences. Thus, how to prevent cascading failures in complex networks becomes an important emergent issue. In this paper, we consider an overload-based cascading failure model and design a robust network structure against this type of cascading failure. Numerical simulations show that the proposed network, which consists of a complete cluster of connected hub nodes, and periphery nodes connecting one of hub nodes in the cluster, is least susceptible to cascading failures compared with other types of networks.**

Keywords- overload; cascading failure; robust network

I. INTRODUCTION

Many complex systems in nature and society can be described by networks, including social and biological systems such as the Internet, the WWW, computer networks, electrical power grid networks, metabolic networks, and so on. In recent years, complex network research has attracted a lot of attention and scientists have made major advances in understanding the topological properties of networks. Interestingly, evidences have been demonstrated that most of nature networks share some important topological similarities, e.g. the small-world and scale-free property. Moreover, a vast number of research have clarified that certain topological properties of complex networks have strong impacts on their stability. Here, network's stability refers to the malfunction avoiding ability of a network when a fraction of its elements are damaged. Previous works have demonstrated that the heterogeneity of a network induces its robustness against errors. That is, scale-free networks with degree distribution heterogeneity might be strong to errors but at the same time, fragile to malicious attacks. On the other hand, homogeneous networks might be robust against attacks but vulnerable to random failures. In our daily life, many important real networks bear the "robust yet fragile" property [1].

While the ongoing progress of networking in essential utilities brings significant benefits to the quality of our life, networked systems often hold a certain danger that a failure of only single element in the system can diffuse to other elements. This kind of failure is widely recognized as cascading failure in which, though errors or intentional attacks emerge locally, the damage is propagated largely, even resulting in global collapse. Recently, many scholars have investigated cascading failures due to overload mechanism. Mechanism behind this type of cascade is explained as follows: there is a critical load at which risk sharply increases toward a threshold for cascading failure. If external shocks or excess loads at some nodes are propagated to other connected nodes due to failure, the domino effects often come with disastrous consequences. In traffic of electrical systems, a high load on some components cause failures, such as traffic jams or electrical line failures, with the potential to sever links or removes nodes from the network. A number of important aspects of this type of cascading failures in complex networks have been discussed in the literature and many valuable results have been found.

When we may model and understand the behaviour of cascading failures, the robustness of a network against cascading failures due to intentional attacks has become a topic of recent interest. While new forms of attacks are developed every day to compromise essential infrastructures, service providers are also expected to develop defense strategies to mitigate the risk of extreme failures. In this context, tools for network science have been used to evaluate network robustness and propose resilient topologies against attacks. In addition, a number of aspects of cascading failures have been discussed in some literature, including the cascade control and defense strategy. A lot of authors have considered both (i): active approaches, in which they try to mitigate cascade damage while cascade is in progress, and (ii): topological approaches, in which they try to design robust network structure against cascade. When topological robustness is possible, it has more advantages over active robustness because of its simplicity and efficiency.

In this paper, we present a novel network design and show that the introduced network structure is least susceptible against overload based cascading failures. In such cascading failure, the flow diffuse on the shortest path, every pairs of nodes should select hub nodes as relaying points to decrease the average path length of the network, thus increase its communication efficiency. Then the failures of hub nodes will cause the major redistribution of flows. To design robust network against overflow based cascading failure, it is intuitive idea that the homogeneous network is the best, because all nodes have sufficient alternative adjacent nodes after some nodes may fail. However, the homogeneous network has side effects for the network performance that the average shortest path length between nodes prone to be large due to the lack of hub nodes. In this paper, the proposed network consists of hub nodes and periphery nodes. Hubs compose complete sub-graph to prevent the disconnection when some important nodes fail, and periphery nodes, which are belongs to singe hub nodes, are useful to reduce the total load of the system. By numerical simulations, we show that the introduced network is more robust and stable than other types of network.

We organize our paper as follows: we give the brief instruction of an overload based cascading model in section 2, introduce a heuristic method for designing the least susceptible networks against cascading failures in section 3, show the performance of the introduced network by numerical simulations in section 4 and finally, summary the paper in section 5.

II. An Overload-Based Cascading Failure Model

A. *Overload-based Model*

In this section, we investigate some insights about the situations of cascading failures due to overload model. This overload model considers loads of physical quantities such as load of TCP and UDP packets in the Internet or the current load in the power grid systems. Cascading failures triggered by an initial failure of a single node due to overload are sometimes occurred and propagated to very large damage such as packet congestion in the Internet, chain reaction bankruptcies, blackouts of power grid networks, and so on.

Motter and Lai [2] were the first to address this type of cascading failure in distributed network. Their model is generally applicable to realistic networks, yet simple enough to support tractable analysis, and it consists of several key elements:

(i) The traffic is simulated by the exchange of one unit of the relevant quantity (information, energy, etc.) between every pair of nodes along the shortest-hop path connecting them. The load placed on a node is considered as the betweenness centrality of a node which is equivalent to the total number of shortest-hop paths passing through the node.

(ii) The capacity of a node is defined as the maximum load that it can handle. For simplicity, the capacity C_i of node i is assumed to be linearly proportional to its initial load L_i

$$C_i = (1+\alpha)L_i \tag{1}$$

where, □ is the *tolerance parameter*, indicating the maximum load that a node can handle. Here, the tolerance parameter □ also implies the budget of constructing network or allocating resources. The most effective and simple way to prevent cascade is to increase this tolerance parameter □ as much as possible, meaning that all nodes have sufficient resources to prevent failure due to overload. But □ is often limited by cost. Therefore, to validate the robustness of our proposed network structure, we assume that the tolerance parameter □ is small and the maximum value of the tolerance parameter is *□=1*. If the load of a node exceeds its capacity, it will be failed, otherwise, it will be safe

$$If \quad \begin{cases} L_i > C_i \rightarrow i \ will\ be\ \ failed \\ L_i \le C_i \rightarrow i \ will\ be\ safe \end{cases}. \tag{2}$$

Cascading failure is then a result of load redistribution when some nodes initially fail. When all nodes are operational, network operates steadily because there is no overload at each node. However, the removal of a node when it failed, will naturally cause a redistribution of the shortest-hop paths. And this will generally increase load at some other nodes. If the redistributed load exceeds the given capacity of any node, it will fail, triggering a new redistribution, and possible subsequent cascading failures. Eventually, the failure will stop, when all remaining nodes can handle their load.

B. *Robustness Metric*

In complex network research, the evaluation of robustness focuses on some generic topological metrics of network such as, size of the *Largest Connected Component (LCC)*-in which there is a path between any pair of nodes in a network-, the average shortest path length in the *LCC*, the efficiency of the *LCC*, etc. Besides considering properties of the *LCC*, some other metrics are also considered, e.g. the average avalanche size, the avalanche size distribution, the critical point of phase transition from absorbing state to cascading state and so on. Since the connectivity of the system is important and topological connectivity is often measured by the size of the *LCC*, in this paper, we quantify the damage caused by a cascading failure by *G*, which is the ratio of the number of functional nodes in the *LCC* after and before cascading event

$$G = \frac{N'}{N} \tag{3}$$

where *N'* and *N* is the size of the *LCC* of network after and before cascading failure, respectively. Evidently, *N* is the size of initial network. A network shows its integrity if G≈1, i.e. there is no cascade in network and all nodes are connected, and G≈0, meaning that a network disconnects in several small sub-networks. Thus, the relative size of *G* then represents the robustness of a network against cascading failures.

III. A Network Design Model of Core-Periphery Structure

A. *Core-Periphery Network*

Generally, based on the degree centrality, we can classify nodes in a network into two categories: hub nodes and periphery nodes (we call hubs and peripheries in the following).

In complex networked system, hubs play an important role because they connect other nodes and guarantee the connectivity of the network. In overload models, hubs are usually selected as a pathway to reduce the average shortest hop paths length between every pairs of nodes, then increase the efficiency of network. Thus, hubs might carry large amount of flows as relaying points. Normally, the failure of hubs causes major changes in the network connectivity and the balance of loads. That is the reason why the existence of hubs becomes the weak point of the network and can be targets of malicious attacks. The connection between hub nodes then, plays a role key in preserving the connectivity of the whole network when some hubs may fail.

Motter [8] introduced and investigated a costless strategy of defense based on a selective further removal of nodes and edges, right after the initial attack or failure. Their main result is, the size of the cascade can be drastically reduced with the *Intentional Removals* of nodes having small load and edges having large excess of load. Even though any removal always increases the immediate damage on the network, the resulting *G* is in this case significantly larger as compared to the case without defense, because these *Intentional Removals* strongly suppress the propagation of the cascade. Based on this study, we now understand the role of peripheries with small degree is that, they mainly contribute to generate load rather than to transmit information, then the removal or shutdown of one of them may reduce the total load of the system, and then support the overload avoiding of other nodes in the network.

We now know that the connection between hubs and the shutdown of peripheries are important in terms of network robustness against cascading failures. We now introduce a heuristic method to build least susceptible network to overload cascading failures in the following sub-section, in which the hub-hub and the hub-periphery connection are implemented.

B. Network Design Model

Our model consists of two simple steps to build a network, as shown in FIGURE I. We assume that we have a determined resources, consist of *N* nodes and *M* links to construct a network. At first, we built *n* complete graph as a core of the network, in which *n* nodes are connected to each other completely. This core therefore has *n-1* links. We then add new nodes, that each node has only one link, to the existing core. New nodes are attached to the existing core by using preferential attachment algorithm.

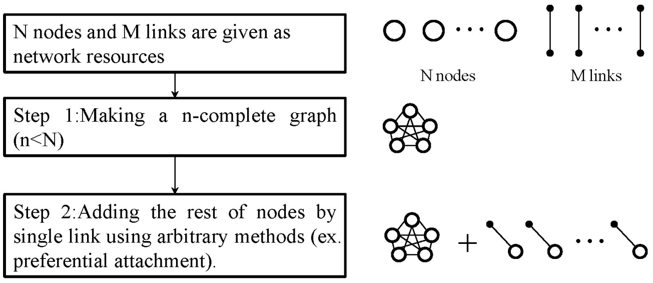

N nodes and M links are given as network resources
Step 1:Making a n-complete graph (n<N)
Step 2:Adding the rest of nodes by single link using arbitrary methods (ex. preferential attachment).
N nodes
M links
+

FIGURE I. THE DESIGN MECHANISM OF PROPOSED NETWORK

The relationship between the number of nodes *N*, the number of links *M*, and the core size *n* can be described as follows

$$M = \frac{n(n-1)}{2} + N - n\,. \tag{4}$$

By isolating *n* from (4), we obtain

$$n = \left\lfloor \frac{3+\sqrt{9+8(M-N)}}{2} \right\rfloor \tag{5}$$

where $\lfloor . \rfloor$ represents the floor function.

FIGURE II shows the introduced network which have N=100 and M=200. As showed in the figure, here, peripheries belongs to a single hub and communicate to each other via the center core cluster. We call the proposed network as the **C**ore **P**referential **A**ttachment network (**CPA**).

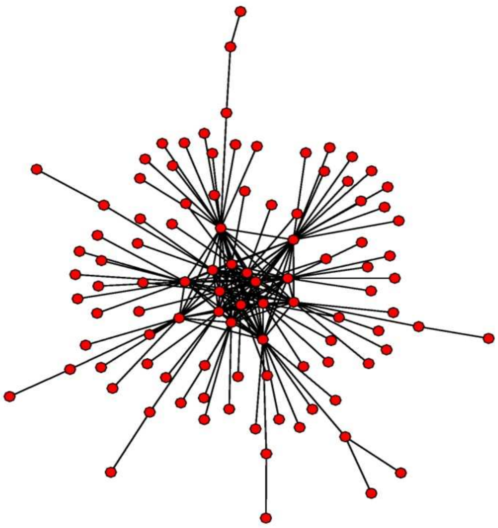


FIGURE II. THE VISUALIZATION OF AN EXAMPLE CPA NETWORK WITH N=100 AND M=200.

Yuan [10] estimated the theoretical maximum eigenvalue of a network as follows

$$\lambda_1 \le \sqrt{1+N(<k>-1)} \tag{6}$$

where, <*k*> is the average degree of the network.

We then, calculate the largest eigenvalues of the proposed CPA networks and compare with the theoretical upper limit eigenvalues and the eigenvalues of other networks. The largest eigenvalue of the adjacency matrix of each type of network with N=500 is showed in FIGURE III as a function of the networks' average degree <*k*>. Here, CPA is the proposed complete graph with preferential attachment algorithm, SF is the scale free network based on Barabási-Albert model [12], and RND is the random network based on Erdos-Renyi model [13]. In the case of CPA, SF and RND network, the result was obtained by averaging 10 individual networks. The theoretical upper limit is defined and calculated by (6).

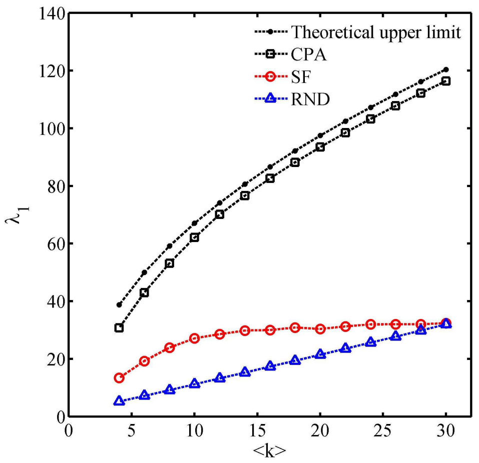


FIGURE III. COMPARISON OF LARGEST EIGENVALUES

The introduced networks also have discriminative value of the largest eigenvalue, which characterize the network topology. Interestingly, the introduced CPA networks have the largest eigenvalues that almost equal to the upper limit along the increasing of the average degree <*k*>.

IV. Comparative Simulation Study on Cascading Failure

We conduct simulations to validate the robustness of our proposed network against cascading failures. We compare the robustness of several networks including the introduced networks, generated scale-free networks and random networks. All networks have the same number of nodes N=500 and the same average degree <k>=4. We compare these networks in various values of the tolerance parameter ⍰.

For the study of attack vulnerability of network, the selection procedure of the order in which nodes are removed is an open choice. A tractable choice, used in the original study of complex networks, is to select nodes with descending order of loads (the load, here, can be regarded as degree centrality, betweenness centrality, etc.) in the initial network and then to remove single nodes one by one starting from the node with the highest load. In this paper, we assume that attackers know the whole topology of the network and chose a number *m* of highest load nodes to attack simultaneously, which is expected to bring the most damage to the network stability. We assume that attackers are able to attack m=1~50 nodes simultaneously.

As showed in FIGURE IV, the robustness of each network is the area composited by the horizontal axes and the line that represents each network. As the initial number of removal nodes *m* increases, the relative *G* decreases, indicating network with low performance. When m>30, all the networks are almost disconnected. On the other hand, as the tolerance parameter ⍰ increases, the robustness of random network and scale-free network also increases, meaning that if we have large budget to allocate resources, we might mitigate the damage of cascading failures due to malicious attacks. Interestingly, despite of the increasing of the tolerance parameter, the robustness of the CPA is stable because of its core-periphery structure.

V. Conclusion

In this paper, we studied the robustness of the network against cascading failures based on the overload model. We introduced the structure and the algorithm to build the least susceptible network to the cascading failures. The proposed network consists of a complete connected hub nodes cluster and periphery nodes that are belong to one of hub nodes. One hub node and periphery nodes make a module which can be regarded as a simple tree structure. The network consists of many the modules (trees), and a center cluster of hub nodes unifies them.

Simulation results showed that the proposed network topology can drastically reduce the damage of the cascading failures. The center cluster of hub nodes contributes to prevent the disconnecting, and the failure of periphery nodes contribute to decrease the total load of the system when an intentional attack happened. This module architecture is useful to suppress the turbulence of load by failures of nodes in both the case of intentional attacks and random failures.

In the study of overload cascading failures, the load on a node (or an edge) is generally estimated by its degree or its betweenness. The degree method is inferior owing to its consideration of only a single node degree, which loses much information in many actual applications while the betweenness principle, however, is only practical for small and medium-sized networks but invalid for large scale ones such as the Internet or World Wide Web, due to its consideration of topological information for the whole network. Therefore, the requirement for an applicable model becomes an indispensable issue. Our future work then focuses on building more realistic overload model and study cascading failures on it.

References

[1] R. Albert, H. Jeong and A. Barabasi, “Error and attack tolerance of complex networks”, Nature 406, pp. 378-382, 2000.

[2] A. E. Motter and Y. C. Lai, “Cascade-based attacks on complex networks”, Phys. Rev. Lett. 66, 2002.

[3] W. X. Wang, G . R. Chen, “Universal robustness characteristic of weighted networks against cascading failure”, Phys. Rev. E 77, 2008.

[4] Z. X. Wu, G. Peng, W. X. Wang, S. Chan, E. W. M. Wong, “Cascading failure spreading on weighted heterogeneous networks”, J. Stat. Mech. P05013, 2008.

[5] R. Yang, W. X. Wang, Y. C. Lai, G. Chen, “Optimal weighting scheme for suppressing cascades and traffic congestion in complex networks”, Phys. Rev. E 79, 026112, 2009.

[6] P. Crucitti, V. Latora, M. Marchiori, “Model for cascading failures in complex networks”, Phys. Rev. E 69 045104, 2004.

[7] H. A. Q. Tran, T. Komatsu, A. Namatame , “Mitigating cascading failure with adaptive networking”, Journal of New Mathematics and Natural Computation, in press.

[8] A. E. Motter, “Cascade control and defense in complex networks”, Phys. Rev. Lett. 93, 2004.

[9] A. Ash and D. Newth, “Optimizing complex networks for resilience against cascading failure”, Phys. A. 380 673, 2007.

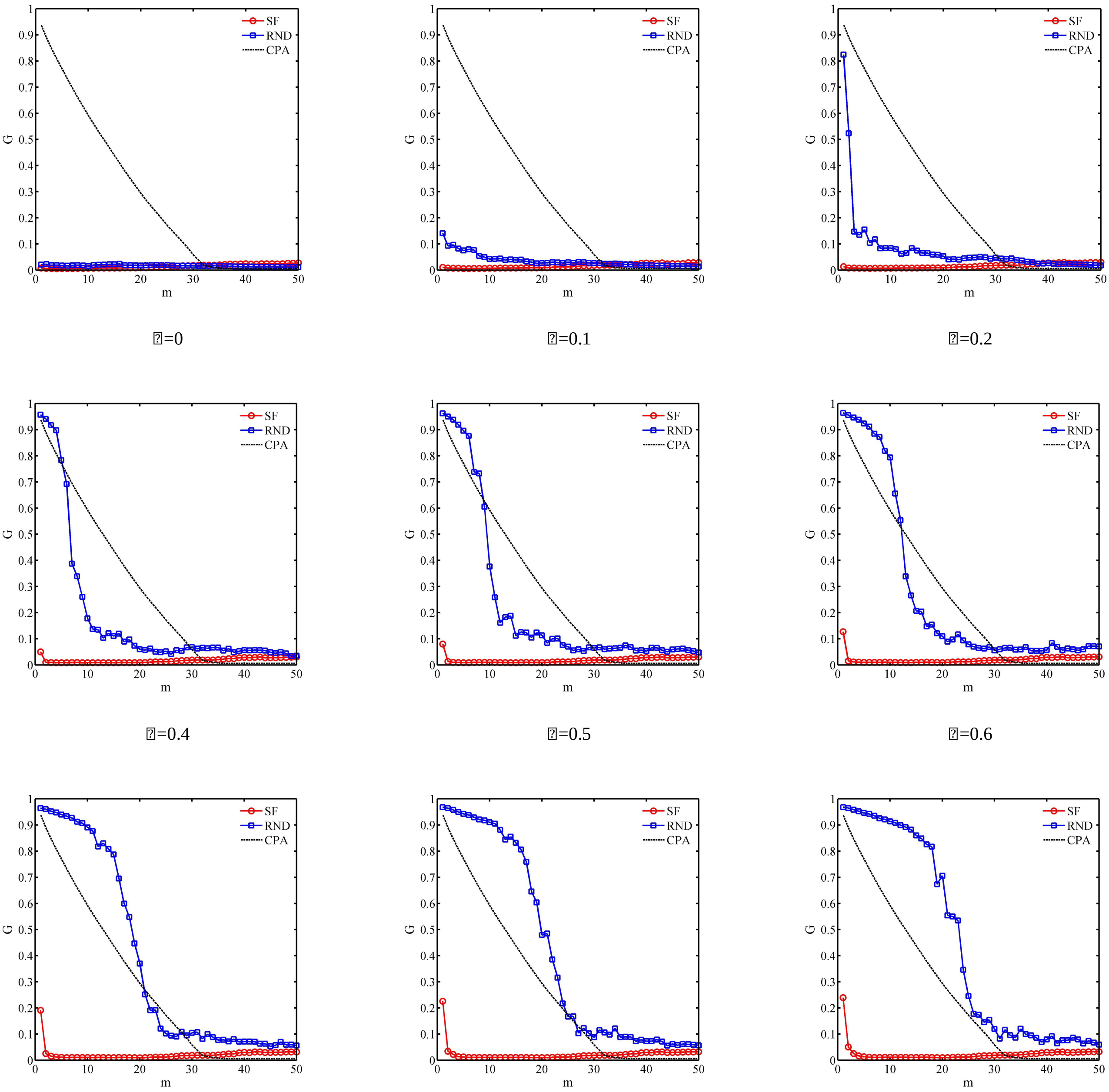
[10] H. Yuan , “A bound on the spectral radius of graphs”, Linear Algebra and its Applications, 108, pp. 135-139, 1988.

[11] J. W. Wang, L. L. Rong, “A model for cascading failures in scale-free networks with a breakdown probability”, Phys. A. 388, pp. 1289-1298, 2008.

[12] A Barabási, R. Albert and H. Jeong, “Scale-free characteristics of random networks: the topology of the World-Wide Web”, Phys. A. 281, pp. 69-77, 2000.

[13] P. Erdös and A. Rényi, “On random graphs”, Publications Mathematica 6, pp. 290-297, 1959.

[14] T. Komatsu and A. Namatame, “Dynamic diffusion processes in evolutionary optimized networks”, Int. Journal of Bio-Inspired Computation, Vol. 3, pp. 384-392, 2011.



⍰=0

⍰=0.1

⍰=0.2

⍰=0.4

⍰=0.5

⍰=0.6

⍰=0.8

⍰=0.9

⍰=1

FIGURE IV. ROBUSTNESS COMPARISON BETWEEN THE PROPOSED NETWORK CPA, THE SCALE-FREE NETWORK, AND THE RANDOM NETWORK. EACH LINE REPRESENTS THE AVERAGE RESULT OF 10 INDIVIDUAL NETWORKS.