Strategies for Suppressing Cascading Failures

Hoang Anh Q. TRAN[1], Akira NAMATAME[2],

[1,2]Dept. of Computer Science, National Defense Academy of Japan 1-10-20, Hashirimizu, Yokosuka, Kanagawa, 239-0811 Japan

E-mail: [1]ed13004@nda.ac.jp

Abstract

Cascading failures are crucial issues for the study of survivability and resilience of our infrastructures and have attracted much interest in complex networks research. In this paper, we study an overload-based cascading failure model and propose defense strategies to mitigate the damage from such cascading failures. We design a novel core-periphery network topology that is robust to cascading failures, as *hard* strategy. For *soft* strategy, we assign adjustable weights to individual links of a network and control the weight parameter to effectively modify the information flow and the routing patterns in the network without changing its given topological structure.

Keyword: Cascading Failures, Network Robustness

1 Model

It has been suggested [1] that the information flow across the network – namely, the load L, can be captured well by the betweenness centrality, which can be calculated as the number of shortest paths that pass through a node when flow is sent from each available generation node to each distribution node. The capacity of a node is defined as the maximum load that the node can handle

$$C_i = (1+\alpha)L_i(0), \quad i = 1, 2, ..., N \tag{1}$$

where $0 \leq \alpha \leq 1$ is the *tolerance parameter*, $L_i(0)$ is the load of node i at time step $t = 0$, and N is the initial number of nodes in the network.

Suppose that $s_i(t)$ represents the state of node i at time step t. A very simple condition to recognize that node i will fail or not at time step t is the following relation

$$s_i(t) = \left\{ \begin{array}{ll} 1, & if\ L_i(t) > C_i \\ 0, & otherwise \end{array} \right\} \tag{2}$$

where $s_i(t) = 1$ indicates that node i will fail at time step t, and $s_i(t) = 0$ indicates that node i will be safe.

We quantify the robustness of a network using G, which is the ratio of functional nodes in the *Largest Connected Component* before and after a cascading event caused by the failure of some nodes with highest loads

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

where N and N' are sizes of the *Largest Connected Component* of the network before and after cascade, respectively.

2 Hard Strategy

Based on the fact that, the connection between hubs plays a key role in preserving the connectivity of the whole network when some hubs with high load, fail, and the *Intentional Removal* of nodes with small loads could drastically reduce the damage of cascades [2]. We build a network in two simple steps, as shown in Figure1.

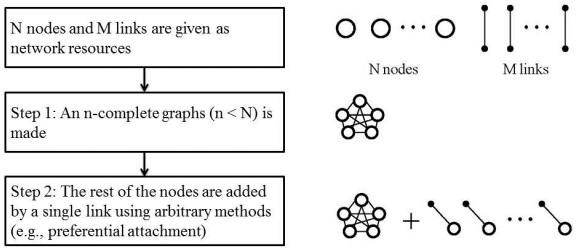

Figure1: The design mechanism of proposed network.

A predetermined resource to construct the network that consists of N nodes and M links is assumed. First, n complete graph is built to form the core of the network. Then, new nodes are added such that each node has only one link to the existing core until the predetermined number of nodes N is reached.

New nodes are added to an existing node with a probability that is proportional to its degree in the case of preferential attachment, or with a probability based on a uniform probability distribution in the case of random attachment. The networks obtained by preferential attachment are referred to as *Core Preferential Attachment CPA* networks and

networks that are obtained by random attachment are referred to as *Core Random Attachment CRA* networks.

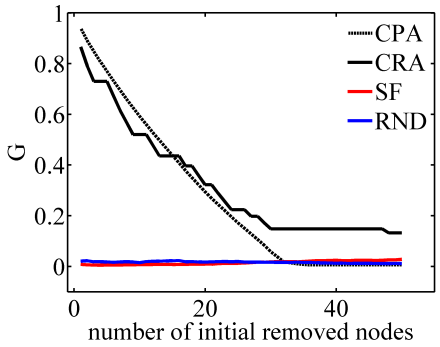

Figure2: Comparison of robustness for the proposed CPA and CRA, scale-free SF, and random RND networks for the case $\alpha = 0$.

The resulting robustness of each network with $N = 500$ and $M = 1000$ when the severity of the initial failures is varied, is shown in Figure2. As the initial number of removed nodes increases, the robustness G decreases, indicating networks with low performance. As seen, even when α is the lowest value ($\alpha = 0$), the proposed networks have a stable performance, and much higher than others.

3 Soft Strategy

We assume that a weight of an arbitrary link connecting a node i and j is assigned proportionally to the connectedness of the two nodes as follows

$$w_{ij} = a_{ij}(k_i k_j)^{\beta} \tag{4}$$

where a_{ij} is the element in the i^{th} row and j^{th} column of the adjacency matrix of the network. k_i and k_j is the degree of node i and j, respectively, and β is the weight control parameter.

The weight of a path from a node m to node n, that passing thought a set of l intermediate nodes $S = 1, 2, ..., l$ is the total link weights including in the path

$$w_{m \to n} = \sum_{i=1}^{l-1} w_{ij}, \quad j = i + 1 \tag{5}$$

from which, the shortest path on the weighted network, within all possible weighted paths between m and n can be obtained. Then, the load of a node i can be approximated by the total number of shortest *weighted* paths that pass through that node.

We conduct simulations with some realistic networks such as: the top 500 busiest commercial airports in the U.S; the Euro-road network; the e-mail network; and the power grid of the Western States of the U.S.

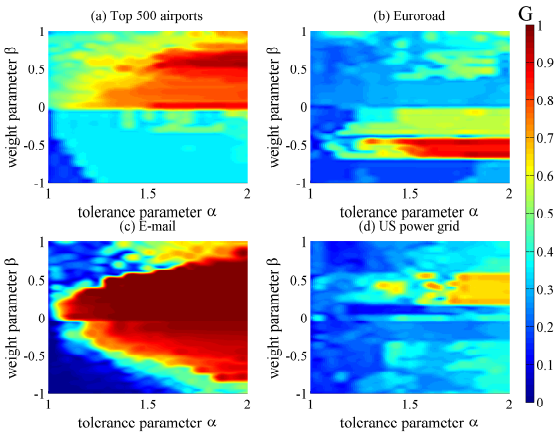

Figure3: Network robustness of the Top 500 airports, Euro-road, E-mail and US power grid as the function of the tolerance parameter α and weight control parameter β. Hot colors show the area of high robustness and cold colors correspond to the rest.

As shown in Figure3, we can classify strategies that enhance network robustness into four following classes by the proposed routing strategy: (a) Hub avoidance strategy ($\beta > 0$): efficient for top 500 airports network; (b) Hub oriented strategy ($\beta < 0$): efficient for Euro-road network; (c) Strategy that increases the tolerance parameter: efficient for E-mail network; (d) Strategy of both hub avoidance ($\beta > 0$) and increase of the tolerance parameter: efficient for U.S power grid network.

4 Conclusions

In this paper, we proposed strategies to enhance network robustness against cascading failures caused by overload mechanism. We could design robust CPA and CRA networks from scratch, or modify the flow of the given network without impacting to its topological structure. Our strategies may contribute to existing strategies because of the effectiveness and the availability for critical infrastructure networks.

References

[1] A. E. Motter, Y. C. Lai, "Cascade-based attacks on complex networks", Phys. Rev. E.66, (2002).

[2] A. E. Motter, "Cascade control and defense in complex networks", Phys. Rev. Lett., Vol. 93, (2004).