Mitigation of Cascading Failures with Link Weight Control

Hoang Anh Tran Quang
Dept. of Computer Science
National Defense Academy of Japan
Yokosuka, Kanagawa, Japan

Akira Namatame
Dept. of Computer Science
National Defense Academy of Japan
Yokosuka, Kanagawa, Japan

***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 the overload-based cascading failure model and propose a *soft defense strategy* to mitigate the damage from such cascading failures. In particular, we assign adjustable weights to individual links of a network and control the weight parameter. The information flow and the routing patterns in a network are then controlled based on the assigned weights. The main idea of this work is to control the traffics on the network and we verify the effectiveness of the load redistribution for mitigating cascading failure. Numerical results imply that network robustness can be enhanced significantly using the relevant smart routing strategy, in which loads in the network are properly redistributed.**

Keywords—cascading failures; link's weight; network robustness

I. INTRODUCTION

Nowadays, many complex systems in nature and society can be described by intricate network patterns, including technological, social and biological systems such as the Internet, the World-Wide Web, electrical power grid networks, metabolic networks and so on. In recent years, complex network research has also attracted much attention and becomes an useful tool for scientists to make major advances in understanding salient properties of complex human engineered systems, that go beyond the single component behaviour. A vast number of studies have clarified that certain topological properties of complex networks have strong impacts on their stability. An early important work of Albert, Jeong and Barabasi [1] showed that scale-free networks which have heterogeneous degree distributions, are remarkably resistant against random errors, but at the same time, targeted malicious attacks can easily disrupt the networks by removing only a small fraction of nodes or links. On the other hand, homogeneous degree distribution networks – namely, random networks, might be considerably stable against attacks but somewhat vulnerable to random failures.

Since a vulnerability is a weakness which might reduce a system performance, recently, one of the major focuses of complex network research, is the vulnerability management. In our daily life, cascading failures are common phenomenon and can occur in many natural and man-made systems, due to endogenous or exogenous (or can be both in some cases) factors.

There are many types of cascading failures that are mentioned, from some critical infrastructures such as electrical power grids and computer networks, to economic, ecological, even political systems. A common yet hard-to-predict property of cascading failures is that even a single point of failure emerges locally, the damage is widely propagated and could result in global collapse.

In decades, a number of important aspects of cascading failures in complex networks have been discussed and many valuable results have been found. There several works studied the impact of cascading failures on different types of power grid networks such as the North American power grid network [2], the European power grid network [3], and the Italy power grid network [4]. Other works studied cascading failures in other types of complex networks, such as telecommunication networks [5], or socio-technological networks [6]. As we further model and understand the behaviour of cascading failures, how to build in safeguards that may be able to prevent them in the future, has become a central topic of interest.

Available set of existing methods to enhance network robustness against cascading failures can be generally divided into two classes

- A set of methods to improve network robustness *statically*, which has been developed in order to prevent cascading failures before the occurrence of initial failures.
- A set of methods to improve network robustness *dynamically*, which has been developed in order to minimize the damage of cascading failures after some initial failures occurred.

An example study of the former is the paper of Shin and Namatame [7]. In their paper, they considered network robustness and design cost as a trade-off function and used an evolutionary algorithm to evolve networks. Their results revealed that clustering, modularity, and long path lengths all play an important part in the design of robust large-scale infrastructure.

Typical examples of the latter include the well-known method proposed by Motter [8]. In his paper, he introduced and investigated a costless defense method based on a selective removal of nodes and edges immediately after initial failure and showed that the proposed method is practical and can drastically reduce the size of the cascade.

The main idea in [8] is that a selective set of *insignificant* nodes that process little but contribute relatively large loads to the network are removed so as to reduce the overall load in the network. This approach has the advantage of a low incremental investment cost, as it requires the ability to perform a remote shutdowns of nodes. However, it also has a strong disadvantage since it is difficult to provide early detection of cascading failures and it requires knowledge of the global topology.

There are essentially two types of strategies for defending or mitigating cascading failures

- *Hard strategy* to prevent cascading failures. This type of strategy has a disadvantage of impacting the topology of networks.
- *Soft strategy* to minimize the damage of cascading failures without any change in the connection of networks.

Both of the above-mentioned methods [7, 8] can be regarded as *hard strategy* type. While the latter shows its disadvantage in directly impacting to the topological structure of networks, the former may become a harder strategy since the purpose is to design robust networks from the beginning while it has been showed that most of networks in reality already have their own specific existing structures.

To overcome the difficulties of *hard strategy*, some *soft strategies* to counter cascading failures without impacting to the connections of given networks, have been recommended. Wang and Kim [9], Li, Wang, Sun, Gao, and Zhou [10] developed new capacity models to cascading failures to make the network more robust, while at the same time the cost to assign capacities is drastically reduced. Meanwhile, in the survey of Chen, Huang, Cattani, and Altieri [11], they reviewed strategies for improving transport efficiency, including soft strategies to design efficient routing strategies and also hard strategies to adjust the underlying network structure.

Because *hard strategies* are not always applicable in many cases, we mainly focus on *soft control strategy* in this work. Among existing literature, the most related work to ours is the paper by Yang, Wang, Lai, and Chen [12]. In their paper, they discovered an optimal solution to both cascading failures and traffic congestion problem. They provided numerical evidence and theoretical analysis to show that, by choosing a proper weighting parameter, a maximum level of robustness against cascades and traffic congestion can be simultaneously achieved. However, the critical tolerance parameters which are the minimal values to prevent cascading failures that they showed in their paper are applied for all nodes in the network. It implies that, to prevent overload in some nodes, they unexpectedly increased the capacities in other nodes which are may be unnecessary and become waste redundancy, and of course it leads to much cost. Besides, they did not consider the connectivity of the network after initial failures, which is a relevant index in studying network robustness.

In this paper, we control load distribution in a network via several smart routing schemes. We define network robustness in considering the connectivity of the network.

We evaluate network robustness to capture the effectiveness of the proposed method on an artificial generated scale-free network and some realistic networks subjected to intentional attacks. Simulation results show the significant enhancement of network robustness when a smart routing strategy is adapted.

The reminder of this work is organized as follows: we first present the cascading failure model in Section II. We then introduce the proposed routing strategy and simulation settings in Section III and IV. We present numerical results in Section V, and finally summarize this work in Section VI.

II. A Cascading Failure Model

Cascading breakdown in complex networks is regarded as an avalanching failure, where the failure of a few local nodes can result in a global-scale breakdown of the network. In various types of existing cascading failures, one of the most prominent cascade phenomenon that occurs in most infrastructure networks, is overloaded cascading failure.

This type of cascading failures can take place in electrical power grid networks, when for any reason a line breaks down, its power is automatically shifted to the neighbouring lines. In most of the cases, the neighbouring lines can handle the extra load, but sometimes, these lines are also overloaded and continuously shift their load to their neighbours. This eventually leads to a cascade of failures where a large number of transmission lines are overloaded and malfunction at the same time. For instance, due to the power redistribution, some typical incidents have taken place in history, such as the blackout on August 14, 2003 when an initial disturbance in Ohio led to the largest blackout in the history of the United States and millions of people throughout parts of North Eastern and Mid-Western United States, and Ontario, Canada, were without power for as long as 15 hours [13].

Furthermore, the overloaded cascading failures can also take place on the Internet, where traffic is rerouted to bypass breakdown routers, eventually leading to an avalanche of overloads on other routers which do not have enough capability to handle extra traffic, and a large drop in the performance. A prominent example is the congestion on the early Internet in October 1986, when the NSFnet phase-I backbone dropped three orders of magnitude from its capacity of 32 kbit/s to 40 bit/s, and this continued to occur until end nodes started implementing Van Jacobson's congestion control between 1987 and 1988 [14].

The interesting feature of this type of overloaded cascading failures is that it does not necessarily propagate through adjacent physical contact, i.e. the single failure of one node in a network may cause failures to non-adjacent nodes due to the network's load redistribution. The potential impact of this type of cascading breakdown on the security of large complex networks, has been firstly investigated by Motter and Lai [15].

Since traffic or information is usually transmitted along the shortest paths in most communication networks, it has been suggested 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 (load in unweighted networks)

$$L = \textit{shortest path betweenness}. \quad (1)$$

We consider the networked system with N nodes. The possibility of observing cascading failures is enabled by assigning flow capacities to each of the nodes of the system. Here, the capacity of a node is defined as the maximum load that the node can handle. Since engineered systems are optimized for maximum capacity and minimum cost, it is assumed that the capacity of the nodes is proportional to the initial load [15, 16]

$$C_i = \alpha L_i(0), \quad i = 1,2,\ldots,N \quad (2)$$

where C_i is the capacity of node i, $L_i(0)$ is the initial load of node i which is defined in (1). The tolerance parameter α ($\alpha \geq 1$) captures the relationship between network component capacity and load demand levels. Here, the tolerance parameter α also implies the budget of network construction or resource allocation.

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

$$s_i(t) = \begin{cases} 1, & \textit{if } L_i(t) > C_i \\ 0, & \textit{otherwise} \end{cases} \quad (3)$$

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.

Each disruptive event triggers flow redistribution within the networks and can potentially lead to cascading failures. Initially, a network is in a stationary state in which the load at each node is smaller than its capacity. It is possible that from some reasons a breakdown occurs at one or more nodes – some nodes in the system is overloaded beyond the given capacity, so that they cannot work at all, and can be assumed that be removed from the network, causing the change of transmission paths in the network. The breakdown of one or some heavily loaded nodes will cause the redistribution of loads over the remaining nodes, which can trigger breakdowns of newly overloaded nodes. These additional failures require a new redistribution of loads, which either stabilizes and the failures are locally absorbed, or grows until a large number of nodes are compromised to a failure point.

Using the model, we are able to follow the dynamical response of the system to failures, and in particular to model how the failure in one location can propagate and have consequences over the whole network. The model is applicable to many realistic situations in which the flow of physical quantities in the network, as characterized by the loads on nodes, is important.

III. SMART ROUTING STRATEGY

Any network can be represented by an adjacency matrix A.

The element of matrix A in the i^{th} row and the j^{th} column is expressed as a_{ij}. If $a_{ij} = 1$, node i and node j are connected, and if $a_{ij} = 0$, these two nodes are not connected.

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

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

where k_i and k_j is the degree – the number of links, of node i and j, respectively, and β is the weight control parameter.

The introduced weight of a link connecting a node i and j can be also referred to as resistance of the link against the flow, which is determined, for example, by the conductance in an electrical network. As it can be observed in (4), the control parameter $\beta > 0$ indicates that links connecting hubs – node with high degrees, have high weights, and will be avoided using to transmit information. This assumption matches the reality since lines that have high resistances will obstruct the flow in networks. In contrast, $\beta < 0$ implies that low weights are assigned to links connecting hubs, meaning that these links have low resistances and are frequently used to transmit information. The final regime $\beta = 0$ corresponds to the case in which all links have the equal weight (same resistance). In this case, the flow will be transmitted by a predetermined rule, e.g. via the shortest paths in networks. It is worth noting that the weights we assign for links in networks here, are only dummy values – these values do not correspond to any measurement in reality, e.g. the geographical distance between two cities, the resistance of a transmission line between two substations, etc. The idea of this work is to control the flow of communication in networks based on these dummy values.

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

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

from which, the shortest path on the weighted network, within all possible weighted paths between m and n can be obtained.

As introduced in section II, the shortest path based betweenness of a node i can be used as an approximation of the load that flows through i. Nevertheless, this definition of load has the disadvantage that is only applicable for unweighted networks. Based on the mentioned weight in (4), we extend the definition of load that is also applicable for weighted networks.

In particular, the load of a node i can be approximated by the total number of shortest *weighted* paths that pass through that node (load in weighted networks)

$$L = \textit{shortest weighted path betweenness}. \quad (6)$$

IV. Simulation Settings and Performance Measurement

We conduct simulations with both artificial generated and realistic networks. We use a scale-free network generated by Barabasi-Albert model [17] as a benchmark network, which has the number of nodes $N = 1000$ and the average degree $\langle k \rangle = 4$. We use realistic networks such as: the Euro-road network – a road network located mostly in Europe where nodes represent cities and a link denotes that nodes are connected by a road [18, 19]; the Western States of the United States of America – a node is either a generator, a transformer or a substation, and a link represents a power supply line [18, 20]; the autonomous system peering information inferred from Oregon route-views between March 31, 2001 and May 26, 2001 [21]; the network of e-mail interchanges between members of the University Rovira I Virgili [18, 22]; and the top 500 busiest commercial airports in the United States [23, 24]. These networks have been chosen in order to represent a wide variety of complex network topologies. Additional statistical information of the networks used in this paper is summarized in Table 1, where N is the number of nodes; E is the number of links; $\langle k \rangle$ is the average degree; and k_{max} is the maximum degree.

We first show the effect of the weight control parameter β in (4) to the load distribution of the benchmark scale-free network in Fig. 1.

As shown in the figure, by adjusting the weight control parameter β, the scale-free network discloses its load distributions in different manners while its topological structure is kept unchanged. $\beta = 0$ corresponds to the case where all links in the network are assigned an equal weight ($w_{ij} = 1$, for all i, j). In this case, the scale-free network shows its heterogeneous load distribution – the higher degree a node has, the higher load it carries, since all nodes tend to use hubs as shortcuts to transmit information along the network. If we reduce the parameter β to -1, we obtain the most heterogeneous load distribution among three cases. In this case, low weights are assigned to links connecting hubs, meaning that hubs are more and more frequently used to transmit information. As expected, $\beta = 1$ shows the most homogeneous load distribution where links connecting hubs will be avoided using to transmit information. In this case, hubs experience a significant decrease in load. On the other hand, nodes which carried a small load, may acquire a larger one. In other words, all nodes contribute equivalently to transmitting information along the network.

If a node has a relatively small load, its removal will not cause major changes in the load balance, and subsequent overload failures are unlikely to occur. However, when the load at a node is relatively large, its removal is likely to significantly affect loads at other nodes and possibly start a sequence of overload failures. To study the attack vulnerability of a network, the procedure for selecting the order in which nodes are removed is an open choice. A tractable choice, used in the original study of complex networks, is based on aiming at the most connected nodes, and highest loaded nodes. This is a deterministic process since the topology of the network is known at every point in time. To explore the effects of our proposed method, only nodes disrupted at intentional attacks are included in the analysis. The node with the largest load L_{max} is chosen for node attacks, and L_{max} is recalculated after every node removal when more than one element is eliminated according to the intensity of the disruptive events.

TABLE I. Statistical Information of Networks Used in this Paper

Network	Category	N	E	$\langle k \rangle$	k_{max}
Scale-free	Artificial generated	1000	1997	3.99	72
Euro-road	Physical	1174	1417	2.41	10
US power grid	Physical	4941	6594	2.67	19
Internet	Physical	10670	22003	4.12	2312
E-mail	Communication	1133	5451	9.62	71
Top 500	Physical	500	2980	11.92	145

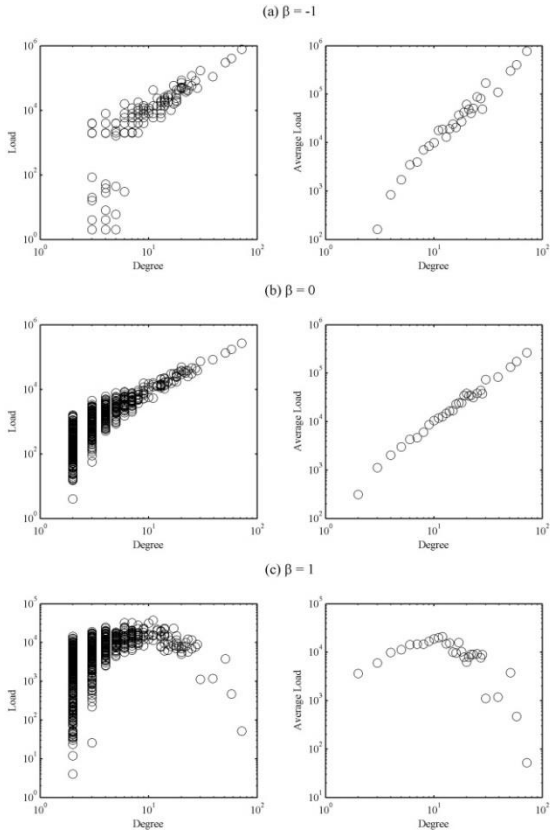

Fig. 1. The relation of load distribution vs. degree and average load vs. degree of scale-free network with the weight control parameter (a) $\beta = -1$, (b) $\beta = 0$, (c) $\beta = 1$.

The evaluation of robustness focuses on some generic topological metrics of network such as the size, efficiency, and average shortest path length of the *Largest Connected Component LCC* – the component for which there is a path

between any pair of nodes in a network. In addition to considering properties of the *LCC*, some other metrics are also considered, e.g., the average avalanche size and distribution, the critical point of phase transition from an absorbing to cascading state. Since the connectivity of the system is important, it is reasonable to consider the *LCC* as network robustness.

In this paper, we quantify the network robustness using R, the ratio of functional nodes in the LCC before and after the cascading event caused by the failure of a single node with highest load

$$R = N^{'} / N \tag{7}$$

where N and N' are the sizes of the *LCC* of the network before and after cascading failure event, respectively. Evidently, N is the size of the initial network and $0 \le R \le 1$. A network has high integrity if $R \approx 1$, i.e., there is no cascade in the network and all nodes are almost fully connected and functional after initial failure. Otherwise, $R \approx 0$ indicates that a network has been disintegrated into several small sub-networks. Thus, the relative size of R is appropriate for representing the robustness of a network to cascading failures. Using the model presented in Section II and this definition of network robustness, we obtain the familiar property "robust yet fragile" for which, in scale-free networks, R remains close to unity in the case of random breakdowns, but is significantly reduced under attacks that target nodes with the highest loads.

V. Simulation Results

Intuitively, the most effective and simple method to prevent a cascading failures is to increase the tolerance parameter α so that all nodes have sufficient resources to prevent failure due to overload. Another solution is redistributing load of a failure node.

The resulting networks provide information about the minimum capacity that each remaining node must be able to carry to survive without triggering cascade. The capacity that a node i must have for preventing cascade at any initial one node failure, is the maximum overall networks with single removal: $C_i = \max_{j \in N_i} L_i(N_i \setminus j)$, where $L_i(N_i \setminus j)$ is the load on the node i in the network with the node j removed. However, the capacity is often limited by cost thus it is impractical to assign sufficient large capacity to all nodes in networks. Based on this fact, and also to validate the effectiveness of our method, we assume that the tolerance parameter α is taken as $1 \le \alpha \le 2$, implying that there is no much redundant capacity in the system. We evaluate the efficiency of our proposed approach for small value of α, and show we can mitigate cascading failures without needing to increase the capacity of each node.

Since the difficulty of early detection makes the reactive defense strategy after initial attack but prior to the cascade an unrealistic damage control strategy for many real-world networks, we focus on the scenario of seeking an appropriate routing strategy before initial failures, indicating the static proactive defense strategy where we design a robust routing strategy against predicted attacks a priori.

Fig. 2 shows the network robustness defined in (7) with the assumption of only a single node with the highest load is failed initially.

The Euro-road and US power grid network are more likely random network, i.e. the degree and load distribution of the networks are homogeneous. On the other hand, the scale-free, Internet, E-mail and Top 500 have the degree and load heterogeneously distributed. It is obviously shown in Fig. 2 that network robustness can be enhanced for all values of weight control parameter β if we simply increase the tolerance parameter α to allocate as much capacities as possible to nodes. However, it also exhibits that without considering a proper parameter β, the enhancement is not noticeable even when we have sufficient large α – a little change in the value of the weight control parameter may leads to the dramatic decrease of network performance. It implies that, to enhance network robustness significantly, we have to consider adjusting properly both tolerance parameter α and weight control parameter β. Simulation results show that the relation between the weight control parameter β and the tolerance parameter α strongly impacts to network robustness, and this relation is irregular for each individual network. In particular, as shown in the figure, we are able to archive high network robustness for

- Scale-free network with: $\beta \ge 0.5$, $\alpha \ge 1.3$.
- Top 500 airports network with: $0.5 \le \beta \le 0.7$, $\alpha \ge 1.5$.
- E-mail network with: $0 \le \beta \le 0.6$, $\alpha \ge 1.3$.
- The Internet with: $0 \le \beta \le 1$, $\alpha \ge 1.6$.
- Euro-road network with: $-0.75 \le \beta \le -0.5$, $\alpha \ge 1.5$.
- US power grid network with: $0.2 \le \beta \le 0.5$, $\alpha \ge 1.7$.

Fig. 2 shows the similar tendency of overwhelming hot color area where $\beta > 0$ compared with other area ($\beta \le 0$) for heterogeneous networks. It indicates that we can significantly enhance network robustness against intentional attacks by choosing a proper routing strategy with $\beta > 0$, which transforms a network from heterogeneous state to homogeneous one.

Interestingly, we obtain different results for Euro-road and US power grid although they are both homogeneous networks. While network robustness may be enhanced due to some positive values of β in the case of US power grid network, the result in Euro-road network shows a different manner, i.e. network robustness is enhanced significantly with some negative values of β.

An evident truth emerges when β is small for all networks. With these β, load distribution of a network becomes extreme heterogeneous, and a single attack to a single highest load node may disrupt the whole system.

One more interesting result is also observed with some large values of β, in which network robustness start to decrease. We can explain this tendency as follows: with some intermediate values of β, a network is transformed from heterogeneous load distribution to a more homogeneous one gradually.

However, too large β leads a homogenized network once again becomes heterogeneous load distributed – nodes with small degrees become very high load nodes, and this makes intentional attacks devastate the system.

As shown in Fig. 2, we can classify strategies that enhance network robustness into four following classes

- Hub avoidance strategy ($\beta > 0$): efficient for scale-free network, top 500 airports network, the Internet.
- Hub oriented strategy ($\beta < 0$): efficient for Euro-road network.
- Strategy that increases the tolerance parameter: efficient for E-mail network.
- Strategy of both hub avoidance ($\beta > 0$) and increase of the tolerance parameter: efficient for US power grid network.

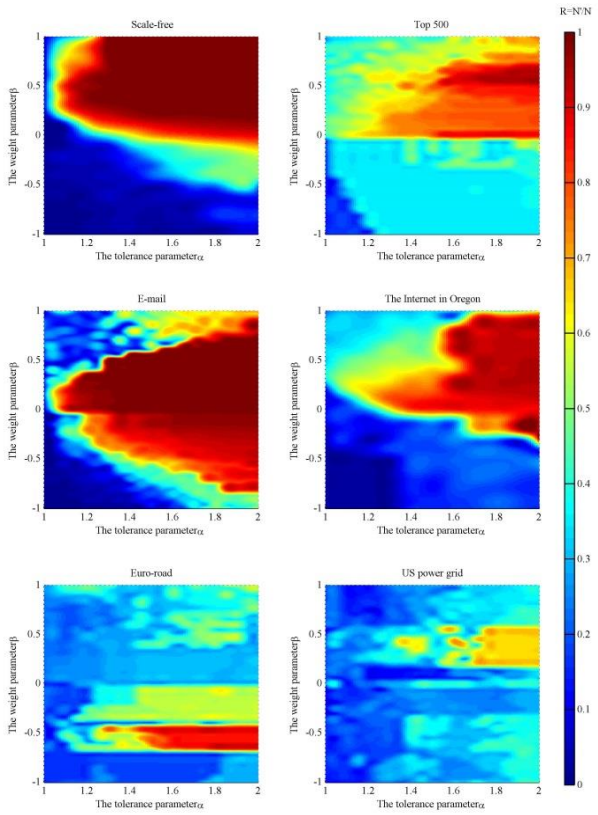

Fig. 2. Network robustness of the scale-free, Euro-road, US power grid, E-mail and Internet as the function of the tolerance parameter α in (2) and weight control parameter β in (4). In the figure, hot colors show the area of high robustness and cold colors correspond to the rest. In this scenario, we intentionally seek for an efficient design of routing strategy as a proactive defense strategy.

VI. Conclusions

In this paper, we proposed a routing strategy to mitigate the damage of cascading failures caused by overload. We assigned weighs to links in networks and control the weight by an adjustable parameter. Numerical results showed the effectiveness and the availability of our proactive method for critical infrastructure networks such as electrical power grid networks, the Internet, and so forth. Routing traffic in this manner can limit the damage of cascades by turning a heterogeneous load distribution into a more homogeneous one, reduces the need to shutdown nodes to stop a cascade, and simultaneously lowers the investment costs in network capacity layout.

For simplicity, in this paper, we assigned a weight to a link connecting two nodes, a value that proportional to the connectedness of the two nodes. However, almost systems in reality have more complicated, even unpredictable links weights. In addition, there are several alternative possibilities to the node load for the case in which the physical quantity of interest (information, packets, electric power, etc) does not travel through shortest paths only. Therefore, our future work is to investigate the two questions: how to logically assign weights to links of a network; and how to determine general flow manner. Thereto, infrastructure systems are becoming more interdependent and failures within a given system are more likely to reduce the performance of other systems [25, 26, 27, 28, 29]. Hence, how to mitigate cascading failures in such interdependent networks becomes an indispensable issue and will be also our future work.

References

[1] R. Albert, H. Jeong, A. Barabási, "Error and Attack Tolerance of Complex Networks", Nature. 406, pp. 378–382, 2000.

[2] R. Albert, I. Albert, G. L. Nakarado, "Structural Vulnerability of the North American Power Grid", Phys. Rev. E, 69(2), 2005.

[3] M. Rosas-Casals, S. Valverde, R. V. Sole, "Topological Vulnerability of the European Power Grid under Errors and Attacks", International Journal of Bifurcation and Chaos, 17(7), pp. 2465–2475, 2007.

[4] P. Crucitti, V. Latora, M. Marchiori, "A Topological Analysis of the Italian Electric Power Grid", Phys. A: Statistical Mechanics and its Applications, 338(1), pp. 92–97, 2004.

[5] M. F. Habib, M. Tornatore, F. Dikbiyik, B. Mukherjee, "Disaster Survivability in Optical Communication Networks", Computer Communications, 36(6), pp. 630–644, 2013.

[6] C. Barret, K. Channakeshava, F. Huang, J. Kim, A. Marathe, M. V. Marathe, G. Pei, S. Saha, S. P. Subbiah, A. K. S. Vullikanti, "Human Initiated Cascading Failures in Societal Infrastructures", PloS ONE, 7(10), 2012.

[7] S. Y. Shin, A. Namatame, "Evolutionary Optimized Networks and Their Properties", International Journal of Computer Science and Network Security, Vol. 9, No. 2, pp. 4–12, 2009.

[8] A. E. Motter, "Cascade Control and Defense in Complex Networks", Phys. Rev. Lett., Vol. 93, 2004.

[9] B. Wang, B. J. Kim, "A High Robustness and Low Cost Model for Cascading Failures", EPL Vol. 78, No. 4, 2007.

[10] P. Li, B. H. Wang, H. Sun, P. Gao, T. Zhou, "A Limited Resource Model of Fault-Tolerant Capability against Cascading Failure of Complex Network", The European Physical Journal B 62(1), pp 101–104, 2008.

[11] S. Chen, W. Huang, C. Cattani, G. Altieri, "Traffic Dynamics on Complex Networks: A Survey", Mathematical Problems in Engineering, 732698, 2012.

[12] 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.

[13] J. Glanz, R. Perez-Pena, "90 Seconds that Left Tens of Millions of People in the Dark", New York Times, 2003.

[14] V. Jacobson, "Congestion Avoidance and Control", in ACM SIGCOMM '88, Stanford, CA, pp. 314–329, 1988.

[15] A. E. Motter, Y. C. Lai, "Cascade-based Attacks on Complex Networks", Phys. Rev. E.66, 2002.

[16] P. Crucitti, V. Latora, M. Marchiori, "Model for Cascading Failures in Complex Networks", Phys. Rev. E 69, 045104, 2004.

[17] A. Barabási, R. Albert, H. Jeong, "Scale-free Characteristics of Random Networks: the Topology of the World-Wide Web," Phys. A. Vol. 281, pp. 69–77, 2000.

[18] Network dataset – KONECT, http://konect.uni-koblenz.de/networks, 2014.

[19] L. Subelj, M. Bajec, "Robust Network Community Detection using Balanced Propagation", European Phys. Jour. B.81, pp. 353–362, 2011.

[20] D. J. Watts, S. H. Strogatz, "Collective Dynamics of Small-world Networks", Nature. 393, No. 6684, pp. 440–442, 1998.

[21] J. Leskovec, J. Kleinberg, C. Faloutsos, "Graphs over Time: Densification Laws, Shrinking Diameters and Possible Explanations", International Conference on Knowledge Discovery and Data Mining, 2005.

[22] R. Guimera, L. Danon, A. Diaz-Guilera, F. Giralt, A. Arenas, "Self-similar Community Structure in a Network of Human Interactions", Phys. Rev. E.68, 2003.

[23] Tore Opsahl Network Dataset, http://toreopsahl.com/datasets.

[24] V. Colizza, R. Pastor-Satorras, A. Vespignani, "Reaction-Diffusion Processes and Metapopulation Models in Heterogeneous Networks", Nature Phys. 3, pp. 276–282, 2007.

[25] S. E. Chang, H. A. Seligson, R. T. Eguchi, "Estimation of the Economic Impact of Multiple Life-line Disruption: Memphis Light, Gas, and Water Division Case Study", Technical Report No. NCEER-96-0011. Multidisciplinary Center for Earthquake Engineering Research, Buffalo, New York, 1996.

[26] P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann, "Critical Infrastructure Interdependency Modeling: a Survey of US and International Research", Report INL/EXT-06-11464, Idaho Falls: Idaho National Laboratory, 2006.

[27] Y. Y. Haimes, B. M. Horowitz, J. H. Lambert, J. R. Santos, C. Lian, K. G. Crowther, "Inoperability Input-Output Model for Interdependent Infrastructure Sectors I: Theory and Methodology", Journal of Infrastructure Systems, 11(2), pp. 67–79, 2005.

[28] L. Dueñas-Osorio, J. I. Craig, B. J. Goodno, "Seismic Response of Critical Interdependent Networks", Earthquake Engineering and Structural Dynamics, pp. 285–306, 2007.

[29] C. D. Brummitt, R. M. D. Souza, E. A. Leicht, "Suppressing Cascades of Load in Interdependent Networks", Proc. of the National Academy of Sciences, 2012.