An Optimization Procedure for Enhancing Network Robustness against 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

Augie Widyotriatmo
Faculty of Industrial Technology
Institut Teknologi Bandung
Bandung, Indonesia
augie@tf.itb.ac.id

Endra Joelianto
Faculty of Industrial Technology
Institut Teknologi Bandung
Bandung, Indonesia
ejoelianto@yahoo.com

***Abstract*— Complex network theory has recently been used as a framework to describe the behavior of several networks in nature including physical, chemical, biological, technological and social networks. Some of those, such as electric power grids, transportation systems, communication networks, and others, must maintain their stability even after several failures, or targeted attacks. In this paper, we study network vulnerability in terms of cascading breakdown and outline an optimization procedure to enhance network robustness. We propose a rewiring method using simulated annealing algorithm to increase the robustness of a given network while keeping its property unchanged. Analyzing optimized networks in several aspects, simulation results showed that community structure and core-periphery structure may have a negative effect to the robustness of a network while homogeneous load distribution may improve network performance.**

Keywords— network robustness; rewiring; simulated annealing

I. INTRODUCTION

Within the span of decades, a lot of attention has been devoted to studying statistical and dynamical properties of large-scale networks with complex structures. This is motivated by the fact that complex networks occur everywhere in nature and they are essential for the infrastructure of a modern society. Examples of complex networks in our daily life include information communication networks, transportation networks, power grid networks, biological networks, social networks, economic networks, and so on. Understanding of the structure, dynamics, functioning of these networks and their interrelationships is crucial to decide how to construct robust systems against internal failures or to protect them from external attacks in the most efficient way. In recent years, complex network science has become an useful tool for scientists to make major advances in understanding salient properties of complex human engineered systems, that go beyond the single component behavior.

Current and past research has shown that in real life networks, there is a strong feedback between micro and macro states of the network, in which the micro is represented by the nodes of the network and the links between them, and the macro by the network itself, its topology, dynamics and function [1]. Some basic works on large networks were carried out by Erdös and Rényi [2, 3], who analyzed rigorously randomly connected networks; Watts and Strogatz [4], who discovered the small-world property which is representative of real networks such as social and linguistic networks; Barabási and Albert [5], who discovered the power law degree distribution of many complex networks. Based on these fundamental studies, extensive research has focused on some hot topics such as network growth, network resilience, diffusion process, cascading breakdown, community structure, consensus and synchronization, etc. In this work, we focus on the robustness characteristic of complex networks against cascading failures.

Cascading failure phenomenon in complex networks has been extensively studied. There has been a growing concern about the overload status of infrastructure networks increasing possibility of cascading failures. Recent studies have demonstrated that small initial breakdowns can lead to global cascade of overloading failures in communication and technological systems. For example, in power grid networks, if a single line is overloaded or breaks, its power is immediately rerouted to neighboring lines and the disturbance can be suspended. However, there is also a case where the neighboring line is already overloaded and must reroute its increased load to its neighbors. This redistribution of power may lead to the subsequent overloading of other lines, causing simultaneous malfunction and resulting in a cascade of overloading failures. Such knowledge will make it possible to develop strategies to mitigate the damage of cascading failures.

Much work is being devoted to define suitable measures to quantify system robustness and to identify the mechanisms

responsible for cascades. Available set of existing methods can be generally divided into two classes

- *Ex-ante* methods class, which has been developed in order to prevent or minimize the damage of cascading failures before the occurrence of initial failures.
- *Ex-post* methods class, which has been developed in order to minimize the damage of cascading failures after some initial failures occurred.

Typical examples of the latter include the well-known method proposed by Motter [6]. 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 [6] 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 shutdown 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.

For the former, Wang and Kim [7], Li, Wang, Sun, Gao, and Zhou [8] 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. Yang, Wang, Lai, and Chen [9] discovered an optimal solution to both cascading failures and traffic congestion problem by introducing and controlling a tunable weight parameter. Another prominent work was done by Ash and Newth [10], who developed an evolutionary algorithm to evolve complex networks that are resilient to cascading failures. Their results revealed that clustering, modularity, and long path lengths all play important parts in the design of robust large-scale infrastructure.

In this work, we address the dynamical origin of cascading processes on complex networks and investigate how such a network can be made secure in response to targeted attacks. We consider an appropriate definition of network robustness and propose an optimization procedure that successfully modifies a given network so that the network still has a considerable robustness under several attacks targeted at the most important nodes while keeping their functionality unchanged. The topological structure of optimized networks after intervention is also discovered.

This paper is organized as follows: a cascading failure model is introduced in section II, a network robustness measurement is demonstrated in section III, an optimization procedure is proposed in section IV, the performance of the proposed method is verified by numerical simulations in section V, and finally, the paper is summarized in section VI.

II. CASCADING FAILURE MODEL

Cascading breakdown in complex networks is often regarded as an avalanching failure. That is to say, the failure of a few local nodes can result in a global-scale breakdown in networks. In various types of existing cascading failures, one of the most prominent cascades that occur in most infrastructure networks is overloading cascade. The potential impact of this type of cascading breakdown on the security of large complex networks was firstly investigated by Motter and Lai [11].

We consider the networked system with N nodes. Since traffic or information is usually transmitted along the shortest paths in most communication networks, it has been suggested that the information flow across a node i – namely the load L_i, can be captured well by its betweenness centrality, which can be calculated as the number of shortest paths that pass through node i when flow is sent from each available generation node to each distribution node

$L_i(t)$ = the shortest path betweenness of node i at time step t (1)

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 reasonable to assume that the capacity of a node i is proportional to its initial load [11, 12]

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

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

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

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

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.

Initially, a network is in a stationary state if the load at each node is smaller than its capacity. However, it is possible that from some reasons a breakdown occurs at one or more nodes, so that they cannot work at all, and can be assumed that to 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 continuously grow until a large number of nodes are compromised to a failure point.

Using this model, we are able to investigate the potential cascading failure triggered by targeted attacks or perturbations, and to follow the dynamical response of the system to failures. 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. Network Robustness Measurement

In complex network research, the definition of network robustness might vary according to a specific application. Usually robustness is measured by the critical fraction of attacks at which the network completely collapses [13, 14]. Nevertheless, this measure ignores situations in which the network suffers a big damage without completely collapsing. Thus, a network should be considered as robust when as many as possible nodes of the network remain globally connected after an event of cascade of failures. For example, an Air-transportation network in real world is regarded as robust when it allows a passenger to travel between most of the airports even considering the disruption of the service in some major airports [15, 16].

Since the topological connectivity of a network is important, we define the robustness of a network by R, which can be quantified by the size of the Giant Connected Component (GCC) – the component for which there is a path between any pair of nodes in the network, as follows

$$R = \frac{1}{n+1}\sum_{0}^{n}\frac{GCC(n)}{N} = \frac{1}{n+1}\sum_{0}^{n}S(n) \qquad (4)$$

where N is the size of the initial network, $S(n) = GCC(n)/N$ is the fraction of nodes in the giant connected component that is reached by the network when it stabilizes after the initial failure of n nodes. The normalization factor $1/(n+1)$ ensures that the robustness of networks with different number of initial failed nodes can be compared.

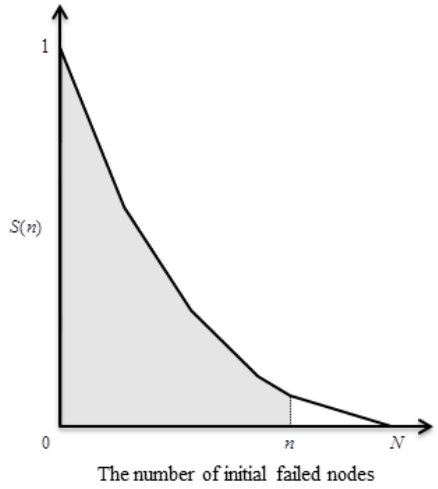

Fig. 1. Schematic profiles of $S(n)$ defined in (4) as a function of the number of initial failed nodes n. A network is obviously most robust when $n = 0$ ($S(0) = 1$) and most vulnerable when $n = N$ ($S(N) = 0$). The grey area as shown in the figure can be used to represent the robustness of a network.

The proposed definition of robustness R which corresponds to the integral of the curve in Fig. 1, not only measures after how many failed nodes the network fall apart, but also considers individually the size of the giant connected cluster from each number of failed nodes. A small R is associated to a fragile network and a larger R to a robust one.

IV. Defense Strategy

When designing a new network from scratch, designers have an excellent opportunity to predict and warrant rigorously its future robustness against failures. However, most of the current infrastructure systems have been built and grown in a non-supervised fashion, mostly through a preferential attachment mechanism, in which highly connected nodes have a higher probability of receiving a new link. Inspired by this situation, we attempt to develop a defense strategy to improve the robustness of a given network.

For a given network, the robustness can be enhanced in many ways. Given a value of α defined in (2) to determine the value of C, when C is small, the whole network gets into fully collapse easily when some nodes initially failed. On the other hand, for sufficiently large C, the destructive impacts caused by the failure of those nodes might be absorbed by other nodes, and no cascade emerges. Thus, increasing C might be the most effective way to reduce large scale breakdowns to small scale ones. One can also simply add more links between nodes as much as possible to improve network robustness. As a result, the network becomes fully connected assuring that some nodes disruption do not affect others.

However, numerous examples of infrastructure networks pointed out that the abovementioned methods are impractical due to cost and capacity constraint. Therefore, a strategy where links of a given network are only rewired is more appropriate. We consider a strategy by which we reroute links in the network to create new connection possibilities without changing the degree of each node to preserve network property.

Let $G(N, E)$ be the initial network with N nodes, E links, and the robustness R defined in (4) as an objective function. We present a rewiring method using simulated annealing algorithm to modify G in order to optimize R, while keeping the degree of each node in G fixed. Our proposed method's mechanism can be described as the following steps

Step 1. Randomly choose two pairs of links (i, j) and (h, k) in E.

Step 2. Delete (i, j) and (h, k); and add (i, h) and (k, j) to obtain new network G_{new} with new robustness R_{new}.

Step 3. G_{new} will be accepted with a transition probability p

$$p = \begin{cases} 1, & if\ R < R_{new} \\ \exp((R_{new} - R)/T), & otherwise \end{cases} \qquad (5)$$

where T represents the temperature in simulated annealing process.

Step 4. Return to step 1 and repeat the procedure until a predetermined number of iterations.

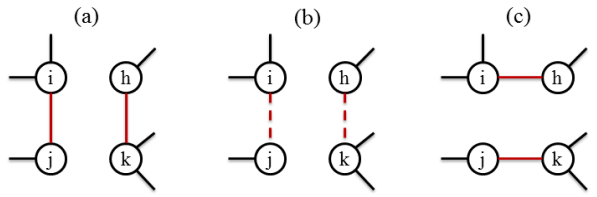

Fig. 2. Illustration of the rewiring mechanism in step 2. A pair of links (i, j) and (h, k) are randomly chosen in (a) and deleted in (b). The new connections (i, h) and (j, k) are added in (c). Note that all nodes in the figure retain nodal degree throughout rewiring process.

This approach allows new network G_{new} where $R_{new} < R$ to be chosen with a finite transition probability p to avoid local optimization search. By decreasing the temperature T according to the number of iterations, we are able to reduce the acceptance rate p when an optimal point is close.

We summary our proposed defense strategy in algorithmic representation as follows

for $t = 1$ to t **do**
  Choose (i, j) and (h, k) randomly;
  Delete (i, j) and (h, k);
  Add (i, h) and (j, k);
  if $R < R_{new}$ **then**
    $p = 1$;
    $G \leftarrow G_{new}$;
    Next t;
  else
    $p = \exp((R_{new} - R)/T)$;
    Generate a random r from uniform distribution $U(0, 1)$;
    if $r < p$ **then**
      $G \leftarrow G_{new}$;
      Next t;
    else
      Next t;
    end if
  end if
end for

V. Numerical Results

A. Simulation Settings

Networks: We focus on the simple case of networks where all links have the same importance and no orientation – unweighted and undirected networks. To confirm the generality of the proposed method, we consider different types of networks as initial state for our optimization procedure. We use an artificial network: a scale-free network generated by Barabasi-Albert model [17], with the number of nodes $N = 500$ and the average degree $\langle k \rangle = 4$, as well as a real network: the top 500 busiest commercial airports in the United States, in which nodes represent airports and a tie exists between two airports if a flight was scheduled between them [18, 19].

Initial failure: if a node has a relatively small load, its failure (removal) will not cause major changes in the load balance, and subsequent overloading failures are unlikely to occur. However, when the load at a node is relatively large, its failure (removal) is likely to significantly affect loads at other nodes and possibly start a sequence of overloading failures. To study attack vulnerability of networks, we select nodes in order of descending load, which would be expected to bring the most damage to network stability, to remove initially from the network.

Number of initial failures n: we assume that attackers can remove up to 1% highest load nodes of the network ($n = 5$ in (4)).

Tolerance parameter α: we focus on small tolerance parameter to validate the effectiveness of our proposed method. If we can optimize a given network even for small α, cascading failures may be mitigated without needing to consider how to efficiently allocate capacity in the network. In particular, we set $\alpha = 1$ for the Top 500 airports network and $\alpha = 1.2$ for the artificial scale free network.

Number of iterations: $t = 10^5$.

The temperature T: we empirically set T as a function of the iteration number t, i.e. $T = 0.9999^t$.

B. Simulation Results

To test the generality of our proposed method, we firstly generated 10 different scale-free networks. We then perform 10 randomization pairs of links as introduced in Step 1 of our proposed method mentioned in section IV for each generated scale-free network and also for the top 500 airports network and start the optimization process individually. Simulation result showed that the robustness of each network is remarkably enhanced and the optimized networks for all trials are almost identical. This suggests that our algorithm is efficient in increasing network robustness of a given network with a given degree distribution independent on its initial state.

We chose from all trials of each type of network the case where network robustness was most enhanced to analyze the result, shown in Fig. 3 and Fig. 4. As shown in left figures of Fig. 3 and Fig. 4, optimized networks have much better performance compared to initial networks in both case of scale-free network and top 500 airports network, in which the rewired times $t^* = 0$ corresponds to initial networks before intervention. As shown, network robustness R fluctuates with small t^* and reaches higher values as t^* increases. When t^* is sufficient large, positive swaps are executed in sequence, bringing a systematic increase in the network robustness. The results revealed that all networks investigated can be improved significantly.

On the other hand, right figures in Fig. 3 and Fig. 4 represent $S(n)$ defined in (4) as a function of the number of the initial failed nodes n. As shown, the initial networks become significantly more robust after rewiring, keeping a considerable connectivity after several targeted attacks.

C. Analysis of Optimized Network Structure

To verify that successive swaps of the proposed method might change some characteristics of initial networks, we

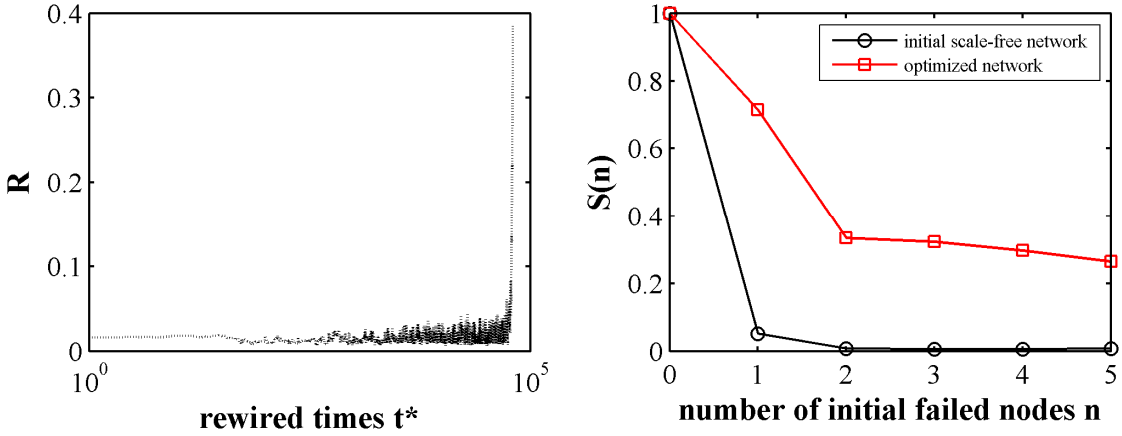

Fig. 3. Network robustness evolution during rewiring process (left figure) and $S(n)$ defined in (4) as a function of initial failed nodes n (right figure), for scale-free network.

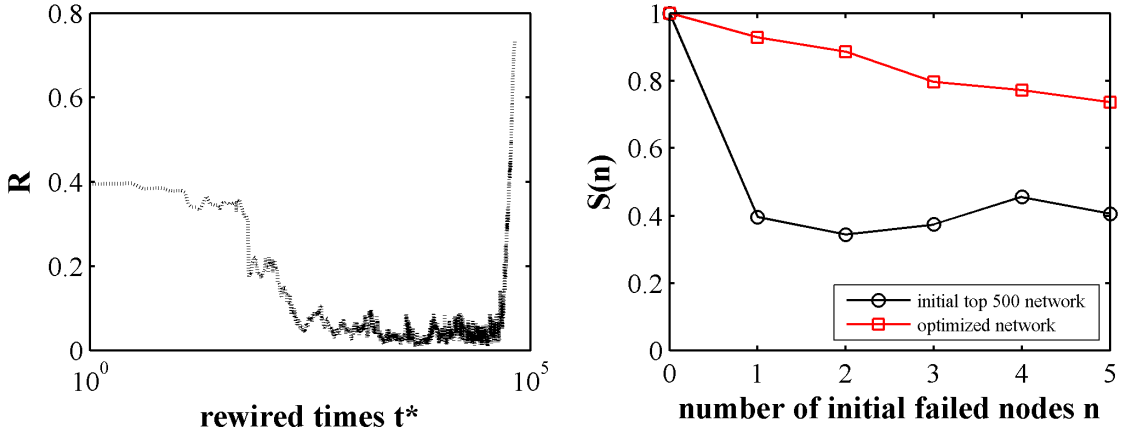

Fig. 4. Network robustness evolution during rewiring process (left figure) and $S(n)$ defined in (4) as a function of initial failed nodes n (right figure) for top 500 airports network.

analyzed the structure of optimized networks in comparison with initial networks, using complex network macroscopic and microscopic indexes including local and global assortativity [20, 21, 22], modularity [23], core-periphery and centralization [24], and load distribution.

The higher local assortativeness [22] in high degree nodes of optimized networks in Fig. 5 indicates that there are more connections between hub nodes in optimized networks than in initial networks. Moreover, optimized networks also have higher global assortativeness [20] than initial networks, meaning that not only hub nodes but also other nodes in optimized networks tend to connect to nodes with similar level of degree.

We calculated the modularity defined in [23] to compare community structure between optimized networks and initial networks. We obtained that optimized networks have smaller modularity, indicating that community structure may have negative effects to network robustness.

Comparison of network core-periphery profiles [24] between optimized networks and initial networks are plotted in Fig. 6, where x-axis represents the fraction of peripheral nodes and y-axis is the coreness of nodes. As shown in the figure, optimized networks in both cases of scale-free network and top 500 airports network, are closer to complete network – namely the perfectly equalized network. This supports that optimized networks obtained after using our proposed method, evolve to a non-core-periphery structure.

We plotted the cumulative distribution function of the load in initial networks and optimized networks in Fig. 7 to observe the load distribution transition. As showed, optimized networks have a more homogeneous load distribution than initial networks, although the transition was not so clear in two types of networks we used in simulation. The result pointed out that a network with homogeneous load distribution is more robust against cascades. This result also meets our another study [25].

VI. Conclusions

In this paper, we studied network vulnerability in terms of cascading failures. We considered overloading cascading failures that have been demonstrated to mainly occur in communication and technological systems. We presented a measure for network robustness that outperforms the common robustness measure by focusing on the size of the

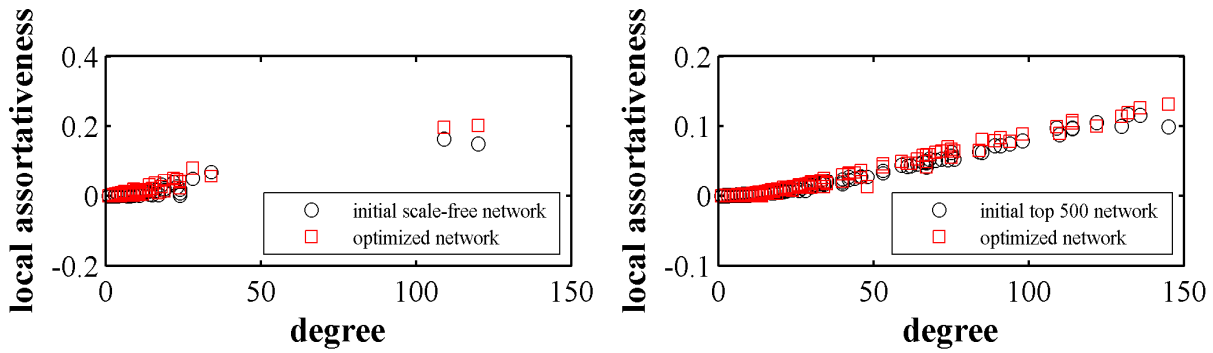

Fig. 5. Local assortativeness comparison between initial networks and optimized networks for scale-free network (left figure) and top 500 airports network (right figure).

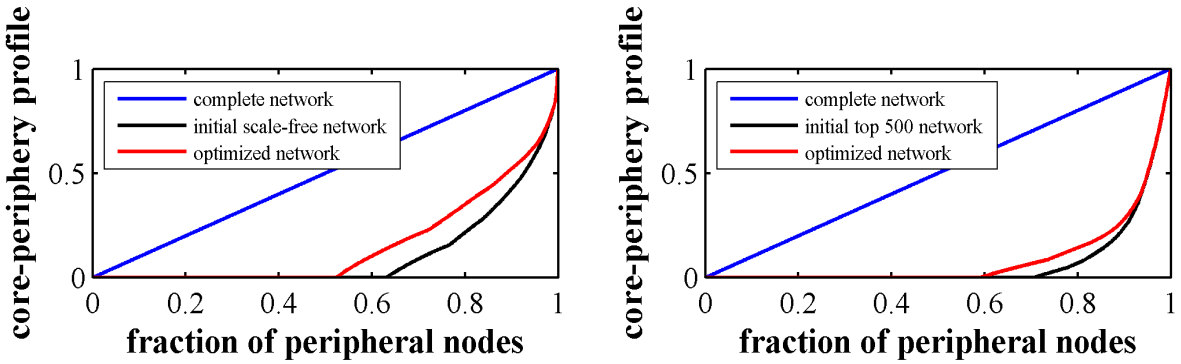

Fig. 6. Core periphery profile comparison between initial networks and optimized networks for scale-free network (left figure) and top 500 airports network (right figure).

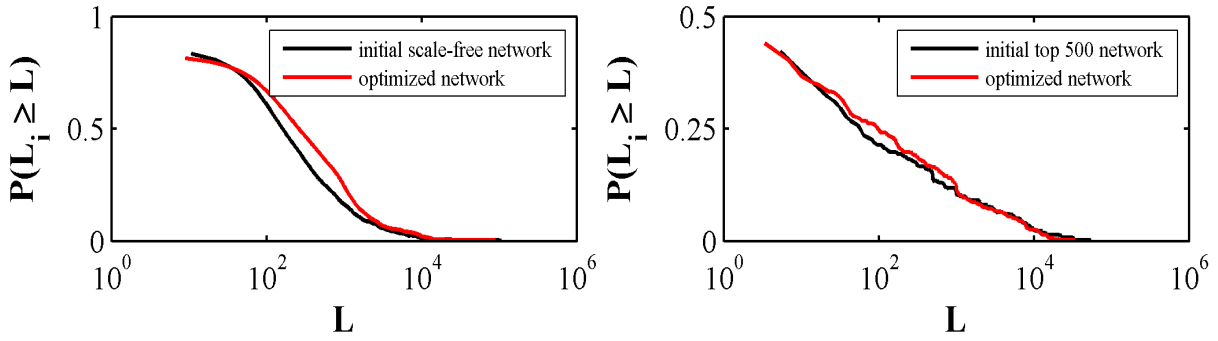

Fig. 7. Load distribution comparison between initial networks and optimized networks for scale-free network (left figure) and top 500 airports network (right figure).

giant connected component under a sequence of targeted attacks. We developed an optimization procedure to generate robust networks, as well as to substantially improve the robustness of a given network by swapping links while keeping the degree distribution of the network fixed.

We analyzed optimized networks in several aspects and found that, a network evolves to a special structure to be robust against cascades. That is, non-community structure, non-core-periphery structure and homogeneous load distribution are remarkable factors to suppress cascades.

The result makes the proposed strategy a potential tool for network designers having the task of protecting already built infrastructure, or designing networks from scratch with desired features. The proposed method also suggests that the same findings would apply to all real networks with a broad degree distribution since swapping links is general and not limited to a particular network class.

While cascading failures in one network can have dramatic consequences for a system, social disruptions caused by recent disasters ranging from hurricanes to large power blackouts and terrorist attacks have shown that the most dangerous vulnerability hides in the many interdependent networks. Our future work then will be investigating network vulnerability of interdependent systems.

ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers for their valuable comments. This research is supported in part by

Grant-in-Aid for Scientific Research in Japan No.25330277 & No.26282089.

REFERENCES

[1] S. Havlin, D. Y. Kenett, E. B. Jacob, A. Bunde, R. Cohen, H. Hermann, J. W. Kantelhardt, J. Kertesz, S. Kirkpatrick, J. Kurths, J. Portugali, S. Solomon, "Challenges in network science: Applications to infrastructures, climate, social systems and economics", Eur. Phy. J. Special Topics, 214, pp. 273-293, 2012.

[2] P. Erdös and A. Rényi, "On random graphs", Publications Mathematica, Vol. 6, p. 290–297, 1959.

[3] P. Erdös, A. Rényi, "On the strength of connectedness of a random graph", Acta Math. Acad. Sci. Hung. 12, pp. 261-267, 1961.

[4] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-world networks", Nature, Vol. 393 No. 6684, p. 440–442, 1998.

[5] A. L. Barabási and R. Albert, "Emergence of scaling in random networks", Science, Vol. 286 No. 5439, pp. 509-512, 1999.

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

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

[8] 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.

[9] 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.

[10] A. Ash and D. Newth, "Optimizing complex networks for resilience against cascading failure," *Phys. A.*, vol. 380, 673, 2007.

[11] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks", Phys. Rev. Lett., Vol. 66, 2002.

[12] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks", Phys. Rev. E., Vol. 69 045104, 2004.

[13] P. Holme, B. J. Kim, C. N. Yoon, S. K. Han, □Attack vulnerability of complex networks□, *Phys. Rev. E* **65**, 056109, 2002.

[14] P. Holme, J. Zhao, □Exploring the assortativity-clustering space of a network□s degree sequence□, *Phys. Rev. E* **75**, 046111, 2007.

[15] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks", Proc. of the National Academy of Sciences of the United States of America, 2011.

[16] V. H. P. Louzada, F. Daolio, H. J. Herrmann, M. Tomassini, "Smart rewiring for network robustness", Jour. of Complex Networks, 2013.

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

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

[20] M. E. J Newman, "Assortative mixing in networks", Phys. Rev. Lett. 89, 208701, 2002.

[21] M. Piraveenan, M. Prokopenko, A. Y. Zoyama, "Local assortativeness in scale-free networks", EPL 84, 28002, 2008.

[22] M. Piraveenan, M. Prokopenko, A. Y. Zoyama, "Classifying complex networks using unbiased local assortativity", Proc. of the Alife XII Conference, 2010.

[23] M. E. J Newman, "Modularity and community structure in networks", Proc. of the National Academy of Sciences of the USA, Vol. 103 No. 23, pp. 8677-8582, 2006.

[24] F. D. Rossa, F. Dercole, C. Piccardi, "Profiling core-periphery network structure by random walkers", Scientific reports, 2013.

[25] Hoang Anh Q. Tran, Akira Namatame, "Mitigation of Cascading Failures with Link Weight Control", IJACSA, Vol. 5, Iss. 7, 2014.