Design Robust Networks against Overload-Based Cascading Failures

Hoang Anh Q. Tran[*1], Akira Namatame[2]

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

[*1]ed13004@nda.ac.jp; [2]nama@nda.ac.jp

***Abstract*-Cascading failures are an interesting phenomenon in the study of complex networks and have attracted great attention. Examples of cascading failures include disease epidemics, traffic congestion, and electrical power system blackouts. In these systems, if external shocks or excess loads at some nodes are propagated to other connected nodes because of failure, a domino effect often occurs with disastrous consequences. Therefore, how to prevent cascading failures in complex networks is emerging as an important issue. A vast amount of research has attempted to design large networked infrastructures with the capability to withstand failures and fluctuations; this can be thought of as an optimal design task. In this paper, a cascading failure on an overload-based model was studied and a novel core-periphery network topology was heuristically designed to mitigate the damage of cascading failures. Using the Largest Connected Component after a sequence of failures as the network robustness measure, numerical simulations show that the proposed network, which consists of a complete core of connected hub nodes and periphery nodes connecting to the core, is the least susceptible to cascading failures compared to other types of networks.**

Keywords- Overload Cascading Failure; Robust Network; Core-Periphery

I. INTRODUCTION

It is broadly recognized that most complex systems in nature are organized in intricate network patterns. Hence, many complex systems in nature and society can be described by networks, including social and biological systems such as the Internet, World-Wide Web, computer networks, electrical power grid networks, and metabolic networks. In recent years, complex network research has attracted much attention and scientists have made major advances in understanding the topological properties of networks. Interestingly, it has been demonstrated that most networks in nature share some important topological similarities, e.g., the small-world and scale-free properties [1, 2]. Moreover, a vast number of studies have clarified that certain topological properties of complex networks have strong impacts on their stability. Here, a network's stability refers to its malfunction-avoiding ability when a fraction of its elements is damaged. Network topologies are often not static; the applications on the network can change and its topology can evolve [3]. This observation has triggered an intense research effort aimed at understanding the organizing principles of these networks and the interplay between topology and network dynamics [4, 5]. An early important work in this field was undertaken by Albert et al. [1], who showed by numerical simulations that scale-free networks are robust against the random removal of nodes but significantly more vulnerable to the removal of high degree nodes. In other words, in a scale-free network, if the nodes are removed in decreasing order of degree, starting with the most connected ones, then the network is disconnected into fragments very quickly because the highly connected nodes hold the network together. That is, scale-free networks with heterogeneous degree distributions are remarkably resistant against random errors, but at the same time, targeted malicious attacks can disrupt the network by removing only a small fraction of nodes or links. On the other hand, homogeneous networks might be robust against attacks but are vulnerable to random failures. In our daily life, many important real networks have the "robust yet fragile" property. A simple solution to preventing disruption and improving security is to add as many links as possible between nodes. However, the addition of links also leads to a significant increase in cost. To solve this problem, Schneider et al. [6] developed a method to generate a robust network by swapping links of a given network while keeping the degree distribution fixed. Their results showed that robust networks have an onion-like topology, consisting of a core of highly connected nodes hierarchically surrounded by rings of nodes with decreasing degree.

While the ongoing progress of networking in essential utilities brings significant benefits to our quality of life, networked systems often hold a certain danger where the actions of a single actor could have an impact on all the other actors. Thus, the failure of only a single element in the system can diffuse to other elements. This kind of failure is widely recognized as a cascading failure for which, through errors or locally emerging intentional attacks, the damage is widely propagated and could even result in global collapse. Previous studies [7] have demonstrated that the increasing interdependencies in many types of real networks in areas such as financial institutions and enterprise risk management create challenges for managing risks. While more links between banks might be expected to increase the risk of contagion, a densely connected network was proven to be less susceptible to contagion than those with a sparse network structure of few connections. That is to say, better-connected networks are more resilient, since the proportion of losses from one node is transferred to more nodes through a network. On the other hand, in the case of a sparse network, the failure of one node may trigger the failure of the entire network.

Many scholars have investigated cascading failures caused by the overload mechanism. The mechanism behind this type of cascade is that there is a critical load for which risk sharply increases towards the threshold for the cascading failure. If

DOI: 10.5963/IJCSAI0402002

external shocks or excess loads at some nodes are propagated to other connected nodes because of failure, domino effects often occur with disastrous consequences. In the traffic of electrical systems, a high load on some components causes failures such as traffic jams or electrical line failures with the potential to sever links or remove nodes from the network. Recently, a study of power grid systems has received significant attention because of its importance to daily life. There has been a growing concern about the overload status of the power grid networks and the increasing possibility of cascading failures. In power grid networks, if a single line is overloaded or broken, its power will immediately re-routed to a different line and the disturbance can be suspended. There is also a case where the other line is already overloaded and must re-route its increased load to its neighbors. This redistribution of power may lead to the subsequent overloading of other lines, causing their simultaneous malfunction and resulting in a cascade of overloading failures. Power redistribution incidents such as these have taken place in history, for instance, the blackout on August 10, 1996 when a 1300 MW electrical line in Southern Oregon sagged in the summer heat, initiating a chain reaction that cut power to more than four million people in 11 states of western U.S. [8, 9]. Another example is 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 the northeastern and mid-western United States and Ontario, Canada were without power for as long as 15 hours [10]. There have also been chains of blackouts that have taken place over several countries, such as the electric power system collapses in Denmark, Italy, and the United Kingdom that occurred within months of the U.S. blackout [11]. In the study of power grid networks, topological analysis is a component of system analysis and many researchers have attempted to provide design guidelines for power grid networks that are more robust against cascading failures.

A number of important aspects of this type of overload-based cascading failure in complex networks have been discussed in the literature and many valuable results have been discovered. Motter and Lai [12] proposed a simple model for overload or congestion breakdown for data packet transport in complex networks by assigning capacity on a node. Their 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. Using the model, they showed that for such networks where loads can redistribute among the nodes, a large-scale cascade can be triggered by disabling a single key node. In contrast to the research where the immediate removal of an instantaneously overloaded node is widely adopted, Crucitti et al. [13] considered the case where not all overloaded nodes are removed from the network. They modeled certain monitoring and other effective measures that exist in most real-life infrastructure networks, and studied cascading failures by introducing a new measure of network robustness, the efficiency of a network.

As we further model and understand the behavior 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 failure. Many authors have considered both (i) active approaches, in which they try to mitigate cascade damage while the cascade is in progress [14] and (ii) topological approaches, in which they try to design network structures robust against cascades [6]. When topological robustness is possible, it is more desirable than active robustness because of its simplicity and efficiency. Motter [15] introduced and investigated a costless defense strategy based on a selective removal of nodes and edges immediately after the initial attack or failure and showed that this strategy is practical and can drastically reduce the size of the cascade. Wang and Kim [16] studied the cascading failure problem in artificially created scale-free networks and the power grid network. They considered a novel relation between the capacity and load of each node in the network and clarified that their method made networks more robust and less costly. Ash and Newth [17] used 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 paper, we focus on the topological robustness of a network. A novel network design was proposed and it was demonstrated that this proposed network structure is the least susceptible to overload-based cascading failures. In these cascading failures, the flow diffuses on the shortest path. Every pair of nodes should select a hub node as a relaying point to decrease the average path length of the network and thus increase its communication efficiency. However, the failures of hub nodes then cause a major redistribution of the flows. To design a network robust against overflow-based cascading failure, it is intuitively clear that the homogeneous network is the best, because all nodes have sufficient alternative adjacent nodes after some nodes fail. However, a homogeneous network has performance side effects because the average shortest path length between nodes is prone to be long because of the lack of hub nodes. Here, the network proposed in this paper consists of both hub and periphery nodes. The hubs compose a complete sub-graph to prevent disruption when some important nodes fail, while the periphery nodes, which belong to single hub nodes, are useful for reducing the total load of the system. Numerical simulations showed that cascading failures do not occur in the proposed networks.

This paper is organized as follows: an overload-based cascading model is briefly reviewed in section 2, a heuristic method for designing the least susceptible network to cascading failure is introduced in section 3, the performance of the proposed network is verified by numerical simulations in section 4, and finally, the paper is summarized in section 5.

II. TRAFFIC DYNAMICS IN NETWORKS

In this section, some insights about cascading failure situations due to overload will be discussed. The overload model

DOI: 10.5963/IJCSAI0402002

considers the loads of physical quantities, such as the load of TCP and UDP packets on the Internet or the current load in power grid systems. Cascading failures triggered by the initial failure of a single node can sometimes occur because of overload; this can propagate to very large scales, causing widespread damage such as blackouts of power grid networks, packet congestion on the Internet, and chain reaction bankruptcies.

Motter and Lai [12] were the first to address this type of cascading failure in a distributed network. Their model is generally applicable to realistic networks, yet is simple enough to support tractable analysis. In this study, cascading failures were studied based on this original model. The model 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, 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 a node i is assumed to be linearly proportional to its initial load L_i,

$$C_i = (1+\alpha)L_i, \qquad \mathrm{i} = 1,2,\ldots \mathrm{N}, \tag{1}$$

where, α is the *tolerance parameter*, indicating the maximum load that a node can handle, and N is the initial number of nodes. Here, the tolerance parameter α also implies the budget of network construction or resource allocation. A node will fail if its load exceeds its capacity. Otherwise, it will be safe, i.e.

$$\begin{aligned} L_i > C_i &\rightarrow i \ will \ fail \\ L_i \le C_i &\rightarrow i \ will \ be \ safe \end{aligned}. \tag{2}$$

The topology of a network determines the arrangement of the nodes in the network and how they are connected to each other. A small change in the network topology, such as the removal or addition of nodes or links, may lead to changes in the network properties and may affect its dynamics and robustness. In this model, a cascading failure is a result of load redistribution when some nodes initially fail. When all nodes are operational, the network operates steadily because there is no overload at each node. However, the removal of a node when it fails will naturally cause a redistribution of the shortest-hop paths. This will generally increase the load at some of the other nodes. If the redistributed load exceeds the given capacity of any other node, it will also fail, triggering a new redistribution and possible subsequent cascading failures. Eventually, the failure will stop when all remaining nodes can handle their load. After the initial failure, the network goes through multiple stages of failures before it finally stabilizes.

In complex network research, the evaluation of robustness focuses on some generic topological metrics of network such as the size, efficiency, and average shortest path length of the ***L**argest **C**onnected **C**omponent (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, and the critical point of phase transition from an absorbing to cascading state. Because the connectivity of the system is important, and the topological connectivity is often measured by the size of the *LCC*, in this paper the damage caused by a cascading failure was quantified using *G*, the ratio of functional *LCC* nodes after the cascading event to those before, i.e.

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

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

III. A NETWORK DESIGN MODEL FOR CORE-PERIPHERY STRUCTURE

Different types of networks occurring in nature and societies have been shown to share some universal properties. The most promising models are those in which the structures of the social network determine the processes, which in turn shape the network structures. Some mechanisms for growing networks have been suggested, including preferential attachment-related rules for which external parameters have to be tuned. When dealing with biological networks, for example, the interplay between emergent properties derived from network growth and selection pressures has to be taken into account. The aim of this section is to investigate network dynamics with growth properties in which network topology evolves according to a specific rule.

DOI: 10.5963/IJCSAI0402002

A. The Principle of the Proposed Core-Periphery Network

Generally, based on the degree centrality, the nodes in a network can be classified into two categories, hub nodes and periphery nodes (called hubs and peripheries hereinafter). In complex networked systems, hubs play important roles because they connect other nodes and guarantee the connectivity of the network. In overload models, hubs are usually selected as pathways to reducing the average shortest hop path lengths between every pair of nodes, and the absence of hubs in that case increases the efficiency of network. Therefore, a hub might carry a large amount of flow as a relay point. Normally, the failure of hubs causes major changes in the network connectivity and load balances. Hence, the existence of hubs becomes a weak point of the network and they could be targeted by malicious attacks. The connection between hubs then plays a key role in preserving the connectivity of the whole network when some hubs fail.

Motter [15] introduced and investigated a costless defense strategy based on the selective further removal of nodes and edges right after an initial attack or failure. Their main result was that the size of the cascade could be drastically reduced by the *Intentional Removal* of nodes with small loads and edges with a large excess of load. Even though a removal always increases the immediate damage to the network, the resulting *G* is in this case significantly larger compared to the case without defense because these *Intentional Removals* strongly suppress the propagation of the cascade. Based on this study, it is now understood that the role of peripheries with small degree is mainly to contribute to load generation rather than information transmission. Hence, the removal or shutdown of one of them may reduce the total load of the system and help avoid overloading other nodes in the network.

It is now known that the connection between hubs and the shutdown of peripheries are important in terms of network robustness against overload-based cascading failures. Based on some logical principles as mentioned above, an algorithm was constructed to build the least susceptible network to overload cascading failures, in which hub-hub and hub-periphery connections are implemented.

B. Core-Periphery Network Design Model

Our model [18] builds a network in two simple steps, as shown in Fig. 1. A pre-determined resource to construct the network that consists of *N* nodes and *M* links was assumed. First, *n* complete graphs were built to form the core of the network, in which *n* nodes were connected to each other completely. This core therefore has *n-1* links. Then, new nodes were added so that each node has only one link to the existing core.

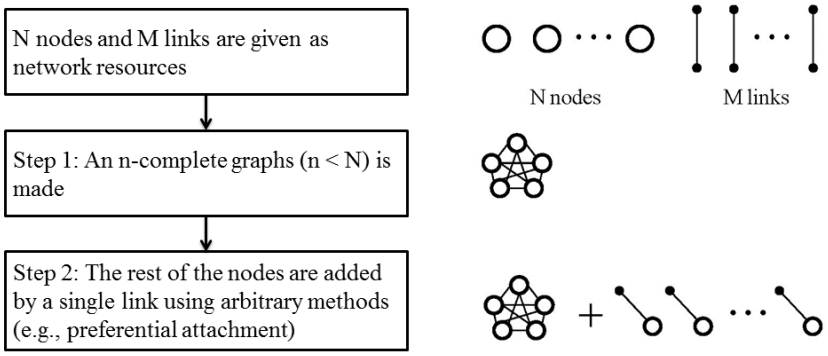


Fig. 1 The design mechanism of proposed network

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

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

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

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

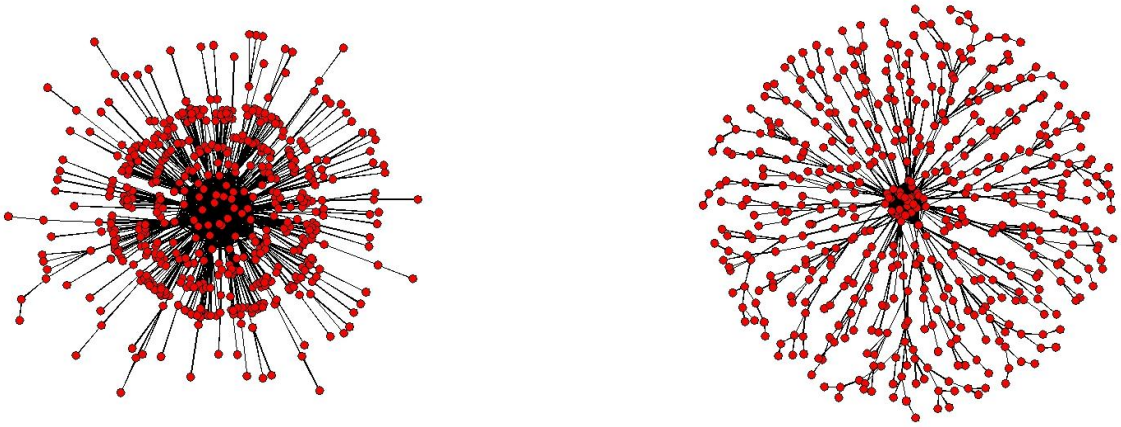
where $\lfloor . \rfloor$ represents the floor function.

Here, the arbitrary methods to adding new nodes to a given core were preferential attachment and random attachment. New nodes were 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

DOI: 10.5963/IJCSAI0402002

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.

Fig. 2 shows examples of generated *CPA* and *CRA* networks, both of which have $N = 500$ and $M = 1000$. It is observed that peripheries belong to single hubs and communicate with each other via the center core cluster in both types of networks. Each network has a similar core size, as determined by Equation (5). However, hubs in the core of the *CPA* network have higher degrees than hubs in the core of the *CRA* network because of the different attachment methods.



(a) *CPA* network: complete core and preferentially attached nodes (b) *CRA* network: complete core and randomly attached nodes

Fig. 2 Visualized snapshot of (a) *CPA* and (b) *CRA* networks with the number of nodes $N = 500$ and the number of links $M = 1000$

C. Topological Analysis of the Proposed Core-Periphery Network

Any network can be represented by an adjacency matrix A. The element of matrix A in the i^{th} row and 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. The adjacency matrix is often used as a suitable tool for manipulating and investigating some properties such as the diffusion dynamics of a network. Here, the diffusion process is a process by which new products and practices are invented and successfully introduced into a society.

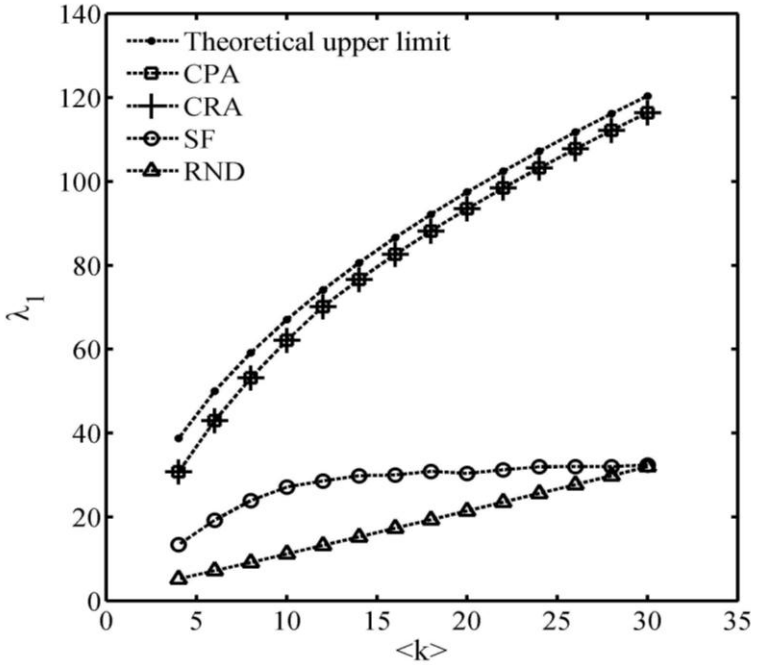


Fig. 3 The largest eigenvalues λ_1 of the theoretical upper limit, the proposed *CPA* and *CRA*, scale-free (SF), and random (RND) networks to average degree $<k>$. Here, each network has 500 nodes.

Previous studies have proposed some possible explanations for this phenomenon in terms of a network of interacting agents

DOI: 10.5963/IJCSAI0402002

whose decisions are determined by the action of their neighbors according to a probabilistic model. It is known that the maximum eigenvalue of the network decides the tipping point of a diffusion process by the probabilistic model [19]. The network with a larger maximum eigenvalue has better diffusion compared to others with smaller maximum eigenvalues. In this sub-section, the diffusion performance of the proposed networks is evaluated by comparing them with the Erdös-Rényi (ER) model-based random networks [20] and Barabási-Albert (BA) model-based scale-free networks [21]. If the proposed networks have relatively larger maximum eigenvalues compared to other types of networks, then they are more susceptible in the context of diffusion dynamics. Yuan [22] 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.

The largest eigenvalues of the proposed *CPA* and *CRA* networks were the calculated and compared to 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 shown in Fig. 3 as a function of the networks' average degree $<k>$. In the figure, SF is the scale free network based on the BA model, and RND is the random network based on ER model. The results were obtained for all methods by averaging ten individual networks. The theoretical upper limit was defined and calculated with Equation (6). Simulation result shows that the proposed networks have discriminative value of the largest eigenvalue, which characterize the network topology and interestingly, these largest eigenvalues are almost equal to the upper limit with the increase of the average degree $<k>$. That is to say, the suggested network shows its ease for diffusing innovation.

IV. COMPARATIVE SIMULATION STUDY ON CASCADING FAILURE

Two kinds of simulations were conducted to validate the robustness of the proposed network against cascading failures. In the first simulation, the robustness of the proposed networks, the generated scale-free networks and the generated random networks were compared. All networks had the same number of nodes $N = 500$ and the same average degree $<k> = 4$. These networks were compared for various values of the tolerance parameter α. The most effective and simple method to preventing a cascade is to increase this α as much as possible, meaning that all nodes have sufficient resources to prevent failure due to overload. However, α is often limited by cost. Therefore, to validate the robustness of the proposed network structure, it was assumed that the tolerance parameter α was small. The maximum value of the tolerance parameter was $\alpha = 1$ in this study.

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 to select nodes in order of descending load (the load, here, could also be regarded as degree centrality, betweenness centrality, etc.). In this paper, it is assumed that attackers know the entire topology of the network and choose m nodes with the highest loads to attack simultaneously, as this would be expected to bring the most damage to network stability. It is assumed that attackers are able to attack 1 to 50 nodes simultaneously.

If the severity of the initial attacks varies, the resulting robustness of each network is shown in Fig. 4. In sub-figures (a)–(f), as the initial number of removed nodes m increases, the relative G decreases, indicating networks with low performance. Because the proposed networks were generated with the core size defined by (6), in the case of $N = 500$ and $M = 1000$, the core size was $n = 33$. When the initial failed number of nodes $m \ge 30$, the proposed networks were almost disconnected because of the disconnection of the center clusters. The same tendency was observed for the generated random and scale-free networks. On the other hand, as the tolerance parameter α increased, the robustness of the random and scale-free networks also increased, meaning that the more resources to be allocated, the more efficiently the damage of cascading failures due to malicious attacks can be mitigated. Interestingly, despite the increase of the tolerance parameter, the robustness of *CPA* and *CRA* were stable compared to the scale-free and random networks, even when $\alpha = 0$, indicating that the robustness of the proposed networks did not depend on the tolerance parameter α. In fact, cascading failure did not occur in the proposed networks. The same result was obtained in the case when initial failure nodes were chosen randomly. In this case, peripheries have a higher probability of being chosen than hubs. Because the shutdown of peripheries reduces the total load in the system, this guarantees the stability of other nodes.

In the second simulation, we focused on the proposed network when the tolerance parameter $\alpha = 0$, implying that there is no redundant capacity in the system. If the proposed network is robust even for small values of α, cascading failures may be mitigated without needing to consider how to efficiently allocate capacity in the system.

Fig. 5 and 6 show the robustness stability of the proposed networks. As the number of initial removals m increased, it was observed that there were no overload nodes in both the *CPA* and *CRA* networks after the initial attacks. This indicates that cascading failure does not occur in the proposed networks even if the initial malicious attacks target a large number of the highest load nodes in the network. As the number of initial removals m increased, the number of removed peripheries

DOI: 10.5963/IJCSAI0402002

connecting to core also increased, leading to a decrease in the total load of the system. Hence, the gap between the capacity and load became larger for both proposed networks, as shown in the figures.

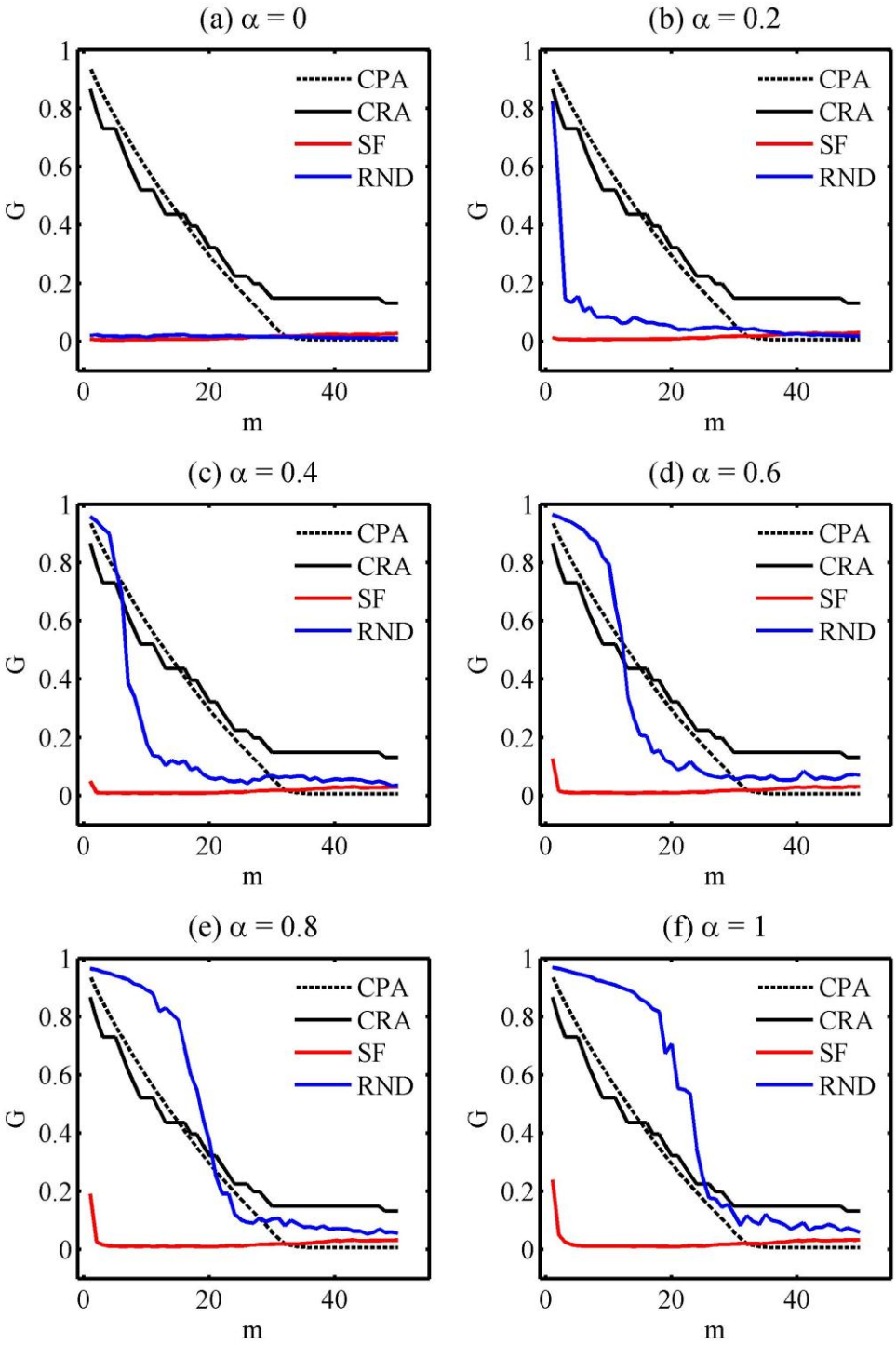


Fig. 4 Comparison of robustness for the proposed *CPA* and *CRA*, scale-free (SF), and random (RND) networks for the case of (a) $\alpha = 0$, (b) $\alpha = 0.2$, (c) $\alpha = 0.4$, (d) $\alpha = 0.6$, (e) $\alpha = 0.8$, and (f) $\alpha = 1$. In each figure, the horizontal axis is the number of removed nodes *m*, and the vertical axis is the relative *LCC* size of the network before and after the cascading event. The results for scale-free and random networks were obtained by averaging the results of ten individual generated networks.

DOI: 10.5963/IJCSAI0402002

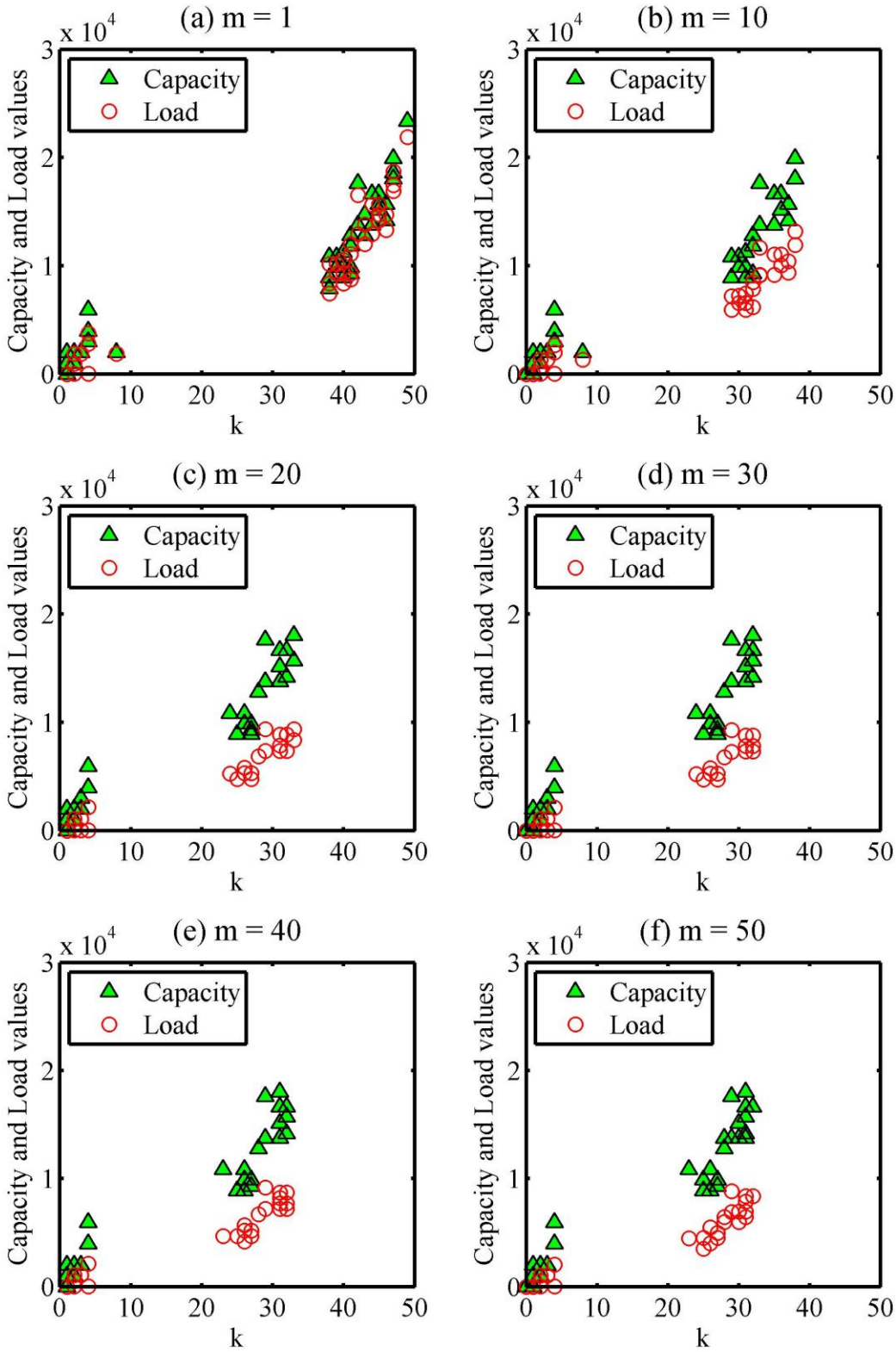


Fig. 5 Relation between load and capacity in the proposed *CPA* network for different numbers of removal nodes: (a) m = 1, (b) m = 10, (c) m = 20, (d) m = 30, (e) m = 40, and (f) m = 50. In each figure, the horizontal axis is the degree *k* of each node and the vertical axis is the value of the load (red circle) and capacity (green triangle), respectively.

DOI: 10.5963/IJCSAI0402002

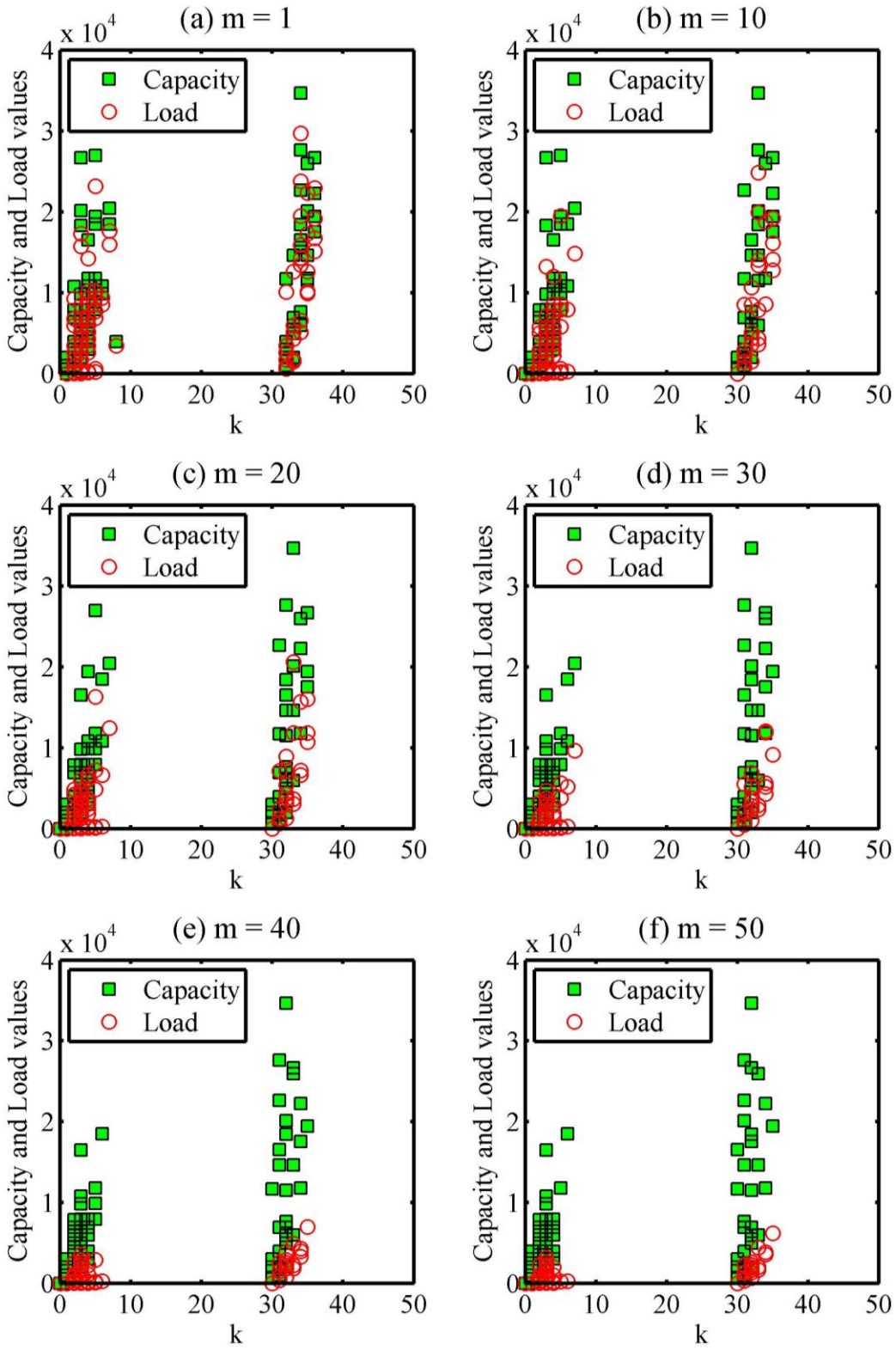


Fig. 6 Relation between load and capacity in the proposed *CRA* network for different numbers of removal nodes: (a) m = 1, (b) m = 10, (c) m = 20, (d) m = 30, (e) m = 40, and (f) m = 50. In each figure, the horizontal axis is the degree *k* of each node and the vertical axis is the value of the load (red circle) and capacity (green square), respectively.

V. CONCLUSIONS

In this paper, network robustness against overload-based cascading failures was studied. The topology of the suggested network was analyzed theoretically beforehand, and an algorithm was proposed to build *CPA* and *CRA* networks. The proposed network consists of a complete core of connected hub nodes and periphery nodes that are added to existing nodes

DOI: 10.5963/IJCSAI0402002

either by preferential or random attachment. One hub node with periphery nodes builds a module that can be regarded as a simple tree structure. In other words, the proposed network consists of many modules (trees), and they are unified via a center cluster of hub nodes.

The simulation results showed that the proposed networks can drastically reduce the damage of cascading failures. In fact, cascading failure does not occur in these networks. The center core of hub nodes prevents fragmentation, and the failure of the periphery nodes decreases the total load of the system when an intentional attack occurs. This module architecture is useful to suppress load turbulence from node failures for both intentional attacks and random failures.

In some overload models, the load on a node (or link) is generally estimated by its degree or betweenness. The degree method has a disadvantage that it is easy to lose much information in many actual applications, while the betweenness principle is practical for small and medium-sized networks but invalid for large-scale ones such as the Internet and the World-Wide Web, because of its consideration of topological information for the whole network. Therefore, the requirement for an applicable model becomes an indispensable issue. Moreover, while cascading failures in one network can have dramatic consequences for a system, social disruptions caused by recent disasters range from hurricanes to large power blackouts and terrorist attacks have shown that the most dangerous vulnerability hides in many interdependent networks. Our future work is then to build an appropriate cascading model and investigate the robustness of the interdependent systems against cascading failures.

REFERENCES

[1] R. Albert, H. Jeong, and A. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378–382, 2000.

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

[3] R. Durrett, *Random graph dynamics*, Cambridge University Press, Cambridge U.K., 2006.

[4] R. Albert and A. Barabási, "Statistical mechanics of complex networks," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 47–97, 2002.

[5] P. L. Krapivsky and S. Redner, "A statistical physics perspective on web growth," *Computer Networks*, vol. 39, pp. 261–276, 2002.

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

[7] F. Allen and D. Gale, "Financial contagion," *The Journal of Political Economy*, vol. 108, no. 1, pp. 1–33, 2000.

[8] B. A. Carreras, D. E. Newman, I. Dobson, and A. B. Poole, "Evidence of self-organized criticality in electric power system blackouts," Proceedings of 34th Annual Hawaii International Conference on System Sciences, 2001.

[9] M. L. Sachtjen, B. A. Carreras, and V. E. Lynch, "Disturbances in a power transmission system," *Phys. Rev. E*., vol. 61, no. 5, 4877, 2000.

[10] J. Glanz and R. Perez-Pena, "90 seconds that left tens of millions of people in the dark," *New York Times*, 2003.

[11] P. Fairley, "The unruly power grids," *IEEE Spectrum*, 2004.

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

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

[14] T. Q. H. Anh, T. Komatsu, and A. Namatame, "Mitigating cascading failure with adaptive networking," *Journal of New Mathematics and Natural Computation*, in press.

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

[16] B. Wang and B. J. Kim, "A high-robustness and low-cost model for cascading failures," *EPL*, vol. 78, 48001, 2007.

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

[18] T. Komatsu and A. Namatame, "Least susceptible networks to cascade failures," in Proc. WCCS, 2012.

[19] Y. Wang and D. Chakrabarti, "Epidemic spreading in real networks: an eigenvalue viewpoint," Proceedings of 22nd Symposium on Reliable Distributed Computing, pp. 242–262, 2003.

[20] P. Erdös and A. Rényi, "On random graphs," *Publications Mathematica*, vol. 6, pp. 290–297, 1959.

[21] A. Barabási, R. Albert, and H. Jeong, "Scale-free characteristics of random networks: the topology of the World-Wide Web," *Phys. A.*, vol. 281, pp. 69–77, 2000.

[22] H. Yuan, "A bound on the spectral radius of graphs," *Linear Algebra and its Applications*, vol. 108, pp. 135–139, 1988.

Hoang Anh Q. Tran holds a B.S. degree and M.S. degree in Computer Science and Engineering from the National Defense Academy of Japan and currently working on his Ph.D. degree at the Artificial Intelligence Laboratory of the National Defense Academy of Japan. His research interests include risk management, network design, and cascading failure on complex networks.

Akira Namatame is a full professor in the Dept. of Computer Science of the National Defense Academy of Japan. He holds a B.S. degree from the National Defense Academy of Japan, and an M.S. degree in Operations Research and Ph.D. degree in Engineering-Economic Systems from Stanford University. His research interests include multi-agents, game theory, evolution and learning, complex networks, economic sciences with interaction agents, and the science of collectives. He is a member of the AAAI, IEEE, and SICE.

DOI: 10.5963/IJCSAI0402002