Network Vulnerability Analysis and Mitigation Strategy against Cascading Failure

Kashin SUGISHITA [a], Yasuo ASAKURA [b]

[a,b] *Department of Civil and Environmental Engineering, School of Environment and Society, Tokyo Institute of Technology, Tokyo, 152-8552, Japan*
[a] *E-mail: k.sugishita@plan.cv.titech.ac.jp*
[b] *E-mail: asakura@plan.cv.titech.ac.jp*

Abstract: Cascading failure is a phenomenon where a small shock or error in a local part of a networked system triggers propagation of failures across the entire network. In this study, we propose 1) a model for cascading failure in the context of disruptions in road networks and 2) a mitigation strategy which eliminates the flow generated from non-influencers to avoid serious consequences. In the numerical analysis, we apply the model to both homogeneous and heterogeneous networks and also investigate the performance of the mitigation strategy. The results give us implications for transportation network management: 1) in most cases, large-scale cascading failure can be avoided by increasing practical capacity as a prevention strategy and 2) in a case of emergency where the practical capacity is extremely small, serious cascading failure can be avoided by eliminating flow generated from non-influencer nodes as a mitigation strategy.

Keywords: Cascading Failure, Network Vulnerability, Network Topology, Mitigation Strategy, Complex Networks

1. INTRODUCTION

Our society is surrounded by a great variety of networked systems such as electrical power grids, communication lines, or transportation networks. These systems normally work in a proper way and they raise the standard living in our society. However, recent studies have pointed out a potential risk in these networked systems. The risk is that only a small shock or error in a local part of a networked system can be a trigger of large-scale propagation of failures and eventually the entire network is seriously damaged. This kind of phenomenon is called *cascading failure*.

Cascading failure is a phenomenon where a small shock/error triggers successive failures throughout large parts of a system. Cascading failure can take place in various systems such as power grids, communication lines, or transportation systems where traffic is reassigned to bypass failed nodes/links, eventually leading to a propagation of overload failures on other nodes/links that cannot handle extra traffic (Crucitti *et al*., 2004). Cascading failure has been mainly researched to discuss the vulnerability of power grids or communication systems (*e.g.* Motter and Lai, 2002; Crucitti *et al.*, 2004; Buldyrev *et al*., 2010). Only few researches have been conducted in the context of disruptions in transportation networks (*e.g.* Wu *et al*., 2007).

In order to protect networked systems and avoid catastrophic consequences, effective defense strategies are required. Two types of strategies can be considered: prevention and mitigation strategies. A prevention strategy is a strategy which aims to increase the network robustness itself. On the other hand, a mitigation strategy is one which aims to prevent the

propagation of failures and avoid serious consequences.

There are two objectives in this study. First, we propose a model for cascading failure where overloading of links propagate across the entire network. Second, we propose an effective mitigation strategy against cascading failure. In the numerical analysis, we focus on the influence of the network topology on vulnerability against cascading failure and we apply the model to both homogeneous and heterogeneous networks. Also we investigate the performance of the mitigation strategy for both types of networks. The results may give us some implications about the vulnerability of road networks which are classified into homogeneous networks and effective risk management strategies to avoid serious consequences in road networks.

The rest of the paper is consisted as follows. In chapter 2, the literature review is described. In chapter 3, the methodology is explained, followed by numerical analysis in chapter 4. The paper ends with conclusions in chapter 5.

2. LITERATURE REVIEW

Cascading failure has been studied intensively for about fifteen years. Cascading failure can occur when some mechanisms of propagation of failures exist. Without such mechanisms, a removal of a node/link never affects other parts of the network. The simplest evaluation of network robustness can be obtained by studying the influence of removal of nodes/links (*e.g*. Albert *et al*., 2000; Holme *et al*., 2002). According to Mattsson and Jenelius (2015), some studies about transportation network vulnerability applied such simple evaluation of network robustness to transportation networks. However, when those mechanisms are considered, failures can spread out in complicated ways and only a single removal of node/link can be a trigger of serious cascading failure and the whole network can be collapsed.

Some studies have already proposed models for cascading failure in the context of disruptions in power grids or communication networks. Motter and Lai (2002) proposed a model where overloaded nodes (power stations or routers) are successively removed from a network. Crucitti *et al*. (2004) also proposed a model where nodes are successively overloaded and the network performance decreases. Simonsen *et al*. (2008) studied cascading failure using a dynamic model developed from the model proposed by Motter and Lai (2002). They pointed out that transient dynamics increases the network vulnerability. However, even though cascading failure can occur in various systems where traffic is reassigned to bypass failed nodes/links and eventually leading to a propagation of failures on nodes/links which cannot handle extra traffic, there are few studies in the context of disruptions in transportation networks. Thus this study aims to propose a model for cascading failure where overloading of links propagate across the entire network.

It is important to establish effective defense strategies to protect networks from cascading failure. Motter (2004) proposed a strategy which removes low betweenness centrality nodes. However, this strategy requires attention because it eliminates not only 1) the flow generated from the removed nodes, but also 2) the flow concentrating to them, and 3) the flow between other pairs of nodes if there is no path between them because of the removal of nodes. This study then proposes an effective mitigation strategy which is less drastic than the existing strategy. In addition, the existing strategy takes relatively high computational cost because betweenness centrality requires the global topology of a network. Thus this study also aims to propose another way to identify nodes to eliminate the flow which requires only local topology of a network.

3. METHODOLOGY

In chapter 3, the details of the model for cascading failure and the mitigation strategy are explained. Section 3.1 describes the model for cascading failure. In section 3.2, the index for evaluating damage is defined. Finally section 3.3 goes into details of the mitigation strategy.

3.1 Model for Cascading Failure

First of all, the overview of the model is explained. Although this model is based on the model proposed by Crucitti *et al.* (2004) where nodes are successively overloaded, the model in this study aims to represent the propagation of overloading of links. As shown in Fig. 1, the model consists of four parts: 1) normal state, 2) local failure, 3) propagation of failures, and 4) ultimate state. *Italic* terms in this paragraph are described in details later. It is assumed that the network flow is assigned to *the most efficient path* and each link has finite *practical capacity* to handle *load* without loss of *efficiency of link*. Initially, the network is in a stationary state (1. normal state) where all nodes/links function without problems. However, if a few nodes/links in a local part of the network fail (2. local failure), the network flow is reassigned to the most efficient path in that state which bypasses failed nodes/links. In most cases, the effect of the local failure might be immediately absorbed into the system because the diverted traffic can be handled on other links with sufficient practical capacity. However, under specific conditions where the diverted traffic cannot be handled on other links, the local failure might trigger the avalanche of failures by overloading and have a huge impact on the whole network. If a link is overloaded, it is assumed that the efficiency of the link decreases. Because of the reduction of the efficiency of links, the network flow is reassigned again to the most efficient path in a new state and it can create successive overloading of links. The reassignment of the network flow and successive overloading is repeated in the process of the propagation of failures (3. propagation of failures). Eventually the network efficiency relaxes to a steady state (4. ultimate state). In the ultimate state, as described in section 3.2, the drop of *network efficiency* from the normal state to the ultimate state is evaluated as damage.

Now details of the model are described. The model is based on following assumptions:

- at each time step, uniform unit OD matrix is assigned to the most efficient path
- network flow at each time step does not remain to the next time step and congestion of a link does not extend to upper stream
- local failure is represented by the removal of links from the network
- each link has finite practical capacity to handle traffic without loss of efficiency of the link
- when the load exceeds the practical capacity on a link, the efficiency of the overloaded link decreases.

A network is represented as a weighted and undirected graph G with N nodes, forbidding self-loops and multiple edges. A weighted graph is a graph whose links are assigned weights and an undirected graph is one whose links do not have distinguished direction. A self-loop is a link which connects a node to itself and multiple edges are two or more links that connect the same two nodes. The graph G at time step t is represented by

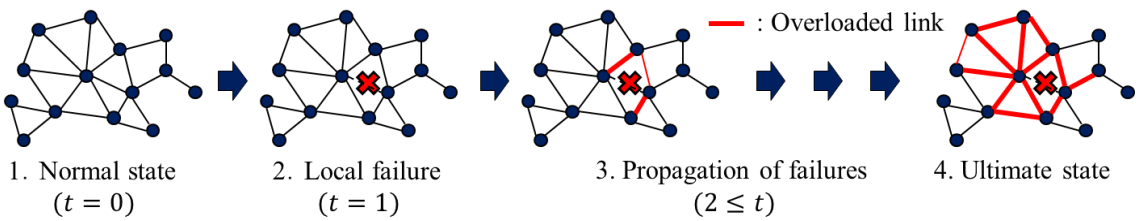


Figure 1. The overview of the model for cascading failure

the $N \times N$ adjacency matrix $\{e_{ij}(t)\}$. The value $e_{ij}(t)$ represents the efficiency of link between node i and node j at time step t. The efficiency of links can be changed by reflecting the degree of congestion. The (i,j) component and (j,i) component of the adjacency matrix take always the same value because the network is undirected one. The diagonal components of the adjacency matrix take zero, because self-loops are forbidden here. Let d_{ij} denote the distance of a link between node i and node j, the efficiency of link in the normal state is defined as the inverse of the distance of link, $e_{ij}(0) = 1/d_{ij}$. If there is no link between node i and node j, the distance between them d_{ij} is practically equivalent to infinity, $d_{ij} = +\infty$, and the efficiency of the link between them is then zero, $e_{ij}(0) = 0$.

Let $\epsilon_{lm}(t)$ denote the efficiency of the most efficient path between node l and node m at time step t. $\epsilon_{lm}(t)$ is represented as follows,

$$\epsilon_{lm}(t) = max_{P_{lm}(t)}\left(\sum_{i,j \in P_{lm}(t)} \frac{1}{e_{ij}(t)}\right)^{-1} \tag{1}$$

where,

$\epsilon_{lm}(t)$: the efficiency of the most efficient path between node l and node m at time step t,
$P_{lm}(t)$: the set of all paths between node l and node m at time step t,
$e_{ij}(t)$: the efficiency of a link between node l and node m at time step t.

In the normal state (time step $t = 0$), all links function properly. Let $L_{ij}(t)$ denote *load* on link ij at time step t. We assume that at each time step, uniform unit OD matrix is assigned to the most efficient path. From this assumption, according to Brandes (2001), the load of link ij in the normal state, $L_{ij}(0)$, is represented as follows,

$$L_{ij}(0) = \sum_{h,k \in V} \frac{\sigma_0(h,k|ij)}{\sigma_0(h,k)} \tag{2}$$

where,

V : the set of all nodes,
$\sigma_0(h,k)$: the number of the most efficient paths from node h to node k in the normal state,
$\sigma_0(h,k|ij)$: the number of paths passing through link ij among the most efficient paths from node h to k in the normal state.

Let C_{ij} denote the practical capacity of link ij. As described in the list of assumptions, practical capacity of a link represents the limitation to handle traffic without loss of efficiency of a link. Here the practical capacity is assumed to be proportional to the load in the normal state and the practical capacity is constant throughout all the time step,

$$C_{ij} = (1 + \alpha)L_{ij}(0) \tag{3}$$

where,

C_{ij} : the practical capacity of link ij,
α : tolerance parameter ($\alpha \geq 0$),
$L_{ij}(0)$: the load of link ij in the normal state.

The condition $\alpha \geq 0$ guarantees that no link is overloaded in the normal state. If the tolerance parameter α is large enough, the network is robust against cascading failure. The effect of local failure can be immediately absorbed by handling the diverted traffic on other links with sufficient practical capacity. However, it is conceivable that when the tolerance parameter α is less than a certain value, failures can spread out easily and eventually the whole network may be collapsed.

It is assumed that a few nodes/links fail as local failures at time step $t = 1$. A failure of a node is practically equivalent to failures of all links connected to the node. Namely failures of nodes are able to be represented as failures of links. Thus any local failures of nodes/links can be represented as failures of links. If local failures occur, links stop functioning and they are substantially removed from the network. Therefore the local failure can be represented by updating the adjacency matrix as follows,

$$e_{ij}(1) = e_{ji}(1) = 0 \quad \forall ij \in E_0 \tag{4}$$

where,

E_0 : a set of links removed from the network because of failures on nodes or links.

After the removal of some links as local failures at time step $t = 1$, the most efficient path between some pairs of nodes may change and the network flow may also shift. Accordingly the load of each link might change as well. The load is then recalculated as follows in the same way as equation (2),

$$L_{ij}(t) = \sum_{h,k \in V} \frac{\sigma_t(h,k|ij)}{\sigma_t(h,k)} \tag{5}$$

where,

$L_{ij}(t)$: the load of link ij at time step t,

$\sigma_t(h,k)$: the number of the most efficient paths from node h to node k at time step t,

$\sigma_t(h,k|ij)$: the number of paths passing through link ij among the most efficient paths from node h to node k at time step t.

If the recalculated load does not exceed practical capacity on any link, influences of local failure can be immediately absorbed into the system. However, if the recalculated load exceeds the practical capacity on some links, such links are overloaded and the efficiency of them is assumed to decrease. The reduction of the efficiency of links is represented by adopting the following rule,

$$e_{ij}(t+1) = \begin{cases} e_{ij}(0)\frac{C_{ij}}{L_{ij}(t)} & if\ L_{ij}(t) > C_{ij} \\ e_{ij}(0) & if\ L_{ij}(t) \leq C_{ij}. \end{cases} \tag{6}$$

If the efficiency of some links decrease, the most efficient path between some pairs of nodes also shift again. The reassignment of the network flow can create further overloading of links and the efficiency of them also decreases as well. This process is repeated and overloading of links propagate across the entire network.

After the propagation of failures, the network relaxes to a stationary state. As described in section 3.2, the damage caused by cascading failure is evaluated using network efficiency in the ultimate state.

3.2 Damage Evaluation

Some previous studies about network vulnerability evaluate the drop of the relative size of the largest connected component in the ultimate state in comparison with that in the normal state (*e.g.* Albert *et al.*, 2000; Holme *et al.*, 2002; Motter and Lai, 2002). A connected component is a subgraph in which every pair of nodes has at least one path between them. The largest connected component is one with the largest number of nodes among all the subgraphs in a network. However, in this study, overloaded links are not removed from the network, but the efficiency of overloaded link is considered to decrease. Only the links where local failures occur, that is to say, elements in the set of links E_0 in equation (4), are removed from the network. In this case, damage brought by propagation of failures cannot be evaluated by observing the relative size of the largest connected component. Another index is required to consider the drop of the network performance.

In this study, the drop of network efficiency is then evaluated as damage caused by cascading failure. The index for the network efficiency was proposed by Latora and Marchiori (2001) as shown below,

$$E(t) = \frac{1}{N(N-1)} \sum_{l \neq m} \epsilon_{lm}(t) \tag{7}$$

where,

$\epsilon_{lm}(t)$: the efficiency of the most efficient path between node l and node m at time step t,
$E(t)$: the network efficiency at time step t,
N : the number of nodes in a network.

If any path does not exist between node i and node j at time step t, the distance is considered as infinity and the value of the efficiency of the most efficient path is zero, $\epsilon_{lm}(t) = 0$. As shown in equation (7), the network efficiency $E(t)$ can be defined for both unweighted and weighted networks with more than one nodes. The network efficiency $E(t)$ can take any value more than zero. If a network is an unweighted complete graph in which every pair of nodes is connected by unique links with the weight $e_{ij}(t) = 1$, the network efficiency $E(t)$ is equal to one. As shown in equation (4), only a few links are removed from a network and the adjacency matrix is updated. On the other hand, nodes are not removed from a network throughout all the time step. The number of nodes N is then always constant from the normal state to the ultimate state.

The drop of the network efficiency is considered as damage. Therefore the index for evaluating damage at time step t is defined as follows,

$$D(t) = \frac{E(0) - E(t)}{E(0)} \quad (0 \leq D(t) \leq 1) \tag{8}$$

where,

$D(t)$: the damage at time step t,
$E(t)$: the network efficiency at time step t.

3.3 Mitigation Strategy

Section 3.3 goes into details of the mitigation strategy. Two types of defence strategies can be considered: prevention and mitigation strategies. A prevention strategy is conducted before

the local failure in preparation for cascading failure. On the other hand, a mitigation strategy is carried out after the local failure. Our strategy is one of mitigation strategies which is conducted after the local failure and before the propagation of failures as shown in Fig. 2.

The strategy aims to reduce the total amount of the network flow by intentionally eliminating flow generated from specific nodes, to prevent the propagation of failures by overloading, and eventually to mitigate damage. Most cases may not require any mitigation strategy because the influences of the local failure can be absorbed into the system. However, under specific conditions where the network itself is fragile or the network is exposed to targeted attacks on important nodes/links, a mitigation strategy is required. One thing to be considered for our strategy is how to specify nodes to eliminate flow for mitigating damage effectively. However, identifying the optimal set of nodes to eliminate flow is a non-deterministic polynomial-time hard (NP-hard) problem. Accordingly this study proposes a mitigation strategy which eliminates flow generated from *non-influencers* identified by an index called *collective-influence (CI)* .

The details of the index called collective-influence (CI) are described here. CI was originally proposed for identifying set of nodes whose removal break up a network effectively (Morone and Makse, 2015). Dismantling a network is sometimes useful. For instance, breaking up a contact network may be desirable to prevent the spreading of infectious diseases. It has been believed that the most effective way to dismantle a network is the removal of a few nodes with the largest number of links (hubs). However, it may be more effective to remove a combination of hubs and nodes with low degree centrality.

Morone and Makse (2015) then proposed an index called collective-influence defined by local topology in a network. They showed that the removal of nodes with high CI (known as *influencers*) is more effective in dismantling a network than removal of hubs. They also showed that the set of influencers include a lot of low degree nodes which do not seem to have important role for network robustness. They expressed this finding as “strength of weak nodes” in similar way as “strength of weak ties” (Granovetter, 1973).

Another important aspect for CI is related to its relatively small computational complexity. According to Kovács, and Barabási (2015), the computational complexity for CI can be reduced to $O(NlogN)$ because CI is defined by only local topology in a network. On the other hand, for instance, the computational complexity for betweenness centrality which is defined by global topology of a network is $O(NM)$ and $O(NM + N^2logN)$ for unweighted and weighted networks respectively when a network has N number of nodes and M number of links (Brandes, 2001). It has been mentioned that potential applications of CI include cybersecurity or disease control (Kovács, and Barabási, 2015). However, this study aims to show that CI also can be applied for an effective mitigation strategy against cascading failure.
The definition of collective-influence is described here. As shown in Fig. 3, a spherical subgraph of radius r around every node i is defined and the set of nodes belonging to the spherical surface of the subgraph is represented by $\partial Ball(i,r)$. The collective-influence of node i at the radius r is defined as follows,

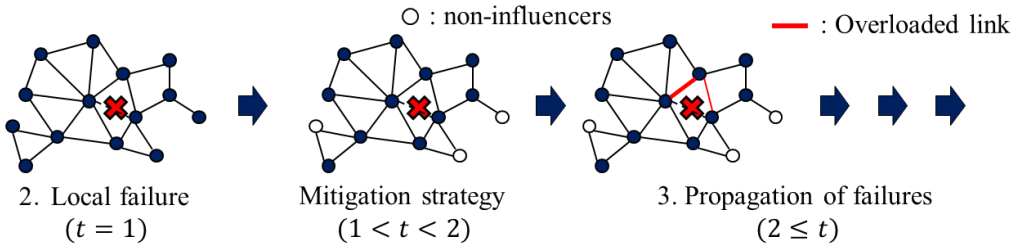


Figure 2. The timing of the mitigation strategy

$$CI_r(i) = (k_i - 1)\sum_{j \in \partial Ball(i,r)}(k_j - 1) \quad (9)$$

where,

$CI_r(i)$: collective-influence of node i at the radius r,
k_i : the number of links connected to the node i (degree of node i),
$\partial Ball(i, r)$: the set of nodes placed on the spherical surface of the subgraph.

When the radius r is zero, $CI_0(i)$ dependents on only the degree of node i, $CI_0(i) = (k_i - 1)^2$. In other words, $CI_0(i)$ substantially equals to degree centrality. The $CI_r(i)$ for $r \geq 1$ has richer topological features than $CI_0(i)$. Even if a node itself is one with small number of links, "weak node", the value of $CI_r(i)$ can be high and become an influencer when high degree nodes are included in the set $\partial Ball(i, r)$.

In this study, we propose a strategy which specifies the fraction $f[\%]$ of nodes with low collective-influence, *non-influencers*, and eliminates the flow generated from them intentionally right after a local failure in order to reduce the total amount of the network flow and prevent the propagation of failures of links by overloading. The process of the mitigation strategy is inserted between 2) local failure and 3) propagation of failures in the model as shown in Fig. 2. As a similar but different mitigation strategy, Motter (2004) proposed a strategy which specifies nodes with low betweenness centrality and intentionally *removes these nodes themselves* from the network. The removal of nodes brings more serious damage to the network than the elimination of the flow generated from specific nodes. It is because the removal of nodes eliminates not only 1) the flow generated from them in the same way as our strategy, but also 2) the flow concentrating to them, and 3) eliminates flow between other pairs of nodes if there is no path between them because of the removal of nodes. The strategy proposed by Motter (2004) identifies nodes with low betweenness centrality and removes them because it is conceivable that these nodes do not contribute global traffic. However, it is still not certain whether betweenness centrality is the best index for mitigation strategies. In this context, the numerical analysis in chapter 4 includes the comparison between collective-influence and betweenness centrality for identifying nodes to eliminate flow.

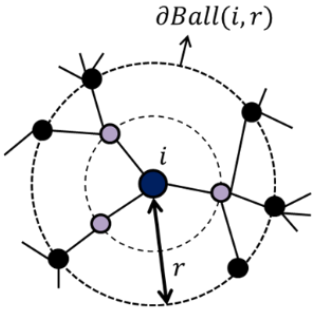


Figure 3. The spherical subgraph to define collective-influence of node i at the radius r

4. NUMERICAL ANALYSIS

In chapter 4, we focus on the influence of network topology on the vulnerability against cascading failure and we apply the model to both homogeneous and heterogeneous networks in section 4.1. In section 4.2, we also investigate the performance of the mitigation strategy for both types of networks. The results may give us some implications about the vulnerability of road networks which are classified into homogeneous networks and how we

should conduct risk management strategies to avoid serious consequences in road networks.

In order to investigate the vulnerability of networks with different topological features, we apply the model to random networks and scale-free networks as typical homogeneous and heterogeneous networks respectively. Figure 4 represents the difference between random and scale-free networks. Color and size of a node represent the degree of the node. Deeper colored and larger nodes have higher degree (the number of links). According to Barrat *et al*. (2008), a random network is a typical homogeneous network whose degree distribution almost follows Poisson distribution, $P(k) \approx e^{-\langle k \rangle} \langle k \rangle^k / k!$, where the degree distribution $P(k)$ is the probability that any randomly chosen node has degree k (the number of directly connected to the node is k). On the other hand, a scale-free network is a typical heterogeneous network whose degree distribution follows a power-low distribution, $P(k) \propto k^{-\gamma}$, where γ is a scale parameter. In this study, both networks are initially unweighted network and they have $N = 100$ nodes and average degree $\bar{k} \approx 4.0$. They are stochastically generated by Erdős–Rényi model (Erdős and Rényi, 1959) and Barabási-Albert model (Barabási and Albert, 1999) respectively. Networks with $N = 100$ nodes seem to be relatively small, however, as shown in section 4.1 and 4.2, these networks are large enough to show the difference of network vulnerability against cascading failure and the performance of the mitigation strategy.

In the numerical analysis, it is assumed that the node with the largest betweenness centrality fails in order to examine whether our strategy can work well under serious situations where networks are exposed to targeted attacks and require a mitigation strategy. The local failure on the node with the largest betweenness centrality is represented by setting the set E_0 in equation (4) consisting of all links directly connected to the node.

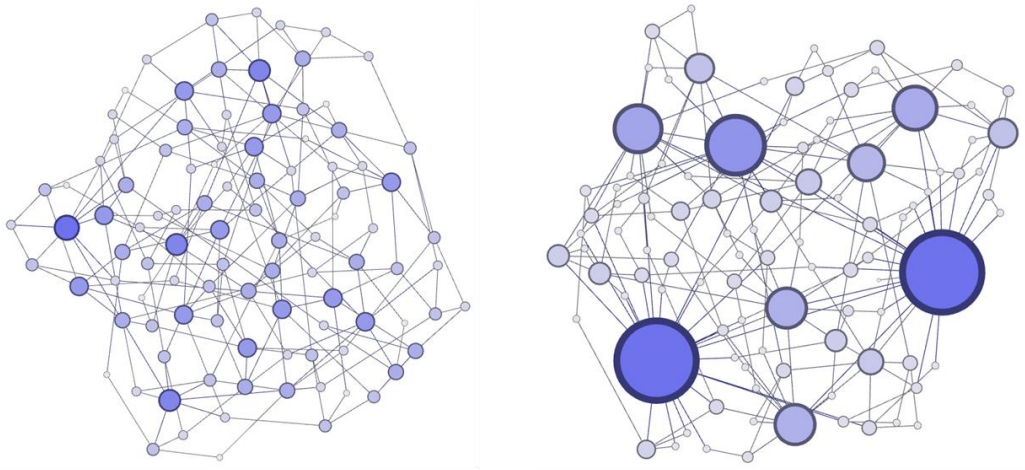


Figure 4. The difference between random and scale-free networks

4.1 The Network Vulnerability against Cascading Failure

Section 4.1 describes the network vulnerability against cascading failure. At the beginning, we show examples of the drop of the network efficiency $E(t)$ caused by cascading failure triggered by the breakdown of the node with highest betweenness centrality.

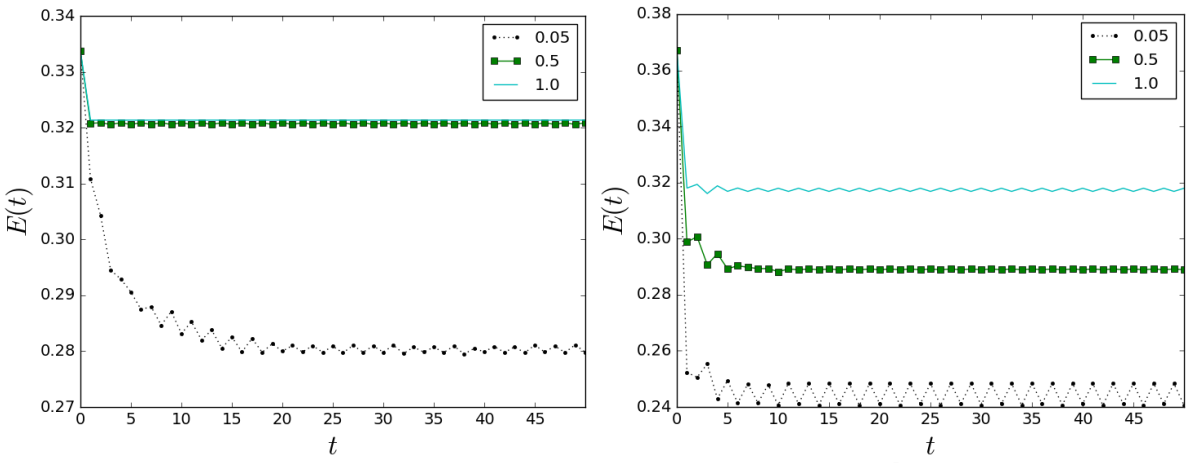
Fig. 5 (a) and (b) represent the decrease of the network efficiency $E(t)$ for random networks and scale-free networks respectively with different values of the tolerance parameter $\alpha = 0.05, 0.5, 1.0$. The horizontal axis represents the time step t and the vertical axis represents the network efficiency $E(t)$.

As you can see in Fig. 5 (a), in the case of random networks, the network efficiency $E(t)$ decreases about 3.59% (from 0.334 to 0.322) when the tolerance parameter $\alpha = 0.5, 1.0$. The influences by the local failure are absorbed into the system by handling the diverted traffic with sufficient practical capacity. However, when the tolerance parameter $\alpha = 0.05$, the network efficiency drops for about 15.6% (from 0.334 to 0.282). Similarly, Fig. 5 (b) represents the decrease of the network efficiency $E(t)$ in the case of scale-free networks. The network efficiency drops relatively large for all the three cases $\alpha = 0.05, 0.5, 1.0$ in comparison with the case of random networks. The network efficiency $E(t)$ decreases for about 12.4% (from 0.364 to 0.319), 20.3% (from 0.364 to 0.290), and 32.7% (from 0.364 to 0.245) for the three cases $\alpha = 0.05, 0.5, 1.0$ respectively.

The results shown in Fig. 5 represent the differences of the spreading of overload failures between random networks (homogeneous networks) and scale-free networks (heterogeneous networks). Not only the topological features but also the tolerance parameter α seems to affect strongly the network vulnerability against cascading failure for both two types of networks. The relationships between the tolerance parameter α and the damage caused by cascading failure are then investigated.

Fig. 6 shows the relationships between the tolerance parameter α and damage for random networks and scale-free networks. Let D represent damage in the ultimate state. In order to calculate the value of D, the network efficiency at 50 time step, $E(50)$, is used as the network efficiency at the ultimate state. The horizontal axis shows the tolerance parameter α from 0.0 to 4.0. The vertical axis shows the damage D. The red (square) and blue (circle) curves correspond to random and scale-free networks. Each curve corresponds to an average over 50 independent realizations. It means that we generated 50 networks for both kinds of networks. As the tolerance parameter α increases, the network robustness also increases. It means that the damage D decreases as the tolerance parameter α increases regardless of the types of networks. When the tolerance parameter α exceeds a certain value and links with sufficient practical capacity can handle diverted flow from failed nodes/links, any link does not fail by overloading and the damage D converges at a value which is caused not by propagation of failures but by the local failure itself.

As shown in Fig. 6, there are clear differences between both random networks and scale-free networks. When the tolerance parameter α is 0.0, the damage D for random networks is about 0.185. It means that about 18.5% of the initial network efficiency is lost



(a) (b)

Figure 5. The drop of network efficiency for (a) random and (b) scale-free networks with $\alpha = 0.05, 0.5, 1.0$

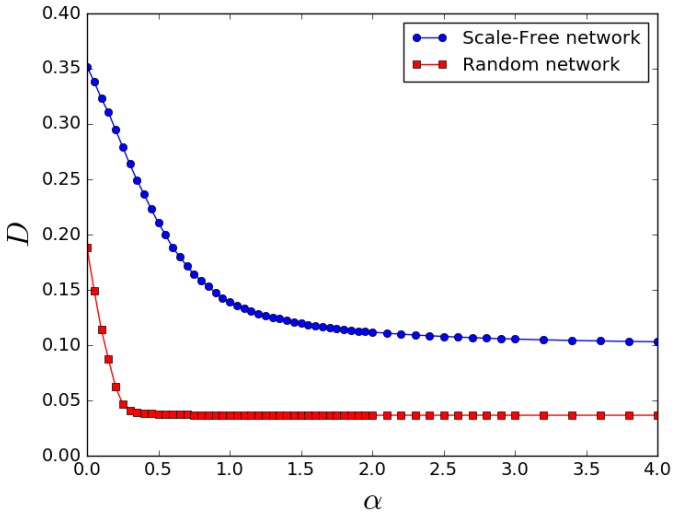


Figure 6. The relationships between the tolerance parameter α and the damage D

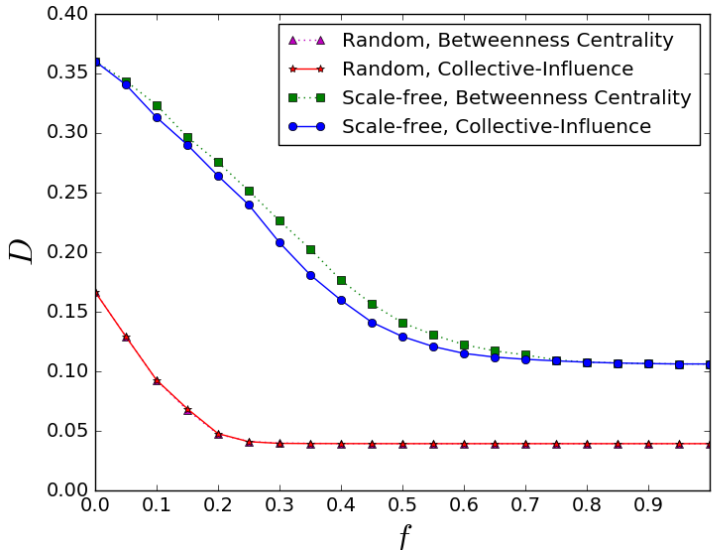
by cascading failure. On the other hand, in the case of scale-free networks, 35.1% of the initial network efficiency is lost. From these values in the case of $\alpha = 0.0$, both curves decrease and converge at certain values as the tolerance parameter α increases. However, there is a difference of the sharpness (kind of the speed of the convergence) of two curves. Although the curve of random networks converges at $D \approx 0.037$ when the tolerance parameter α exceeds about 0.75, another curve for scale-free networks converges much more gradually at $D \approx 0.10$. Even when the tolerance parameter $\alpha = 4.0$, the blue/circle curve still decreases and does not converge completely at a stationary value.

The results obtained in this section give us implications about the vulnerability of road networks which are classified into homogeneous networks. In a homogeneous network, overloading of links rarely propagate across the large parts of a network. Only in the case where the practical capacity is extremely small, overloading of links spread out and the damage becomes high. It means that increasing the practical capacity is more effective prevention strategy for homogeneous networks than for heterogeneous networks.

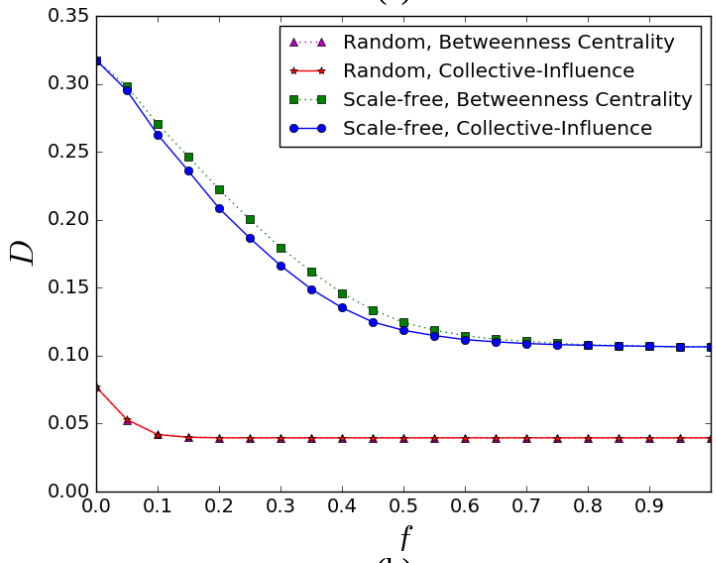
4.2 The Performance of the Mitigation Strategy

Section 4.2 describes the performance of the mitigation strategy. As shown in Fig. 6, when the tolerance parameter α is small, both networks become fragile and overloading of links easily propagate across the network. Under such conditions, a mitigation strategy is required to protect networks. Here the performance of the proposed mitigation strategy is examined as shown in Fig. 7.

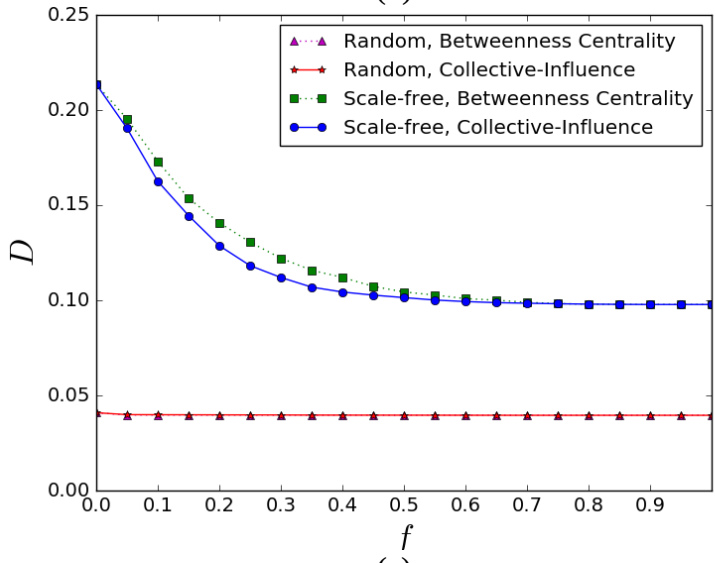
Fig. 7 shows the performance of the mitigation strategies for both random networks and scale-free networks with relatively small values of the tolerance parameter $\alpha = 0.05, 0.2, 0.5$ in Fig. 7 (a), (b), and (c) respectively. Solid curves represent the performance of the mitigation strategy proposed in this study which identifies nodes to eliminate flow by collective-influence (CI) and dotted curves represent the performance of a strategy which identifies nodes based on betweenness centrality in similar way as the existing strategy (Motter, 2004). Each curve corresponds to the average over 50 independent realizations. In the numerical analysis, the radius r of CI is set to be 2 (the effects of the radius r on mitigation performance is discussed in Appendix A). The horizontal axis shows the fraction f of nodes to eliminate flow and the vertical axis shows the damage D. The damage D of the fraction $f = 0.0$ represents the damage without any mitigation strategy. As the fraction f



(a)



(b)



(c)

Figure 7. The performance of the mitigation strategies for different values of the tolerance parameters α (a) 0.05, (b) 0.2, and (c) 0.5

increases, the total amount of the network flow decreases and damage diminishes as well. However, a smaller fraction f is more desirable for mitigating damage without unnecessary elimination of the network flow.

In Fig. 7 (a), the performance of mitigation strategies in the case of the tolerance parameter $\alpha = 0.05$ is illustrated. As you can see in Fig. 7 (a), scale-free networks require larger fraction f to mitigate damage in comparison with random networks. Also there is a clear difference between random networks and scale-free networks when we focus on solid and dotted curves. In the case of scale-free networks, our strategy represented by the solid curve performs better than the strategy using betweenness centrality for all the fraction f. Eliminating flow generated by non-influencers performs well to mitigate damage and protect the networks effectively. On the other hand, in the case of random networks, solid and dotted curves take almost the same values and the way of specifying nodes is not sensitive problem. These features are observed not only Fig. 7 (a) but also Fig. 7 (b) and (c).

These results give us following implications about effective mitigation strategies to avoid serious disruptions in road networks which are classified into homogeneous networks: 1) homogeneous networks require less amount of elimination of the network flow than heterogeneous networks and 2) the way of identification of nodes to eliminate flow is less sensitive problem for homogeneous networks.

5. CONCLUSIONS

There are two objectives in this study. Firstly, this study proposes a model for cascading failure where overloading of links propagate across the entire network triggered by a small shock/error in a local part of a network. Differently from the existing models in the context of disruptions in power grids or communication networks where nodes (power stations or routers) are successively overloaded, the model in this study aims to represent the propagation of overloading of links in the context of disruptions in road networks. In this model, the removal of a few nodes/links can be a trigger of large-scale propagation of the decrease of the efficiency of links. The damage caused by cascading failure is evaluated by the drop of the network efficiency.

Secondly, this study proposes a mitigation strategy against cascading failure. In most cases, influences of the local failures might be immediately absorbed into the system by handling the diverted flow from failed nodes/links on other links with sufficient practical capacity. However, under specific conditions where the network itself is fragile or the network is exposed to targeted attacks on important nodes/links, a mitigation strategy is required to protect the network. This paper then proposes a mitigation strategy which aims to reduce the total amount of the network flow, to prevent the propagation of failures of links by overloading, and to eventually mitigate damage. In order to reduce the total amount of the network flow effectively, our strategy identifies non-influencers based on an index called collective-influence and eliminates the flow generated from them. This index was originally proposed by Morone and Makse (2015) for identifying influencers to break up a network effectively and possible applications for cybersecurity or disease control have been pointed out by Kovács and Barabási (2015). However, this paper shows another possible application for an effective mitigation strategy against cascading failure.

In the numerical analysis, we apply the model to both random networks and scale-free networks as typical homogeneous and heterogeneous networks. In addition, we investigate the performance of the proposed mitigation strategy for both types of networks. The results give us implications for risk management of road networks which are classified into homogeneous

networks: 1) in most cases, large-scale cascading failure can be avoided by increasing practical capacity as a prevention strategy and 2) in a case of emergency where the practical capacity is extremely small, serious cascading failure can be avoided by eliminating flow generated from non-influencer nodes as a mitigation strategy. These implications can be applied to establish practical risk management for transportation networks including both prevention and mitigation strategies in the future.

ACKNOWLEDGEMENTS

This work was supported by JSPS KAKENHI Grant Numbers 6220906A and 25249070.

APPENDIX A. The Effect of the Radius on Mitigation Performance

In the appendix A, the effects of the radius r of collective-influence on mitigation performance is investigated. As represented by equation (9), the radius r has to be set to calculate collective-influence (CI), $CI_r(i)$. The radius r should be zero or more, but less than the diameter of the network. The diameter d_G is the maximum distance between pair of nodes among all the shortest distance of any pair of nodes, $d_G = \max_{i,j} l_{ij}$, where l_{ij} is the shortest distance between node i and node j. When the radius $r = 0$, $CI_0(i)$ substantially equals to degree centrality as mentioned in section 3.3. The radius $r > 0$ has richer topological features, but a too large radius reaches the boundary of the network and CI approaches zero. Fig. A. 1 shows the effects of the radius r on mitigation performance in the case of scale-free networks with the tolerance parameter $\alpha = 0.2$. In the same way as Fig. 7, the horizontal axis shows the fraction f of nodes to eliminate flow and the vertical axis represents the damage caused by cascading failure D. Each curve corresponds to the average over 50 independent realizations. Here the radius r is set from 0 to 5 because the average of the diameter of the networks about 5.48. As shown in Fig. A. 1, the mitigation performance is dependent on the radius r. In this case, the radius $r = 2$ performs the best to mitigate damage effectively. In contrast, when the radius approaches the diameter, $r = 4, 5$, the performance deteriorates. At this moment, the optimal radius r cannot be found without trial and error. Finding a firm criterion to choose an optimal radius r for maximizing damage mitigation will be desirable as future works.

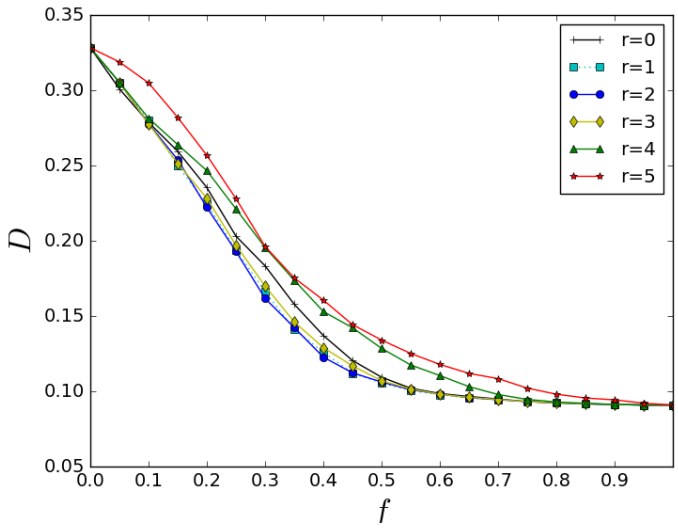


Figure A. 1. The effects of the radius r on mitigation performance

REFERENCES

Albert, R., Jeong, H., Barabási, A.-L. (2000) Error and attack tolerance of complex networks. *Nature* 406 (6794), 378-382.

Barabási, A.-L., Albert, R. (1999) Emergence of scaling in random networks. *Science* 286 (5439), 509-512.

Barrat, A, Barthelemy, M., Vespignani, A. (2008) *Dynamical processes on complex networks*. Cambridge University Press.

Brandes, U. (2001) A faster algorithm for betweenness centrality. *Journal of mathematical sociology* 25 (2) 163-177.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., Havlin, S. (2010) Catastrophic cascade of failures in interdependent networks. *Nature* 464 (7291), 1025-1028.

Crucitti, P., Latora, V., Marchiori, M. (2004) Model for cascading failures in complex networks. *Physical Review E* 69 (4), 045104.

Erdös, P, Rényi. A. (1959) On random graphs I. *Publicationes Mathematicae (Debrecen)* 6, 290-297.

Granovetter, M. S. (1973) The strength of weak ties. *American journal of sociology* 78, 1360-1380.

Holme, P., Kim, B. J., Yoon, C. N., Han, S. K. (2002) Attack vulnerability of complex networks. *Physical Review E* 66 (6), 065102.

Kovács, I. A., Barabási. A.-L. (2015) Network science: Destruction perfected. *Nature* 524 (7563), 38-39.

Latora, V., Marchiori, M. (2001) Efficient behavior of small-world networks. *Physical Review Letters* 87, 198701.

Mattsson, L.-G., Jenelius, E. (2015) Vulnerability and resilience of transport systems–A discussion of recent research. *Transportation Research Part A* 81, 16-34.

Morone, F., Makse, H. A. (2015) Influence maximization in complex networks through optimal percolation. *Nature* 524 (7563), 65-68.

Motter, A. E. (2004) Cascade control and defense in complex networks. *Physical Review Letters* 93 (9), 098701.

Motter, A. E., Lai, Y.-C. (2002) Cascade-based attacks on complex networks. *Physical eview E* 65 (5), 056109.

Simonsen, I., Buzna, L., Peters, K., Bornholdt, S., Helbing, D. (2008) Transient dynamics increasing network vulnerability to cascading failures. *Physical Review Letters* 100 (21), 218701.

Wu, J., Sun, H., Gao, Z. (2007) Cascading failures on weighted urban traffic equilibrium networks. *Physica A* 386 (1), 407-413.