Physica A 515 (2019) 324–331

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Bypass rewiring and extreme robustness of Eulerian networks

Junsang Park [a,*], Seungwon Shin [a], Sang Geun Hahn [b]

[a] School of Electrical Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

[b] Department of Mathematical Sciences, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

HIGHLIGHTS

- A concept of bypass rewiring on directed networks is proposed.
- Random bypass rewiring can guarantee extreme robustness of random networks.
- Bypass rewiring can make the percolation threshold 0.
- Bypass rewiring guarantees extreme robustness of Eulerian networks.
- Bypass rewiring can guarantee extreme robustness of the Internet topology.

ARTICLE INFO

Article history:
Received 18 December 2017
Received in revised form 15 September 2018
Available online xxxx

Keywords:
Networks
Random networks
Directed networks
Eulerian networks
Percolation
Robustness

ABSTRACT

A concept of bypass rewiring on directed networks is proposed, and random bypass rewiring on infinite directed random networks is analytically and numerically investigated with double generating function formalisms and simulations. As a result, it is derived that random bypass rewiring makes infinite directed (undirected) random networks extremely robust for arbitrary occupation probabilities if and only if in-degree of every node except a fixed number of nodes is equal to the out-degree (every node except a finite number of nodes has even degree); random bypass rewiring can make the percolation threshold 0 on infinite directed (undirected) random networks. From the results on infinite random networks, it is generalized that a finite network has a strongly connected spanning sub-network which has an Eulerian path or cycle if and only if there exists an way of bypass rewiring to make the finite network extremely robust for every combination of removed nodes; Eulerian networks are extremely robust with bypass rewiring for every combination of removed nodes. The generalized results say that bypass rewiring improves connectivity and robustness of not only infinite networks but also real-world networks, like the Internet, with a finite number of nodes.

1. Introduction

Many systems in real-world (the Internet, electric power grids, and others) can be represented by complex networks with many nodes (vertices) and links (edges) between nodes [1–3]. Complex networks are relatively robust to failures or errors (random removal of nodes) but fragile and vulnerable to intended attacks (targeted removal of nodes in decreasing order of degree from the highest degree); a network is fragmented into smaller components when nodes are deleted [4,5,1,2,6–12]. Even though there are various mitigation methods attempted to improve robustness of networks, they have technical,

* Corresponding author.
E-mail address: junsp85@kaist.ac.kr (J. Park).

https://doi.org/10.1016/j.physa.2018.09.073
0378-4371/

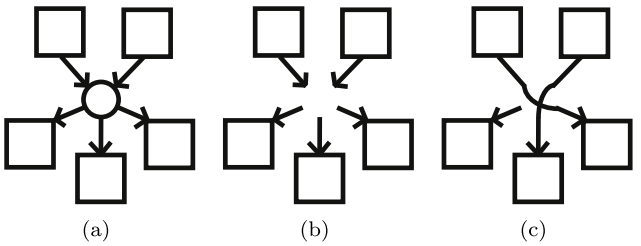

Fig. 1. (a) Before removal of the node, one node (circle) and five components (square) are connected. (b) After removal of the node, the network fragments into five smaller components without bypass rewiring. (c) After removal of the node, the network fragments into two larger connected components and one smaller out-component with bypass rewiring.

economic, or geographical problems and limitations when applied to real-world systems [13–17]. From the practical point of view, bypass rewiring is a technically, economically, and geographically realistic mitigation method against removal of nodes including failures and attacks because bypass-rewiring the links of a removed node under failures or attacks is easy and simple work; an engineer or equipment can easily and simply rewire cables (links) of a router (node) and repeat the signals directly when the router does not work under failures or attack or is under repair [18].

In this paper, we propose a concept of bypass rewiring on directed networks and give generalized results on not only infinite networks but also real-world networks with a finite number of nodes. In Section 2, a concept of bypass rewired is proposed. In Section 3, we derive analytical and simulation results of random bypass rewiring on infinite directed random networks with using double generating function formalisms. In Section 4, the results in Section 3 and [18] with a real-world example, the Internet topology, are discussed and generalized results on infinite random networks and finite networks are derived from the discussion. In Section 5, we summarize the paper and comment on further work.

2. A concept of bypass rewiring on directed networks

We propose a concept of bypass rewiring on directed networks. A node in Fig. 1(a) is removed by failures or attacks and turns into the removed nodes in Fig. 1(b). Bypass rewiring on a directed network is to directly connect each pair of in-links and out-links of the removed node like Fig. 1(c). Each pair of in-links and out-links for rewiring can be chosen in various ways including random bypass rewiring by which each pair of in-links and out-links of the removed nodes are randomly chosen. If in-degree k_{in} is larger (smaller) than out-degree k_{out} of the removed node, $k_{\text{in}} - k_{\text{out}}$ in-links ($k_{\text{out}} - k_{\text{in}}$ out-links) remain open.

3. Random bypass rewiring on infinite directed random networks

3.1. Analytical results

Using double generating functions based on the generating function formalism introduced in [5,19,8,12,20], we define

$$G_{0,0}(x,y) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} p_{j,k}x^j y^k, \tag{1}$$

$$H_{\text{in},1}(x) = \sum_{k=0}^{\infty} h_{\text{in},k}x^k, \tag{2a}$$

$$H_{\text{out},1}(x) = \sum_{k=0}^{\infty} h_{\text{out},k}x^k, \tag{2b}$$

for

$$\sum_{j=0}^{\infty}\sum_{k=0}^{\infty} jp_{j,k} = \sum_{j=0}^{\infty} jp_{\text{in},j} = \langle j\rangle = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} kp_{j,k} = \sum_{k=0}^{\infty} kp_{\text{out},k} = \langle k\rangle, \tag{3}$$

where $p_{j,k}$ is the probability that a randomly chosen node has in-degree j and out-degree k, and $h_{\text{in},k}$ ($h_{\text{out},k}$) is the probability that a randomly chosen link originates from (leads to) a small in-component (out-component) which has k nodes; Eq. (3) is naturally assumed since average in-degree $\langle j\rangle$ and average out-degree $\langle k\rangle$ are equal on directed networks. Since nodes of the giant strongly connected component do not belong to any small in- and out-component which has a fixed number of

nodes on an infinite directed random networks, the probability that a randomly chosen node belongs to the giant strongly connected component is

$$S_s = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} p_{j,k}\phi_{j,k}(1 - u_{\text{in}}^j - u_{\text{out}}^k + u_{\text{in}}^j u_{\text{out}}^k), \tag{4}$$

for

$$H_{\text{in},1}(x) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} \frac{(k+1)p_{j,k+1}}{\langle k\rangle}\{1 - \phi_{j,k+1} + \phi_{j,k+1}[H_{\text{in},1}(x)]^j\}, \tag{5a}$$

$$H_{\text{out},1}(x) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} \frac{(j+1)p_{j+1,k}}{\langle j\rangle}\{1 - \phi_{j+1,k} + \phi_{j+1,k}[H_{\text{out},1}(x)]^k\}. \tag{5b}$$

u_{in} (u_{out}) is the average probability that there exists no path from (to) the giant strongly connected component to (from) the node from (to) which a randomly chosen link originates (leads) where u_{in} and u_{out} are the smallest non-negative real solutions of

$$u_{\text{in}} = H_{\text{in},1}(1) = f_1(u_{\text{in}}) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} \frac{kp_{j,k}(1 - \phi_{j,k} + \phi_{j,k}u_{\text{in}}^j)}{\langle k\rangle}, \tag{6a}$$

$$u_{\text{out}} = H_{\text{out},1}(1) = f_2(u_{\text{out}}) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} \frac{jp_{j,k}(1 - \phi_{j,k} + \phi_{j,k}u_{\text{out}}^k)}{\langle j\rangle}, \tag{6b}$$

respectively, and $\phi_{j,k}$ is the occupation probability that a randomly chosen node with in-degree j and out-degree k is not removed; the average occupation probability is defined as

$$\phi = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} p_{j,k}\phi_{j,k}. \tag{7}$$

From now on, we formulate the equations corresponding to Eqs. (5a), (5b), (6a), and (6b) with considering random bypass rewiring. Based on the idea seen in Fig. 2 which illustrates random bypass rewiring on an infinite directed random network,

$$H_{\text{in},1}(x) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} \frac{kp_{j,k}}{\langle k\rangle}\left\{\phi_{j,k}[H_{\text{in},1}(x)]^j + (1 - \phi_{j,k})\left[\min(\frac{j}{k}, 1)H_{\text{in},1}(x) + \max(0, \frac{k-j}{k})\right]\right\}, \tag{8a}$$

$$H_{\text{out},1}(x) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} \frac{jp_{j,k}}{\langle j\rangle}\left\{\phi_{j,k}[H_{\text{out},1}(x)]^k + (1 - \phi_{j,k})\left[\min(\frac{k}{j}, 1)H_{\text{out},1}(x) + \max(0, \frac{j-k}{j})\right]\right\}, \tag{8b}$$

$$u_{\text{in}} = H_{\text{in},1}(1) = f_3(u_{\text{in}}) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} \frac{kp_{j,k}}{\langle k\rangle}\left\{\phi_{j,k}u_{\text{in}}^j + (1 - \phi_{j,k})\left[\min(\frac{j}{k}, 1)u_{\text{in}} + \max(0, \frac{k-j}{k})\right]\right\}, \tag{9a}$$

$$u_{\text{out}} = H_{\text{out},1}(1) = f_4(u_{\text{out}}) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} \frac{jp_{j,k}}{\langle j\rangle}\left\{\phi_{j,k}u_{\text{out}}^k + (1 - \phi_{j,k})\left[\min(\frac{k}{j}, 1)u_{\text{out}} + \max(0, \frac{j-k}{j})\right]\right\}, \tag{9b}$$

are derived.

In the case of undirected networks, the average probability that a randomly chosen link is not connected to the giant component is

$$u = \sum_{k=0}^{\infty} q_k\phi_{k+1}u^k + u\sum_{k=0}^{\infty} q_k(1 - \phi_{k+1}) + (1-u)\sum_{k=0}^{\infty} \frac{p_{2k+1}(1 - \phi_{2k+1})}{\sum_{k'=1}^{\infty} k'p_{k'}}, \tag{10}$$

for $q_k = (k+1)p_k/\sum_{k=0}^{\infty} kp_k$ [18].

The self-consistent equations like Eqs. (6a), (6b), (9a), and (9b) can be solved as follows by the fixed-point iteration [21]. Iterating

$$u_{\text{in},i+1} = f_1(u_{\text{in},i}), \tag{11a}$$

$$u_{\text{out},i+1} = f_2(u_{\text{out},i}), \tag{11b}$$

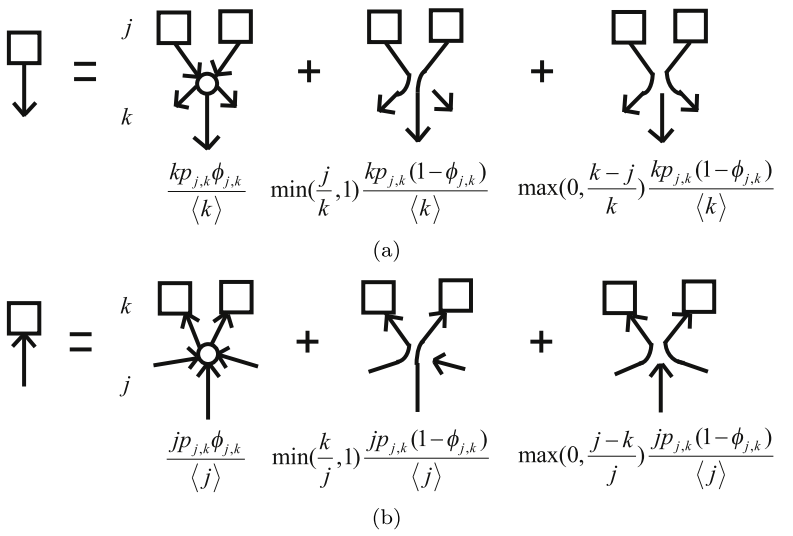

Fig. 2. (a) A schematic diagram to calculate the probability that a randomly chosen in-link originates from a small in-component [square] with random bypass rewiring under removal of a node [circle]. (b) A schematic diagram to calculate the probability that a randomly chosen out-link leads to a small out-component [square] with random bypass rewiring under removal of a node [circle].

$$v_{\text{in},i+1} = f_3(v_{\text{in},i}), \tag{12a}$$
$$v_{\text{out},i+1} = f_4(v_{\text{out},i}), \tag{12b}$$

for $u_{\text{in},0} = u_{\text{out},0} = v_{\text{in},0} = v_{\text{out},0} = 0$, $u_{\text{in},i}$, $u_{\text{out},i}$, $v_{\text{in},i}$, and $v_{\text{out},i}$ approaches to $\bar{u}_{\text{in}}$, $\bar{u}_{\text{out}}$, $\bar{v}_{\text{in}}$, and $\bar{v}_{\text{out}}$, respectively, as i goes to infinity, for

$$\bar{u}_{\text{in}} = f_1(\bar{u}_{\text{in}}), \tag{13a}$$
$$\bar{u}_{\text{out}} = f_2(\bar{u}_{\text{out}}), \tag{13b}$$

$$\bar{v}_{\text{in}} = f_3(\bar{v}_{\text{in}}), \tag{14a}$$
$$\bar{v}_{\text{out}} = f_4(\bar{v}_{\text{out}}). \tag{14b}$$

Since

$$f_1(u_{\text{in}}) \geq f_3(u_{\text{in}}), \tag{15a}$$
$$f_2(u_{\text{out}}) \geq f_4(u_{\text{out}}), \tag{15b}$$

hold from $u_{\text{in}} \min(\frac{j}{k}, 1) + \max(0, \frac{k-j}{k}) \leq 1$ and $u_{\text{out}} \min(\frac{k}{j}, 1) + \max(0, \frac{j-k}{j}) \leq 1$ for $j, k \geq 0$ and $0 \leq u_{\text{in}}, u_{\text{out}} \leq 1$,

$$u_{\text{in},i} \geq v_{\text{in},i}, \tag{16a}$$
$$u_{\text{out},i} \geq v_{\text{out},i}, \tag{16b}$$

are derived for all i from Eqs. (11a), (11b), (12a), and (12b). Therefore, S_s on an infinite directed random network with random bypass rewiring is always equal to or larger than without random bypass rewiring; the percolation threshold on an infinite directed random network with random bypass rewiring is always equal to or smaller than without random bypass rewiring.

For even degree infinite undirected random networks; that is,

$$p_{2k+1} = 0, \tag{17}$$

the probability that a randomly chosen node belongs to the giant component is

$$S = \sum_{k=0}^{\infty} p_k \phi_k (1 - u^k) = \sum_{k=0}^{\infty} p_k \phi_k = \phi, \tag{18}$$

since Eq. (10) is reduced to

$$u = \sum_{k=0}^{\infty} q_k \phi_{k+1} u^k + u \sum_{k=0}^{\infty} q_k (1 - \phi_{k+1}), \tag{19}$$

and $u = 0$ is the smallest non-negative real solutions of Eq. (19) [18]. Similarly, if every node, except a fixed number of nodes, on infinite directed random networks has in-degree equal to the out-degree; that is,

$$p_{j,k} = 0 \text{ for } j \neq k, \tag{20}$$

holds, Eqs. (9a) and (9b) are reduced to

$$u_{\text{in}} = \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \frac{k p_{j,k}}{\langle k \rangle} \left[\phi_{j,k} u_{\text{in}}^j + (1 - \phi_{j,k}) u_{\text{in}} \right], \tag{21a}$$

$$u_{\text{out}} = \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \frac{j p_{j,k}}{\langle j \rangle} \left[\phi_{j,k} u_{\text{out}}^k + (1 - \phi_{j,k}) u_{\text{out}} \right]. \tag{21b}$$

Therefore, the smallest non-negative real solutions of Eqs. (21a) and (21b) are $u_{\text{in}} = u_{\text{out}} = 0$ for which Eq. (4) corresponds to

$$S_s = \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} p_{j,k} \phi_{j,k} = \phi, \tag{22}$$

from Eq. (7). Therefore, S_s is equal to ϕ, and the percolation threshold is 0 on an infinite directed random network with random bypass rewiring for Eq. (20); that is, infinite directed random networks are extremely robust with random bypass rewiring for arbitrary $\phi_{j,k}$ where Eq. (20) holds.

3.2. Simulation results

To simulate attacks, a node with the highest product of in-degree and out-degree is firstly removed and nodes are removed one by one in decreasing order of the product of in-degree and out-degree while randomly chosen nodes are removed one by one in the case of failures ($\phi_{j,k} = \phi$). For a numerical simulation of attacks for Eqs. (6a), (6b), (9a), and (9b),

$$\phi_{j,k} = \begin{cases} 1, & \sum\limits_{\{j'k' \leq jk\}} p_{j',k'} < \phi \\ \frac{\phi - \sum_{\{j'k' \leq jk-1\}} p_{j',k'}}{\sum_{\{j'k' = jk\}} p_{j',k'}}, & \sum\limits_{\{j'k' \leq jk-1\}} p_{j',k'} < \phi \text{ and } \sum\limits_{\{j'k' \leq jk\}} p_{j',k'} \geq \phi \\ 0, & \text{otherwise} \end{cases} \tag{23}$$

is set for given average occupation probability ϕ. In the simulations, in-degree and out-degree of each node is not recalculated while nodes are removed. To simulate random bypass rewiring, each pair of in-links and out-links of the removed node are randomly chosen and rewired until there is no pair to match.

The directed network for Fig. 3(b) is randomly generated by in-degree distribution $p'_{\text{in},j} = p_{\text{in},j}$, out-degree $p'_{\text{out},k} = p_{\text{out},k}$, and degree distribution $p'_{j,k} = 0$ for $j \neq k$ where $p_{\text{in},j}$ and $p_{\text{out},k}$ are the in-degree distribution and the out-degree distribution of the original directed network for Fig. 3(a), respectively. In other words, the directed network for Fig. 3(b) has a perfect positive correlation between in-degree and out-degree while the original directed network for Fig. 3(a) has an almost uncorrelated relationship between in-degree and out-degree.

Fig. 3(b) shows that almost all nodes except the removed nodes on the directed network are strongly connected by random bypass rewiring. The percolation threshold with random bypass rewiring in Fig. 3(b) is close to 0, while the percolation threshold in Fig. 3(a) is not.

Without random bypass rewiring, the original directed network for Fig. 3(a) is more robust than the directed network for Fig. 3(b) under attacks while it is not under failures, even though the directed network for Fig. 3(b) is randomly generated by the same in-degree distribution and out-degree distribution of the original directed network for Fig. 3(a). On the other hand, with random bypass rewiring, the directed network for Fig. 3(b) is more robust than the original directed network for Fig. 3(a) against removal of nodes including failures and attacks. In other words, the directed network for Fig. 3(b) is more robust than the original directed network for Fig. 3(a) with random bypass rewiring, while the original directed networks for Fig. 3(a) is more robust than the directed network for Fig. 3(b) under attacks without random bypass rewiring.

4. Discussion

4.1. Generalized results on infinite random networks

From Eq. (18) [Eq. (22)], S [S_s] is equal to ϕ for Eq. (17) [Eq. (20)] on an infinite undirected [directed] random network. S [S_s] is always smaller than ϕ with random bypass rewiring if Eq. (17) [Eq. (20)] does not hold on an infinite undirected

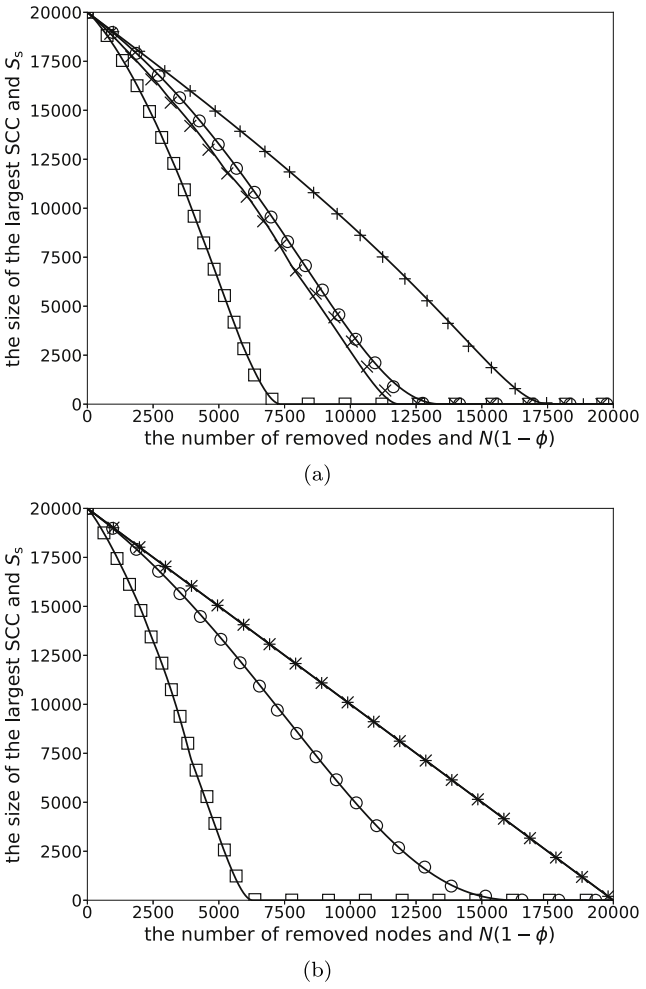

Fig. 3. The size of the largest SCC (strongly connected component) with respect to the number of removed nodes under failures [circles (plus signs)] and attacks [squares (crosses)] without (with) random bypass rewiring. The solid lines are for numerically calculated S_s with respect to $N(1-\phi)$ from Eqs. (4), (6a), (6b), (9a), and (9b) on an infinite directed random network with the same degree distribution. (a) On the directed network randomly generated by the configuration model with in-degree distribution $p_{\text{in},j} \sim j^{-3}$, out-degree distribution $p_{\text{out},k} \sim k^{-3}$, $N = 20000$ nodes, and $M = 61438$ links where j and k are almost uncorrelated. (b) On the directed network randomly generated by the configuration model with in-degree distribution $p'_{\text{in},j} = p_{\text{in},j}$, out-degree distribution $p'_{\text{out},k} = p_{\text{out},k}$, $N = 20000$ nodes, and $M = 61438$ links where each node has in-degree equal to the out-degree ($p'_{j,k} = 0$ for $j \neq k$). Two diagonal lines in (b) overlap.

[directed] random network. Therefore, S [S_s] is equal to ϕ with random bypass rewiring if and only if Eq. (17) [Eq. (20)] holds on an infinite undirected [directed] random network; that is, an infinite undirected [directed] random network is extremely robust with random bypass rewiring if and only if Eq. (17) [Eq. (20)] holds.

4.2. Generalized results on finite networks

From Eqs. (17) and (20), we recall a necessary condition for the existence of Eulerian cycles on a finite network [22]. In the case of finite networks, Eq. (17) [Eq. (20)] is interpreted that an undirected [directed] network has no node with odd degree [different in-degree and out-degree].

From the interpretation of Eqs. (17) and (20), we hypothesized that a finite network has a strongly connected spanning subnetwork which has an Eulerian path or cycle if and only if there exists an way of bypass rewiring to strongly connect all nodes except the removed nodes on the finite network for every combination of removed nodes. The hypothesis is proved as follows.

We prove that a finite network has a strongly connected subnetwork which has an Eulerian path or cycle if there exists an way of bypass rewiring to strongly connect all nodes except the removed nodes on the finite network for every combination of removed nodes. Suppose there exists an way of bypass rewiring to strongly connect all nodes except the removed nodes on a finite network for every combination of removed nodes. Then, there exists a set of bypass-rewired links which strongly

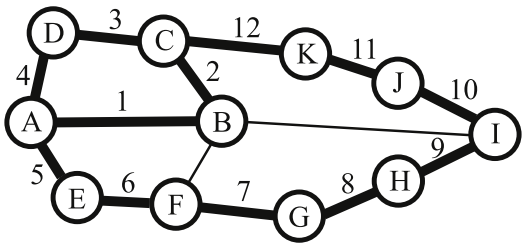

Fig. 4. Compuserve topology, a part of the Internet topology, in U.S. on Jan 2011, publicly available in [23]. The spanning subnetwork with the bold links has an Eulerian path with $L = 12$ links. Each number of the bold links denotes the sequential order of the Eulerian path.

connect all nodes except the removed nodes on the finite network for every combination of removed nodes. In other words, the finite network has a strongly connected spanning subnetwork which is composed of the bypass-rewired links and all nodes on the network. Since each bypass-rewired link (in-link) of a node on the strongly connected spanning subnetwork is paired with another bypass-rewired link (a bypass-rewired out-link) of the node, the number of the bypass-rewired links (in-links) of every node is even (is equal to the number of the bypass-rewired out-links). Therefore, the strongly connected spanning subnetwork with the bypass-rewired links has an Eulerian path or cycle.

We prove that there exists an way of bypass rewiring to strongly connect all nodes except the removed nodes on a finite network for every combination of removed nodes if the finite network has a strongly connected spanning subnetwork which has an Eulerian path or cycle. Suppose that a finite network has a strongly connected spanning subnetwork which has an Eulerian path or cycle. Then, the degree (in-degree) of every node, except the starting and ending node of the Eulerian path, on a strongly connected spanning subnetwork which has an Eulerian path or cycle is even (is equal to the out-degree). Since a half of the links (all in-links) of a node on the Eulerian path or cycle always match another half of the links (all out-links) of the node, each link (in-link) of a node on the Eulerian path or cycle can be bypass-rewired to the next sequenced link (out-link), which is a link (an in-link) of the next sequenced node, of the Eulerian path or cycle which has sequentially ordered links. Therefore, there exists at least one way of bypass rewiring to connect all nodes except the removed nodes on the finite network for every combination of removed nodes. For example, the ith link of an Eulerian path or cycle with L links can be bypass-rewired to the $(i + 1)$th link of the Eulerian path or cycle for $1 \leq i < L$ (and the Lth link of the Eulerian cycle can be bypass-rewired to the 1st link of the Eulerian cycle since the starting and ending node of an Eulerian cycle are same), as seen in Fig. 4.

In consequence, it is derived that a finite network has a strongly connected spanning subnetwork which has an Eulerian path or cycle if and only if there exists an way of bypass rewiring to make the finite network extremely robust for every combination of removed nodes; it is naturally satisfied that Eulerian networks are extremely robust with bypass rewiring for every combination of removed nodes.

Even though an way of bypass rewiring based on the sequentially ordered links of a strongly connected spanning subnetwork which has an Eulerian path or cycle is enough to strongly connect all nodes on the network, not yet rewired links of each node can be additionally bypass-rewired to improve connectivity. For example, link F–B and link B–I of node B in Fig. 4 can be additionally bypass-rewired to improve connectivity.

4.3. A real-world example: the Internet topology

From the consequence derived in Section 4.2, the network in Fig. 4 is extremely robust with bypass rewiring for every combination of removed nodes since the network has a spanning subnetwork which has an Eulerian path (A–B–C–D–E–F–G–H–I–J–K–C). To connect all nodes except the broken nodes on the network in Fig. 4 for every combination of removed nodes, the bypass rewiring policy is defined as follows, based on the sequentially ordered links of the Eulerian path of the spanning subnetwork. When node B is broken, the 1st link (link A–B) should be bypass-rewired to the 2nd link (link B–C) and link F–B can be additionally bypass rewired to link B–I. When node C is broken, the 2nd link (link B–C) should be bypass-rewired to the 3rd link (link C–D). When node D is broken, the 3rd link (link C–D) should be bypass-rewired to the 4th link (link D–A). When node A is broken, the 4th link (link D–A) should be bypass-rewired to the 5th link (link A–E). When node E is broken, the 5th link (link A–E) should be bypass-rewired to the 6th link (link E–F). When node F is broken, the 6th link (link E–F) should be bypass-rewired to the 7th link (link F–G). When node G is broken, the 7th link (link F–G) should be bypass-rewired to the 8th link (link G–H). When node H is broken, the 8th link (link G–H) should be bypass-rewired to the 9th link (link H–I). When node I is broken, the 9th link (link H–I) should be bypass-rewired to the 10th link (link I–J). When node J is broken, the 10th link (link I–J) should be bypass-rewired to the 11th link (link J–K). When node K is broken, the 11th link (link J–K) should be bypass-rewired to 12th link (link K–C).

The network in Fig. 4 can be fragmented into two parts, a part (node A, B, C, D, E, and F) and another part (node H, I, and J), when node G and K are broken under failures or attacks or are under repair. According to the bypass rewiring policy defined above, link F–G would be bypass-rewired to link G–H, link J–K would be bypass-rewired to link K–C, and then all nodes except the broken node (node G and K) on the network can be connected.

5. Conclusions

In summary, we have introduced a concept of bypass rewiring on directed networks and conducted analytical and numerical investigations of random bypass rewiring with double generating function formalisms and simulations. The results have shown that random bypass rewiring improves robustness of infinite directed (undirected) random networks under removal of nodes including failures and attacks. In particular, random bypass rewiring makes infinite directed (undirected) random networks extremely robust for arbitrary occupation probabilities if and only if in-degree of every node except a fixed number of nodes is equal to the out-degree (every node except a finite number of nodes has even degree); random bypass rewiring can make the percolation threshold 0 on infinite directed (undirected) random networks. From the results on infinite random networks, we have generalized that a finite network has a strongly connected spanning subnetwork which has an Eulerian path or cycle if and only if there exists an way of bypass rewiring to guarantee extreme robustness of the finite network for every combination of removed nodes; Eulerian networks are extremely robust with bypass rewiring for every combination of removed nodes. If the Internet topology has a spanning subnetwork which has an Eulerian path or cycle like Compuserve topology in Fig. 4, the Internet can be extremely robust against breakdown of routers (nodes) since links of a broken router on the Internet can be bypass-rewired by an engineer or equipment. Therefore, it is suggested that bypass rewiring equipment and routers be implemented and deployed on the Internet. In addition, variations on bypass rewiring theory including optimal bypass rewiring algorithms and more applications to many fields like electric circuits and power grids are expected.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP), Korea grant funded by the Korea government (MSIP) (No. 2016-0-00078, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning).

References

[1] R. Cohen, K. Erez, D. ben Avraham, S. Havlin, Phys. Rev. Lett. 85 (2000) 4626.
[2] R. Cohen, K. Erez, D. ben Avraham, S. Havlin, Phys. Rev. Lett. 86 (2001) 3682.
[3] R. Albert, I. Albert, G.L. Nakarado, Phys. Rev. E 69 (2004) 025103(R).
[4] R. Albert, H. Jeong, A.-L. Barabasi, Nature 406 (2000) 378.
[5] D.S. Callaway, M.E.J. Newman, S.H. Strogatz, D.J. Watts, Phys. Rev. Lett. 85 (2000) 5468.
[6] R. Albert, A.-L. Barabási, Rev. Modern Phys. 74 (2002) 47.
[7] S.N. Dorogovtsev, J.F.F. Mendes, Adv. Phys. 51 (2002) 1079.
[8] N. Schwartz, R. Cohen, D. ben Avraham, A.-L. Barabási, S. Havlin, Phys. Rev. E 66 (2002) 015104(R).
[9] M.E.J. Newman, SIAM Rev. 45 (2003) 167.
[10] S. Boccaletti, V. Latora, M.C. Y. Moreno, D.-U. Hwang, Phys. Rep. 424 (2006) 175.
[11] S.N. Dorogovtsev, A.V. Goltsev, J.F.F. Mendes, Rev. Modern Phys. 80 (2008) 1275.
[12] M.E.J. Newman, Networks: An Introduction, Oxford University Press, Oxford, 2010.
[13] A. Beygelzimer, G. Grinstein, R. Linsker, I. Rish, Physica A 357 (2005) 593.
[14] S. Xiao, G. Xiao, T.H. Cheng, S. Ma, X. Fu, H. Soh, Europhys. Lett. 89 (2010) 38002.
[15] C.M. Schneider, A.A. Moreira, J.S. Andrade, S. Havlin, H.J. Herrmann, Proc. Natl. Acad. Sci. USA 108 (2011) 3838.
[16] W. Quattrociocchi, G. Caldarelli, A. Scala, PLoS ONE 9 (2014) e87986.
[17] Y. Shang, Phys. Rev. E 91 (2015) 042804.
[18] J. Park, S.G. Hahn, Phys. Rev. E 94 (2016) 022310.
[19] M.E.J. Newman, S.H. Strogatz, D.J. Watts, Phys. Rev. E 64 (2001) 026118.
[20] H.S. Wilf, Generatingfunctionology, second ed., Academic Press, London, 1994.
[21] R.L. Burden, J.D. Faires, Numerical Analysis, ninth ed., Brooks/Cole, Boston, MA, 2011.
[22] B. Bollobás, Modern Graph Theory, Springer-Verlag, New York, 1998.
[23] The internet topology zoo, http://www.topology-zoo.org.