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/© 2018 Published by Elsevier B.V.

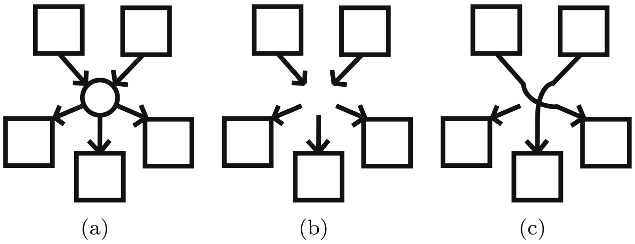

Fig. 1. (a) Before removal of the node, one node (circle) and five components (square) are connected. (b) After removal of the node, the network fragments into five smaller components without bypass rewiring. (c) After removal of the node, the network fragments into two larger connected components and 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, $k_{\mathrm{in}} - k_{\mathrm{out}}$ in-links ($k_{\mathrm{out}} - k_{\mathrm{in}}$ 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

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

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

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

for

$$\sum_{j=0}^{\infty}\sum_{k=0}^{\infty} j p_{j,k} = \sum_{j=0}^{\infty} j p_{\mathrm{in},j} = \langle j \rangle = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} k p_{j,k} = \sum_{k=0}^{\infty} k p_{\mathrm{out},k} = \langle k \rangle, \tag{3}$$

where $p_{j,k}$ is the probability that a randomly chosen node has in-degree j and out-degree k, and $h_{\mathrm{in},k}$ ($h_{\mathrm{out},k}$) 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