Physica A 506 (2018) 451–461

Contents lists available at ScienceDirect

Physica A

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

Abnormal phenomenon in robustness of complex networks with heterogeneous node functions

Jiajing Wu [a,b,*], Wei You [a,b], Taocheng Wu [c], Yongxiang Xia [d]

[a] *School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, China*
[b] *National Engineering Research Center of Digital Life, Sun Yat-sen University, Guangzhou 510006, China*
[c] *School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China*
[d] *College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China*

HIGHLIGHTS

- We consider the process of cascading failure in complex networks with heterogeneous node functions.
- We observe that the increase of some nodes' capacity sometimes results in the decline of the whole network's robustness.
- We find that this abnormal phenomenon is related to a particular structure in scale-free networks.

ARTICLE INFO

Article history:
Received 11 February 2018
Received in revised form 8 April 2018
Available online 24 April 2018

Keywords:
Complex network
Heterogeneous node functions
Cascading failures
Robustness

ABSTRACT

Cascading failure occurring on complex networks has received increasing research attentions in the past decades. In most current studies, a basic assumption is that each node in the network serves the same function and shares the same capacity redundancy. However, many real networked systems may have heterogeneous node functions. In this paper, we consider a data-transmission network which contains two types of nodes: routers and hosts, and study how the capacity redundancy of different nodes affects network robustness. It is well acknowledged that more capacity redundancy usually leads to better network robustness. However, we observe a counter-intuitive phenomenon that the increase of some nodes' capacity redundancy sometimes results in the decline of the whole network's robustness. Next, we try to explain this paradox of capacity redundancy by analyzing the process of cascading failure on a small-size scale-free network, and find that this abnormal phenomenon is related to a particular structure in both theoretical and realistic scale-free networks. Our results advance understanding of the robustness for networks with heterogeneous node functions.

1. Introduction

Cascade of failures is a ubiquitous phenomenon in many real-world networked systems, such as transportation networks, power grids, the Internet, and so forth [1]. In many networked systems, the cascading failure process usually begins with the failure of a single node or a small fraction of the network caused by intentional attacks or random failures. Take the data communication network as an example, if some nodes in the network fail, the data packets which pass these failed nodes

[*] Corresponding author at: School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, China.
E-mail address: wujiajing@mail.sysu.edu.cn (J. Wu).

https://doi.org/10.1016/j.physa.2018.04.090
0378-4371/© 2018 Elsevier B.V. All rights reserved.

will be redistributed to other nodes. This redistribution may trigger a larger scale of overloaded nodes at the same time, causing catastrophic effects on the network.

The past decade has seen increasing interests in the exploitation of the cascading failure phenomenon from the perspective of complex networks. Existing studies on cascading failure mainly focus on cascading models [2–5], network structure [6–13], defense strategies [14–17], attack types [18–20] and so on.

In terms of the cascading models, Motter et al. [2] proposed a simple global load-based cascading model, where the load of each node is estimated by the node betweenness and the node capacity is set proportional to its initial load. After that, a model based on a dynamical traffic load redistribution was proposed by Crucitti et al. [3]. In 2008, Wang et al. [4] proposed a cascading model based on a local load redistribution principle. Moreover, a cascading model with a local flow redistribution mechanism on weighted networks was proposed in [5].

Much prior work has been devoted to the investigation of the relationship between network robustness and the underlying network structure. Some pioneering researchers discussed cascading failures on various network models, such as random graphs, scale-free networks, and small-world networks [6,7]. Recently, studies on cascading failures have been extended to coupled network models, such as interconnected networks [8,21], interdependent networks [9–11], and cyber–physical systems [12,13].

For defense strategies, an effective method to mitigate the propagation of failures was proposed in [14] by intentional removals of some network components after the initial attacks. Moreover, Wang et al. [15] proposed a load-based resource allocation method to improve network robustness. Recently, Jiang et al. proposed a novel spare capacity-based load redistribution mechanism to make the networks more robust against cascading failures [16], and developed a greedy method to find the set of key nodes which can trigger subsequent failures [17].

Attack types, which determine the initial failures which triggers the process of cascading failures, is also a non-negligible factor in the study of cascading failure. Albert et al. [18] revealed that the scale-free networks are quite robust to failures occurring on random network components but extremely fragile to intentional attacks on hub nodes. However, the random graphs are relatively robust to both random failures and intentional attacks. This is called the robust-yet-fragile property of the scale-free networks. Later in [19], the scale-free networks are found to be more vulnerable to the removal of the edges with low traffic loads than that with high traffic loads. More recently, Tan et al. [20] found that the robust-yet-fragile property also exists in interdependent networks under random failures or intentional attacks.

In many infrastructure networks, each node can only handle limited loads and the maximal load a node can handle is defined as the capacity of this node. To ensure the normal network operation, there is usually some redundancy between each node's capacity and its actual load. For simplicity, most previous studies assume that each node serves the same function and shares the same capacity redundancy. However, many infrastructure networked systems do not work under this assumption and the networks may contain different types of nodes which serve different functions [22]. In most real-world applications, different types of nodes are usually designed with different capacities [23]. This fact makes the networks more complicated and may lead to some important features which distinguish such networks from the networks with solo-type of nodes.

In this paper, we consider a generic data-transmission network model which contains two types of nodes: routers and hosts, and study the robustness of the system under such a more realistic assumption. Moreover, we try to explore how the capacity redundancy of different nodes and the ratio of host number to router number affect network robustness, we find a counter-intuitive phenomenon that the increase of capacity redundancy may cause more severe cascading failure of the system. Moreover, this abnormal phenomenon is also found in realistic Internet Autonomous System-level networks.

2. Model

Unlike much of the previous work which assumes that all nodes in the network serve the same function, in this paper, we consider a generic type of networks which consist of two basic kinds of nodes: hosts and routers. This two kinds of nodes serve different functions in data transmission process. Routers can only store and forward packets as transfer stations; Hosts can not only work as routers to relay packets, but also generate and receive packets.

In this work, we consider the process of data transmission in discrete time steps. For each time step, new packets are generated in the network with randomly chosen source and destination nodes and transmitted along the shortest path towards their destinations. Meanwhile, the nodes receives packets from their neighbors and store the new generated or received packets in their buffers according to the first-in-first-out principle. Moreover, the packets that have successfully reached their destinations will be released from the network immediately.

To estimate the traffic load $L(i)$ of each node i, we calculate the total number of paths that passing through it [24], i.e.,

$$L(i) = \sum_{\substack{u,w \in V_{\text{host}},\\ u \neq w}} \sigma_{uw}(i), \tag{1}$$

where V_{host} is the set of hosts in the network, and $\sigma_{uw}(i)$ is defined as 1 if node i lies on the path between nodes u and w under a specific routing algorithm; otherwise, it is 0.

The transmission capacity of a node represents the maximum number of packets it can handle at each step. Generally speaking, the transmission capacity of each node should be greater than its initial load to ensure that the network works