Physica A 492 (2018) 871–877

Contents lists available at ScienceDirect

Physica A

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

Effects of traffic generation patterns on the robustness of complex networks

Jiajing Wu [a,*], Junwen Zeng [a], Zhenhao Chen [a], Chi K. Tse [b], Bokui Chen [c]

[a] School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, China
[b] Department of Electronic and Information Engineering, Hong Kong Polytechnic University, Hong Kong, China
[c] School of Computing, National University of Singapore, Singapore

HIGHLIGHTS

- Cascading failures in networks with heterogeneous node functions are studied.
- Three kinds of algorithms to locate the hosts are applied to scale-free networks.
- It is found that placing the hosts at hub nodes can make the network more robust.

ARTICLE INFO

Article history:
Received 19 August 2017
Received in revised form 10 October 2017
Available online 16 November 2017

Keywords:
Complex networks
Traffic generation patterns
Robustness
Cascading failures

ABSTRACT

Cascading failures in communication networks with heterogeneous node functions are studied in this paper. In such networks, the traffic dynamics are highly dependent on the traffic generation patterns which are in turn determined by the locations of the hosts. The data-packet traffic model is applied to Barabási–Albert scale-free networks to study the cascading failures in such networks and to explore the effects of traffic generation patterns on network robustness. It is found that placing the hosts at high-degree nodes in a network can make the network more robust against both intentional attacks and random failures. It is also shown that the traffic generation pattern plays an important role in network design.

1. Introduction

Since the discovery of the small-world and scale-free structural features in complex networks, a wealth of research work has been devoted to studying statistical and dynamical properties of large-scale infrastructure networks. Typical examples of complex networks in real life include the Internet, the World-Wide-Web, power grids, social networks, transportation networks, and so on. In the past two decades, the interplay between network structure and dynamics has been widely studied [1], including traffic dynamics [2], cascading failures [3–5], and epidemic spreading [6–8]. Among them, the phenomenon of cascading failures has received much attention and has been extensively studied. Taking the Internet as an example, when a router fails, its traffic load will be redistributed to other routers. The redistribution of traffic loads may lead to subsequent overloads of other routers, causing simultaneous malfunctions and resulting in a cascade of failure events.

Previous studies on network robustness have focused on a few key areas including cascading failure models [9,10], cascading defence strategies [11,12], failure types [13], etc. Most of these studies focused on a cascade of failure events triggered by the failure of a single node. If the node has a relatively low load, its failure usually has limited impact on the traffic loads of most other nodes. On the contrary, the malfunctioning of a node with a relatively high traffic load will significantly

* Corresponding author.
E-mail address: wujiajing@mail.sysu.edu.cn (J. Wu).

https://doi.org/10.1016/j.physa.2017.11.016
0378-4371/

affect the loads of other nodes and may even cause a cascade of failures due to repeated overloading events. A pioneering study [10] demonstrated that if a network exhibits a highly heterogeneous distribution of loads, the removals of nodes with high loads will trigger global cascading failures in the whole network.

Recently, several coupled network models [14–19] have been developed to mimic the interactions between two real-world networks. Among them, Tan et al. [15] first extended the robust-yet-fragile nature to interdependent networks. Also, Chen et al. [18] investigated the processes of cascading failures in interdependent power grids and communication networks from a complex network perspective. Besides, Zhang et al. [19] introduced a model for generating the propagation profiles of cascading failures in power networks.

It has been widely revealed that the robustness of networks is closely related to the network topology and the adopted routing algorithms. Previous studies have demonstrated that the Barabási–Albert (BA) scale-free networks [20] are robust against random failures but fragile to intentional attacks, while the Erdös–Rényi (ER) random graphs [21] are robust against both random failures and intentional attacks [4,5,10,22]. On the other hand, with a fixed network structure, the choice of routing algorithm determines the routing path for each packet to reach its destination from its source, thus playing an important role in determining the distribution of traffic loads in the network. Therefore, two general types of strategies have been proposed to suppress cascade of failures and improve network robustness, namely, adjustment of network structure [11,23–25] and design of efficient routing algorithms [26–31].

In most current studies, the cascading failures are discussed under a simplistic assumption: each node in the network serves the same function of generating and delivering packets. However, many real networked systems have heterogeneous node functions. For example, in the Internet, there are two kinds of nodes at autonomous system-level, namely, stubs and transits. The stubs in the Internet can generate or receive data packets, whereas the transits connecting the stubs can only store and forward packets.

To better mimic real-world communication networks, in this paper, we consider a generic type of networks which have two basic kinds of nodes: *routers* and *hosts*. In this kind of networks, the distribution of traffic loads and network robustness are not only influenced by the underlying network topology and the routing strategy, but also dependent on the traffic generation patterns, which are determined by the locations of the hosts. Therefore, it is of interest to explore how traffic generation patterns influence the process of cascading failures triggered by intentional attacks or random failures.

The rest of this paper is organized as follows. In Section 2, the traffic model and the mechanism of cascading failures are introduced. In Section 3, several indicators for performance comparisons are defined, and simulation results of different traffic generation patterns under intentional attacks and random failures are discussed. Finally, a conclusion is given in Section 4.

2. Model

In this section, we will describe the traffic model in detail, and explain the mechanism of cascading failures.

2.1. Traffic model

We consider a generic type of traffic model, in which data or information is presented as packets and sent through the network in discrete time steps. Unlike most prior studies which assume that each node serves the same function in traffic transmission, here we classify the nodes in a network into two categories: *hosts* and *routers*. Packets are generated only by the hosts and sent through the links one hop at a time step until they reach their destinations, whereas the routers can only relay packets.

- Packet Generation: At each time step, new packets are generated with randomly selected sources and destinations from the hosts. If the average number of generated packets in each time step by each host is λ, and the total number of the hosts in the network is N_{host}, then the number of packets generated in the network at each time step is λN_{host}.
- Packet Transmission: At each time step, each node in the network receives packets from its neighbours and each node has a buffer queue to store the packets waiting to be processed. Each queue works under the first-in–first-out principle and the new generated or received packet will be put at the end of the queue. Each packet is transmitted one step along the shortest path between its source and destination, and the packets that have already reached their destinations are removed from the network.

To quantify the traffic intensity of a particular node in the network, we use the node usage probability $U(i)$ for node i, which is defined as [32]

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

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