Journal of Network and Computer Applications 40 (2014) 97–104

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Robustness of Internet under targeted attack: A cascading failure perspective

Jianwei Wang *, Chen Jiang, Jianfei Qian

School of Business Administration, Northeastern University, Shenyang 110819, PR China

ARTICLE INFO

Article history:
Received 1 May 2012
Received in revised form
27 April 2013
Accepted 24 August 2013
Available online 17 September 2013

Keywords:
Cascading failure
Robustness
Attack
Internet

ABSTRACT

In many networks, there exist some heterogeneous nodes, for example the hosts and the routers in the Internet, and the users and the supply-grid stations in the power grid. In the previous studies, however, few cascading models were constructed in the heterogeneous networks. Considering two types of nodes, we propose a new cascading edge model and investigate the cascading dynamic behaviors in the Internet. Compared with an extending Barabási–Albert (BA) network with two types of nodes, we find that the Internet displays the stronger robust level under two targeted attacks and propose some effective methods to protect these networks. The cascading model in the Internet can be extensively applied to other real-life networks, and may provide a new perspective to study the network safety.

1. Introduction

In recent years, owing to the importance of the network safety in our daily life, the question of the robustness of complex networks has attracted a large amount of interests from many researchers (Lin, 2007; Bossardt et al., 2007; Wu et al., 2007a,b, 2011; Holme et al., 2002; Xia and Hill, 2008). In particular, there has been the extensive effort to study and understand the Internet robustness, which has been one of the most central topics in the network safety. An important conclusion in this context is that the Internet displays the stronger robustness against random failure, but shows the exceptional vulnerability against intentional attack (Albert et al., 2000). Since the earlier studies mainly focus on the static properties of a network (Cohen et al., 2000, 2001), recently cascading failures induced by the redistribution dynamics of the load on a network have been highly concerned and widely investigated. Cascading failures are common in real-life systems and can occur not only in the Internet but also in many other infrastructure networks. Typical examples include several blackouts in some countries, e.g., the largest blackout in US history took place on 14 August 2003 and the Western North American blackouts in July and August 1996, and the Internet collapse caused by the submarine earthquake near Taiwan in December 2006.

A number of important aspects of cascading failures have been discussed in the literature and many valuable results have been found, including the robustness of interdependent networks (Vespignani et al., 2010; Buldyrev et al., 2010; Parshani et al., 2010; Huang et al., 2011; Shao et al., 2011), the cascading control and defense strategies (Wang and Rong, 2009a,b; Yang et al., 2009; Wang et al., 2010; Simonsen et al., 2008; Motter, 2004; Ash and Newth, 2007), the models for describing the cascading phenomena (Crucitti et al., 2004; Wang and Chen, 2008; Wang and Xu, 2004; Wang and Rong, 2009c; Lehmann and Bernasconi, 2010; Goh et al., 2001; Sandro et al., 2008), and cascading failures triggered by intentional attacks (Motter and Lai, 2002; Wang et al., 2008; Wang and Rong, 2008; Zhao et al., 2004, 2005; Ricard et al., 2008). These studies not only construct cascading models from single networks but also pay close attention to cascading models from coupled networks. However, in all studies cited above, a few works explore cascading failures in the Internet with two types of nodes, i.e., the routers and the hosts. Therefore, in the Internet, how to construct a cascading model with heterogeneous nodes and investigate its robustness against cascading failures is a significant topic.

To this end, the aim of this paper is to construct a new cascading model and investigate the roles of different edges in the cascading propagation in the Internet. Considering two types of nodes, we construct a new cascading model and compare the effects of different ways of attacking edges in the Internet. We numerically find some interesting and important results, such as, targeted attacks are not always effective and the Internet is more robust than Barabasi and Albert (1999) (BA) networks under targeted attacks. In addition, we carefully analyze these results by the local topological structure of two kinds of networks. Our findings may be useful in further studies on how to build attack-robust networks and increase the robustness of real-life networks against cascading failures.

The rest of this paper is organized as follows: in Section 2, we describe the cascading model in detail. In Section 3, we analyze the robustness of the Internet under two targeted attacks. Finally, some summaries and conclusions are shown in Section 4.

* Corresponding author. Tel.: +86 024 83672631.
E-mail address: jwwang@mail.neu.edu.cn (J. Wang).

1084-8045/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2013.08.007

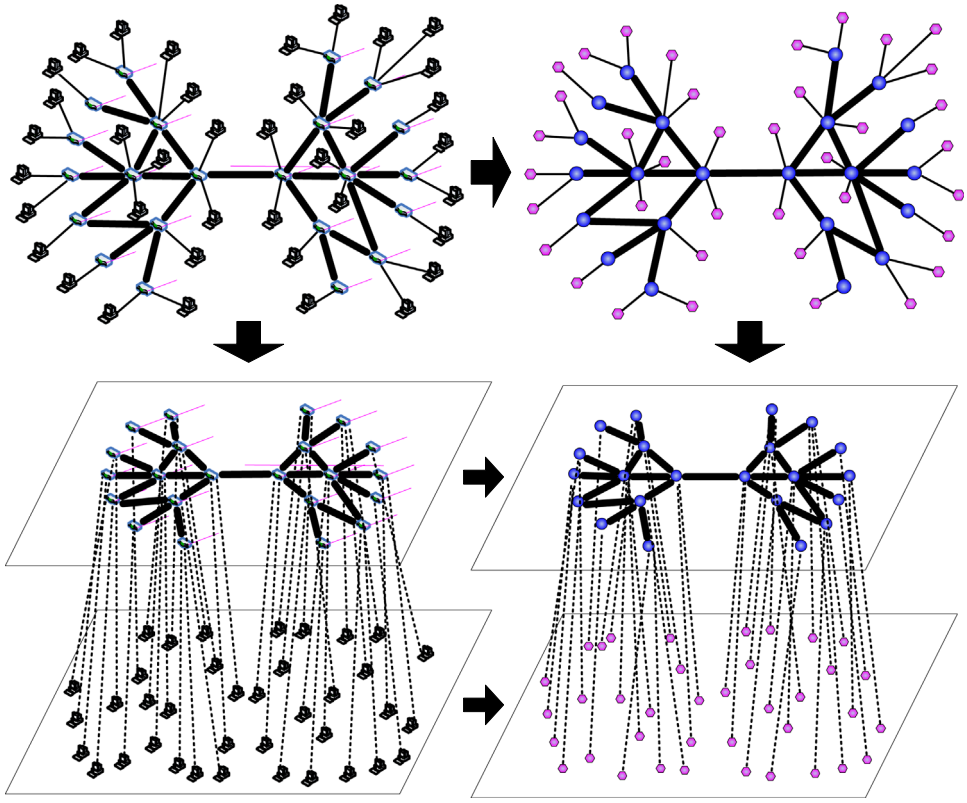

Fig. 1. The scheme demonstrates that the Internet with the routers and the computers can be represented by two layers networks.

2. The model

In general, the Internet contains two types of nodes, the routers and the computers, which play different roles in the function. The computers are the terminal users, while the cables between the routers can transport the load. We can simply use a two-layer network to represent the Internet (see Fig. 1), in which the routers and the computers lie in the top layer and the bottom layer, respectively. When the cable between two routers fails owing to some reasons, the load on it will be redistributed to other cables, which may further lead to the malfunction of other cables and eventually trigger the larger cascading failures in the whole Internet. According to the cascading evolving process mentioned above, a cascading model should include three aspects: how to define the initial load on an edge, how to assign the capacity of an edge, and how to redistribute the load on it after an edge fails. Therefore, considering the different roles of the routers and the computers in the cascading propagation and three aspects related with cascading failures, we propose a new cascading model.

Next, we briefly introduce our cascading edge model. Firstly, we give a new method to assign the initial load on an edge. In the Internet, the load on the cable between two routers A and B is generally decided by the number of the routers and the computers connected with A and B. Therefore, considering the effects of the routers in the R layer and the computers in the C layer on the initial load on an edge, we assume the initial load L_{ij} of edge ij to be

$$L_{ij} = \delta f_R(k_{i,R\to R}, k_{j,R\to R}) f_C(k_{i,R\to C}, k_{j,R\to C}) \tag{1}$$

where $k_{i,R\to R}$ and $k_{i,R\to C}$ is the degrees of node i connecting with the routers in the R layer and the computers in the C layer, respectively, and δ is a tunable parameter, governing the strength of the initial load on an edge. Two functions f_R and f_C represent the effects of the routers and the computers connected with routers i and j on the initial load on edge ij, respectively. Our main aim is to investigate the robustness of the Internet under targeted attacks against cascading failures. Therefore, we assume

$$f_R(k_{i,R\to R}, k_{j,R\to R}) = \delta_1 (k_{i,R\to R} k_{j,R\to R})^{\alpha} \tag{2}$$

$$f_C(k_{i,R\to C}, k_{j,R\to C}) = \delta_2 (k_{i,R\to C} k_{j,R\to C})^{\beta} \tag{3}$$

of which δ_1, δ_2, α, and β are tunable parameters. The definitions of Eqs. (1) and (2) are supported by empirical evidences of real networks (Wang and Rong, 2009b; Wang and Chen, 2008; Barrat et al., 2004). Moreover, Holme et al. (2002) shows that the betweenness of an edge has a positive correlation with the product form of node degrees at both ends of the edge. Specially, in a single network with one type of nodes, many cascading models are constructed according to the rules above. In this sense, our assumption about the initial load on the edge is in accordance with the previous models. By analyzing the definition of the initial load on an edge, we can see that the distribution of the initial load is decided by parameters δ, δ_1, δ_2, α, β, and the network topology structure. Therefore, we mainly focus on the correlation between these parameters and the effects of targeted attacks.

Since the capacity of an edge in real-life networks is generally limited by cost, it is natural to assume that the capacity C_{ij} of edge ij is proportional to its initial load for simplicity:

$$C_{ij} = (1+\gamma) L_{ij} \tag{4}$$

where $\gamma(>0)$ is a uniform capacity parameter (Fig. 2).

Considering that the edge with the higher capacity has generally the stronger capacity to handle the extra load, we assume to preferentially redistribute the load along those higher-capacity edges (Wang and Rong, 2008, 2009a,b; Wang and Chen, 2008). Thus, the load on a failed edge ij will be preferentially redistributed to its neighboring edges in the R layer (see Fig. 3 for illustration). The additional load ΔL_{im} received by edge im is proportional to its