Accepted Manuscript

Overload cascading failure on complex networks with heterogeneous load redistribution

Yueyi Hou, Xiaoyun Xin, Menghui Li, An Zeng, Yougui Wang

PII: S0378-4371(17)30342-4
DOI: http://dx.doi.org/10.1016/j.physa.2017.04.039
Reference: PHYSA 18141

To appear in: *Physica A*

Received date : 6 September 2016
Revised date : 7 February 2017

Please cite this article as: Y. Hou, et al., Overload cascading failure on complex networks with heterogeneous load redistribution, *Physica A* (2017), http://dx.doi.org/10.1016/j.physa.2017.04.039

Overload cascading failure on complex networks with heterogeneous load redistribution

Yueyi Hou[1], Xiaoyun Xin[2], Menghui Li[3], An Zeng[2,*], Yougui Wang[2]

1. Department of Management Science, School of Government, Beijing Normal University, 100875 Beijing, China
2. School of Systems Science, Beijing Normal University, 100875 Beijing, China
3. Beijing Institute of Science and Technology Intelligence, 100044 Beijing, China

Abstract

Many real systems including the Internet, power-grid and financial networks experience rare but large overload cascading failures triggered by small initial shocks. Many models on complex networks have been developed to investigate this phenomenon. Most of these models are based on the load redistribution process and assume that the load on a failed node shifts to nearby nodes in the networks either evenly or according to the load distribution rule before the cascade. Inspired by the fact that real power-grid tends to place the excess load on the nodes with high remaining capacities, we study a heterogeneous load redistribution mechanism in a simplified sandpile model in this paper. We find that weak heterogeneity in load redistribution can effectively mitigate the cascade while strong heterogeneity in load redistribution may even enlarge the size of the final failure. With a parameter θ to control the degree of the redistribution heterogeneity, we identify a rather robust optimal $\theta^* = 1$. Finally, we find that θ^* tends to shift to a larger value if the initial sand distribution is homogeneous.

Keywords: Cascading failure; sandpile model; heterogeneous load redistribution

1. Introduction

Infrastructure networks are an essential part of a modern society and the security of these systems is of great importance [1, 2, 3, 4]. However, such kind of networks may suffer from cascading failure which is usually initialized by the failure of a small part but eventually trigger the disfunction of successive parts of the network [5]. This could happen in real infrastructure networks of various types, including the power transmission, computer networking, financial and mechanical systems [6, 7, 8]. Even though the cascading failure is rare, it usually causes serious loss when it happens. Take power grid as an example, a widespread power outage happened in Southern Brazil in 1999, causing a blackout and finally affecting an estimated 75 to 97 million people [9].

There are many pioneering studies trying to model the cascading failure in infrastructure systems. The models based on percolation theory measure the network functionality by the size of giant component in the network, and indicate that real scale-free networks is robust against random failure but sensitive to intentional attacks [10, 11, 12]. These networks are found to be more fragile if they are interdependent [3, 13, 14]. Another type of models consider the load redistribution of the failed nodes and the successive failures are caused by the remaining nodes taking up the load for the failed node which we call overload cascading failures. [15, 16, 17]. It has been mostly studied using sandpile as a prototypical model introduced by Bak, Tang and Wiesenfeld (BTW) [18]. Varieties of sandpile models were then constructed and their critical properties were analyzed incorporating different toppling rules and external conditions on original BTW model such as Manna's stochastic model (MSM) [19], directed sandpile model [20], sandpile in disordered system [21], rotational sandpile model (RSM) [22] and many others can be found in ref. [23]. In these models, when the network reaches in a state of self-organized criticality (SOC), a small attack will lead to a massive damage through the process of overload cascading failure [5, 18]. To characterize the overload cascading

Email address: anzeng@bnu.edu.cn (An Zeng[2,*])