Safety Science 65 (2014) 1–9

Contents lists available at ScienceDirect

Safety Science

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

Modeling and analysis of cascading failure in directed complex networks

Xinli Fang, Qiang Yang *, Wenjun Yan

College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China

ARTICLE INFO

Article history:
Received 22 November 2012
Received in revised form 18 October 2013
Accepted 17 December 2013
Available online 21 January 2014

Keywords:
Cascading failure
Neighbor link
Attack strategy
Tolerance parameter

ABSTRACT

This paper exploited the cascading failure behavior in the new context of directed complex networks by introducing the concept of neighbor links. Two novel network attack strategies, i.e. the minimum in-degree attack strategy (MIAS) and the maximum out-degree attack strategy (MOAS), are proposed and their impacts are assessed through simulation experiments by using the random attack strategy (RAS) as the comparison benchmark for a range of network scenarios (directed random network, directed scale-free network and the IEEE 118 network model). The numerical result shows that the cascading failure propagation in directed complex networks is highly dependent on the attack strategies and the directionality of the network, as well as other network configurations.

1. Introduction

For many realistic large-scale systems, e.g. the power grid and Internet, the occurrence of some disastrous failures may be due to the faults at only one or a few network components. Due to the coupling property of the network, these faults can be extended to a large scale, which may eventually lead to a chain reaction and cause a paralysis or even entire collapse of the network. Such phenomenon is known as the network cascading failure or "network avalanche" (Lelarge, 2012). In recent years, many countries have suffered from serious blackout crisis in the power utilities, e.g. the Western North American blackout in July 8th 1996 made more than 4 million people lose power service, and the major power blackout on August 14th 2003 lasted up to 4 days, which brought America and Canada 61,800 MW power loss (Wang and Rong, 2011; Chang and Wu, 2011). These accidents have imposed an urgent demand on the investigation of the cascading network behaviors in power systems and cost-effective protection strategies.

As a response, much research efforts on the investigation of cascading failures in complex networks have been carried out from different aspects and a collection of findings have been reported in the literature (Bao et al., 2009; Dou et al., 2010; Xia et al., 2010; Xu and Wang, 2005; Wu et al., 2007; Wang et al., 2008; Wang and Rong, 2009a; Bao and Cao, 2008; Wang and Rong, 2009b; Zhang et al., 2012; Wei et al., 2012; Liu et al., 2011; Chen et al., 2009; Dwivedi et al., 2009; Wang et al., 2011; Nasiruzzaman and Pota, 2011; Zhu et al., 2011; Lv and Yu, 2010; He et al., 2007; Bompard et al., 2009; Bao et al., 2008, 2009; Wang and Rong, 2009c; Duenas-Osorio and Vemuru, 2009; Albert et al., 2004; Kinney et al., 2005; Chen et al., 2007; Cao et al., 2009). Bao et al. (2009) and Dou et al. (2010) studied the propagation mechanism of cascading failure in small-world network and scale-free network respectively, and pointed out that the scale-free network is more vulnerable to intentional attacks (Bao et al., 2009; Dou et al., 2010). Xia et al. (2010) adopted the concepts of node degree and betweenness to the cascading failure analysis in Watts–Strogatz (WS) small-world networks (Xia et al., 2010), while the work presented by Xu and Wang (2005), Wu et al. (2007), Wang et al. (2008) and Bao et al. (2008) focused on cascading failures in the scale-free networks (Xu and Wang, 2005; Wu et al., 2007; Wang et al., 2008; Wang and Rong, 2009a) and local-world networks (Bao and Cao, 2008) respectively; Wang and Rong (2009b) considered the network link load distribution problem in the cascading failure analysis of the scale-free network, and proposed a load distribution pattern for failed links in the undirected networks, which confirmed that scale-free networks are more sensitive to attacks on the edges with the lowest loads (Wang and Rong, 2009b); Zhang et al. (2012) explored the vulnerability characteristic of the self-organized network through the study of IEEE 118-bus systems and presented an optimal design of the US power grid (Zhang et al., 2012); Wei et al. (2012) analyzed the cascading failure based on the local preferential redistribution rule for the failed nodes and pointed out that there exists a threshold such that cascading failure is induced and enhanced when the value of tolerance parameter is smaller than the threshold (Wei et al., 2012). Liu et al. (2011) assessed the model of cascading failures based on the nodes with different tolerance parameters and presented some viable solutions for reducing the damage (Liu et al., 2011). In addition, a

* Corresponding author. Tel.: +86 571 8795 3204; fax: +86 571 8795 1625.
E-mail address: qyang@zju.edu.cn (Q. Yang).

0925-7535/$ - see front matter
http://dx.doi.org/10.1016/j.ssci.2013.12.015

number of studies have considered specific network scenarios to address certain engineering challenges. For example, Chen et al. (2009) took the impedance into account in the cascading failure problems in electric power networks (Chen et al., 2009; Dwivedi et al., 2009; Wang et al., 2011; Nasiruzzaman and Pota, 2011; Zhu et al., 2011), while Bao et al. (2009) and Lv and Yu (2010) introduced the power flow entropy into the reliability analysis of power networks to identify the key network nodes during the cascading failure process (Lv and Yu, 2010; He et al., 2007; Bompard et al., 2009; Bao et al., 2008, 2009). Also, some specific studies have been carried out for a set of realistic networks, e.g. applying the research outcomes and insights into the stability analysis of regional power grid of China, North America and Europe (Wang and Rong, 2009c; Duenas-Osorio and Vemuru, 2009; Albert et al., 2004; Kinney et al., 2005; Chen et al., 2007; Cao et al., 2009).

The aforementioned research outcome of cascading failures are encouraging, however, these studies have been based on a strong assumption that the network topologies are unidirectional. In reality, most of the systems are observed as networks with directional flows, e.g. the integration of a massive number of distributed generators (DGs) can result in bidirectional power flows across the power distribution network, and the data packets can be delivered between any pair of routers in the communication network. It should be noted that the malfunctions will only be propagated along the direction of flows in the networks during the cascading failure, which implies that the existing investigations and solutions based on the undirected networks become insufficient or even not applicable to the analysis of many realistic networks.

With such recognition, this paper attempts to address the cascading failure issue in a new context: the directed complex networks. We investigate the failure propagation mechanism and assess the cascading failure model in the directed networks with random, scale-free and the standard IEEE 118-bus topologies, and evaluate the network prevention approaches under various attack strategies. The rest of the paper is organized as follows: Section 2 introduces the model of directed network and presents the concept of neighbor links; in Section 3, we analyze the failure propagation and load distribution mechanism during the network cascading failure; numerical simulation experiments are carried out to evaluate the network performance under three different attack strategies in Section 4; and finally, some conclusive remarks and future works are given in Section 5.

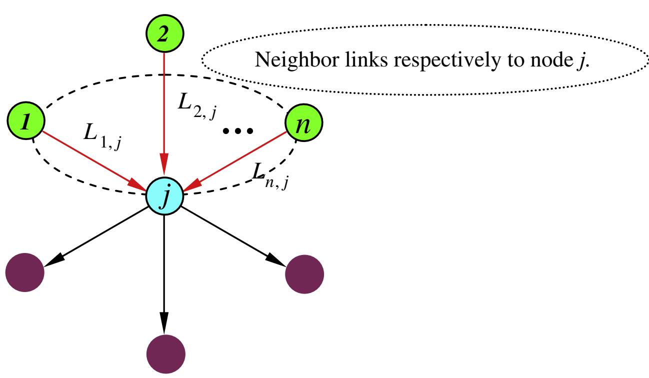

Fig. 1. The illustration of the neighbor links in the directed networks.

2. Directed network

For most of the realistic networks, e.g. power grid, Internet and transportation networks, they can be modeled as directed networks, where the end to end path consisting of a set of intermediate nodes form the source to the destination. To study the cascading failure process of such directed networks, we firstly present the network model as follows.

2.1. Directed network model

The network topology is modeled as a graph, $G(N,K)$, with N nodes and K edges, where G can be denoted by an $N \times N$ adjacency matrix with the elements $e_{i,j}$.

For the directed network, the adjacency matrix can be expressed as follows:

$$\vec{e}_{i,j} = \begin{cases} +1 & i \text{ to } j \\ -1 & j \text{ to } i \\ 0 & \text{no connetctions or flows between } i \text{ and } j \end{cases} \quad (1)$$

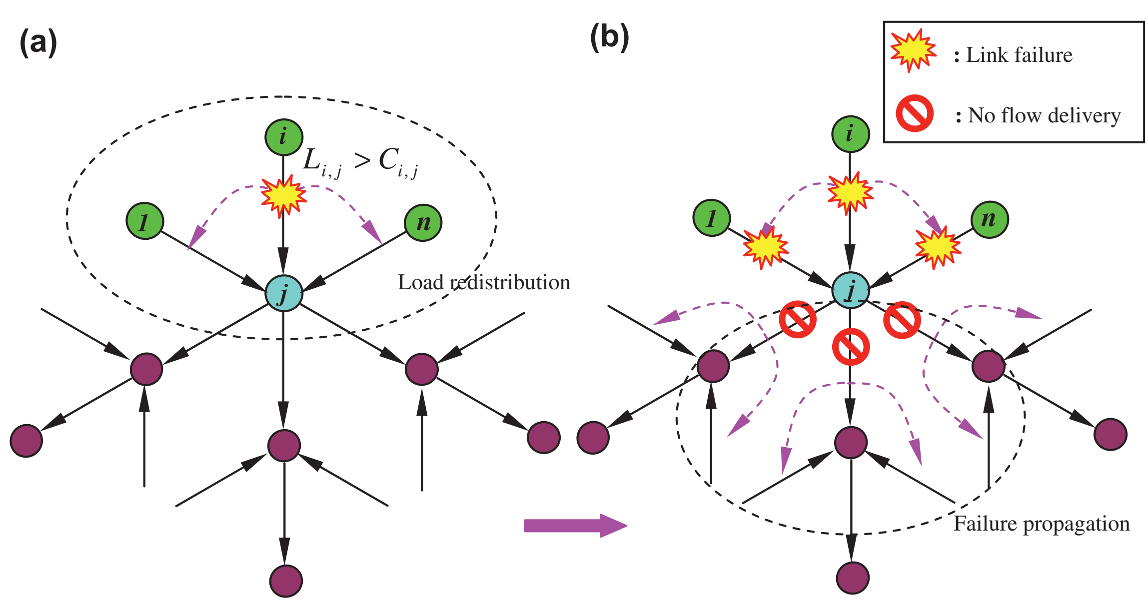

Fig. 2. An illustration of the cascading failure propagation in a directed network: (a) load redistribution to the neighbor links of the failed link $L_{i,j}$; and (b) failure propagation to the downstream links of node j as no flows can be delivered from j due to the malfunctions of its all input links.