Theoretical Computer Science 607 (2015) 306–319

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Catastrophic cascading failures in power networks ☆

Jungtaek Seo [a], Subhankar Mishra [b], Xiang Li [b], My T. Thai [c,b,*]

[a] The Attached Institute of ETRI, Republic of Korea
[b] Dept. of Comp. and Info. Sci. and Eng., University of Florida, Gainesville, 32611, USA
[c] Division of Algorithms and Technologies for Networks Analysis, Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Viet Nam

ARTICLE INFO

Article history:
Received 17 July 2015
Accepted 24 August 2015
Available online 24 September 2015

Keywords:
Cascading failure
Power network
Optimization

ABSTRACT

The high demand of electricity makes power networks more vulnerable under cascading failures. Because of the operational dependencies between nodes, the failure of a small set of nodes can cause a large cascade of failures which results in the breakdown of the network. Thus, it is crucial to study the vulnerability of the power network under the cascading failures.

In this paper, we study the cascading critical node (CasCN) problem which asks to find a set of nodes whose failure maximizes the number of failed nodes under the effect of cascading failures. We first show that the problem is NP-hard to approximate within the factor of $O(n^{1-\epsilon})$. We then design a new metric to evaluate the importance of nodes in the network and use it as the base to design the Fully Adaptive Cascading Potential algorithm. In the case where the network is robust, we propose an alternative algorithm, the Cooperating Attack algorithm, which includes several novel properties to solve the problem. Simulation results demonstrate the efficiency of proposed algorithms and provide more insight into the vulnerability of the power network.

1. Introduction

The complex network systems are now the essential parts of a modern society. Many complex systems are extremely vulnerable to attacks, that is, the failures of a few key nodes that play a vital role in maintaining the network's connectivity can break down their operation. In addition, this vulnerability may be propagated, leading to a much more devastating consequence. A failure within a single component may have a profound impact on large parts of the system. The nodes' failures may change the balance of flows and lead to a global redistribution of loads over the entire network. This can trigger a cascade of overload failures. Cascades can therefore be regarded as a specific manifestation of the robust yet fragile nature of many complex systems: a system may appear stable for long periods of time and withstand many external shocks (robust), then suddenly and apparently inexplicably exhibit a large cascade (fragile). These phenomena are all examples of what economists call information cascades (Ref. [4]; but which are herein called simply cascades), during which individuals in a population exhibit herd-like behavior because they are making decisions based on the actions of other individuals

☆ The first two authors contribute equally to this work.

[*] Corresponding author at: Division of Algorithms and Technologies for Networks Analysis, Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Viet Nam and Dept. of Comp. and Info. Sci. and Eng., University of Florida, Gainesville, 32611, USA.

E-mail addresses: seojt@ensec.re.kr (J. Seo), mishra@cise.ufl.com (S. Mishra), xixiang@cise.ufl.com (X. Li), thaitramy@tdt.edu.vn, mythai@cise.ufl.com (M.T. Thai).

http://dx.doi.org/10.1016/j.tcs.2015.08.021
0304-3975/© 2015 Elsevier B.V. All rights reserved.

rather than relying on their own information about the problem. Although they are generated by quite different mechanisms, cascades in social and economic systems are similar to cascading failures in physical infrastructure networks and complex organizations in that initial failures increase the likelihood of subsequent failures, leading to eventual outcomes, are extremely difficult to predict, even when the properties of the individual components are well understood.

The common denominator of large blackouts is that the failures of components happened according to the cascading manner. It often starts with the failure of one or a few components, then some other components are failed due to the dependencies with previous failed components. The failure of these components continue to cause other components fail. The process continues until there is no more failed component. In power networks, generator, distribution, and consumption stations can only work well if the load is under the maximum capacity they can handle. When a station is overloaded, it cannot work with the best performance or even fails. During the operation, the power network is designed such that all stations work under their capacity. But when some stations fails, other stations which are directly or indirectly connected with failed ones may have bear more load. If the load of a station surpasses its capacity, it will fail and continue to shred their load to other stations. As a result of the load redistribution process, a large number of failed stations may be failed at the end. The dependencies between stations in the network make the outcome difficult to be predicted. Thus, it is necessary to develop efficient tools to analyze the sophisticated cascading process of failures in power networks.

The cascading failure has attracted a lot of attention and been studied in various perspective [1–8]. The structural vulnerability of power networks was studied in [2]. The authors showed that removing small fraction of highest degree nodes significantly reduces the connectivity of the network. After that, Hines et al. [4] studied the network vulnerability of different classes of scale-free networks including Erdos–Renyi, preferential-attachment, and small-world networks. They showed that different types of networks behave differently under node failures. Various models of cascading failures were later proposed to study the vulnerability of networks under the targeted attack [6,9,10,7]. However, these works mainly present different ranking methods for nodes and select most the highest ranked nodes as the critical ones. These methods fail to address the effect of the cascading process.

In this paper, we study the vulnerability of power grid under the targeted attack with the effect of the cascading failures. More specifically, we aim to find a set of k nodes whose failures maximize the number of failed nodes when the cascading of failures stops. It is challenging to identify such set of nodes due to the complicated interaction between nodes in the network. Thus, it is impossible to solve the problem optimally, especially on large networks. Our approach is to design a new measure for the importance of nodes considering the cascading effect, then develop efficient algorithms from that.

Our main contributions are summarized as follows:

- Evaluate the vulnerability of the power grid under a new kind of attack in which nodes are attacked one by one to increase the damage. Since the cascading failures happen fast, an attacker can choose the next attacked node based on the status of the network after the effect of previous attacks. By this way, the attacker can gain more failed nodes.
- Show that the proposed problem is NP-hard to approximate within the ratio of $O(n^{1-\epsilon})$.
- Introduce a new metric called *cascading potential* to measure the importance of nodes when the cascading effect is considered.
- Propose various algorithms which can work well under the variety of network settings.
- Validate the efficiency of proposed algorithms in a wide range of network configurations and provide new insights into the vulnerability of the power grid.

The rest of the paper is organized as follows. In Section 2, we present the failure cascading model and formulate the problem. Then, we show the hardness result in Section 3. After that, we propose the cascading potential metric and design various algorithms in Section 4. We next introduce the cooperating algorithm which is efficient on robust networks in Section 5. Section 6 shows the experimental evaluation. Finally, we conclude the paper in Section 7.

2. Network model and problem formulation

2.1. Graph notations

The network is modeled by a weighted directed graph $G = (V, E)$ with the node set V of $|V| = n$ nodes and the edge set E of $|E| = m$ oriented connections between nodes. Each edge (u, v) is associated with a weight $w(u, v)$ representing the operating parameter of the network. The higher $w(u, v)$ is, the more load is distributed from u to v. In addition, each node u has a current load $L(u)$ and a capacity $C(u)$. The capacity $C(u)$ is the maximum load that node u can accept. Finally, we denote the set of incoming neighbors, outgoing neighbors of u by N_u^- and N_u^+, respectively.

2.2. Cascading failure model

In this paper, we adopt the Load Redistribution model (LR-model) which was widely used in the research community [11,6]. In this model, nodes are failed in the cascading manner due to the load redistribution of failed nodes. Initially, a set of nodes S are failed, then the failures are propagated to other nodes in time steps. When node u fails, its load is redistributed to its neighbors as illustrated in Fig. 1. Each alive neighbor v will received an additional load which is proportional to weight $w(u, v)$ of edge from u to v. Precisely, v will receive additional load: