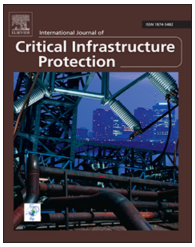
Available online at www.sciencedirect.com
ScienceDirect
www.elsevier.com/locate/ijcip



Using interdependency matrices to mitigate targeted attacks on interdependent networks: A case study involving a power grid and backbone telecommunications networks

Diego F. Rueda[*], *Eusebi Calle*

Institute of Informatics and Applications, Universitat de Girona, P-IV Building, Campus Montilivi, Girona 17071, Spain

ARTICLE INFO

Article history:
Received 25 November 2015
Received in revised form
29 June 2016
Accepted 16 November 2016
Available online 9 December 2016

Keywords:
Interdependent Critical Infrastructures
Interdependent Networks
Failure Propagation
Attack Mitigation
Robustness
Interdependency Matrices
Power Grid
Backbone Telecommunications Networks

ABSTRACT

Analysis of the interdependencies between interconnected critical infrastructures can help enhance the robustness of the individual infrastructures as well as the overall interconnected infrastructures. One of the most studied interdependent critical infrastructure network scenarios is a power grid connected to a backbone telecommunications network. In this interdependent infrastructure scenario, the robustness of the entire system is usually analyzed in the context of cascading failure models in the power grid. However, this paper focuses on targeted attacks, where an attack on a telecommunications network node directly affects a connected power grid node, and vice versa. Cascading failures are outside the scope of this paper because the objective is to enhance the robustness of the interconnections between the infrastructures. In order to mitigate the impacts of targeted attacks on the interdependent infrastructures, three interdependency matrices for connecting the infrastructures are specified and analyzed. The analysis identifies the interdependency matrix that best reduces the impacts of targeted attacks and the propagation of failures between the infrastructures. Additionally, the impacts of interconnecting a power grid to different telecommunications networks, each with different susceptibilities to targeted attacks, is evaluated.

1. Introduction

Large-scale critical infrastructure failures rarely occur, but when they do, the consequences are catastrophic and expensive. In 2014, a human error in configuring Time–Warner's Internet routers in the United States resulted in a failure that prevented 11.4 million clients from accessing broadband services for three hours [21]. Network robustness, defined as the ability of a network to continue to operate when subjected to failures [2], can be evaluated by measuring the impacts of large-scale failures. However, most critical infrastructures, such as water supply systems, transportation systems, power grids, oil and gas pipelines, and telecommunications systems, need to interact with other networks to provide goods and services.

Interdependencies between critical infrastructures mean that the behavior and reliability of one network depend on the other networks [1]. A fundamental property of

[*] Corresponding author.
E-mail address: u1930599@campus.udg.edu (D.F. Rueda).

http://dx.doi.org/10.1016/j.ijcip.2016.11.004

interdependent networks is that a node failure in one network can spread to nodes in other networks, leading to cascading failures and dramatic consequences [1]. A good example of interdependent networks is a power grid and a telecommunications network, where the power grid relies on the telecommunications network for control and the telecommunications network relies on the power grid for electricity supply [14]. An example of a large-scale failure in interdependent networks is the Italian blackout of 2003, where a single failure in the power grid resulted in failures that propagated over a telecommunications network, ultimately affecting more than 55 million people [1,14]. The robustness of this interdependent critical infrastructure to cascading failures has been studied, but the impacts and mitigation of targeted attacks have yet to be analyzed.

This paper focuses on identifying critical nodes that are targeted by attacks. Whether or not a failure spreads and generates a cascading failure is beyond the scope of this paper. Instead, the focus is on protecting telecommunications and power grid networks from propagating failures. By identifying the appropriate models for interconnecting the two types of networks, it is possible to enhance their robustness.

In targeted attacks, the most important nodes, usually determined according to a centrality metric, are first removed. In such a scenario, it is possible to discern the nodes that could have serious impacts on the interdependent networks. Therefore, it is important to study network robustness under targeted attacks when a backbone telecommunications network and power grid are interconnected. Through this analysis, the best interdependency matrix for mitigating the impacts of targeted attacks on the interdependent critical infrastructures can be identified. The interdependent critical infrastructures also support analyses of the effects of the interdependency matrices on the propagation of targeted attacks between the two networks, which may have different topological properties.

Drawing on the results of Sydney et al. [20] and Iyer et al. [7], it is possible to determine which attacks would produce the greatest damage based on the topology of a single network. A backbone telecommunications network can be modeled as an Erdos–Renyi (ER) graph [3] while a power grid may be modeled as a Watts–Strogatz small-world (SW) graph [28]. An Erdos–Renyi graph shows vulnerability to targeted attacks based on node betweenness centrality b_c [20]. Moreover, the less robust Erdos–Renyi networks under targeted attacks have low values of average nodal degree $\langle k \rangle$ and high values of average shortest path length $\langle l \rangle$ and diameter D. Based on [7], it can be concluded that, for disassortative networks (with disassortative values $r<0$), simultaneous targeted attacks based on node degree centrality d_c are most effective at degrading the networks. In contrast, assortative networks (with assortative values $r>0$) are more vulnerable to sequential targeted attacks based on node betweenness centrality [7]. Interested readers are referred to [8] for a detailed coverage of graph theory and its relevance to this research.

The primary goal of this paper is to use interdependency matrices to evaluate and mitigate the impacts of the most dangerous attacks on a backbone telecommunications network interconnected with a power grid. Specifically, the backbone telecommunications network is targeted by sequential attacks that leverage betweenness centrality while the power grid is targeted simultaneously by attacks based on degree centrality; this enables the robustness of the interconnected networks to be measured. In order to simplify the interdependency model, it is assumed that investments have been made in the power grid to prevent the failure of one node from inducing cascading failures and to redistribute excessive loads to other network elements. In other words, a targeted attack on one node in the telecommunications network only damages the power grid node to which it is directly connected and the failure does not spread to other power grid nodes, and vice versa.

2. Previous work

Previous research has focused on analyzing the robustness of interdependent networks to cascading failures resulting from random and targeted initial failures. Buldyrev et al. [1] have examined the robustness of interdependent networks to cascading failures using the notion of percolation ρ. They show the existence of a critical percolation threshold ρ_c above which a considerable fraction of the nodes in the two networks remain functional at steady state. However, if $\rho<\rho_c$, then both networks fragment completely and the entire system collapses.

Parandehgheibi and Modiano [14] have shown that the robustness of the interdependent Italian telecommunications and power grid networks can be evaluated using the notion of minimum total failure removal (MTFR). In this situation, the larger the minimum total failure removal, the more robust are the networks. Other researchers have used algebraic connectivity λ_2 to analyze the robustness of interdependent networks. Martin-Hernandez et al. [10] analyze the critical number of interlinks beyond which any further inclusion does not enhance the algebraic connectivity; this phase transition depends on the topology of the graph model and they discovered that the transition point also increases with assortativity. Tauch et al. [22] evaluate algebraic connectivity as a robustness metric and use it to rewire interlinks. They also employ the effective graph resistance (EGR) as a robustness metric for interdependent networks by considering the Laplacian matrix of the entire system [23].

Several researchers have analyzed the robustness of interdependent networks to cascading failures generated by initial targeted attacks on high-degree nodes in two scale-free (SF) networks. Huang et al. [6] introduce a general technique that maps the targeted attack problem in interdependent networks to a random attack problem; they discovered that, when the highly-connected nodes are protected and have lower probabilities of failure compared with single networks, then the coupled networks are more vulnerable with ρ_c values significantly greater than zero. Zhang et al. [29] extend the interdependent network model by considering network flows and study the robustness under different attack strategies; in their model, nodes fail due to overloading or loss of interdependency. Pinnaka et al. [16] analyze the robustness of the U.S. critical infrastructure network to cascading failures; they