Physica A 491 (2018) 329–339

Contents lists available at ScienceDirect

Physica A

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

Robustness of networks formed from interdependent correlated networks under intentional attacks

Long Liu [a,*], Ke Meng [a], Zhaoyang Dong [b]

[a] *School of Electrical and Information Engineering, The University of Sydney, Sydney, NSW 2006, Australia*
[b] *School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW 2052, Australia*

HIGHLIGHTS

- Models for two types of interdependent networks with correlated structure under various attacks are proposed.
- The model can be used to effectively identify the robustness of the system under various attacks.
- The interdependent networks with positive correlation structure perform better under random attacks and attacks targeted to low-degree nodes.
- The resistance to the failure caused by targeted attack can be improved by modifying the broadness of each network's degree distribution.

ARTICLE INFO

Article history:
Received 7 November 2016
Received in revised form 12 May 2017
Available online 28 September 2017

Keywords:
Complex networks
Interdependent networks
Correlated networks
Targeted attacks
Cascading failure

ABSTRACT

We study the problem of intentional attacks targeting to interdependent networks generated with known degree distribution (in-degree oriented model) or distribution of interlinks (out-degree oriented model). In both models, each node's degree is correlated with the number of its links that connect to the other network. For both models, varying the correlation coefficient has a significant effect on the robustness of a system undergoing random attacks or attacks targeting nodes with low degree. For a system with an assortative relationship between in-degree and out-degree, reducing the broadness of networks' degree distributions can increase the resistance of systems against intentional attacks.

1. Introduction

Modern systems can be formed by several networks with interconnection to cooperate in performing complex and reliable functions. For example, an intelligent energy network consists of a power grid, a communication network and a gas pipeline network. The power grid and gas pipeline network can provide energy to each other and the communication network; however, they rely on the communication network for control and supervision. The structural vulnerability of the electricity network was studied based on complex network theory in [1,2]. Due to the interdependency of each network, failures occurring in one network may cause cascading effects to interfere with other networks and distort the stability of the whole system [3,4].

[*] Corresponding author.
E-mail address: l.liu@sydney.edu.au (L. Liu).

https://doi.org/10.1016/j.physa.2017.08.061
0378-4371/

1.1. Related work

Buldyrev et al. studied the system formed by mutually dependent networks in [3]. In their model, the interconnection between networks is one-to-one and random. The further work in [5] shows that arranging the interconnection can produce even opposite behaviour with respect to the effect of various degree distributions on the system's robustness. The interconnection between networks varies from one-to-one mode to multiple-to-multiple mode. Cascading failures of interdependent networks with multiple interconnections between each node have been studied in [6]. Gao et al. further extended the model to a system formed by multi-coupled networks [7]. The strength of a system can be improved by applying regular interlink allocation regardless the structure of each network [8]. The authors of [9] proposed a deterministic model for analysing the interdependent networks' robustness. Applications in reinforcing a Smart Grid by enhancing the interconnection have been studied in [10]. Furthermore, networks can be coupled with partial interdependency [11], and elements in a network can have redundant supporters from other networks [12]. Modifying the coupling strength can lead the percolation transition of interdependent networks from first to second order [13]. The robustness of a system is related to the correlation between each node's degree and the number of its links that connected to nodes in the other network and the assortativity of interconnected nodes [12]. When a system suffers from an intentional attack, the protection measures for a single network [14] will not be as effective as expected for interdependent networks [15]. Moreover, the target of a malicious attack can be nodes with a critical role in networks' interconnection [16].

1.2. Contributions

This paper is an extension of the research in [12] and [15]. This work develops a theoretical model to analyse intentional attacks on interdependent networks with correlated in-degree and out-degree. When the networks suffer from attacks that target to nodes with high or low degree, because of the correlation between in-degree and out-degree, the damage to both inner connection and interconnection will be analysed collectively. In this paper, links between nodes in the same network are in-links; links interconnecting each network are out-links. The number of in-links and out-links that a node has are in-degree and out-degree respectively. In order to exhibit the effects of intentional attacks, networks in this paper have degree distributions follow a power-law.

Apart from the traditional interdependent networks models, this paper introduces an out-degree oriented network model that is built based on the predefined out-degree distribution. This model can be utilised to analyse scenarios in which the interactions among different networks have leading situations in a system, such as economical systems [17] or social networks.

The resistance of networks with various structures against different attack modes is compared to show the impact of correlation on the robustness of interdependent networks. Measures are introduced to enhance a system's robustness, including modifying correlation parameters and the broadness of degree distribution. Furthermore, models in this paper can be applied to analyse various network structures and interdependency modes. This work can be extended to multiple interconnected networks.

The outline of this paper is as follows. Section 2 introduces the concept of interdependent networks, including the correlation between in-degree and out-degree and the interdependency mode of a system. Section 3 describes the intentional attacks and the approach to modify the degree distribution of a network undergoing a malicious attack. Section 4 demonstrates the technique to calculate the size of a giant component applying site percolation theory. Section 5 shows analysis of the damaged interdependent networks. Section 6 shows simulations and results. Section 7 is the summary and work proposed for future research.

2. Interdependent correlated networks

The characteristic that describe a network is its degree distribution, which is also used in [3] . The degree distribution provides important information, which is the probability that a randomly selected node has degree k. The interdependent networks mean that each individual node in each network have connections to nodes in the other network, and these bidirectional connections provide interdependency between nodes in different networks. The correlation means that for a node i, its in-degree k_i and out-degree ϕ_i are correlated.

2.1. Correlation between in-degree and out-degree

A node's in-degree k is the number of links connecting to nodes in its own network. The out-degree ϕ of a node is the number of interlinks it has that are connecting to the other network. Following [12] the correlation between a node's k and ϕ is

$$P(\phi \mid k) \sim B(\phi; m, Ck^{\alpha}), \tag{1}$$

$$P(\phi \mid k) = \binom{m}{\phi} (Ck^{\alpha})^{\phi} (1 - Ck^{\alpha})^{m-\phi}, \tag{2}$$

where the function B is the binomial, m is the number of interlinks and C is a constant. $\alpha > 0$ indicates the nodes with high degree have more interlinks; instead, $\alpha < 0$ indicates lower-degree nodes have more interlinks. For $\alpha = 0$, the interlinks are randomly allocated to each node, and the in-degree and out-degree are unrelated.