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.

2.2. Interdependency between networks

In this paper, there are two interaction modes, namely conditional interaction mode and redundant interaction mode [12]. The conditional interaction mode is similar to the case in [3], in which a node can function when the following conditions are met: (1) the node belongs to the giant connected component and (2) the node links to at least one functioning node in the other network. Nodes in the redundant interaction mode can survive when either they are locating in the giant component of their own network or they have connections to the giant component of the other network. The redundant interaction mode is useful to model the coupled networks that the elements in each network can support the other network. For instance, the communication equipments can be powered via communication cables using power over Ethernet (PoE). When a communication node's power node fails, it can still function depending on its neighbours of the communication network . Nodes in the conditional interaction mode are more vulnerable, because in order for a node to function, it must connect to both of the largest connected components of the two interdependent networks.

3. Intentional attack

In a network with size N and degree distribution $P(k)$, nodes are targeted correlating to their degree [15]. For a node i with degree k_i, the probability that it is attacked is

$$\omega_\tau(k_i) = k_i^\tau / \sum_{i=1}^{N} k_i^\tau, -\infty < \tau < +\infty. \tag{3}$$

If $\tau < 0$, nodes with a lower degree are likely to be attacked; for $\tau = -\infty$, nodes with the lowest degree are definitely targeted. However, for $\tau > 0$, nodes with higher degree is prone to being attacked; if $\tau = +\infty$, the attack is strictly targeted to the nodes with the highest degree. If $\tau = 0$, $\omega_0(k_i) = 1/N$, which means the attack is random.

An initial attack removes $(1 - p)$ fraction of nodes from a network, and the attacked nodes are selected based on Eq. (3). Links between attacked nodes and remaining nodes are kept and counted in the degree of the remaining nodes. The degree distribution of the remaining p fraction of the network is $P_p(k)$ and the number of nodes with degree k is $A_p(k)$. So,

$$P_p(k) = \frac{A_p(k)}{Np}. \tag{4}$$

If one more node is removed, the probability of removing a node with degree k is $P_p(k)k^\tau / \sum_k P_p(k)k^\tau$; the number of nodes with degree k in the remaining network is

$$A_{(p-\frac{1}{N})}(k) = A_p(k) - \frac{P_p(k)k^\tau}{\langle k^\tau(p)\rangle}, \tag{5}$$

where $\langle k^\tau(p)\rangle = \sum_k P_p(k)k^\tau$. If $N \to +\infty$,

$$\frac{d(A_p(k))}{dp} = \frac{NP_p(k)k^\tau}{\langle k^\tau(p)\rangle}. \tag{6}$$

Differentiating Eq. (4) with respect to p and using Eq. (6),

$$-p\frac{dP_p(k)}{dp} = P_p(k) - \frac{P_p(k)k^\tau}{\langle k^\tau(p)\rangle}. \tag{7}$$

When $N \to +\infty$, Eq. (7) is rigorous. Following [15,18], define $G_\tau(x) = \sum_k P(k)x^{k^\tau}$, and a new variable $t \equiv G_\tau^{-1}(p)$. The solution of Eq. (7) is:

$$P_p(k) = \frac{1}{p}P(k)t^{k^\tau}. \tag{8}$$

By differentiating $P_p(k)$ with respect to t,

$$\langle k^\tau(p)\rangle = \frac{tG'_\tau(t)}{G_\tau(t)}. \tag{9}$$

The average degree of the remaining network is:

$$\langle k(p)\rangle = \sum_k kP_p(k). \tag{10}$$

If the network's degree distribution $P(k)$ is known, t and $P_p(k)$ can be calculated. Because the nodes in the network are randomly connected, the probability that a randomly chosen in-link is attached to a remaining node equals the ratio of the

number of links that attach to the remaining network to the number of links in the original network:

$$\tilde{p} = \frac{pN\langle k(p)\rangle}{N\langle k\rangle} = \frac{p\sum_k kP_p(k)}{\sum_k kP(k)} = \frac{\sum_k P(k)t^{k^\tau}k}{\sum_k P(k)k}. \tag{11}$$

4. Percolation of a single network

According to [12,19], if we randomly choose a link in a network and select one of its ends with equal probability, the probability that following the link in the chosen direction does not reach the giant component [20] is $(1-X^0)$. The probability of reaching a node with degree k is $kP(k)/\langle k\rangle$. $P(k)$ and $\langle k\rangle$ are the degree distribution and average degree of the network, respectively. If the giant component cannot be reached by following the other $k-1$ links of the selected node, this link must lead to a finite component. Thus, X^0 is shown as the following transcendental equation:

$$X^0 = 1 - \sum_k \frac{kP(k)}{\langle k\rangle}\mathcal{G}(X^0), \tag{12}$$

where $\mathcal{G}(X^0) = (1-X^0)^{k-1}$. After solving X^0, the probability $1-S$ that a randomly selected node does not belong to the giant component can be obtained. If a node with degree k does not belong to the giant component, none of its edges can lead to the giant component. Therefore,

$$1 - S = \sum_k P(k)(1-X^0)^k. \tag{13}$$

The above equation can be rewritten as follows:

$$S = 1 - \sum_k P(k)\mathcal{H}(X^0), \tag{14}$$

where $\mathcal{H}(X^0) = (1-X^0)^k$.

5. Analytical method for two interdependent networks

5.1. Analysis for two interdependent networks

Similar to [12], this work applies the approach developed by Moore and Newman in [19] to derive the giant component of each network. The generating function technique proposed in [3] is convenient to analytically derive the components' sizes when interlinks are regularly allocated but is too mathematically complicated to be utilised in scenarios when nodes with correlated in-degree and out-degree and the redundant interaction mode.

There are two networks A and B with sizes N_A and N_B, respectively. These networks are connected by bidirectional interlinks emanating from each node. The interconnected nodes are randomly assigned. The initial attack happens to both networks, which removes $1-p_A$ and $1-p_B$ fraction of nodes. Based on Eqs. (11) and (12), after attacking network A, the probability X_A of reaching the giant component with randomly selected link changes to $\widetilde{p_A}$ times the original X_A^0 (i.e., no failure happens, $p_A = 1$). $\widetilde{p_A}$ is the probability of a link attaching to a remaining node (a remaining node refers to the node that is not attacked but may not be functioning). The node's survivability is related to both inner links and inter-connections with the other network; therefore, the equation for X_A is

$$X_A = \widetilde{p_A}\left[1 - \sum_{k_A,\phi_A} \frac{k_A P(k_A,\phi_A)}{\langle k(p)_A\rangle}\mathcal{G}(X_A, Y_A, k_A, \phi_A)\right], \tag{15}$$

where

$$P(k_A,\phi_A) = P(\phi_A \mid k_A)\widetilde{P_{pA}}(k_A). \tag{16}$$

The conditional probability $P(\phi_A \mid k_A)$ presents the correlation between a node's in-degree and out-degree from Eq. (1). This probability indicates the out-degree distribution of a node with known in-degree, so that the damage to the in-degree and out-degree of a network are analysed collectively. $\widetilde{P_{pA}}(k_A)$ and $\langle k(p)\rangle$ are the modified degree distribution and mean degree of network A, as shown in Eqs. (8) and (10). Y_A refers to the possibility that an interlink of network A connects to the giant component of network B. The probability that a randomly chosen out-link belongs to a node in network B with k_B degree

and ϕ_B interlinks is $\phi_B P(k_B, \phi_B)/\langle\phi(p)_B\rangle$. Therefore, the possibility that a node in network A links to the giant component of network B is expressed as:

$$Y_A = \widehat{p_{\phi_B}}\left[1 - \sum_{k_B,\phi_B} \frac{\phi_B P(k_B, \phi_B)}{\langle\phi(p)_B\rangle}(1 - X_B)^{k_B}\right]. \tag{17}$$

Due to the removal of nodes in network A and B, some out-links of node A may have no connections to the survival nodes in network B, and vice versa. $\widehat{p_{\phi_B}}$ is the probability that an interlink is emanated from a remaining node of network B. $\langle\phi(p)_B\rangle$ is the expected value of out-degree that network B has after the attack. Similar to Eq. (11),

$$\widehat{p_{\phi_B}} = \frac{pN\langle\phi(p)_B\rangle}{N\langle\phi_B\rangle} = \frac{\sum_{k_B} p_B k_B^{\alpha} P_p(k_B)}{\sum_{k_B} k_B^{\alpha} P(k_B)}, \tag{18}$$

$\langle\phi_B\rangle$ is the original mean of out-degree of network B. Similar equations for X_B and Y_B are

$$X_B = \widetilde{p_B}\left[1 - \sum_{k_B,\phi_B} \frac{k_B P(k_B, \phi_B)}{\langle k(p)_B\rangle}\mathcal{G}(X_B, Y_B, k_B, \phi_B)\right], \tag{19}$$

$$Y_B = \widehat{p_{\phi_A}}\left[1 - \sum_{k_A,\phi_A} \frac{\phi_A P(k_A, \phi_A)}{\langle\phi(p)_A\rangle}(1 - X_A)^{k_A}\right]. \tag{20}$$

When X_A, X_B, Y_A, Y_B are known, the fraction of functioning nodes in the giant component of both networks, denoted as S_A and S_B, can be calculated. Similar to Eq. (14),

$$S_A = p_A\left[1 - \sum_{k_A,\phi_A} P(k_A, \phi_A)\mathcal{H}(X_A, Y_A, k_A, \phi_A)\right], \tag{21}$$

$$S_B = p_B\left[1 - \sum_{k_B,\phi_B} P(k_B, \phi_B)\mathcal{H}(X_B, Y_B, k_B, \phi_B)\right], \tag{22}$$

$\mathcal{G}(\cdot)$ and $\mathcal{H}(\cdot)$ are applied to express the probability of the element being eliminated from the survival components, and they are different in conditional and redundant modes.

The initial attack on the system could result in cascading failures in each network, leaving a certain fraction S_A and S_B of original nodes that can function normally. If the attack is fatal, there will be no functioning nodes, and the values of S_A and S_B are negligible. The metric p_c is a threshold that if $p_x \leq p_c, S_x > 0, x = A, B$. Therefore, the system can survive an initial attack that remove maximum $1 - p_c$ fraction of nodes from each network. Comparing two systems, the one with lower p_c is more robust, because it can resist more serious attacks.

5.1.1. Calculate the giant component in conditional interaction mode

Malfunctioning nodes in conditional interaction mode result from losing interlinks to the giant component of its own network or the other network. The probability that a randomly selected in-link does not attach to the giant component of network A is expressed as $(1 - X_A)$. The possibility that an end node of the selected in-link, whose out-degree is ϕ_A, does not have inter-connection to the giant component of network B is $(1 - Y_A)^{\phi_A}$. These two probabilities are independent of each other. Therefore, the probability of a randomly selected link not leading to the functioning component of network A is

$$\begin{aligned}\mathcal{G}(X_A, Y_A, k_A, \phi_A) = {} & (1 - X_A)^{(k_A-1)} + (1 - Y_A)^{\phi_A} \\ & - (1 - X_A)^{(k_A-1)}(1 - Y_A)^{\phi_A}.\end{aligned} \tag{23}$$

The probability that a node with k_A in-degree does not belong to the functioning component in network A is

$$\begin{aligned}\mathcal{H}(X_A, Y_A, k_A, \phi_A) = {} & (1 - X_A)^{k_A} + (1 - Y_A)^{\phi_A} \\ & - (1 - X_A)^{k_A}(1 - Y_A)^{\phi_A}.\end{aligned} \tag{24}$$

Analogously, the probabilities for elements in network B are

$$\begin{aligned}\mathcal{G}(X_B, Y_B, k_B, \phi_B) = {} & (1 - X_B)^{(k_B-1)} + (1 - Y_B)^{\phi_B} \\ & - (1 - X_B)^{(k_B-1)}(1 - Y_B)^{\phi_B},\end{aligned} \tag{25}$$

$$\begin{aligned}\mathcal{H}(X_B, Y_B, k_B, \phi_B) = {} & (1 - X_B)^{k_B} + (1 - Y_B)^{\phi_B} \\ & - (1 - X_B)^{k_B}(1 - Y_B)^{\phi_B}.\end{aligned} \tag{26}$$

5.1.2. Calculate the giant component in redundant interaction mode

According to the definition of redundant interaction mode, nodes that fail to work should have no connection to the giant components of both networks. Therefore, the probability of a randomly selected link in network A not leading to the giant component of network A is

$$\mathcal{G}(X_A, Y_A, k_A, \phi_A) = (1 - X_A)^{(k_A - 1)}(1 - Y_A)^{\phi_A}. \tag{27}$$

The probability of selecting a malfunctioning node in network A is

$$\mathcal{H}(X_A, Y_A, k_A, \phi_A) = (1 - X_A)^{k_A}(1 - Y_A)^{\phi_A}. \tag{28}$$

Similarly, the corresponding probabilities for links and nodes in network *B* are

$$\mathcal{G}(X_B, Y_B, k_B, \phi_B) = (1 - X_B)^{(k_B - 1)}(1 - Y_B)^{\phi_B}, \tag{29}$$

$$\mathcal{H}(X_B, Y_B, k_B, \phi_B) = (1 - X_B)^{k_B}(1 - Y_B)^{\phi_B}. \tag{30}$$

5.1.3. Targeted attack based on the number of out-degree

Some interdependent networks are led by their interconnections, in which the out-degree distribution of each network is known and the in-degree of each node is correlated to its out-degree. For two interdependent networks *A* and *B*, the out-degree distributions of each network are $P(\phi_A)$ and $P(\phi_B)$. Similar to Eq. (1), the correlation between out-degree and in-degree is

$$P(k_x \mid \phi_x) \sim B(k_x; m, C\phi_x^{\upsilon}) \tag{31}$$

where the function *B* is the binomial, *m* is the number of in-links and *C* is a constant.

If an attacker intentionally removes $(1 - p)$ fraction of nodes from a network, and the node is attacked with probability $\omega_\sigma(\phi_i) = \phi_i^\sigma / \sum_{i=1}^{N} \phi_i^\sigma$. Similar to Eqs. (8) and (11), the modified out-degree distribution $P_p(\phi)$ and the probability for an out-link to belong to a remaining node are:

$$P_p(\phi) = \frac{1}{p} P(\phi) t^{\phi^\sigma}, \tag{32}$$

$$\widehat{p_\phi} = \frac{\sum_{\phi} \phi P(\phi) t^{\phi^\sigma}}{\sum_{\phi} \phi P(\phi)}. \tag{33}$$

The probability that a randomly selected in-link is attached to a remaining node is:

$$\widetilde{p} = \frac{pN\langle k(p)\rangle}{N\langle k\rangle} = \frac{\sum_{\phi} p\phi^\alpha P_p(\phi)}{\sum_{\phi} \phi^\alpha P(\phi)}. \tag{34}$$

If we randomly select an interlink and pick its end node in network *A*, the probability of the end node with ϕ_A out-degree is $\phi_A P_p(\phi_A)/\langle\phi_A\rangle$, and the probability distribution of in-degree that the end node has is $P(k_A \mid \phi_A)$. If the probability that this interlink connects to the largest connected component of the remaining network *A* is Z_A, then

$$Z_A = \widehat{p_{\phi_A}} \left[1 - \sum_{\phi_A, k_A} \frac{\phi_A P(\phi_A, k_A)}{\langle\phi_A\rangle} (1 - X_A)^{k_A} \right], \tag{35}$$

where the joint probability $P(\phi_A, k_A) = P(\phi_A)P(k_A \mid \phi_A)$. $P(k_A \mid \phi_A)$ is quantified by Eq. (31). X_A is the probability that a randomly chosen in-link of network *A* can lead to a functioning node of network *A*. The function for X_A is modified as:

$$X_A = \widetilde{p_A} \left[1 - \sum_{\phi_A, k_A} \frac{k_A P(\phi_A, k_A)}{\langle k_A\rangle} \mathcal{G}(X_A, Z_B, \phi_A, k_A) \right]. \tag{36}$$

Equations $\mathcal{G}(\cdot)$ and $\mathcal{H}(\cdot)$ are same as those in previous sections. Analogously, the probability that a randomly selected interlink leads to the giant component of network B is

$$Z_B = \widehat{p_{\phi_B}} \left[1 - \sum_{\phi_B, k_B} \frac{\phi_B P(\phi_B, k_B)}{\langle\phi_B\rangle} (1 - X_B)^{k_B} \right]. \tag{37}$$

The probability that a randomly chosen in-link of network B can lead to the functioning nodes of network B is

$$X_B = \widetilde{p}_B \left[1 - \sum_{\phi_B, k_B} \frac{k_B P(\phi_B, k_B)}{\langle k_B \rangle} \mathcal{G}(X_B, Z_A, \phi_B, k_B) \right]. \tag{38}$$

With the value of Z and X, the giant component size is derived as:

$$S_A = p_A \left(1 - \sum_{\phi_A, k_A} P(\phi_A, k_A) \mathcal{H}(X_A, Z_B, \phi_A, k_A) \right), \tag{39}$$

$$S_B = p_B \left(1 - \sum_{\phi_B, k_B} P(\phi_B, k_B) \mathcal{H}(X_B, Z_A, \phi_B, k_B) \right). \tag{40}$$

6. Simulation and results

6.1. Network model establishment

6.1.1. Generating interdependent system with known in-degree distribution

In this paper, for the sake of simplicity, the system consists of two interdependent networks with equal size $N = N_A = N_B$ and same degree distribution. These networks are interconnected via N_ϕ interlinks. Links inside each network are assigned to nodes following the predefined degree distribution $P(k) \sim k^{-\gamma}$. In order to form a network, the standard configuration model [21] is applied to connect the nodes of each network together. The number of interlinks for each network is N_ϕ, and each node has at least one interlink. Each node is assigned with one interlink at the first stage. Then, for the remaining interlinks, each one is allocated to node i with probability $k_i^\alpha / \sum_{i=1}^N k_i^\alpha$, and $C = 1/\sum_{i=1}^N k_i^\alpha$ in Eq. (1). Nodes in different networks are connected randomly by applying the standard configuration model. Using this method, the conditional probability $P(\phi_i \mid k_i)$ for node i is

$$P(\phi_i \mid k_i) = \binom{N_\phi - N}{\hat{\phi}_i} \left(\frac{k_i^\alpha}{\sum_{i=1}^N k_i^\alpha} \right)^{\hat{\phi}_i} \left(1 - \frac{k_i^\alpha}{\sum_{i=1}^N k_i^\alpha} \right)^{(N_\phi - N) - \hat{\phi}_i}, \tag{41}$$

where $\phi_i \geq 1$ and $\hat{\phi}_i = \phi_i - 1$.

6.1.2. Generating interdependent system with known out-degree distribution

Similar to generating networks with known in-degree distribution, the networks have the same size. The interlinks of nodes follow the predefined power-law distribution, and nodes in different networks are interconnected randomly. The minimum in-degree of each node is 1, and the total number of in-links is $N_{kA} = N_{kB} = N_k$. To manifest the correlation between in-degree and out-degree, each in-link is randomly assigned to a node with the probability related to its out-degree. The probability of attaching a in-link to a node i with ϕ_i out-degree is $\phi_i^\alpha / \sum_{i=1}^N \phi_i^\alpha$, so the probability that a node with ϕ_i out-degree has k_i in-degree is

$$P(k_i \mid \phi_i) = \binom{N_k - N}{\hat{k}_i} \left(\frac{\phi_i^\alpha}{\sum_{i=1}^N \phi_i^\alpha} \right)^{\hat{k}_i} \left(1 - \frac{\phi_i^\alpha}{\sum_{i=1}^N \phi_i^\alpha} \right)^{N_k - N - \hat{k}_i}, \tag{42}$$

where $k_i \geq 1$ and $\hat{k}_i = k_i - 1$. Each node in a network is connected randomly by applying the standard configuration model.

6.2. Calculating percolation threshold p_c

The survival component size are derived by Eqs. (21) and (22) when the recursive equations Eqs. (15)–(20) are solved. The correlation between in-degree and out-degree shown as the Eqs. (1) and (31) are quantified by the conditional probability $P(k \mid \phi)$ and $P(\phi \mid k)$ and joint probability $P(k, \phi)$. The percolation threshold p_c is the highest value of p that result in a negligible giant component size S_A and S_B. The threshold for negligible giant component size is set as s_n.

6.3. Out-degree oriented interdependent networks in conditional mode

In this paper, networks are generated with power-law distribution using a generalised power-law form. For out-degree oriented networks, the out-degree distribution is

$$P(\phi; \phi_{min}, \phi_{max}) = \frac{\phi^{-\nu}}{\zeta(\nu, \phi_{min}) - \zeta(\nu, \phi_{max})}, \tag{43}$$

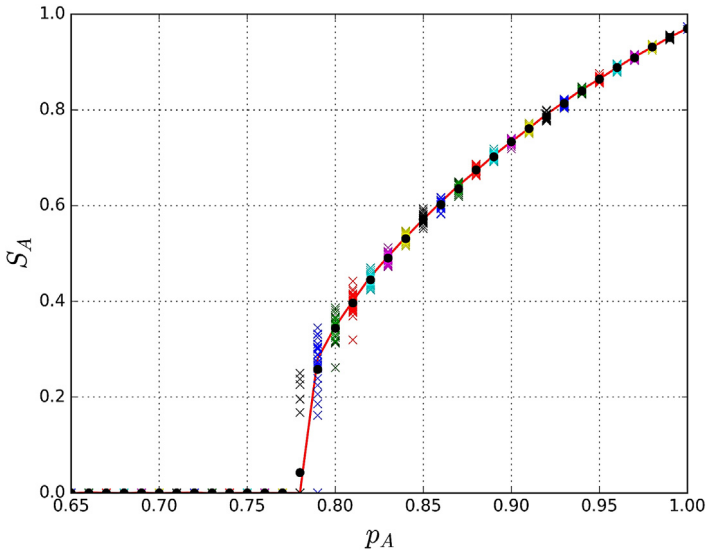

Fig. 1. Values of remaining fraction S_A for theory and simulation with given p_A when network size is 10000, $\nu = 2.5, \phi_{max} = 60, \sigma = 1, \alpha = 1$ and $p_A = p_B$. The solid line is the theoretical result, the cross symbols represent the simulation results, and the solid symbols are average results of simulations.

where ϕ_{min} and ϕ_{max} are the lower and upper limits of the out-degree fitting interval and the Hurwitz ζ function $\zeta(\nu, a) = \sum_i (i + a)^{-\nu}$. The minimum boundary is set as $\phi_{min} = 2$. The theoretical analysis applies the out-degree distribution of the generated networks without multi-edges. Due to the removal of multi-edges, there may be few nodes with degree 1. Fig. 1 shows a good agreement between the theoretical predictions and simulation results in the conditional interaction mode. The value of threshold p_c is around 0.78.

The left figure in Fig. 2 compares the values of p_c for interdependent networks with different correlation factors against attacks with various coefficient σ. Results are obtained in theoretical analysis with degree distribution Eq. (43). The intentional attack targeting the highest degree nodes is most harmful to the cases with positive out-degree and in-degree correlation (the values of p_c are greatest among all attack modes, and a greater p_c means less robustness). The reason is that the removal of nodes with high out-degree undermines the interconnectivity between two networks, which breaks the interdependency and causes the whole system to be vulnerable. Attacking nodes with low out-degree results in the least damage, when the correlation is positive. However, when the correlation $\alpha < -1$, the values of p_c for attacks targeting the low-out-degree nodes are higher. For the negative correlation, nodes with low out-degree will have high in-links. Compared with low-out-degree nodes, the nodes with high-out-degree will provide more interconnections to nodes in the other network. Thus, the high-in-degree nodes will depend on the low-in-degree nodes in the other network. Attacking the nodes with low-out-degree nodes is equivalent to the removal of high-in-degree nodes of one network. Furthermore, nodes with low in-degree in each network will be separated from the giant component, which will further affect the high-in-degree nodes in the other network. Therefore, the positive correlation improves the robustness of system under random attacks and attacks targeting low-out-degree nodes, but it is vulnerable to intentional attacks targeting high-out-degree nodes. However, the system with negative correlation is vulnerable when the attacks are launched targeting low-out-degree nodes.

Results in the right figure of Fig. 2 theoretically reveal the robustness of system with positive correlation coefficient ($\alpha = 1$) under attacks that target to high-degree nodes ($\sigma = 1$). Increasing the average in-degree of each network is a method to enhance the inner-connection of each network, which is an effective approach to improve the system's robustness. In addition, if the mean degree $\langle\phi\rangle$ is kept as a constant, a system with a narrower out-degree distribution (i.e., smaller ν) is more robust. When a network has a broader degree distribution (i.e., greater ν), there will be more low-out-degree nodes, and the maximum degree of node in the network becomes higher. Because the average in-degree $\langle k\rangle$ is fixed, nodes with low out-degree will receive few in-links and the proportion of low-in-degree nodes will increase. When the system is attacked, nodes with high out-degree and in-degree are removed, the resultant network is prone to fragmentation. For some cases, modifying ν from 2.55 to 1.9 produces better performance compared with increasing the average in-degree from 5 to 7.

6.4. In-degree oriented interdependent networks in conditional interaction mode

The in-degree distributions $P(k)$ of the interdependent networks are power-law, which are expressed as Eq. (43) with the letters of in-degree oriented networks. Fig. 3 compares the theoretical predictions of p_c of in-degree oriented networks with similar settings to those in Section 6.3. The results shown in the left figure of Fig. 3 indicate that the system is more vulnerable to intentional attack targeting nodes with high in-degree. If the correlation coefficient $\alpha = 0$, the out-links are randomly

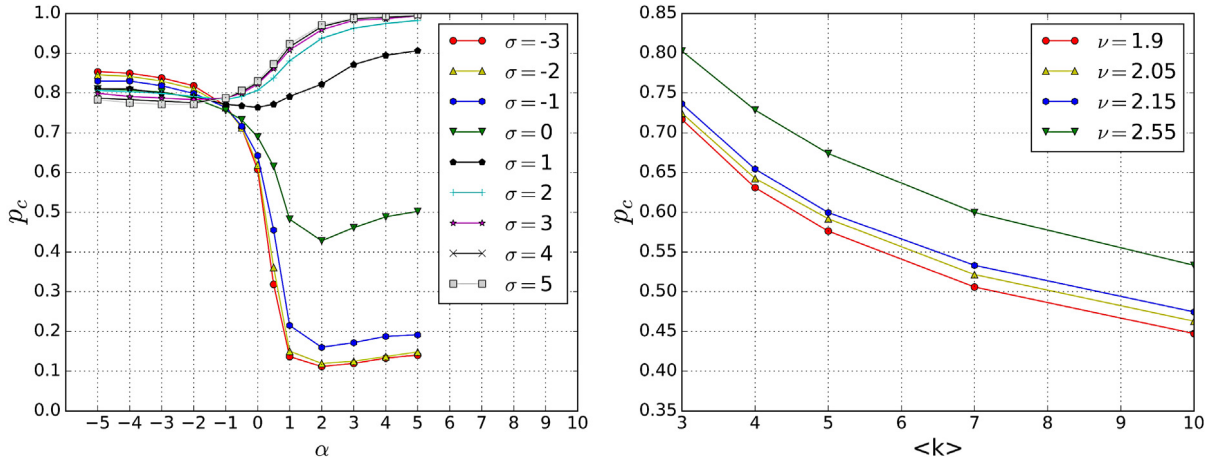

Fig. 2. Left figure: threshold p_c vs. α for $\sigma = -3$ to 5 with exponent $\nu = 2.5$, $\langle k \rangle = 3$, $\phi_{min} = 2$, $\phi_{max} = 60$, $p_A = p_B$ and $s_n = 0.1$. Right figure: threshold p_c vs. average in-degree $\langle k \rangle$ for various exponents of out-degree distribution ν with constant mean degree $\langle \phi \rangle = 4$. $\sigma = 1, \alpha = 1, \phi_{min} = 2, \phi_{max} = 13$, 16, 19 and 100 for networks with exponents $\nu = 1.9$, 2.05, 2.15 and 2.55. $p_A = p_B$ and $s_n = 0.1$.

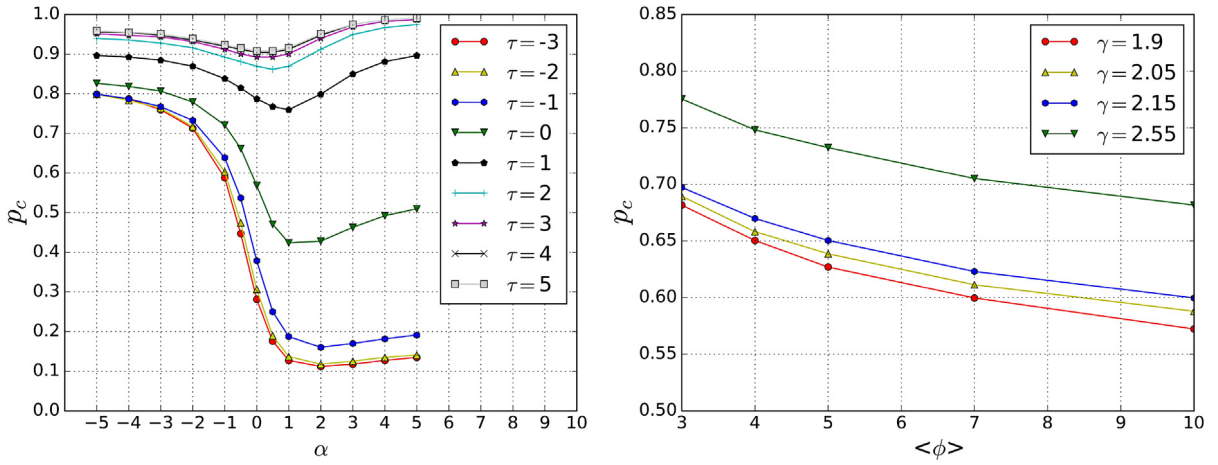

Fig. 3. Left figure: threshold p_c vs. α for $\tau = -3$ to 5 with exponent $\gamma = 2.5$, $\langle \phi \rangle = 3$, $k_{min} = 2$, $k_{max} = 60$, $p_A = p_B$ and $s_n = 0.1$. Right figure: threshold p_c vs. average out-degree $\langle \phi \rangle$ for various exponents of in-degree distribution γ with constant mean degree $\langle k \rangle = 4$. $\tau = 1, \alpha = 1, k_{min} = 2, k_{max} = 13$, 16, 19 and 100 for networks with exponents $\gamma = 1.9$, 2.05, 2.15 and 2.55. $p_A = p_B$ and $s_n = 0.1$.

assigned to each node, and the out-degree distribution follows a Poisson distribution; the system performs better than the system formed by networks generated using a negative correlation. Moreover, the results show a range of correlation value ($0.5 \leq \alpha \leq 2$), in which values of p_c for all attacks are relatively low. This analysis can be applied to identify an appropriate correlation for network design.

The right figure in Fig. 3 shows the effects of the mean out-degree and the in-degree distribution broadness on a system's robustness. Similar to the out-degree oriented system, when an in-degree oriented system suffers from intentional attacks targeting high in-degree nodes, a narrow degree distribution (small value of γ) will improve the robustness. This result complies with the study in [3] but differs from the observation in [5]. With the same mean in-degree $\langle k \rangle$, reducing broadness of degree distribution means to reduce the number of low-degree nodes and the upper bound of degree interval, which also reduces the number of nodes with low out-degree; therefore, the interlinks are enhanced.

6.5. Interdependent networks in redundant interaction mode

The system in redundant interaction mode shows better performance (as shown in Fig. 4), because the condition for a survival node is relaxed. Similar to the conditional interaction mode, positive in-degree-out-degree correlation can improve the robustness of a system when attacks are random or targeted to low-degree nodes; however, the positive correlation is vulnerable to attacks that target to high-degree nodes. Furthermore, the change of the values of p_c in this mode is flatter than the one in the conditional mode, especially for attacks that target to the nodes with low degree. When the in-degree and

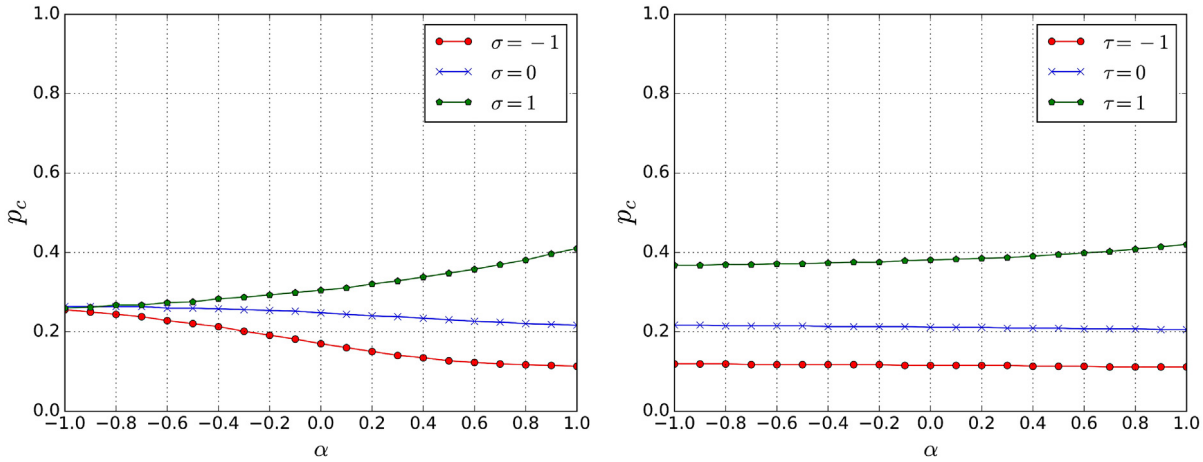

Fig. 4. Threshold p_c vs. α for redundant mode obtained from theoretical analysis $p_A = p_B$. Left: Out-degree oriented model for $\sigma = -1$ to 1 with exponent $\nu = 2.5$, $\langle k \rangle = 3$, $\phi_{min} = 2$, $\phi_{max} = 60$ and $s_n = 0.1$. Right: In-degree oriented model for $\tau = -1$ to 1 with exponent $\gamma = 2.5$, $\langle \phi \rangle = 3$, $k_{min} = 2$, $k_{max} = 60$ and $s_n = 0.1$.

out-degree correlation coefficient α is negative and the low-out-degree nodes are targeted ($\sigma > 0$), the interlinks will not suffer severe damage. Therefore, nodes disconnected from the giant component of their own network can have connections to the giant component of the other network. For the in-degree oriented model, when $\alpha < 0$ and $\tau < 0$, even though the attack will cause significant damage to the interlinks, the intra-connection of each network is not damaged seriously, and most nodes can have connection to the giant component of their own networks. Hence, compared with the system in the conditional interaction model, the system in the redundant interaction mode has higher attack tolerance.

7. Summary

We developed a theoretical model to study the robustness of interdependent correlated networks under intentional and random attacks. Moreover, we have discussed two interdependency scenarios: conditional and redundant interaction modes. When attacks target random nodes or nodes with low-degree, a system with positive in-degree and out-degree correlation outperforms the system with random and negative correlation for both conditional and redundant interaction modes. If the system suffers from intentional attacks against high-degree nodes, varying in-degree and out-degree correlation will not significantly improve the robustness. A narrower degree distribution of in-degree or out-degree (providing the average degree is fixed) enhances the robustness of the corresponding system with positive correlation when the high-degree nodes suffer from intentional attacks.

More scenarios can be analysed using this technique to help design and research the interdependent networks based on either in-degree or interlinks. This research can be further extended to systems considering assortative mixing [22] and partial interdependency. Moreover, when the condition for a component's survivability is relaxed to be larger than a specified size [23], the intentional attack strategy and protection scheme can be further studied.

Acknowledgments

This work was partly supported by Data61, CSIRO, Australia, and the ARC Discovery Grant (DP170103427).

References

[1] G. Chen, Z.Y. Dong, D.J. Hill, G.H. Zhang, An improved model for structural vulnerability analysis of power networks, Physica A 388 (19) (2009) 4259–4266.
[2] G. Chen, Z.Y. Dong, D.J. Hill, G.H. Zhang, K.Q. Hua, Attack structural vulnerability of power grids: A hybrid approach based on complex networks, Physica A 389 (3) (2010) 595–603.
[3] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nat. 464 (7291) (2010) 1025–1028.
[4] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, R. Setola, Modelling interdependent infrastructures using interacting dynamical models, Int. J. Crit. Infrastruct. 4 (1–2) (2008) 63–79.
[5] S.V. Buldyrev, N.W. Shere, G.A. Cwilich, Interdependent networks with identical degrees of mutually dependent nodes, Phys. Rev. E 83 (1) (2011) 016112.
[6] J. Shao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Cascade of failures in coupled network systems with multiple support-dependence relations, Phys. Rev. E 83 (3) (2011) 036116.
[7] J. Gao, S.V. Buldyrev, H.E. Stanley, S. Havlin, Networks formed from interdependent networks, Nat. Phys. 8 (1) (2012) 40–48.

[8] O. Yagan, D. Qian, J. Zhang, D. Cochran, Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness, IEEE Trans. Parallel Distrib. Syst. 23 (9) (2012) 1708–1720.
[9] M. Parandehgheibi, E. Modiano, Robustness of bidirectional interdependent networks: Analysis and design, 2016. ArXiv Preprint arXiv:1605.01262.
[10] L. Liu, J. Ma, Z. Dong, G. Chen, K.P. Wong, Influence of enhanced interconnecting links on cascading failures in smart grid, in: 2015 IEEE Power & Energy Society General Meeting, IEEE, 2015, pp. 1–5.
[11] D. Zhou, J. Gao, H.E. Stanley, S. Havlin, Percolation of partially interdependent scale-free networks, Phys. Rev. E 87 (5) (2013) 052812.
[12] S.D. Reis, Y. Hu, A. Babino, J.S. Andrade Jr., S. Canals, M. Sigman, H.A. Makse, Avoiding catastrophic failure in correlated networks of networks, Nat. Phys. 10 (10) (2014) 762–767.
[13] R. Parshani, S.V. Buldyrev, S. Havlin, Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition, Phys. Rev. Lett. 105 (4) (2010) 048701.
[14] S. Xiao, G. Xiao, T.H. Cheng, Tolerance of intentional attacks in complex communication networks, IEEE Commun. Mag. 46 (1) (2008) 146–152.
[15] X. Huang, J. Gao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Robustness of interdependent networks under targeted attack, Phys. Rev. E 83 (6) (2011) 065101.
[16] Z. Huang, C. Wang, A. Nayak, I. Stojmenovic, Small cluster in cyber physical systems: network topology, interdependence and cascading failures, IEEE Trans. Parallel Distrib. Syst. 26 (8) (2015) 2340–2351.
[17] X. Huang, I. Vodenska, S. Havlin, H.E. Stanley, Cascading failures in bi-partite graphs: model for systemic risk propagation, Sci. Rep. 3 (2013).
[18] J. Shao, S.V. Buldyrev, L.A. Braunstein, S. Havlin, H.E. Stanley, Structure of shells in complex networks, Phys. Rev. E 80 (3) (2009) 036105.
[19] C. Moore, M.E. Newman, Exact solution of site and bond percolation on small-world networks, Phys. Rev. E 62 (5) (2000) 7059.
[20] M. Newman, Networks: An Introduction, Oxford University Press, 2010.
[21] S.N. Dorogovtsev, Lectures On Complex Networks, Vol. 24, Oxford University Press Oxford, 2010.
[22] M.E. Newman, Assortative mixing in networks, Phys. Rev. Lett. 89 (20) (2002) 208701.
[23] M. Di Muro, S. Buldyrev, H. Stanley, L. Braunstein, Cascading failures in interdependent networks with finite functional components, Phys. Rev. E 94 (4) (2016) 042304.