Hindawi
Complexity
Volume 2020, Article ID 2363514, 17 pages
https://doi.org/10.1155/2020/2363514

*Review Article*

# A Survey on Frameworks Used for Robustness Analysis on Interdependent Networks

**Ivana Bachmann**,[1,2] **Javier Bustos-Jiménez**,[1] **and Benjamin Bustos**[2]

[1]*Niclabs, University of Chile, Blanco Encalada 1975, 8370403 Santiago, Chile*
[2]*Millennium Institute for Foundational Research on Data (IMFD), Department of Computer Science, University of Chile, 8370456 Santiago, Chile*

Correspondence should be addressed to Ivana Bachmann; ivana@niclabs.cl

Received 21 August 2019; Revised 10 November 2019; Accepted 19 December 2019; Published 29 April 2020

Academic Editor: Ana Meštrović



The analysis of network robustness tackles the problem of studying how a complex network behaves under adverse scenarios, such as failures or attacks. In particular, the analysis of interdependent networks' robustness focuses on the specific case of the robustness of interacting networks and their emerging behaviors. This survey systematically reviews literature of frameworks that analyze the robustness of interdependent networks published between 2005 and 2017. This review shows that there exists a broad range of interdependent network models, robustness metrics, and studies that can be used to understand the behaviour of different systems under failure or attack. Regarding models, we found that there is a focus on systems where a node in one layer interacts with exactly one node at another layer. In studies, we observed a focus on the network percolation. While among the metrics, we observed a focus on measures that count network elements. Finally, for the networks used to test the frameworks, we found that the focus was on synthetic models, rather than analysis of real network systems. This review suggests opportunities in network research, such as the study of robustness on interdependent networks with multiple interactions and/or spatially embedded networks, and the use of interdependent network models in realistic network scenarios.

## 1. Introduction

To ensure the proper functioning of networks, such as communication networks, electric networks, and transportation networks, we need to have complete knowledge about how these networks work, what their vulnerabilities are, and how these vulnerabilities can be corrected. However, real-world networks do not exist in isolation, but rather interact with other networks. This can be seen on power grid networks interacting with their control network [1], transportation networks where the bus network interacts with the subway network [2], interdependent cyber-physical supply chain networks [3], etc. Thus, to study interactions between different network systems is of special interest, as network vulnerabilities depend on the interactions that the network studied has with other systems, and these dependencies can induce new vulnerabilities not present in single networks [4]. Indeed, big failures due to the interactions of networks have already occurred in the past, such as the Italy blackout of 2003, where a large portion of the country lost power supply, generating further degradation of services such as the railway networks, communication networks, and healthcare systems [5].

In the complex network field, the *interdependent network* area studies the interactions among different networks, while the ability of a network to resist disturbances or failures is referred to as the *robustness* of the network. Thus, to study network robustness from an interdependent network system's perspective, we need to define what it means to be a robust interdependent network system and, given the nature of the system, how the robustness should be measured. To answer these questions, we look at the existing frameworks to study the robustness of interdependent networks.

Several frameworks have been developed to study the robustness of interdependent network systems to better understand complex networks' vulnerabilities. These frameworks may present different interdependent network system models, with different kinds of elements and interactions. For example, the kind of interaction between two networks can be between nodes, edges, or both. These interactions can differ among different interdependent networks, given the networks' behaviour and the way in which these networks interact with one another. A common example is given by the power grid paired with its control network system [1, 4]. Here, we have nodes within the communication network that require energy to properly function, and thus they depend on power grid nodes. Conversely, depending on the model used, some nodes in the power grid depend on the communication network nodes to access the necessary data to the their proper functioning.

These frameworks must also present a way to measure the robustness of the system. The robustness of a network can be measured using one or more robustness metrics that focus on aspects or characteristics relevant to assess the robustness of the system. A robustness measure may be centered on the size of the largest or giant connected component [6–8], the percolation threshold [9], etc.

Besides the robustness measure, frameworks usually perform a variety of studies to better understand the tested scenarios. To perform these studies, the framework tests different model parameters of the interdependent system being studied and measures the effect of these changes over the interdependent network robustness. Some parameters that can be used to perform studies are the kind of failure [10], the node capacity [2], the attack radius [11], etc.

The development of frameworks to study the robustness of interdependent networks is relatively new, starting in 2010 with Buldyrev et al. [4], and has slowly grown over the past few years. In recent years, several types of frameworks have appeared, going from simple and general frameworks, to more complex and specific ones.

It is important to have specific frameworks for the interdependent network case, as they allow us to describe scenarios that would not occur when studying the robustness of single networks. Frameworks also allow us to simplify the analysis process, as they provide a systematic way to study the robustness of interdependent networks.

Currently, there is no easy way to order and classify the methods used to assess the robustness of interdependent network systems. Surveys in the complex network area have not focused on the robustness of interdependent networks. Also, most of the information regarding the study of interdependent networks' robustness has not been unified. This situation has led to the usage of several different names for the same metrics, models, and studies among the literature, or even the lack of names for widely used measures, models, and studies. In this work, we present an approach to solve these problems by surveying frameworks to study the robustness of interdependent networks.

This survey gathers and classifies through a taxonomy the existing frameworks to study the robustness of interdependent networks. The articles collected for this survey must present frameworks to study the robustness of interdependent networks. It was considered that an article presented a framework to study the robustness of interdependent networks if it explicitly analyzed the robustness of two or more interacting networks that depend on one another. The articles included in this survey must also test the proposed framework using real and/or simulated data. For this survey, we only considered articles published between 2005 and 2017 on at least one of the following libraries: APS, Elsevier, PLOS ONE, Nature, ACM Digital Library, and IEEE Xplore (see more details in Section 2). Articles that did not explicitly use a known robustness measure or specify that the measures studied could be interpreted as robustness measures were not considered. To classify the information about the frameworks, the following aspects were studied: the way in which the interdependent networks are modeled, how the robustness is measured, the studies performed to further understand the scenario, and the type of networks used to test the framework.

Our research contributes with a novel approach as an interdependent network survey, focusing specifically on robustness studies. Although there are surveys and reviews of the interdependent network, multilayer network, and multiplex network area, none of these has focused on how to study the robustness of these systems [12–14]. In this survey, we propose a taxonomy that allows the reader to identify many different possible frameworks, based on the main aspects defining an interdependent network's robustness framework. The presented taxonomy takes into account the different reoccurring themes identified during the in-depth review of each article considered in this survey.

In this research, we found that studies of robustness of interdependent networks still mainly focus on rather abstract models that can be used in several types of scenarios if real-world constraints are relaxed. Here, we found that the most commonly used models are those of the "one to one like" family, while the most commonly used metrics are those that count the amount of functional nodes after a cascading failure has occurred. We also found that studies of the size of the giant connected component were the most widely performed and that most of the frameworks were tested using purely simulated data.

The rest of the article is organized as follows. Section 2 explains the methodology used for the article collection, and how we proceeded to determine which papers would be considered in the final taxonomy. Section 3 presents the findings of this survey as a taxonomy. Section 4 summarizes our findings, Section 5 presents the discussion, and Section 6 presents our conclusions and thoughts about future work. In Supplementary Materials (available here), we present a summary of each article reviewed according to the taxonomy proposed and summary tables of articles reviewed and the classifications of our taxonomy.

## 2. Method

To collect the articles that we used in this survey, we opted for a systematic review approach. This systematic review was

performed using Kitchenham's protocol [15] as guideline. In the following sections we present a detailed explanation of the collection, selection, and data extraction process followed for this survey.

*2.1. Background and Objective.* Given the problem of analyzing the robustness of interdependent networks, we would like to answer the following question: *what frameworks exist to study the robustness of interdependent networks?* As far as we know there are no systematic reviews or surveys tackling this question.

This systematic review has as objectives to identify and describe frameworks to study the robustness of interdependent networks and to generate a detailed characterization of these frameworks regarding the usage of models, techniques, and metrics, among other aspects that were to be found relevant for framework characterization.

*2.2. Research Questions.* In this section, we list the research questions that drive this review. These questions were applied to each article studied. For the proper data analysis, each of the following questions was further broke down into subquestions; this is further explained in Section 2.8.

(i) RQ1: which networks' aspects are studied by the framework?

(ii) RQ2: how is the model used by the framework?

(iii) RQ3: how was the framework validated?

*2.3. Data Collection Strategy.* The articles used in this review were collected on the following repositories: APS, Elsevier, PLOS ONE, Nature, ACM Digital Library, and IEEE Xplore. These repositories were selected with the intention of covering most of the publications in the complex network area.

On each repository, the same base query was made to collect the papers considered in this review. We show the query in Figure 1. Here, the logical operators *AND*, *OR*, and *NOT* are used to show the structure of the search query. This query was specifically made over article's titles and abstracts.

This query can be understood as "to search articles that refer to robustness and interdependent networks and that do not refer to neural networks." The actual queries used on each library are listed in Table A.4 in the Supplementary Materials (available here).

With this query, we are considering the definition of interdependent networks to be "systems composed of two or more interacting networks; two networks are said to be interacting with one another if they have some type of dependency between node pairs where each node belongs to a different network." Thus, we considered the following keywords and keyphrases on their title or abstract for the initial collection: "interdependent network(s)," "multilayer network(s)," "multi-layer network(s)," "cascading failures," and "network of networks." Here, the keyphrase "cascading failures" was added in hopes to find articles that did refer to interdependent networks without explicitly using any of the other keyphrases as cascading failures do appear on interdependent networks.

We consider that an article discusses the robustness topic if it refers to the behaviour of a network under adverse scenarios. Thus, we considered the following keywords on their title or abstract for the initial collection: "percolation," "robustness," and "resilience."

Finally, we observed that the keyword "neural networks" tend to appear when searching for the abovementioned keywords and keyphrases; however, these articles do not discuss interdependent networks as we have defined here, we opted for excluding articles that refer to neural networks. Thus, we discarded when possible articles with the keyword "neural" appeared on their title or abstract.

*2.4. Selection Criteria.* After the data collection, we must select which articles will be reviewed in the final systematic review. In order to do this, the following inclusion and exclusion criteria were applied:

(i) Inclusion criteria

  (a) The paper is written in English
  (b) The paper is a primary study
  (c) The paper was published between January 2005 and December 2017
  (d) The paper studies the robustness on interdependent networks
  (e) The paper presents conclusions about the framework

(ii) Exclusion criteria

  (a) The paper is not available online
  (b) The paper does not study the robustness on interdependent networks
  (c) The paper is nonconclusive
  (d) The paper does not test the framework using real or simulated data
  (e) The paper is a survey

*2.5. Selection Process.* Once the initial collection of articles was done, another selection process is performed in order to ensure that the articles considered in the final taxonomy actually meet the previously stated requirements. For this next selection process, two researchers have to apply the inclusion and exclusion criteria over each article found. This is done by reading the title and abstract of each article and determining if they meet the selection criteria. If there was to be a tie on the inclusion or exclusion decision for an article, a third researcher has to read and apply the selection criteria over that article. An article passes to the data extraction stage if at least two researchers agree that the article passes the selection criteria.

Table 1 shows the amount of articles initially found on each repository and how many articles were finally considered for this survey. It is worth noting that no article appeared on more than one repository.

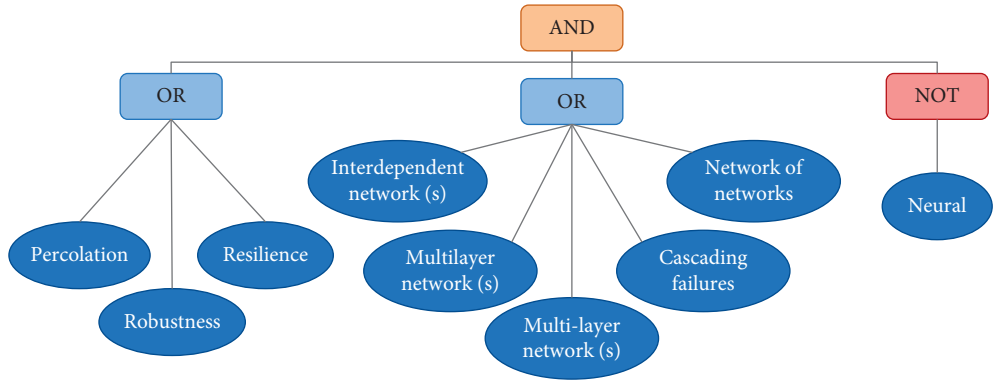


Figure 1: Query diagram.

Table 1: Number of papers by repository and stage.

| Repository | Number of articles on the initial collection | Number of articles on the final survey |
|---|---|---|
| Elsevier | 221 | 28 |
| PLOS One | 24 | 3 |
| ACM | 18 | 2 |
| Nature | 151 | 19 |
| IEEE Xplore | 95 | 27 |
| APS | 44 | 24 |
| Total | 553 | 103 |

*2.6. Quality Assessment.* To ensure the articles' quality, the following questions have to be positively answered by each article found. If an article passes the first selection process but fails to meet the minimum quality determined by the quality assessment process then it is discarded, and thus it is not considered on the final survey.

(i) Is the paper topic properly described?

(ii) Is the framework described in detail?

(iii) Is the model used by the framework properly described?

(iv) Does the paper show results and conclusions?

(v) Are the results shown by the paper concrete and complete?

*2.7. Data Extraction.* In this stage, we collected data that can be extracted without having to analyze in depth the article's content. From each article, we extracted the following data: library, authors and their affiliation, year of publication, type of publication (journal or proceedings), and abstract.

*2.8. Data Analysis.* In contrast with the last step, here an in-depth reading and analysis has to be performed in order to fully understand the contents of the article under revision. Using the information obtained from this in-depth analysis, the final classification or taxonomy emerges. We must note that to the best of the authors' knowledge, there is no previously proposed taxonomy for the area dedicated to the study of robustness of interdependent networks.

In order to perform an exhaustive data analysis, the following research question breakdown was used as a guideline (see Table 2).

## 3. Taxonomy

After analyzing the literature studying the robustness of interdependent networks, a thorough study of it was performed. From that study we identified relevant framework aspects. In Supplementary Tables A.5, and A.6, we have a summary of the model, metric, studies, and networks tested classifications. The details of each aspect are presented in the corresponding sections.

In Section 3.1, frameworks are classified by the kind of model used by such a framework. In Section 3.2, frameworks are classified by the kind of robustness measure used by such a framework. In Section 3.3, frameworks are classified by the kind of studies performed by the framework. Finally, in Section 3.4, frameworks are classified by the kind of networks used to test the framework.

*3.1. Interdependent Network Model.* Each framework must use an interdependent network model, in which the interactions between nodes are defined. The interactions defined by the model may be between nodes within the same network, or from different networks, and these interactions can determine the behaviour and characteristics of nodes and edges. The model used by a specific framework reflects the kind of networks that it studies. Some models will be applicable to more general networks, while some others will be applicable to more specific networks. According to the papers studied for this review, 11 classifications of

Table 2: Research question breakdown (the research questions (RQ) are presented in Section 2.2).

| RQ | Question | Possible answer |
|---|---|---|
| RQ1.1 | What studies does the framework perform? | Study name |
| | | Study description |
| RQ1.2 | What robustness measures are used? | Robustness measure name |
| | | Interpretation of the robustness measure values |
| RQ1.3 | What network parameters does the framework measure? | Set of parameter used by the measure |
| RQ1.4 | What assumptions does the framework do? | List of assumptions made by the framework |
| RQ2.1 | The framework proposes a model or uses an existing one? | { *proposes a model*, *uses an existing one*} |
| RQ2.2 | How is the model studied? | Name of the model |
| | | Model description |
| RQ2.3 | Does the model describe especial nodes and edges? | { *yes*, *no*} |
| | | Kind of nodes and description |
| | | Kind of edge and description |
| RQ2.4 | How are the interactions described by the model? | { *directed*, *nondirected*, *both*} |
| | | Description of the interactions between nodes within a network |
| | | Description of the interactions of the nodes between different networks |
| RQ3.1 | What data were used to obtain the results? | { *simulated*, *real*, *both*} |

interdependent network models were identified. Here, we list each classification, and between parenthesis we show the amount of articles within each one of them: "one to one like" (49), "geometric or spatially embedded" (12), "multiple dependencies" (15), "coupled power grid" (9), "load transfer among networks" (6), "mixed interactions" (6), "mapping" (2), "directed support-dependency" (2), "contagion or influence" (2), "supply-chain" (1), and "defined by probabilities" (2).

The "one to one like" classification contains the models whose main characteristic is that the interactions among networks are one to one with bidirectional dependencies, that is, each node can be connected to exactly one other node in the other network, through a nondirected interlink. If a node fails, then its dependent node will also fail and vice versa. The models within this classification usually present two interacting networks. They do not present interactions between nodes of the same network, and each node on both networks is interconnected through an interlink [4, 10, 16–42]. However, some models do study the case in which there are more than two interacting networks [43–45], or present variations on the behaviour within the network. Among these, we find models that have loads and capacities that can trigger further failure if the load of a node or edge exceeds its capacity due to load redistribution in case of failure [46–51], models where the distances from a node to a control node is relevant to establish connections [52], or models that explore the "average lifetime" of a node after which the node fails [53]. Following a similar idea, Stippinger et al. [54] introduced the concept of "recovery" on a one to one like model. Here, nodes have a probability of reestablishing their connections after losing them. Radicchi et al. [55] used a model with edge weights that affect the percolation phase transition of the system. There are also one to one like models where each node can be connected to at most one other node in the other network [16, 18, 45, 56–61]. Liu et al. [62] presented a case where if a node fails, then its counterpart may lose its edges with some probability. Here, the worst case scenario is the one where all the edges are lost, which is equivalent to the original one to one like model. It is worth noting that in this classification, we also consider multiplex networks whose main characteristic is to be multiplex networks where the failure of a node in any layer means that the node fails in each network [28, 51].

"Geometric or spatially embedded" models are characterized for representing an environment with a "spatial context," meaning that nodes can have a relative or absolute position in space, and this position in space influences whether a pair of nodes get to be connected or not [11, 29, 63–66]. A common model among this classification is the one built using two lattices and one to one like interactions with spatial restrictions to connect two nodes on different networks [11, 29, 63–65, 67]. There are some variations to this last model, such as a model that allows more than two networks to be interconnected [68], a model that considers network "lifetime" [69], a model that uses lattices with an arbitrary number of dimensions [70], or systems where nodes have states that can be propagated over the networks [71]. In the work presented by Kornbluth et al. [66], networks are topologically identical, and two nodes from different networks can be connected if the path length between the topological counterparts of both nodes within a network meets the length restriction. Finally, in the work of Wang et al. [72], nodes from all networks are located within a Euclidean space, and two nodes from different networks are connected if they meet the spatial restrictions.

One main characteristic of "multiple dependencies" models is that the nodes can be interconnected to multiple nodes on other networks. Among these models, we find those with directed support-dependency relations among networks, where a node remains functional if at least one of its supporting nodes in other networks remains functional [16, 73–77], and directed support-dependency relations with node states where a node must also be on an "active" state to remain functional [78]. In this classification, we can find models where the support-dependency relations between nodes from different networks are undirected. Here, just as the directed case, a node remains functional if at least one of its supporting nodes in other networks is functional, but in

this case, supporting nodes are supported by their dependent nodes [18, 79–82]. Among these kinds of models, we find variations such as models that have loads and capacities within the networks [75, 76], models that represent supply-demand dynamics [83], and models where each node requires a specific amount of supporting nodes [84, 85].

For the "coupled power grid" classification, we have models that represent the power grid network coupled to some other network. Most of the models within this classification represent the power grid coupled with its control network. For the "power grid-control network" pairs, the models contain a representation of the power grid and a representation of the control network that supervises the proper functioning of the power grid network (control network or supervisory control and data acquisition). The control network model usually distinguishes between the nodes that represent information sources and the nodes that distribute this information. Among the models that represent the "power grid-control network" pair, there are those whose nodes and edges have loads and capacities, which can get damaged due to overload failures [6, 7, 86–88] and those that do not have loads and capacities [1, 89, 90]. Only one model was found to represent the power grid coupled to another kind of network in the work of Ouyang et al. [91]. Here, the power grid is coupled to the gas distribution network, which depends on the electric supply of the power grid to properly function.

On the "load transfer among networks" classification, a total of 6 articles were found [2, 92–96]. The main characteristic of these models is that the nodes and/or edges have a capacity and a load, where if a node fails, then the load of that node is redistributed within and among networks. It is interesting to notice that a real-world application of these models is presented by Zhao et al. [2], where the system is comprised of the bus network and the subway network, while the passengers represent the network load.

For the "mixed interactions" classification, six articles were found [97–102]. The main characteristic of these models is that there may be more than one type of interaction among them [97, 98, 100, 102] or within them [101]. In this type of model, there are different types of edges, and the type of edge defines what happens to the neighbors of a node when it fails. For the interactions, we may have connectivity and dependency edges [97–99, 101, 102] or dependent and antagonist edges [100]. In this context, an antagonistic relationship between nodes means that losing the antagonistic counterpart has a positive effect over the nodes.

The "mapping" classification contains models that represent network pairs where one network must be "mapped" or "routed" onto other networks [103, 104]. Thus, the mapped network depends on the structure of the other network and the way in which the mapping is done.

On the "directed support-dependency" classification, we find models whose main characteristic is to have support-dependency relations between network pairs. Here, it is clear which node offers support and which node is dependent [105, 106]. If the support node fails, then the dependent node will necessarily fail. However, if the dependent node fails, then the support node will not necessarily fail.

The "contagion or influence" classification contains models whose objective is to model an influence or contagion process within an interdependent networks system. In this revision, two articles were found [107, 108].

Finally, the models classified into the "defined by probabilities" classification are those whose behaviour (dependencies, failures, recoveries, etc.) is defined through probabilities. Two articles were found within this classification [109, 110].

The "supply-chain" classification contains models whose main characteristic is to represent supply chain networks systems. Within this classification, we found a model composed of a physical supply chain network (supplier, distributor, etc.) and a cyber network that represents the digital control system of the supply chain [3].

*3.2. Kind of Robustness Metric Used.* Frameworks can use a variety of metrics to study the robustness of a network. A framework may use one or more metrics to measure the interdependent networks robustness. The metrics used by a framework to measure robustness determine which aspects are relevant for the framework when defining what a robust network is. In this study, 8 metric classifications were identified. Here, we list each classification, and between parenthesis we show the amount of articles within each one of them: "counting elements" (77), "breaking point" (44), "time" (14), "probability" (13), "rate" (3), "cost" (3), "path length" (4), and "performance" (1).

"Counting elements" metrics measure the amount of elements relevant for the robustness, such as the amount of nodes on the largest connected component. In this classification, we also include metrics that extract a value from the amount of elements being counted, such as the average amount of neighbors of a node. Within these metrics, we distinguish between those who measure the amount of nodes that remain functional after a failure or attack (and subsequent cascading failure) [3, 6, 7, 10, 16–21, 23–26, 28, 30, 34–48, 51, 54, 56, 58, 60, 62, 63, 66–68, 71, 72, 77–84, 89, 90–92, 102, 105, 106], those who measure the amount of functional nodes on a recovery process [22, 57], and those that measure the amount of redundant paths of a network onto the network it was mapped on [104] (see Section 3.1).

The "breaking point" classification considers metrics that measure the point at which the interdependent system will collapse. These metrics, for example, could measure the amount of nodes or edges to be removed in order for the networks to collapse, the expected lifetime before collapse, etc. For interdependent networks, the collapse of the system is abrupt once the "breaking point" is reached. Within this classification, we have metrics that measure the amount of nodes that can be removed before collapse [4, 11, 19, 21, 24, 25, 43, 44, 62, 65–67, 73, 79, 80, 83, 84, 97–99, 105, 1, 31, 38, 39, 41, 45, 54, 55, 61, 68, 70, 71, 77, 78, 106],

metrics that measure the critical amount of edges to disconnect [1, 32], metrics that measure how strongly coupled the interdependent networks can be [68, 73, 105], metrics that measure the expected time before collapse [53, 69], and metrics that measures the threshold at which an infection will persist on the networks for a long time [108].

The "time" classification contains metrics that measure the time that a process takes, where this process is relevant for the robustness. Here, the duration of these processes determines how robust (or fragile) the network is under adverse scenarios. Among the reviewed articles, there are metrics that measure the amount of iterations that a cascading failure takes [19, 20, 24, 29, 40–43, 61, 64, 65, 68, 73], the time before a user loses access to the service provided by the interdependent network system [103], and the average delay time of the system [104].

Within the "probability" classification, we have metrics that measure robustness according to how likely that an event is to occur, where this event is relevant for the robustness of the system. Some of these metrics measure how likely it is that a giant mutually connected component exists within the interdependent networks system [4, 23, 29]; others measure how likely it is that a node is still connected to the largest connected component [27, 31], that two nodes are connected with one another [33, 42, 52], how likely a node is to survive a contagion [107], or the probability that more than half of the original nodes survive [88]. Other metrics measure the distribution function of the largest connected cluster size [70] or the distribution function of the load shedding [86], while others measure how reliable the interdependent networks are, given the probability distribution of the cascading failure size [110].

The "rate" classification contains metrics that measure how a specific characteristic behaves in relation to some other characteristic, such as growing rates or derivatives. Here, we found a metric that measures the amount of failed nodes per iteration of the cascading failure [63], a metric that measures the increase rate of failed nodes between consecutive iterations [40], and a metric that is the derivative of the size of the largest connected component respect to the fraction of nodes removed of one of the networks of the interdependent network system [72].

Metrics on the "cost" classification measure how expensive it is to increase the robustness of the system [75, 76, 104]. This can be attained by adding nodes or edges, by changing node dependencies, etc.

On the "path length," metrics measure how well connected the networks are, given the path lengths between nodes [2, 10, 22, 59]. Here, the shorter the path lengths, the more robust the system is considered to be.

Finally, the "performance" classification, as its name suggests, contains metrics that measure the performance of the interdependent network system. Here, the performances must be measured in comparison to an ideal system. In particular, what an ideal performance is will depend on the nature of the interdependent system. Only one metric was found for this classification [91].

*3.3. Studies Performed by the Framework.* Another way to characterize frameworks is by the type of studies that they perform to further understand the robustness of the interdependent network system. Besides the metrics used by the framework, each framework can perform several studies. These studies usually observe the impact of altering variables, over the robustness. From the articles reviewed, 8 main classifications were identified. Here we list each classification, and between parenthesis we show the amount of articles within each one of them: "size of the giant connected component" (58), "coupling" (55), "percolation" (47), "targeted attacks" (27), "load and capacity" (17), "cascading time" (12), "length" (8), and "avalanche" (8). To see the rest of the classifications found, see Supplementary Table A.7.

On the "size of the giant connected component" classification, we have frameworks that studied the changes on the size of the largest connected component under different conditions. This type of study can be the main focus of the framework or complementary information of the robustness of the interdependent networks system. A total of 58 articles performed this type of study [3, 4, 6, 10, 16–21, 23, 24, 26–28, 34–41, 44, 45, 46, 48, 51, 53, 54, 56, 58–62, 64, 69, 70, 72, 77–82, 84, 89, 92, 95, 96, 97, 98, 100, 101, 102, 106].

The "coupling" classification contains frameworks that studied the effect that different types of couplings have over the robustness of the system. In the interdependent network context, the coupling refers to how are the networks coupled with one another. Usually, these studies change the coupling strength or the coupling criteria. The "coupling strength" refers to the amount of interconnections that there are between networks, while the "coupling criteria" refers to the criteria used to determine when two nodes in different networks are connected. Some coupling criteria examples are as follows: to couple high degree nodes with low degree node nodes, to couple nodes with the same degree, to couple nodes at random, etc. A total of 54 articles performed coupling studies [17, 18, 21–23, 26, 27, 43, 46, 57, 64, 65, 73, 79, 80, 84, 86, 87, 92, 97, 98, 105, 7, 32–34, 45, 58, 62, 67, 68, 71, 76–78, 81, 88, 90, 100, 101, 106, 35–37, 48–51, 59–61, 94–96].

It is considered that a framework performed "percolation" studies if it studied the percolation threshold of the system or if it studied measures based on percolation theory [9]. In the context of percolation studies, $1 - p$ is the probability that a node gets disconnected from its network or fails. The percolation threshold, typically denoted by $p_c$, represents the critical value at which if $p < p_c$, then it is not possible to identify a giant connected component on the networks system. Here, the lower the $p_c$ value, the more robust the system is considered to be, as this implies a higher $1 - p_c$ value. The robustness interpretation of this metric is that a lower $p_c$ means that it is possible to disconnect a higher amount of nodes before reaching the system's collapsing point. When studying the percolation of an interdependent system, first- and second-order phase transitions may occur. Second-order phase transitions represent a continuous decay of the system where no abrupt collapse can be detected. Second-

Table 3: Amount of papers published per year.

| Year | Amount of papers published | % of papers published in journals | % of papers published in proceedings | Relative % of papers published |
|---|---|---|---|---|
| 2005 | 0 | 0 | 0 | 0 |
| 2006 | 0 | 0 | 0 | 0 |
| 2007 | 0 | 0 | 0 | 0 |
| 2008 | 0 | 0 | 0 | 0 |
| 2009 | 0 | 0 | 0 | 0 |
| 2010 | 2 | 100 | 0 | 1.9 |
| 2011 | 3 | 33.3 | 66.7 | 2.9 |
| 2012 | 3 | 100 | 0 | 2.9 |
| 2013 | 13 | 69.2 | 30.8 | 12.6 |
| 2014 | 14 | 85.7 | 14.3 | 13.6 |
| 2015 | 19 | 89.5 | 10.5 | 18.5 |
| 2016 | 25 | 84 | 16 | 24.3 |
| 2017 | 24 | 70.8 | 29.2.4 | 23.3 |

order phase transitions are characteristic of single or isolated networks. First-order phase transitions represent an abrupt collapse of the system as $1 - p$ increases. First-order phase transitions usually appear on interdependent networks systems. A total of 47 articles performed percolation studies [4, 6, 11, 19, 20, 23–25, 29–31, 34, 38–45, 54, 57, 58, 61, 62, 64–68, 70, 71, 73, 77–80, 83, 84, 89, 96–101, 105, 106].

The "targeted attacks" classification contains all the frameworks that test the effect of targeted attacks over the system's robustness. In this context, a node or edge attack is a targeted attack if a specific parameter is used to pick the node or edge to be attacked. These attacks can pick nodes or edges using centrality measures, system values such as loads or capacities, etc. A total of 27 articles performed targeted attacks [2, 10, 16, 18, 19, 25, 28, 33, 35, 36, 38, 42–43, 46, 48, 50, 52, 59, 60, 82, 87, 89, 92, 94, 95, 98, 102].

"Load and capacity" studies can be performed on frameworks that consider models where at least one of the system's networks has loads (electric, traffic, passengers, etc). These studies observe the effect of altering variables that define the load capacity of the network's nodes and edges over the robustness. In this review, a total of 17 articles performed this type of study [2, 3, 6, 46–48, 50, 51, 60, 75, 76, 86, 92–95, 103].

On the "cascading time" classification, we have frameworks that study how the duration of cascading failures varies under different conditions. This type of study was performed by a total of 12 papers [19, 40–44, 64, 65, 68, 71, 73, 100, 109].

The "length" classification contains frameworks that observe the effect of changing edge lengths over the robustness of the interdependent networks. Usually, these studies are performed on articles that use models with spatial restrictions. These restrictions can be used to determine if two nodes can be connected or whether this is within the same network or between two networks. Among the articles reviewed, 9 performed length studies [2, 10, 22, 59, 66–68, 70, 72].

On the "avalanche" classification, we have frameworks that study changes on the amount of nodes lost after an initial attack or failure, under different scenarios. This study may be performed as the main focus of the framework or as complementary information. A total of 8 articles conducted this type of study [29, 46, 47, 49, 50, 74, 87, 109].

*3.4. Networks Used to Test the Framework.* Given the requirements that an article had to satisfy in order to be considered in this survey, each article must test its framework using real or simulated networks. From the articles reviewed, only 2 classifications were identified. Here we list each classification, and between parenthesis we show the amount of articles within each one of them: "simulated" (75) and "real and simulated" (28).

On the "simulated" classification, we have articles that only used simulated networks to test their frameworks. Some of the networks used within this category were ErdÃűs-Renyi, Scale-Free, and Random-Regular. A total of 75 articles used simulated networks only to test their frameworks [3, 4, 6, 11, 16–21, 23–30, 33, 35–48, 50, 53–55, 58, 59, 61–63, 65–71, 73–76, 78–80, 83, 84, 87, 90, 92, 94, 95, 97, 98, 100–102, 104, 105, 110].

Finally, on the "real and simulated" classification, we find frameworks that used both real and simulated networks for testing, that is, within the set of networks used for testing there is at least one network that is real and one that is simulated. In this case, real networks may be paired with other real networks on the interdependent networks system, as in the work of Zhao et al. [2] where the interconnected public transportation network is used for testing, or with simulated networks, as shown by Bashan et al. [64], where the European power grid is coupled with a Random-Regular network. A total of 28 articles were found to belong to this classification [1, 2, 7, 10, 22, 31, 32, 34, 49, 51, 52, 56, 57, 60, 64, 72, 77, 81, 82, 85, 86, 88, 89, 91, 93, 96, 99, 103].

## 4. Summary

As we can see in Table 3, the use of frameworks to study the robustness of interdependent network did not start until the year 2010 with the work presented by Buldyrev et al. [4]. The amount of papers published per year in the interdependent network robustness area increased between 2010 and 2016,

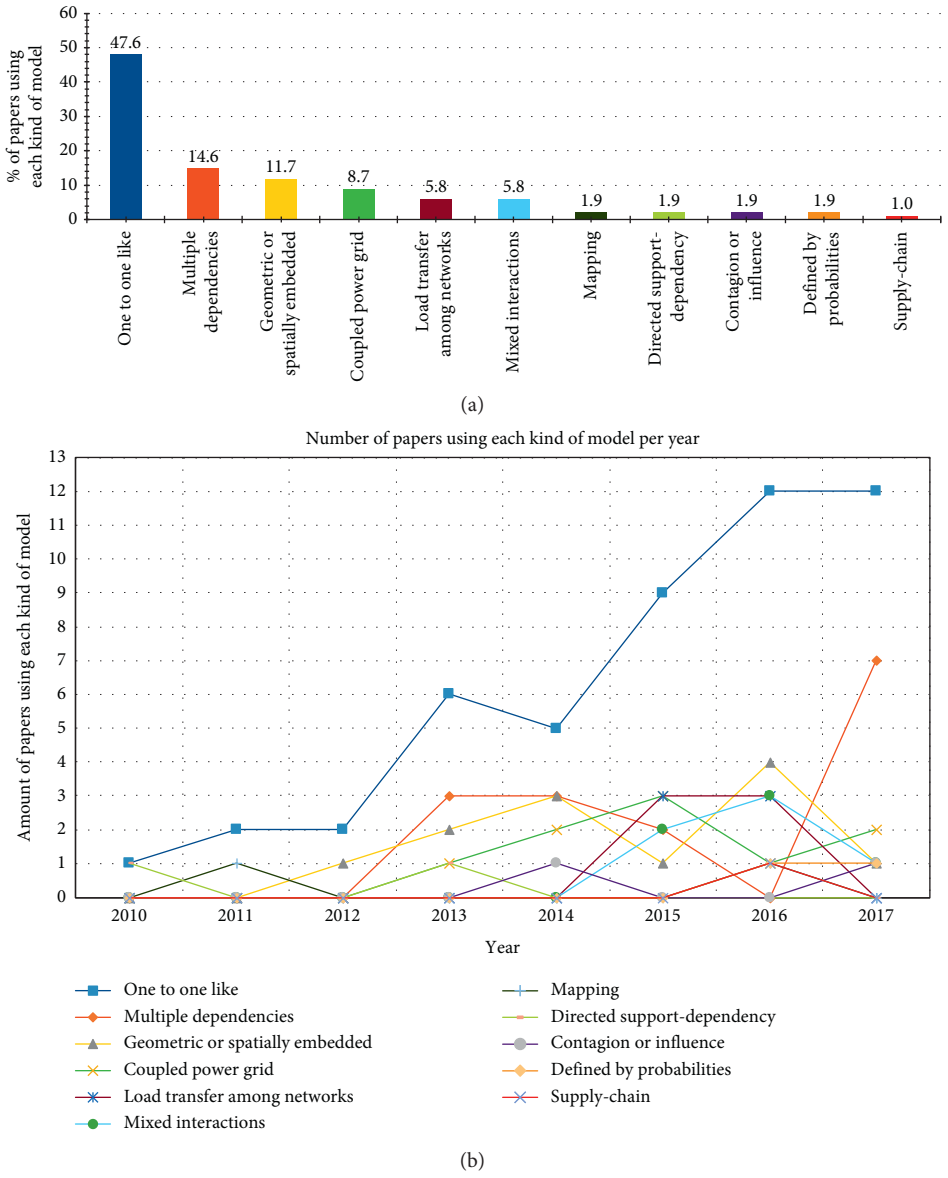


Figure 2: Model usage among the articles reviewed. (a) Percentage of papers using each type of model. (b) Amount of papers per year using each type of model.

going from 13 articles published in 2013 to 25 in 2016. Papers published in the area presented a small decrease between 2016 and 2017, going from 25 to 24 papers published each year, respectively. It is interesting to note that each year since 2013, most of the papers (>50%) have been published in journals rather than proceedings.

Among the model trends, we can see in Figure 2(a) that the most commonly used classification is "one to one like", being used by 47.6% of the articles reviewed. In second place, with less than third the amount of papers of the "one to one" classification, we have the "multiple dependencies" classification with 14.6% of the articles reviewed. We must note that the first article published in interdependent network robustness area presented the "one to one model." This classification positioned itself as the most popular since the beginning, and in 2015, 47.4% of the articles published that year used or presented a "one to one like" model. The next year, 48% for the papers published used or presented "one to one like" models. And in 2017, it represented 50% of the papers published that year. Between the years 2010 and 2014, many types of models appeared; however, most of them did not manage to become or stay popular. Such is the case for "mapping," "directed support-dependency," and "contagion or influence." During 2015 and 2016, "mixed interactions," "load transfer among networks," and "defined by probabilities" models emerged and maintained themselves. However, we can observe in Figure 2(b) that in 2017, most of the models used were "one to one" and "multiple dependencies" models, leaving far behind the models that emerged between 2015 and 2016.

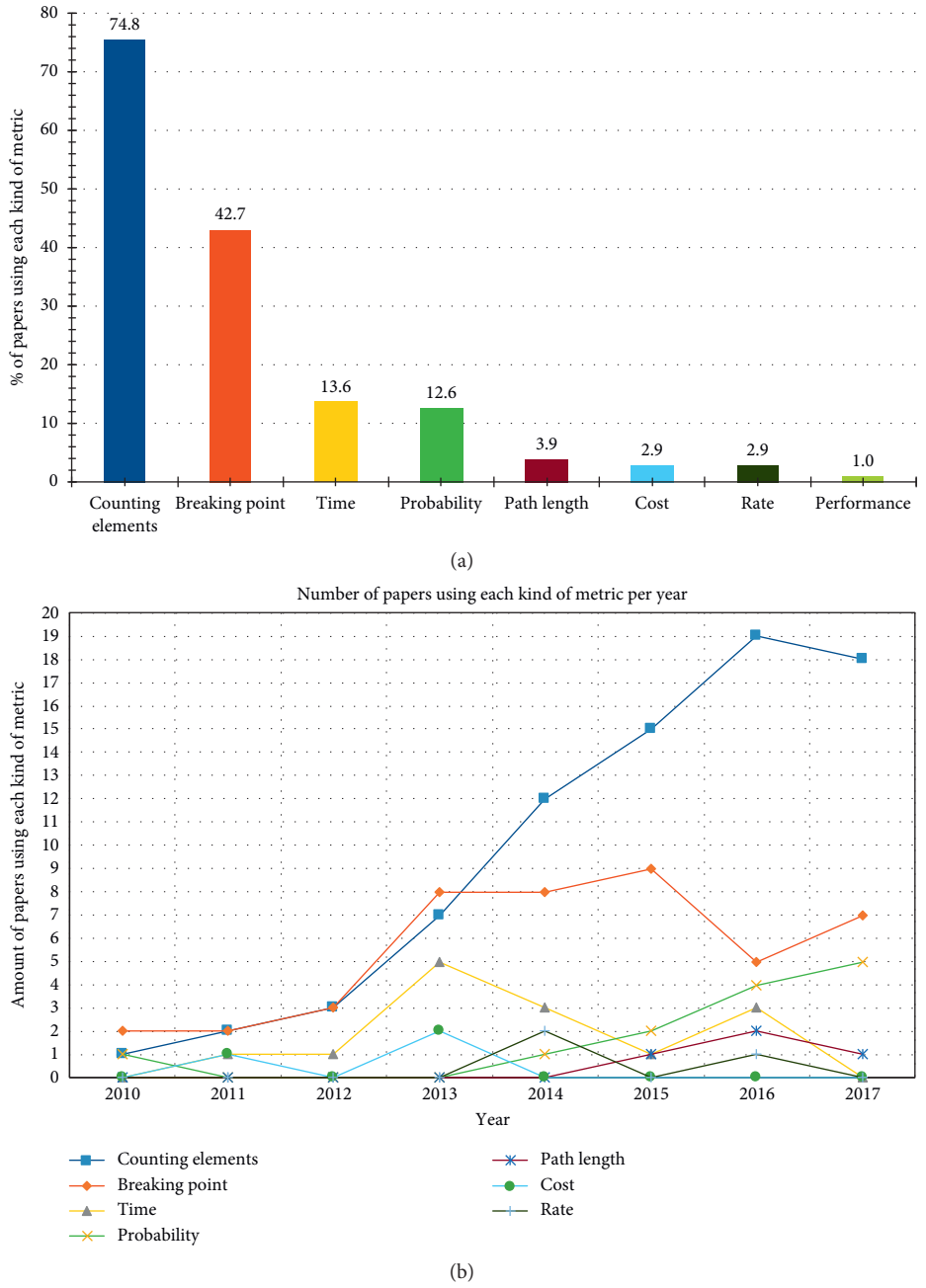


Figure 3: Metric usage among the articles reviewed. (a) Percentage of paper that used each type of metric. (b) Amount of papers per year using each type of metric.

In the metrics category, we can observe from Figure 3(a) that "counting elements" metrics are the most used type of metric with a 74.8% of use among all the articles reviewed. From Figure 3(b), we can see that the use of "counting elements" metrics has steadily grown, being used on 76% of the papers published during 2016 and 75% of the papers published during 2017. In second place, we have "breaking point" metrics, which are used on 42.7% of the articles reviewed. Other kinds of metrics fall far behind these two, each being used in less than 15% of the articles. From the Figure 3(b), we can see that some of these less used metrics, such as "time," "cost," and "rate," appeared between 2013 and 2014 but have not become more popular over time. A similar behaviour can be seen on "breaking point" metrics, whose popularity has stalled and decreased over time, going from being used by 47.4% of the articles published in 2015 to 29.1% in 2017. As for "probability" metrics, we can observe that their popularity has increased slowly since their first appearance in 2014.

From Figure 4(a), we can observe that "size of the giant connected component," "coupling," and "percolation" are the most popular studies performed, each appearing in over 45% of the articles reviewed. In Figure 4(b), we can observe that the use of "coupling" studies has steadily increased since

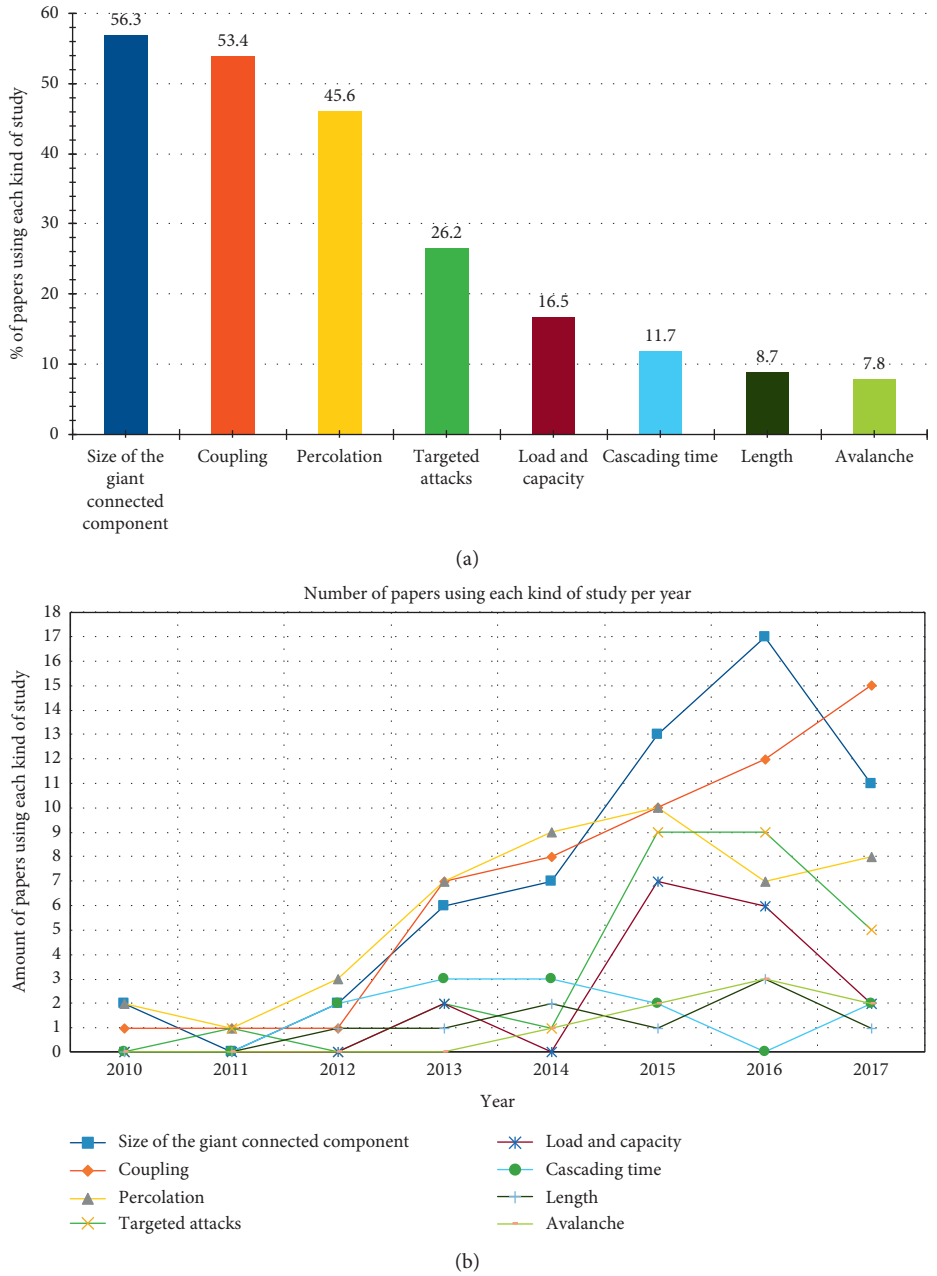


Figure 4: Studies performed among the articles reviewed. (a) Percentage of papers using each type of study. (b) Amount of papers per year using each type of study.

2013. This is not the case for "percolation" studies, whose use has decreased among the articles reviewed, going from appearing on 52.6% of the articles published in 2015 to 33.3% in 2017. A similar scenario can be observed for "size of the giant connected component," "targeted attack," and "load and capacity" studies whose use sharply dropped from 2016 to 2017. "Size of the giant connected component" studies went from being performed on 68% of the papers published in 2016 to 45.8% of the papers published in 2017. "Targeted attacks" studies went from being performed in 36% of the papers published in 2016 to 20.8% of the papers published in 2017. And "load and capacity" studies went from being performed in 24% of the papers published in 2016 to 8.33% of the papers published in 2017. For "avalanche" and "cascading time" studies we can observe that although they have been used since they first appeared, these kinds of studies have not gained much popularity over time. We must note that only the 8 most used studies were discussed here; however, a total of 54 studies were identified (see Supplementary Table A.7).

Finally, for the "networks tested" category, we can observe from Figure 5(a) that "simulated" networks are the most commonly used type of network to test frameworks with 72.8% of the articles using them. This is in contrast with "real and simulated" networks, which are used by only 27.2% of the articles reviewed. In Figure 5(b), we can see that this

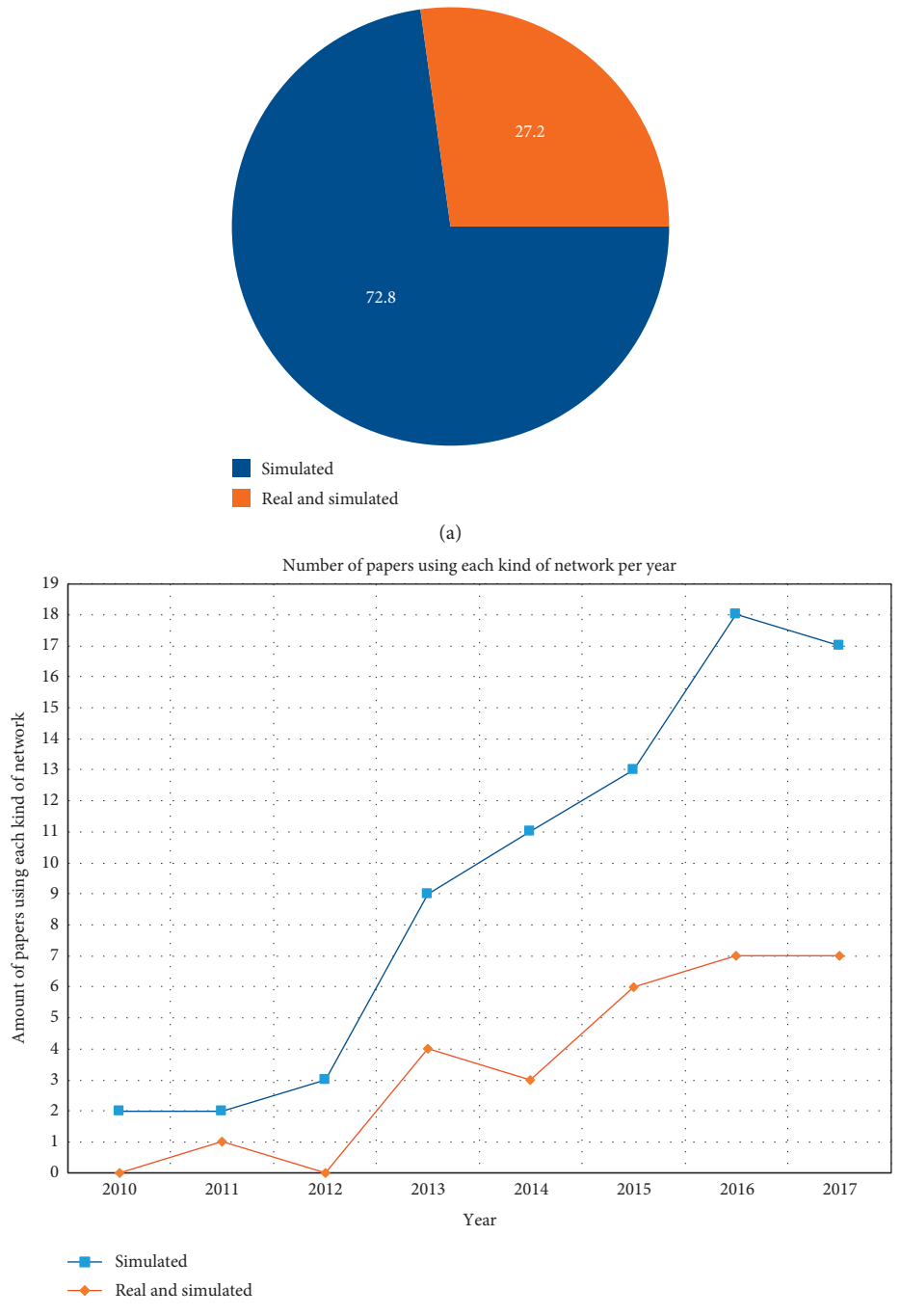


Figure 5: Type of networks to test the framework among the articles reviewed. (a) Percentage of papers using each type of networks to test the framework. (b) Amount of papers per year using each type of networks to test the framework.

usage disparity has been present since 2010, and it has only increased over time. Indeed, the amount of articles that used "simulated" networks during 2017 almost tripled the amount of articles that used "real and simulated networks."

## 5. Discussion

In the past years (2010–2017), several frameworks to analyze the robustness of interdependent networks have emerged. The study of interdependent networks' robustness has remained mostly focused on simple interactions among networks, which are not meant to thoroughly represent real-world networks, but to represent in an abstract way their behaviour and offer a broad spectrum of frameworks. We can appreciate this in the fact that "one to one like" models, "counting elements" metrics, "size of the giant connected component" studies, and "simulated" networks to test the frameworks are the most commonly used. These classifications do not present a high specificity regarding when or where they should be used to represent interdependent

networks, thus allowing them to be used in several different scenarios. However, these abstract frameworks may not be able to properly represent real-world scenarios.

During the first few years, there were attempts to represent real-world interdependent networks' robustness in a more realistic way. This can be seen by the use of "coupled power grid" models and "cost" and "time" metrics. However, most of these trends did not last. Although steps are being taken towards more realistic approaches that are in between the simple and general approaches and the more complex and realistic approaches, the area has been mostly focused on understanding abstract and general systems so far. The steps towards a more realistic approach to study the robustness of interdependent networks can be appreciated in the use of "geometric or spatially embedded" models and "targeted attacks" studies.

Even though we do not observe a great amount of more realistic framework, the articles reviewed in this survey do show a broad range of tools and methods to better understand the robustness of interdependent networks. Each of the variants for models, robustness measures, and studies has their own set of advantages and limitations that each researcher will have to evaluate according to the system they are studying. Thus, systems that might be accurately described by "multiple dependencies" models may not be properly described by using classic "one to one" models. The same goes for robustness measures, where the suitability of a measure will directly depend on how the researchers describe the robustness of the system. Depending on the hypothesis of the research being conducted, different studies will be of more interest than others. Hence, a framework will be more or less appropriate for a specific set of interdependent networks depending on whether it is able to capture the relevant characteristics of those networks as well as the researchers' concerns regarding the robustness of said networks.

## 6. Conclusion

From this review, we can note that the interdependent network robustness area is still young, having been around for a bit less than 10 years. For the most part, there is still no consensus regarding names, methods, and techniques in this area. In this survey, we proposed a way of unifying framework aspects through categories and classifications. The objective of this survey is to serve as an interdependent network robustness framework reference guide, to highlight useful aspects to be considered while searching for a framework, and to unify concepts.

As future work, we think the area should focus more on applications to real-world scenarios of frameworks to study the robustness of interdependent networks. This could also include a more critical approach on the use of general models and metrics to realistic scenarios, evaluating whether or not these frameworks properly describe real-world interdependent networks. Some other challenges include developing "realistic" datasets for testing purposes and establishing name consensus to avoid the reinvention of models and metrics.

Considering the literature presented in this survey, we see the future of this area progressively going from the current more theoretical state to a more applied state. This applied state should take into account the characteristics of real interdependent networks and test the frameworks, comparing the models with real data. The comparison between real data and the models is of great relevance as having progressively more accurate frameworks would allow this area to be used to predict with higher accuracy real-world interdependent network robustness phenomena. This would also allow to test the impact that major changes would have over the robustness of real interdependent networks without having to change the already existing real systems to fully understand the effect that those modifications might have. This increment on predictive power could lead to a generation of interdependent networks that are more robust and efficient.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This study was partially funded by CONICYT Doctorado Nacional (21170165) and by the Millennium Institute for Foundational Research on Data (IMFD).

## Supplementary Materials

We present in Section A.1 complementary tables mentioned throughout this work. In Section A.2, we give a content summary of each article reviewed in this survey with a description of its classification within the taxonomy. Finally in Section A.3, we present a thorough summary of the contents of this survey using tables. In Section A.3, we have summarized the article references contained within each aspect and we present a table showing all the "studies performed" classifications that were not mentioned in Section 3 and show summary tables that succinctly show the classifications to which each article belongs to. (*Supplementary Materials*)

## References

[1] M. Parandehgheibi and E. Modiano, "Robustness of interdependent networks: the case of communication networks and the power grid," in *Proceedings of the Global Communications Conference (GLOBECOM)*, IEEE, Atlanta, GA, USA, pp. 2164–2169, December 2013.

[2] Z. Zhao, P. Zhang, and H. Yang, "Cascading failures in interconnected networks with dynamical redistribution of loads," *Physica A: Statistical Mechanics and Its Applications*, vol. 433, pp. 204–210, 2015.

[3] L. Tang, K. Jing, J. He, and H. E. Stanley, "Complex interdependent supply chain networks: cascading failure and robustness," *Physica A: Statistical Mechanics and Its Applications*, vol. 443, pp. 58–69, 2016.

[4] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[5] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," *International Journal of Critical Infrastructures*, vol. 4, no. 1-2, pp. 63–79, 2008.

[6] Z. Huang, C. Wang, T. Zhu, and A. Nayak, "Cascading failures in smart grid: joint effect of load propagation and interdependence," *IEEE Access*, vol. 3, pp. 2520–2530, 2015.

[7] T. Ouboter, D. Worm, R. Kooij, and H. Wang, "Design of robust dependent networks against flow-based cascading failures," in *Proceedings of the 6th International Workshop on Reliable Networks Design and Modeling (RNDM)*, IEEE, St. Petersburg, Russia, pp. 54–60, October 2014.

[8] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences*, vol. 108, no. 10, pp. 3838–3841, 2011.

[9] D. Stauffer and A. Aharony, *Introduction to Percolation Theory*, CRC Press, Boca Raton, FL, USA, 1994.

[10] W. K. Chai, V. Kyritsis, K. Katsaros, and G. Pavlou, "Resilience of interdependent communication and power distribution networks against cascading failures," in *Proceedings of the 15th IFIP Networking*, Vienna, Austria, May 2016.

[11] Y. Berezin, A. Bashan, M. M. Danziger, D. Li, and S. Havlin, "Localized attacks on spatially embedded networks with dependencies," *Scientific Reports*, vol. 5, no. 1, 2015.

[12] S. Boccaletti, G. Bianconi, R. Criado et al., "The structure and dynamics of multilayer networks," *Physics Reports*, vol. 544, no. 1, pp. 1–122, 2014.

[13] M. De Domenico, C. Granell, M. A. Porter, and A. Arenas, "The physics of spreading processes in multilayer networks," *Nature Physics*, vol. 12, no. 10, pp. 901–906, 2016.

[14] M. Kivela, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter, "Multilayer networks," *Journal of Complex Networks*, vol. 2, no. 3, pp. 203–271, 2014.

[15] B. Kitchenham, *Procedures for Performing Systematic Reviews*, Vol. 33, Keele University, Keele, UK, 2004.

[16] S. Chattopadhyay and H. Dai, "Towards optimal link patterns for robustness of interdependent networks against cascading failures," in *Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM)*, IEEE, San Diego, CA, USA, pp. 1–6, December 2015.

[17] S. Chattopadhyay and H. Dai, "Designing optimal interlink structures for interdependent networks under budget constraints," Technical Report, Department of ECE, NCSU, Raleigh, North Carolina, 2017.

[18] S. Chattopadhyay, H. Dai, D. Y. Eun, and S. Hosseinalipour, "Designing optimal interlink patterns to maximize robustness of interdependent networks against cascading failures," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3847–3862, 2017.

[19] Z. Cheng and J. Cao, "Cascade of failures in interdependent networks coupled by different type networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 430, pp. 193–200, 2015.

[20] M. Di Muro, C. La Rocca, H. Stanley, S. Havlin, and L. Braunstein, "Recovery of interdependent networks," *Scientific Reports*, vol. 6, 2016.

[21] D. Gaogao, D. Ruijin, H. Huifang, and T. Lixin, "Shell attack on interdependent networks," in *Proceedings of the 2016 35th Chinese Control Conference (CCC)*, TCCT, Chengdu, China, pp. 1198–1201, July 2016.

[22] M. Gong, Y. Wang, S. Wang, and W. Liu, "Enhancing robustness of interdependent network under recovery based on a two-layer-protection strategy," *Scientific Reports*, vol. 7, no. 1, p. 12753, 2017.

[23] P. Grassberger, "Percolation transitions in the survival of interdependent agents on multiplex networks, catastrophic cascades, and solid-on-solid surface growth," *Physical Review E*, vol. 91, no. 6, Article ID 062806, 2015.

[24] Y. Hu, D. Zhou, R. Zhang, Z. Han, C. Rozenblat, and S. Havlin, "Percolation of interdependent networks with intersimilarity," *Physical Review E*, vol. 88, no. 5, Article ID 052805, 2013.

[25] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Physical Review E*, vol. 83, no. 6, Article ID 065101, 2011.

[26] X. Ji, B. Wang, D. Liu et al., "Improving interdependent networks robustness by adding connectivity links," *Physica A: Statistical Mechanics and Its Applications*, vol. 444, pp. 9–19, 2016.

[27] W. X. Juan, G. S. Ze, J. Lei, and W. Zhen, "Percolation-cascading in multilayer heterogeneous network with different coupling preference," *Physica A: Statistical Mechanics and Its Applications*, vol. 471, pp. 233–243, 2017.

[28] Y. Kazawa and S. Tsugawa, "On the effectiveness of link addition for improving robustness of multiplex networks against layer node-based attack," in *Proceedings of the IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1, IEEE , pp. 697–700, Turin, Italy, July 2017.

[29] D. Lee, S. Choi, M. Stippinger, J. Kertész, and B. Kahng, "Hybrid phase transition into an absorbing state: percolation and avalanches," *Physical Review E*, vol. 93, no. 4, Article ID 042109, 2016.

[30] J. Pan, Y. Yao, L. Fu, and X. Wang, "Core percolation in coupled networks," in *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, p. 28, ACM, Chennai India, July 2017.

[31] F. Radicchi, "Percolation in real interdependent networks," *Nature Physics*, vol. 11, no. 7, pp. 597–602, 2015.

[32] G. Ranjan and Z.-L. Zhang, "How to glue a robust smart-grid?: a finite-network theory for interdependent network robustness," in *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, p. 22, ACM, Oak Ridge, TN, USA, October 2011.

[33] D. Rueda, E. Calle, F. Maldonado-Lopez, and Y. Donoso, "Reducing the impact of targeted attacks in interdependent telecommunication networks," in *Proceedings of the 23rd International Conference on Telecommunications (ICT)*, IEEE, Thessaloniki, Greece, pp. 1–5, May 2016.

[34] C. M. Schneider, N. Yazdani, N. A. Araújo, S. Havlin, and H. J. Herrmann, "Towards designing robust coupled networks," *Scientific Reports*, vol. 3, 2013.

[35] A. Tyra, J. Li, Y. Shang, S. Jiang, Y. Zhao, and S. Xu, "Robustness of non-interdependent and interdependent networks against dependent and adaptive attacks," *Physica A: Statistical Mechanics and Its Applications*, vol. 482, pp. 713–727, 2017.

[36] S. Wang and J. Liu, "Robustness of single and interdependent scale-free interaction networks with various parameters," *Physica A: Statistical Mechanics and Its Applications*, vol. 460, pp. 139–151, 2016.

[37] X. Wang, J. Cao, R. Li, and T. Zhao, "A preferential attachment strategy for connectivity link addition strategy in

improving the robustness of interdependent networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 483, pp. 412–422, 2017.

[38] S. Watanabe and Y. Kabashima, "Cavity-based robustness analysis of interdependent networks: influences of intra-network and internetwork degree-degree correlations," *Physical Review E*, vol. 89, no. 1, Article ID 012808, 2014.

[39] X. Yuan, S. Shao, H. E. Stanley, and S. Havlin, "How breadth of degree distribution influences network robustness: comparing localized and random attacks," *Physical Review E*, vol. 92, no. 3, Article ID 032122, 2015.

[40] D. Zhou, A. Bashan, R. Cohen, Y. Berezin, N. Shnerb, and S. Havlin, "Simultaneous first-and second-order percolation transitions in interdependent networks," *Physical Review E*, vol. 90, no. 1, Article ID 012803, 2014.

[41] D. Zhou, H. E. Stanley, G. DÂĂŹgostino, and A. Scala, "Assortativity decreases the robustness of interdependent networks," *Physical Review E*, vol. 86, no. 6, Article ID 066103, 2012.

[42] D. F. Rueda and E. Calle, "Using interdependency matrices to mitigate targeted attacks on interdependent networks: a case study involving a power grid and backbone telecommunications networks," *International Journal of Critical Infrastructure Protection*, vol. 16, pp. 3–12, 2017.

[43] G. Dong, J. Gao, R. Du, L. Tian, H. E. Stanley, and S. Havlin, "Robustness of network of networks under targeted attack," *Physical Review E*, vol. 87, no. 5, Article ID 052804, 2013.

[44] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of a network formed by n interdependent networks with a one-to-one correspondence of dependent nodes," *Physical Review E*, vol. 85, no. 6, Article ID 066134, 2012.

[45] S. Shao, X. Huang, H. E. Stanley, and S. Havlin, "Robustness of a partially interdependent network formed of clustered networks," *Physical Review E*, vol. 89, no. 3, Article ID 032812, 2014.

[46] Z. Chen, W.-B. Du, X.-B. Cao, and X.-L. Zhou, "Cascading failure of interdependent networks with different coupling preference under targeted attack," *Chaos, Solitons & Fractals*, vol. 80, pp. 7–12, 2015.

[47] L. Liu, Y. Yin, Z. Zhang, and Y. K. Malaiya, "Redundant design in interdependent networks," *PLoS One*, vol. 11, no. 10, Article ID e0164777, 2016.

[48] F. Tan, Y. Xia, and Z. Wei, "Robust-yet-fragile nature of interdependent networks," *Physical Review E*, vol. 91, no. 5, Article ID 052809, 2015.

[49] J. Wang, C. Jiang, and J. Qian, "Robustness of interdependent networks with different link patterns against cascading failures," *Physica A: Statistical Mechanics and Its Applications*, vol. 393, pp. 535–541, 2014.

[50] J. Wang, Y. Li, and Q. Zheng, "Cascading load model in interdependent networks with coupled strength," *Physica A: Statistical Mechanics and Its Applications*, vol. 430, pp. 242–253, 2015.

[51] D. Zhou and A. Elmokashfi, "Overload-based cascades on multiplex networks and effects of inter-similarity," *PLoS One*, vol. 12, no. 12, Article ID e0189624, 2017.

[52] D. F. Rueda, E. Calle, and J. L. Marzo, "Improving the robustness to targeted attacks in software defined networks (SDN)," in *Proceedings of 13th International Conference on DRCN 2017-Design of Reliable Communication Networks*, VDE, Ghent, Belgium, pp. 1–8, October 2017.

[53] Q. Zhang, D. Li, R. Kang, E. Zio, and P. Zhang, "Reliability analysis of interdependent networks using percolation theory," in *Proceedings of the International Conference on Signal-Image Technology & Internet-Based Systems*, IEEE, pp. 626–629, Kyoto, Japan, December 2013.

[54] M. Stippinger and J. Kertész, "Enhancing resilience of interdependent networks by healing," *Physica A: Statistical Mechanics and Its Applications*, vol. 416, pp. 481–487, 2014.

[55] F. Radicchi and A. Arenas, "Abrupt transition in the structural formation of interconnected networks," *Nature Physics*, vol. 9, no. 11, pp. 717–720, 2013.

[56] A. A. Ganin, E. Massaro, A. Gutfraind et al., "Operational resilience: concepts, design and analysis," *Scientific Reports*, vol. 6, no. 1, 2016.

[57] M. Gong, L. Ma, Q. Cai, and L. Jiao, "Enhancing robustness of coupled networks under targeted recoveries," *Scientific Reports*, vol. 5, 2015.

[58] N. K. Panduranga, J. Gao, X. Yuan, H. E. Stanley, and S. Havlin, "Generalized model for k-core percolation and interdependent networks," *Physical Review E*, vol. 96, no. 3, Article ID 032317, 2017.

[59] S. Sun, Y. Wu, Y. Ma, L. Wang, Z. Gao, and C. Xia, "Impact of degree heterogeneity on attack vulnerability of interdependent networks," *Scientific Reports*, vol. 6, 2016.

[60] X.-J. Zhang, G.-Q. Xu, Y.-B. Zhu, and Y.-X. Xia, "Cascade-robustness optimization of coupling preference in interconnected networks," *Chaos, Solitons & Fractals*, vol. 92, pp. 123–129, 2016.

[61] D. Zhou, J. Gao, H. E. Stanley, and S. Havlin, "Percolation of partially interdependent scale-free networks," *Physical Review E*, vol. 87, no. 5, Article ID 052812, 2013.

[62] R.-R. Liu, M. Li, and C.-X. Jia, "Cascading failures in coupled networks: the critical role of node-coupling strength across networks," *Scientific Reports*, vol. 6, 2016.

[63] C. O. Adler and C. H. Dagli, "Study of the use of a genetic algorithm to improve networked system-of-systems resilience," *Procedia Computer Science*, vol. 36, pp. 49–56, 2014.

[64] A. Bashan, Y. Berezin, S. V. Buldyrev, and S. Havlin, "The extreme vulnerability of interdependent spatially embedded networks," *Nature Physics*, vol. 9, no. 10, pp. 667–672, 2013.

[65] M. M. Danziger, A. Bashan, Y. Berezin, and S. Havlin, "Interdependent spatially embedded networks: dynamics at percolation threshold," in *Proceedings of the 2013 International Conference onSignal-Image Technology & Internet-Based Systems (SITIS)*, IEEE , pp. 619–625, Kyoto, Japan, December 2013.

[66] Y. Kornbluth, S. Lowinger, G. Cwilich, and S. V. Buldyrev, "Cascading failures in networks with proximate dependent nodes," *Physical Review E*, vol. 89, no. 3, Article ID 032808, 2014.

[67] W. Li, A. Bashan, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Cascading failures in interdependent lattice networks: the critical role of the length of dependency links," *Physical Review Letters*, vol. 108, no. 22, Article ID 228702, 2012.

[68] L. M. Shekhtman, Y. Berezin, M. M. Danziger, and S. Havlin, "Robustness of a network formed of spatially embedded networks," *Physical Review E*, vol. 90, no. 1, Article ID 012809, 2014.

[69] Z. Limiao, L. Daqing, Q. Pengju et al., "Reliability analysis of interdependent lattices," *Physica A: Statistical Mechanics and Its Applications*, vol. 452, pp. 120–125, 2016.

[70] S. Lowinger, G. A. Cwilich, and S. V. Buldyrev, "Interdependent lattice networks in high dimensions," *Physical Review E*, vol. 94, no. 5, Article ID 052306, 2016.

[71] P. Shu, L. Gao, P. Zhao, W. Wang, and H. E. Stanley, "Social contagions on interdependent lattice networks," *Scientific Reports*, vol. 7, p. 44669, 2017.

[72] X. Wang, R. E. Kooij, and P. Van Mieghem, "Modeling region-based interconnection for interdependent networks," *Physical Review E*, vol. 94, no. 4, Article ID 042315, 2016.

[73] G. Dong, L. Tian, R. Du, M. Fu, and H. E. Stanley, "Analysis of percolation behaviors of clustered networks with partial support-dependence relations," *Physica A: Statistical Mechanics and Its Applications*, vol. 394, pp. 370–378, 2014.

[74] Z. Liu, Q. Li, D. Wang, and M. Xu, "Balancing interdependent networks: theory and algorithm," in *Proceedings of the IEEE 36th International Performance Computing and Communications Conference (IPCCC)*, IEEE, pp. 1-2, San Diego, CA, USA, December 2017.

[75] Y. Qiu, "The effect of clustering-based and degree-based weighting on robustness in symmetrically coupled heterogeneous interdependent networks," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, IEEE, pp. 3984–3988, Manchester, UK, October 2013.

[76] "Optimal weighting scheme and the role of coupling strength against load failures in degree-based weighted interdependent networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 392, no. 8, pp. 1920–1924, 2013.

[77] S. D. S. Reis, Y. Hu, A. Babino et al., "Avoiding catastrophic failure in correlated networks of networks," *Nature Physics*, vol. 10, no. 10, pp. 762–767, 2014.

[78] K. Roth, F. Morone, B. Min, and H. A. Makse, "Emergence of robustness in networks of networks," *Physical Review E*, vol. 95, no. 6, Article ID 062308, 2017.

[79] W. Fan, D. Gaogao, D. Ruijin, and T. Lixin, "Robustness of multiple interdependent networks under shell attack," in *Proceedings of the 2017 36th Chinese Control Conference (CCC)*, IEEE, pp. 1447–1450, Dalian, China, July 2017.

[80] J. Jiang, W. Li, and X. Cai, "The effect of interdependence on the percolation of interdependent networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 410, pp. 573–581, 2014.

[81] X. Li, H. Wu, C. Scoglio, and D. Gruenbacher, "Robust allocation of weighted dependency links in cyber-physical networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 433, pp. 316–327, 2015.

[82] D. T. Nguyen, Y. Shen, and M. T. Thai, "Detecting critical nodes in interdependent power networks for vulnerability assessment," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 151–159, 2013.

[83] M. Di Muro, L. Valdez, H. A. Rêgo, S. Buldyrev, H. Stanley, and L. Braunstein, "Cascading failures in interdependent networks with multiple supply-demand links and functionality thresholds," *Scientific Reports*, vol. 7, no. 1, p. 15059, 2017.

[84] P. Cui, P. Zhu, C. Shao, and P. Xun, "Cascading failures in interdependent networks due to insufficient received support capability," *Physica A: Statistical Mechanics and Its Applications*, vol. 469, pp. 777–788, 2017.

[85] Y. Zhao and C. Qiao, "Enhancing the robustness of interdependent cyber-physical systems by designing the interdependency relationship," in *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, IEEE, pp. 1–6, Paris, France, May 2017.

[86] Y. Cai, Y. Li, Y. Cao, W. Li, and X. Zeng, "Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids," *International Journal of Electrical Power & Energy Systems*, vol. 89, pp. 106–114, 2017.

[87] Y. Han, Z. Li, C. Guo, and Y. Tang, "Improved percolation theory incorporating power flow analysis to model cascading failures in cyber-physical power system," in *Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM)*, IEEE, pp. 1–5, Montreal, Canada, August 2016.

[88] M. Korkali, J. G. Veneman, B. F. Tivnan, J. P. Bagrow, and P. D. Hines, "Reducing cascading failure risk by increasing infrastructure network interdependence," *Scientific Reports*, vol. 7, p. 44499, 2017.

[89] Z. Huang, C. Wang, A. Nayak, and I. Stojmenovic, "Small cluster in cyber physical systems: network topology, interdependence and cascading failures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 8, pp. 2340–2351, 2015.

[90] Y. Matsui, H. Kojima, and T. Tsuchiya, "Modeling the interaction of power line and SCADA networks," in *Proceedings of the IEEE 15th International Symposium on High-Assurance Systems Engineering*, IEEE, pp. 261-262, Miami Beach, FL, USA, January 2014.

[91] M. Ouyang and Z. Wang, "Resilience assessment of interdependent infrastructure systems: with a focus on joint restoration modeling and analysis," *Reliability Engineering & System Safety*, vol. 141, pp. 74–82, 2015.

[92] S. Hong, B. Wang, and J. Wang, "Cascading failure propagation in interconnected networks with tunable load redistribution strategy," in *Proceedings of the Prognostics and System Health Management Conference (PHM)*, IEEE, pp. 1–7, Beijing, China, October 2015.

[93] X. Wang, J. Cao, and X. Qin, "Study of robustness in functionally identical coupled networks against cascading failures," *PLoS One*, vol. 11, no. 8, Article ID e0160545, 2016.

[94] Y. Xia, W. Zhang, and X. Zhang, "The effect of capacity redundancy disparity on the robustness of interconnected networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 447, pp. 561–568, 2016.

[95] W. Zhang, Y. Xia, B. Ouyang, and L. Jiang, "Effect of network size on robustness of interconnected networks under targeted attack," *Physica A: Statistical Mechanics and Its Applications*, vol. 435, pp. 80–88, 2015.

[96] Q. Zhu, Z. Zhu, Y. Wang, and H. Yu, "Fuzzy-information-based robustness of interconnected networks against attacks and failures," *Physica A: Statistical Mechanics and Its Applications*, vol. 458, pp. 194–203, 2016.

[97] G. Dong, R. Du, L. Tian, and R. Liu, "Robustness of network of networks with interdependent and interconnected links," *Physica A: Statistical Mechanics and Its Applications*, vol. 424, pp. 11–18, 2015.

[98] R. Du, G. Dong, L. Tian, and R. Liu, "Targeted attack on networks coupled by connectivity and dependency links," *Physica A: Statistical Mechanics and Its Applications*, vol. 450, pp. 687–699, 2016.

[99] D. F. Klosik, A. Grimbs, S. Bornholdt, and M.-T. Hütt, "The interdependent network of gene regulation and metabolism is robust where it needs to be," *Nature Communications*, vol. 8, no. 1, p. 534, 2017.

[100] B. Kotnis and J. Kuri, "Percolation on networks with antagonistic and dependent interactions," *Physical Review E*, vol. 91, no. 3, Article ID 032805, 2015.

[101] R.-R. Liu, M. Li, C.-X. Jia, and B.-H. Wang, "Cascading failures in coupled networks with both inner-dependency and inter-dependency links," *Scientific Reports*, vol. 6, 2016.

[102] D.-w. Zhao, L.-h. Wang, Y.-f. Zhi, J. Zhang, and Z. Wang, "The robustness of multiplex networks under layer node-based attack," *Scientific Reports*, vol. 6, 2016.

[103] A. Alashaikh, D. Tipper, and T. Gomes, "Supporting differentiated resilience classes in multilayer networks," in

*Proceedings of the 2016 12th International Conference on the Design of Reliable Communication Networks (DRCN)*, IEEE, pp. 31–38, Paris, France, March 2016.

[104] X. Zhang, C. Phillips, and X. Chen, "An overlay mapping model for achieving enhanced QoS and resilience performance," in *Proceedings of the 2011 3rd International Congress onUltra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, IEEE, pp. 1–7, Budapest, Hungary, October 2011.

[105] J. Gao, S. V. Buldyrev, H. E. Stanley, X. Xu, and S. Havlin, "Percolation of a general network of networks," *Physical Review E*, vol. 88, no. 6, Article ID 062816, 2013.

[106] R. Parshani, S. V. Buldyrev, and S. Havlin, "Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition," *Physical Review Letters*, vol. 105, no. 4, Article ID 048701, 2010.

[107] Y. Min, J. Hu, W. Wang, Y. Ge, J. Chang, and X. Jin, "Diversity of multilayer networks and its impact on collaborating epidemics," *Physical Review E*, vol. 90, no. 6, Article ID 062803, 2014.

[108] F. D. Sahneh, J. Melander, C. Scoglio et al., "Contact adaption during epidemics: a multilayer network formulation approach," *IEEE Transactions on Network Science and Engineering*, vol. 6, no. 1, pp. 16–30, 2017.

[109] D. Liu, X. Zhang, and K. T. Chi, "A stochastic model for cascading failures in smart grid under cyber attack," in *Proceedings of the IEEE 3rd International Future Energy Electronics Conference and ECCE Asia (IFEEC 2017-ECCE Asia)*, IEEE, pp. 783–788, Kaohsiung, Taiwan, June 2017.

[110] M. Rahnamay-Naeini and M. M. Hayat, "Cascading failures in interdependent infrastructures: an interdependent Markov-chain approach," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1997–2006, 2016.