Submitted: 14 April 2022

Published online in 'accepted manuscript' format: 02 June 2023

Manuscript title: A survey on multilayer networks modelled to assess robustness in infrastructure systems

Authors: Zahra Mahabadi, Liz Varga, Tom Dolan

Affiliation: Department of Civil, Environmental and Geomatic Engineering, University College London, London, UK.

Corresponding author: Zahra Mahabadi, Department of Civil, Environmental and Geomatic Engineering, University College London, London WC1E 6BT, UK.

E-mail: zahra.mahabadi.19@ucl.ac.uk

Accepted manuscript
doi: 10.1680/jsmic.22.00015

Abstract

The development of modern societies places particular demands on the consistent performance of infrastructure systems. Because multilayer network models are capable of representing the interdependencies between infrastructure components, they have been widely used to analyse the robustness of infrastructure systems. This present study is a systematic review of literature, published since 2010. It aims to investigate how multilayer network models have been used in analysing the robustness of infrastructure systems. According to findings, percolation theory was the most popular method used in about 57% of papers. Regarding the properties, coupling strength and node degree were the most common while directed links and feedback conditions were the least common. The following gaps were identified which provide opportunities for further research. These include the absence of models based on real-world data and the need for models that make fewer simplifying assumptions about complex systems. No papers considered all potential properties, and their effect on boosting or weakening each other's effect. By considering all properties, the importance of different properties on the robustness of infrastructure systems can be quantified and compared in future studies.

1. Introduction

The robustness of infrastructure systems is essential for providing a continuous flow of goods and services in modern societies. Any interruption in their performance can cause economic loss and affect societal wellbeing. Thus, it is essential to analyse how they can be designed and improved to sustain in the face of disruption. In recent years, infrastructure systems have been developing into more and more interdependent and interconnected systems where the performance of each system is interlinked with the performance of the other sectors. In this regard, multilayer networks are capable of modelling different sectors of infrastructure including the power grid, water supply, transportation system, and telecommunication as different layers with all interdependencies and interconnections within and between the sectors (Heracleous et al. 2017). Besides, robustness in network models is defined and studied as the resistance of the network to sequential nodes/links removals (Danziger et al., 2016) to see what properties have an influence on the vulnerability and or robustness of the models.

While most of the studies analysing the robustness of infrastructure systems applied single layer networks (Heracleous et al. 2017), it is better to model and analyse interdependencies and interconnections of different sectors as multilayer networks. Complex interrelations in multilayer networks can make them more fragile than single-layer networks by inducing cascading failures among all layers (Li et al, 2021). Furthermore, multilayer and single-layer networks with similar properties can have different reactions to failure. For example, higher degree distribution increases vulnerability in multilayer networks whilst it has inverse effects on single-layer networks (Buldyrev et al., 2010). Similarly, longer links increase

the vulnerability of multilayer networks while they improve the robustness in single-layer networks (Danziger et al., 2016).

Although there are reviews about network models, none of them focused specifically on how multilayer network models were applied to study the robustness in infrastructure systems. This present study provides a systematic review of literature, published since 2010, on the use of multilayer network models to analyse the robustness of infrastructure systems. This review paper aims to investigate how multilayer network models, used to characterize infrastructure systems, have been applied to assess the robustness and vulnerability of such systems. It identifies and analyses two groups of studies based on the methods they applied and then extracts and categorises their metrics, strategies, methods, and nodes/links removal mechanisms. According to the findings, studies taking percolation theory were the most common. They mostly focused on assessing the effect of network properties while the second group of papers was mostly about identifying the critical components under imposing different removal mechanisms.

The rest of the article is organised as follows. Section 2 explains the methodology used for the collection and selection of papers. Section 3 contains an extensive analysis and comparison between identified categories. Section 4 presents the conclusion and thoughts about future works.

2. Methodology

This study is a systematic review using Kitchenham's protocol (Kitchenham, 2004) as a guideline. It aims to analyse different frameworks applied to assess robustness in multilayer

network models of infrastructure systems. The focus is on answering the following questions: (i) what metrics are defined to quantify robustness? (ii) what strategies are indicated to improve the robustness? (iii) what methods are used to assess the robustness? And (iv) what removal mechanisms are employed to simulate real-world failure propagations?

In this regard, the intersection between three search strings was explored on Scopus (Table 1); (i) multilayer networks, (ii) infrastructure systems, and (iii) robustness, connected with "AND" to find the intersection between these three. Here, a general framework is considered to define multilayer networks which can also include interdependent networks, multiplex networks, networks of networks, and so on. Adapted from Boccaletti et al (2014) a multilayer network is defined as "a pair M = (G, C) where G represents different layers of M, made by directed or undirected, weighted or unweighted graphs, and C is the set of interconnections between nodes belonging to different layers". It is a general framework for multilayer networks which can include other types of multilayer networks like interdependent networks, multiplex networks, networks of networks, and so on. In this way, two types of links were considered (i) connectivity links that connect nodes within layers and (ii) dependency links that connect nodes between layers (Buldyrev et al, 2010). Relevant keywords to multilayer networks were identified from (Kivela et al, 2014) connected with "OR" in the search string to include all relevant alternatives. Similar keywords with "system" were also added to make the search result more inclusive.

For this study, peer-reviewed papers published since 2010 on Scopus were considered. The search query was limited to titles, abstracts, and keywords of articles. The language was

limited to English. All obtained papers were reviewed in two phases, first reviewing titles and abstracts and then full-text review, to make sure that all relevant papers were collected. In the end, 60 papers were selected as the most relevant papers based on the defined inclusion/exclusion criteria. In the next stages, in-depth reading and analysing were performed to extract and classify data acquired from the selected papers. The result is discussed in the next section.

3. Discussion

3.1 Robustness assessment

While all papers took a multilayer network approach to assess robustness in infrastructure systems, they can be categorised into two groups based on the methods they used to assess the robustness. About 57% of selected papers applied percolation theory as the assessment method. The percolation theory is about studying the behaviour of the network models when some nodes and links stand removed. In this way, the size of the connected component of the network decreases to a certain threshold called the critical percolation threshold in which the network moves from the connected state to the disconnected state (Li et al, 2021; Havlin et al, 2015). So, below the critical threshold, there is no connected component. In addition, different states of the transitions in the size of the giant component are analysed in the percolation theory whether they happen abruptly or gradually (Zhao et al, 2016). The giant connected component is the largest subnetwork of connected nodes/links remained after the cascade of failures through the whole network (Baxter et al, 2014).

Similar to the first group, the second group of papers (43% of the papers), applied

mathematical/numerical simulations of nodes/links removal mechanisms to evaluate network fragility. However, they did not define critical thresholds and different phase transitions. Each paper in the second group defined its own removal mechanism according to the purpose of the paper. Thus, percolation theory is identified as the most common method to assess the robustness in multilayer networks of infrastructure systems.

Most of the papers (82%), applied percolation theory, merely focused on topological properties based on synthetic networks whereas more than half of the papers (54%) in the second group used functional properties and real case studies. However, the only two cases that included dynamical properties belong to the first group as well (Duan et al, 2019; Danziger et al, 2019). The next difference between these two groups of papers is related to the strategies they concluded to improve the robustness which is explained in more detail in the next section.

3.2 Robustness strategies

In addition to assessing the robustness, the collected studies worked on finding strategies and solutions to improve the robustness of multilayer networks and study their vulnerabilities. These strategies can be grouped into two; i) identifying the critical components to make them reinforced, ii) assessing the effect of different network properties on the robustness to mitigate negative impacts and strengthen positive influences. Only 17 percent of the papers considered the first group of strategies while all the papers using percolation theory belonged to the second group.

According to the results, critical nodes/links were identified based on three metrics: node centrality, maximum performance loss, and historical failures. Node centrality was defined in

three ways; nodes with higher degree, nodes with higher betweenness centrality, and clustering property in which removing them can result in more damage than the other nodes (Qi et al, 2019). The degree of a node is defined as the number of links connected to the node, the betweenness centrality is the number of shortest paths passing through the node (Wang et al, 2018), and the clustering property refers to the connection of a node to its neighbouring nodes (Limiao et al, 2016). Han et al (2021) declared when nodes have the same degree in multiplex networks, removing those nodes with less link overlap improves the attack performance (as a deliberately or not deliberately failure mechanism). Attacking nodes with higher betweenness centrality is more destructive than nodes with higher degree of connections (Limiao et al, 2016; Wang et al, 2021). Nodes with a better connection to their neighbouring nodes show high clustering properties and play a more critical role than the two other centrality properties (Limiao et al, 2016).

In the second group (Zhang et al, 2014; Moussa et al, 2018), node/link criticality was measured according to the sum of performance loss after removing each node/link by computing the change made in the network flow before and after the attack. The network flow was defined as the average number of paths passing a link (Wang et al, 2018). Zhao et al (2018) used the PageRank algorithm assigning each node a value called the PR value which at convergence reflects purely topological importance of the nodes, as all child nodes get the same share of PR values from their parent nodes. In the third group, Liu et al (2016) used historical failure distribution (HFD) to assess the criticality of nodes removal. It is based on the simulation results of cascading failure over large-scale simulation times to select those nodes

with a higher frequency of overload or interdependent failure compared to other nodes.

As mentioned earlier, there were a group of papers that assessed the effects of network properties on robustness. There were different network properties evaluated by different studies. However, regardless of the method they applied, almost all studies admitted a similar effect of the network properties on the robustness of multilayer networks. In this regard, the increasing average degree of nodes, correlation of dependency links, number of fully overlapped links, and capacity of nodes can improve the robustness while the higher length of links, the strength of interdependency, size and number of communities, and number of layers can result in more vulnerable multilayer networks. Likewise, unidirectional links can make multilayer networks more fragile. Zhang et al (2019) declared that if node failure in a network layer does not cause node failure of the interdependent nodes in other layers, an increasing number of layers can make multilayer networks more robust. In Zhou et al (b) (2020), it was indicated that targeted attacks can undo the improving effect of correlated dependency links. While Dong et al (2020) considered feedback conditions in the model, the effect of feedback conditions on the robustness was not assessed. As it is shown in Table 2, the most common properties are coupling strength and node degree respectively while directed links and feedback conditions are the least common properties assessed in the studies. In total, almost all papers aimed at optimising the physical structure of the systems to strengthen infrastructures against failures, rather than evaluating decisions and strategies toward robustness. In more detail, studying the effect of costs, development plans, human operators, and the organisers' interactions gained less attention than adding and removing physical assets and components.

The vulnerability of an interdependent network is shown to be reducible either by optimising inter-network connections, load redistribution mechanisms or by hardening high degree nodes (Liu et al, 2016; Zio et al, 2011). Similarly, Munikoti et al (2021) indicated that securing system information is more crucial than physical hardening as results showed that a targeted attack on nodes with interdependency links causes higher damage than a random attack.

3.3 Robustness quantification

The measures to quantify the vulnerability of multilayer networks under attacks can be grouped into five; based on network connectivity, network performance, network efficiency, network stability, and network reliability. According to Beyza et al (2019) using the topological metrics can reduce the computation time needed to perform the studies by more than 80% in comparison to the load flow measurement. The first group which is topological-oriented and contains 77% of papers, includes 8 different metrics. Most of the papers in this group focused on the relative size of the remained giant component after the cascading failure in comparison to the initial size of the network. This metric usually comes with a threshold which is the minimum size of the remained nodes causing the network to a complete collapse (Liu et al, 2016). The larger the threshold the network is more robust. Below the critical threshold, there is no giant component, whereas above the critical threshold a giant component exists (Buldyrev et al, 2010). Limiao et al (2016) defined the threshold differently as the smallest size of the giant component, set according to the network operator's requirements for service continuity.

To evaluate the vulnerability of multilayer networks based on the network connectivity,

Rueda et al (2017) used Average Two-terminal Reliability (ATTR) measuring the sum over the number of node pairs in each connected component divided by the total number of node pairs in the initial network. In a case with the same percentage of nodes/links removal, the network with the highest ATTR value is considered to be more robust. In addition to the relative size of the giant component, Munikoti et al (2021) applied three other metrics including the number of remaining connected components (NCC), flow robustness (FR), and service robustness (SR). FR is the total number of nodes in all remaining components divided by the total number of nodes in the initial network that quantifies the overall reachability of the network. SR is the total weighted out-degree of nodes (the total sum of outgoing links weights) after cascading failure divided by the total weighted out-degree of all nodes in the initial network. Unlike the three other metrics, SR is capable of incorporating the weights that indicate the degree of dependency between two nodes. Similarly, Wu et al (2016) assessed the vulnerability by dividing the sum of links after cascading failure by the sum of links in the initial network. It can show the rate of service loss. They also used the sum of clusters in the remained giant component that each one includes at least one generation node and one distribution node divided by the initial number of the clusters in the initial network. Li et al (2015) employed a clustering coefficient to measure the robustness of the network. The clustering coefficient can be regarded as a local measure of connectivity since it characterises the extent to which nodes are adjacent to each other. Wu et al (2016) evaluated robustness based on the sum of links before and after the attack.

While all vulnerability metrics mentioned so far are based on the loss of network

connectivity, five papers considered the loss of network efficiency. Wang et al (2013) focused on network efficiency which was defined as the average shortest path length between pairs of nodes. Commodity flowing on longer paths needs more time and resources, so the efficiency of the network is lower. To avoid the infinity caused by the disconnection between two nodes, some other papers measured the efficiency of the network based on the average reciprocal shortest path length (Qi et al, 2019; Tian et al, 2017; Limiao et al, 2016; Zhang et al, 2016).

Five papers considered the loss of network performance. In two of these studies (Zhang et al, 2014; Zhao et al, 2018), the network performance was calculated based on the difference between the maximum flow in the network before and after the cascading failure. Maximum flow is a maximum amount of a commodity that can be routed without exceeding the capacity of any link through all possible paths between pairs of nodes (or source and sink nodes). It can be achieved by having a greater number of paths between source and sink nodes. Similarly, the Redundancy ratio was used by (Qi et al, 2019) as the average number of paths that only share their start and end nodes enabling the network to redistribute the flow at the location of the disruption. A low redundancy ratio implies low robustness as it indicates a fragmenting network. The network performance loss was calculated based on the betweenness centrality and degree of nodes before and after the attack varying according to the dependent intensity between the source and sink nodes (Beyza et al, 2019). Beyza et al (2019) assessed the network performance by quantifying the loads that remain connected in the network that allows the circulation of flows. In this case, loads were measured based on a real case study of power and gas networks.

Zhang et al (2019) used the network entropy to assess the network stability. It evaluates the ordered or disordered structure of the network according to the degree of nodes. The lower the entropy, the network structure tends to be more robust since it shows more stability. Limiao et al (2016) utilised network reliability which was calculated by using the number of realizations of which the system collapses before time t divided by the total number of realizations.

3.4 Testing robustness strategies

There are four types of attacks in general (Figure 1); (i) random attacks, (ii) localized attacks, (iii) targeted attacks, and (iv) probabilistic attacks. Random attacks represent a random failure of nodes as accidental damages in real-world systems. Localised attacks were applied to represent natural disasters like earthquakes and flooding (Wang et al, 2018). It can be grouped into two groups of localised attacks; oriented and focused attacks. In oriented localized attacks, some nodes in the same trajectory are removed first and then the failures propagate shell-by-shell or abruptly (Dong et al, 2020). In focused localized attacks, some individual nodes are removed randomly first and then the failures propagate shell-by-shell or abruptly. In targeted attacks, critical components are identified and targeted to maximise the damage. Nodes with a higher degree of links, betweenness centrality, clustering property, and nodes with interdependency links usually play a critical role in multilayer networks. According to this, they can be categorised into four; (i) degree-based attacks, (ii) centrality-based attacks, clustering-based attacks, and (iii) dependency-based attacks. Wu et al (2016) used the attack strength degradation model which is a targeted attack on nodes with higher centrality, but the

difference is that it considers a horizontal distance from the attacked node to show the degrading effect of the attack from the centre to its boundary. Moreover, removing nodes and links can be probabilistic. In other words, nodes and links are assigned a different probability to remove so nodes and links with higher probability are removed first. Dong et al (2020) applied these removal mechanisms to show the likelihood of roads liquefaction after the earthquake.

Amongst the 60 collected papers, only one of them applied probabilistic attacks while more than half of the papers (about 53%) considered random attacks. Targeted attacks and localized attacks are on the second and third rank, respectively. According to the findings, oriented localized attacks and clustering-based attacks are the most distractive than centrality-based attacks (Rueda et al, 2017; Tian et al, 2017). Focused localized attacks and degree-based targeted attacks are at the next level of being distractive (Tian et al, 2017). Random attacks and dependency-based attacks are among the least distractive attacks. However, all these results can be affected by the structure of the network models and removal mechanisms.

4. Results

All the methodologies applied to assess the robustness of multilayer networks have built and used too simplified models to evaluate this feature. Most of the multilayer models were synthetic models of infrastructure systems simplified by considering a few similar properties for all layers while real-world infrastructure systems usually contain multiple different characteristics. Complex systems like infrastructures need complex solutions (Oughton et al,

2018). So, more works are needed to evaluate all potential properties together to see if they have boosting or weakening effects on each other. It is necessary to investigate whether these properties show the same behaviour when they are combined or there are emergent behaviours as unexpected behaviours that stem from the multitude of interactions between different components (Johnson, 2006; Huang et al, 2012). Furthermore, the effect size of each property can be quantified to prioritise them in future planning.

Regarding the scope of this study, future works should focus on evaluating whether a model created by putting different network properties together would show unexpected behaviours or not. In other words, multilayer network models should contain different properties together to investigate if some properties boost or weaken the effect of other properties on the robustness and vulnerability of infrastructure systems. Since the results of the present study about the effect of different network properties on the robustness of infrastructure systems are mostly based on created simple models, it is needed to investigate whether these properties show the same behaviour when they are put together in a complex model and when they are a focus of a simple model. In addition, size of the effect of different properties on the robustness of infrastructure systems should be quantified to make more optimized decisions for improving infrastructure systems.

5. Conclusion

According to the important roles that infrastructure systems play in modern societies, it is necessary to make them as robust as possible to resist failures. In this way, a systematic review of literature was conducted, published since 2010, on the use of multilayer network models to

analyse the robustness of infrastructure systems. Among 60 collected papers, the most popular method is identified as the percolation theory. Most of the papers focused on topological properties rather than functional and dynamical properties. To improve the robustness, two groups of strategies were taken: strengthening the critical components and building up the structure of the network according to the network properties. On the other hand, most of the papers applied network connectivity to measure the robustness which is to calculate and compare the size of connected components before and after the attack. Among all attack types, the random removal mechanism is the most common in these studies. To sum, these studies mainly focused on physical features of multilayer network system and measured the robust performance accordingly. However, these approaches are too simplified.

These simplifications include the absence of models based on real-world data and the need for models that make fewer simplifying assumptions about the complex systems they are modelling. Models adopted different types of networks to represent infrastructure rather than representing infrastructures using real data. Real-world infrastructures have unique properties that are highly simplified in models. No papers considered all potential properties together. Although they could have boosting or weakening effects each other's performance. By considering all properties, the importance of different properties on the robustness of infrastructure systems can be quantified and compared in future studies.

Acknowledgments

Z. Mahabadi acknowledges University College London, Department of Civil, Environmental and Geomatic Engineering doctoral funding. L. Varga and T. Dolan thank EPSRC for grant

EP/R017727/1 relating to UK Collaboratorium for Research on Infrastructure and Cities (UKCRIC).

References

Baxter GJ et al (2014) Weak percolation on multiplex networks, *Physical Review E*, vol. 89.

Beyza J et al (2019) Applying complex network theory to the vulnerability assessment of interdependent energy infrastructures, *Energies*, vol. 12.

Boccaletti S et al (2014) The structure and dynamics of multilayer networks, *Physics Reports*, vol. 544, pp. 1-122.

Buldyrev SV et al (2010) Catastrophic cascade of failures in interdependent networks, *Nature*, vol. 464, pp. 1025–8.

Cao YY et al (2021) Percolation in multilayer complex networks with connectivity and interdependency topological structures, *Communications in Nonlinear Science and Numerical Simulation*, vol. 92.

Cellai D et al (2013) Percolation in multiplex networks with overlap, *Physical Review E*; 88(5):052811.

Cellai D et al (2016) Message passing theory for percolation models on multiplex networks with link overlap, *Physical Review E*, vol. 94.

Chen Y et al (2015) Extreme events in multilayer, interdependent complex networks and control, *Scientific Reports*, vol. 5.

Chen C et al (2017) Towards optimal connectivity on multi-layered networks, *IEEE Transactions on Knowledge and Data Engineering*, vol. 29.

Danziger MM et al (2016) The effect of spatiality on multiplex networks, *EPL*, vol. 115.

Danziger MM et al (2019) Dynamic interdependence and competition in multilayer networks,

Nature Physics, vol. 15, pp. 178-85.

Dong G et al (2013) Robustness of network of networks under targeted attack, *Physical Review E*, vol. 87.

Dong G et al (2015) Robustness of network of networks with interdependent and interconnected links, *Physica A*, vol. 11.

Dong G et al (2019) Localized attack on networks with clustering, *New Journal of Physics*, vol. 21.

Dong S et al (2020) A network-of-networks percolation analysis of cascading failures in spatially co-located road-sewer infrastructure networks, *Physica A*, vol. 538.

Dong Z et al (2019) Research on the connection radius of dependency links in interdependent spatial networks against cascading failures, *Physica A*, vol. 513, pp. 555-64.

Duan D et al (2019) Universal behavior of cascading failures in interdependent networks, *Proceedings of the National Academy of Sciences of the United States of America*, vol. 116, pp. 22452-7.

Dueñas-Osorio L et al (2007) Interdependent response of networked systems, *Journal of Infrastructure Systems*, vol. 13.

Fan J et al (2018) Structural resilience of spatial networks with inter-links behaving as an external field, *New Journal of Physics*, vol. 20.

Feng L et al (2015) The simplified self-consistent probabilities method for percolation and its application to interdependent networks, *New Journal of Physics*, vol. 17.

Fu G et al (2014) Interdependent networks: Vulnerability analysis and strategies to limit

cascading failure, *European Physical Journal B*, vol. 87.

Gross B et al (2020) Interconnections between networks acting like an external field in a first-order percolation transition, *Physical Review E*, vol. 101.

Han J et al (2021) An efficient layer node attack strategy to dismantle large multiplex networks, *European Physical Journal B*, vol. 94.

Havlin Sh et al (2015) Percolation of interdependent network of networks, *Chaos, Solitons & Fractals*, vol. 72, pp. 4-19.

Heracleous C et al (2017) Hybrid systems modeling for critical infrastructures interdependency analysis, *Reliability Engineering & System Safety*, vol. 165, pp. 89-101.

Hong S et al (2015) Failure cascade in interdependent network with traffic loads, *Journal of Physics A: Mathematical and Theoretical*, vol. 48.

Huang X et al (2012) The robustness of interdependent clustered networks. *Physics and Society*, vol. 101:18002.

Jiang WJ et al (2020) Depth Penetration and Scope Extension of Failures in the Cascading of Multilayer Networks, Complexity, vol. 2020.

Johnson CW (2006) What are Emergent Properties and How Do They Affect the Engineering of Complex Systems. Department of Computing Science, University of Glasgow, Glasgow.

Johnson CA et al (2019) Characterising the robustness of coupled power-law networks, *Reliability Engineering and System Safety*, vol. 191.

Kadović A et al (2018) Bond and site color-avoiding percolation in scale-free networks,

Physical Review E, vol. 98.

Kitchenham B (2004) Procedures for performing systematic reviews, UK, Keele University.

Kivela M et al (2014) Multilayer networks, *Journal of Complex networks*, vol. 2, pp. 203-71.

Li R et al (2015) Effect of clustering on attack vulnerability of interdependent scale-free networks, Chaos, Solitons and Fractals, vol. 80.

Li Y et al (2020) Vulnerability Assessment of Community-Interdependent Infrastructure Network Based on PSDA, Journal of Infrastructure Systems, vol. 26.

Li M et al (2021) Percolation on complex networks: Theory and application, *Physics Reports*, vol. 896, pp. 1-84.

Limiao Z et al (2016) Reliability analysis of interdependent lattices, *Physica A*, vol. 452.

Liu L et al (2016) Redundant design in interdependent networks, *PLoS ONE*, vol. 11.

Liu RR et al (2018) The weak interdependence of infrastructure systems produces mixed percolation transitions in multilayer networks, *Scientific Reports*, vol. 8.

Liu S et al (2021) Cascading Failure in Multiple Critical Infrastructure Interdependent Networks of Syncretic Railway System, *IEEE Transactions on Intelligent Transportation Systems*.

Mahabadi Z et al (2021) Network Properties for Robust Multilayer Infrastructure Systems: A Percolation Theory Review. *IEEE Access*, vol. 9, p.p. 135755-73.

Moussa B et al (2018) Critical links identification for selective outages in interdependent power-communication networks, IEEE Transactions on Industrial Informatics, vol. 14.

Munikoti S et al (2021) Robustness assessment of Hetero-functional graph theory-based model

of interdependent urban utility networks, *Reliability Engineering and System Safety*, vol. 212.

Oughton E et al (2018) Infrastructure as a Complex Adaptive System. *Complexity*, vol. 2018.

Qi M et al (2019) Optimal disintegration strategy in multiplex networks under layer node-based attack, *Applied Sciences (Switzerland)*, vol. 9.

Rueda DF et al (2017) 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.

Shekhtman LM (2018) Percolation of hierarchical networks and networks of networks, *Physical Review E*, vol. 98.

Shekhtman LM et al (2015) Resilience of networks formed of interdependent modular networks, *New Journal of Physics*, vol. 17.

Tian M et al (2017) Cascading failures in interdependent modular networks with partial random coupling preference, *Modern Physics Letters B*, vol. 31.

Vaknin D et al (2017) Spreading of localized attacks in spatial multiplex networks, *New Journal of Physics*, vol. 19.

Wang S et al (2013) Vulnerability analysis of interdependent infrastructure systems under edge attack strategies, *Safety Science*, vol. 51.

Wang S et al (2018) A methodological framework for vulnerability analysis of interdependent infrastructure systems under deliberate attacks, *Chaos, Solitons & Fractals*, vol. 117, pp.

21-9.

Wang W et al (2018) An approach for cascading effects within critical infrastructure systems, *Physica A*, vol. 510.

Wang J et al (2019) Targeted attack on correlated interdependent networks with dependency groups, *Physica A*, vol. 536.

Wang N et al (2021) Cascading failures of overload behaviors on interdependent networks, *Physica A*, vol. 574.

Wu B et al (2016) Modeling cascading failures in interdependent infrastructures under terrorist attacks, *Reliability Engineering and System Safety*, vol. 147.

Xie J et al (2017) Eradicating abrupt collapse on single network with dependency groups, *Proceedings of the National Academy of Sciences of the United States of America*, vol. 114, pp. 3311-15.

Yağan O et al (2012) Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness, *IEEE Transactions on Parallel and Distributed Systems*, vol. 23.

Yuan X et al (2017) Eradicating catastrophic collapse in interdependent networks via reinforced nodes, *Proceedings of the National Academy of Sciences of the United States of America*, vol. 114, pp. 3311-5.

Zhang Y et al (2016) Modeling and simulation of the vulnerability of interdependent power-water infrastructure networks to cascading failures, *Journal of Systems Science and Systems Engineering*, vol. 25.

Zhao DW et al (2016) The robustness of multiplex networks under layer node-based attack, Scientific Reports, vol. 6.

Zhao C et al (2018) Criticality assessment of urban interdependent lifeline systems using a biased PageRank algorithm and a multilayer weighted directed network model, *International Journal of Critical Infrastructure Protection*, vol. 22.

Zhao D et al (2018) Optimal dismantling of interdependent networks based on inverse explosive percolation, *IEEE Transaction on Circuits and Systems II*, vol. 65, pp. 953-7.

Zhang J et al (2014) An approach for modeling vulnerability of the network of networks, *Physica A*, vol. 412.

Zhang M et al (2019) Analysis of overload-based cascading failure in multilayer spatial networks", Chinese Physics B, vol. 29.

Zhou D et al (a) (2020) Dependency-based targeted attacks in interdependent networks. *Physical Review E*, vol. 102.

Zhou L et al (b) (2020) The Robustness of Interdependent Networks with Traffic Loads and Dependency Groups, *IEEE Access*, vol. 8, pp. 98449-59.

Zhou D (2012) Assortativity decreases the robustness of interdependent networks, *Physical Review E*, vol. 86.

Zio E et al (2011) Modeling interdependent network systems for identifying cascade-safe operating margins, *IEEE Transactions on Reliability*, vol. 60.

Zorn C et al (2020) Evaluating the magnitude and spatial extent of disruptions across interdependent national infrastructure networks, ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering, vol. 6.

Table 1. Search query

Search query	Search string 1	("complex system*" OR "inter$dependent system*" OR "system of systems" OR "inter$linked network*" OR "inter$related network*" OR "inter$active network*" OR "inter$connected network*" OR "hierarchical network*" OR "inter$dependent network*" OR "complex network*" OR "multi$layer network*" OR "multiple network*" OR "multiplex network*" OR "Multi$variate network*" OR "Multi$network*" OR "Multi$relational network*" OR "Multi$dimensional network*" OR "Multi$slice network*" OR "Multi$type network*" OR "network of networks" OR "coupled network")
		AND
	Search string 2	infrastructur*
		AND
	Search string 3	robust*

Accepted manuscript
doi: 10.1680/jsmic.22.00015

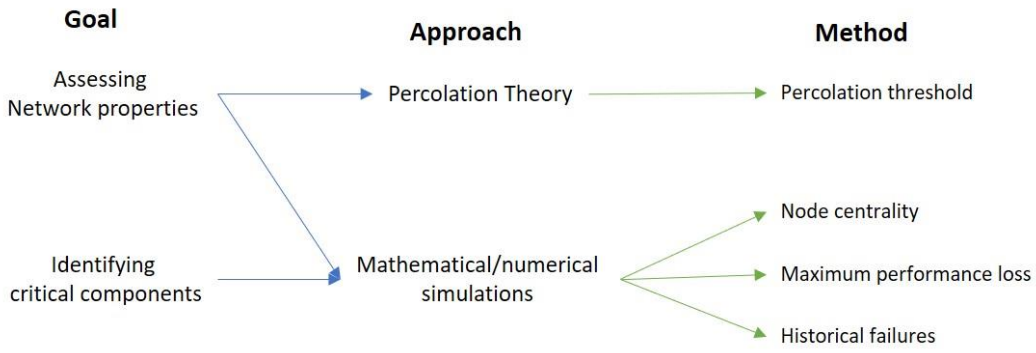
Table 2. Applied network properties

Network property	Definition	Number of studies	References
Strength of interdependency between nodes	Number of dependency links/ the tolerance of nodes in layer A to the failure of their interdependent nodes	12	Dong et al, 2019; Gross et al, 2020; Wang et al, 2018; Duan et al, 2019; Fan et al, 2018; Danziger et al, 2019; Jiang et al, 2020; Cao et al, 2021; Zhou et al (a), 2020; Shekhtman et al, 2015; Dong et al, 2013; Yuan et al, 2017.
Average degree of nodes within layers	Average number of links per node in a layer	9	Vaknin et al, 2017; Duan et al, 2019; Liu et al, 2018; Jiang et al, 2020; Zhou et al (a), 2020; Zhou et al (b), 2020; Wang et al, 2018; Shekhtman, 2018; Dong et al, 2013.
Size and number of nodes community	Groups of nodes in layers as clusters, modules, and dependency groups	8	Dong et al, 2019; Xie et al, 2017; Kadović et al, 2018; Zhou et al (b), 2020; Wang et al, 2018, Wang et al, 2019, Shekhtman, 2018; Shekhtman et al, 2015.
Correlation of dependency links	Interlinking nodes based on their centrality ranks between different layers	5	Danziger et al, 2016; Dong et al, 2019; Feng et al, 2015; Zhou et al (b), 2020; Wang et al, 2019.
Number of layers	Number of network layers	4	Dong et al, 2019; Vaknin et al, 2017; Xie et al, 2017; Cao et al, 2021.

Higher length of links	The spatial distance between two nodes	3	Danziger et al, 2016; Vaknin et al, 2017; Dong et al;2019.
Number of fully overlapped links	When two same nodes are connected in more than one layer	3	Danziger et al, 2016; Cellai et al, 2013; Cellai et al, 2016.
Capacity of nodes	Proportional to the initial load of a node as its betweenness centrality	2	Duan et al, 2019; Zhou et al (b), 2020.
Presence of directed links	One directional links between two nodes	2	Liu et al, 2016; Dueñas-Osorio et al, 2007.
Feedback conditions	When a node in a layer have more than one link to the nodes in the other layer	1	Dong et al (2020).

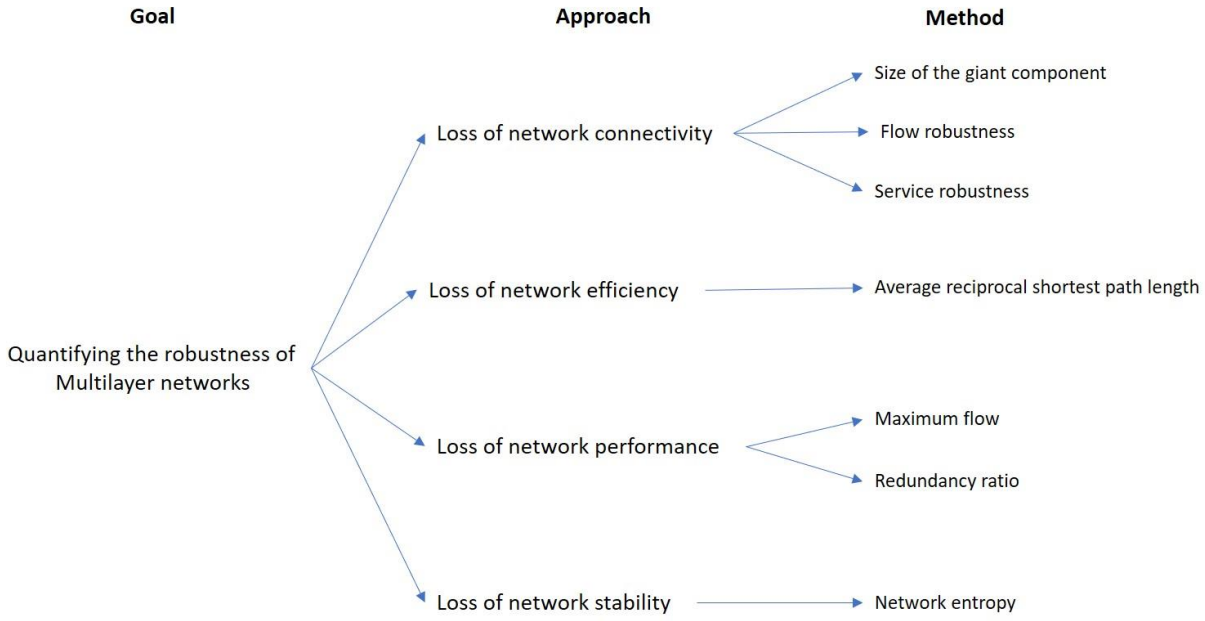
Accepted manuscript
doi: 10.1680/jsmic.22.00015

Figure 1. Approaches to assess the robustness through two strategies; 1- network properties, 2- critical component



Accepted manuscript
doi: 10.1680/jsmic.22.00015

Figure 2. Approaches to quantify robustness



Accepted manuscript
doi: 10.1680/jsmic.22.00015

Figure 3. Schematic diagram to show the initiation of attacks in a layer. The green areas represent the nodes that are attacked. The dashed red line represent dependency links; a) random attacks, b) oriented localized attacks, c) focused localized attacks, d) degree-based targeted attacks, e) dependency-based targeted attacks, f) probabilistic attacks