GEOGRAPHICAL INTERDEPENDENT ROBUSTNESS MEASURES IN TRANSPORTATION NETWORKS

Diego Fernando Rueda Pepinosa

Universitat de Girona

DOCTORAL THESIS

GEOGRAPHICAL INTERDEPENDENT ROBUSTNESS MEASURES IN TRANSPORTATION NETWORKS

Diego Fernando Rueda Pepinosa

2018

Universitat de Girona

DOCTORAL THESIS

GEOGRAPHICAL INTERDEPENDENT ROBUSTNESS MEASURES IN TRANSPORTATION NETWORKS

Diego Fernando Rueda Pepinosa

2018

DOCTORAL PROGRAM IN TECHNOLOGY

Supervisor:
Ph.D. Eusebi Calle

This thesis is presented in fulfillment of the requirement for the conferral of the degree of Doctor of Philosophy by the University of Girona

Girona, 21/09/2018

Thesis Report

Informe favorable del director de la tesis con el visto bueno a este depósito

By Dr. Eusebi Calle, advisor of the thesis:

Geographical interdependent robustness measures in transportation networks

submitted by Diego Rueda.

Summary of the manuscript

This thesis is focused in the study of the robustness of interdependent networks, considering the network model, the interdependency model and the failure model. The robustness of different interdependent networks models under large-scale failures and, in particular, to consider interdependent networks where at least one of the networks is a telecommunication network is presented. Both, the effects of different network models and the dynamic process of failure propagation between networks are considered. New interconnection strategies are proposed to improve the robustness of the interconnected networks in scenarios under targeted attacks and cascading failures.

Evaluation and analysis of the presented work

His research presented in this thesis is a valuable contribution to the Network Robustness analysis in Interdependent networks research field and is validated with his 2 publications in JCR indexed International Journals and several publications in proceedings of high-level international journals.

Acceptance of thesis defense

In my opinion, Diego Rueda has fulfilled the requirements to be recommended to present his thesis at a public defense leading to the Doctor degree at tha University of Girona

Dr. Eusebi Calle

Associated Professor (University of Girona)

Acknowledgments

First at all, a very special thank you to my family for thier unconditional love, support and motivation to help me reach this goal. This accomplishment would not have been possible without them.

I must thank my advisor Dr. Eusebi Calle his constant support, supervision, guidance and encouragement over the last four years of my doctoral studies. I would also like to express my gratitude to Dr. José Luis Marzo for his interesting discussions about this research work. Their knowledge and advice have contributed to the successful results in this dissertation.

I would also like to thank all the members in the Broadband Communications and Distributed Systems (BCDS) research group, especially Dan with whom I had the opportunity to share some good moments of friendship during my time in Girona. I also apprecaite the valuable contributions that Dr. Xiangrong Wang and Dr. Robert Kooij, from TU Delft (The Netherlands), have made to different aspects of this dissertation. Finally, I would like to thank the anonymous reviewers of our papers for their valuable feedback which helped improved the quality of each and every one of the papers presented here.

This research work was partiality supported by the Spanish Spanish Ministry of Economy and Competitiveness and the DURSI consolidated research group (CSI Ref. SGR-1469) through the RoGER (TEC 2012-32336) and GIROS (TEC 2015-66412-R) projects.

List of Acronyms

ACIC Assortative Coupling In Communities

ACWC Assortative Coupling With Communities

AL2S Advanced Layer 2 Service

AS Autonomous System

ATTR Average Two-Terminal Reliability

BC Blocked Connections

BCDS Broadband Communications and Distributed Systems

BN Bayesian Network

CPP Controller Placement Problem

CME Coronal Mass Ejections

D Diameter

DCPP Dynamic Controller Provisioning Problem

DoS Denial of Service

E Elasticity

EC Established Connections

EGR Effective Graph Resistance

EMP Electromagnetic Pulse

EPDs Effective Path Diversities

ER Erdős-Rényi

FTCP Fault Tolerant Controller Placement

GD Graph Diversity

GIROS Geographically-constrained and Interdependent networks: RObustness indicatorS

GMPLS General Multiprotocol Label Switching

HHM Hierarchical Holographic Modeling

HLA High Level Architecture

IDD Inter Degree-Degree

IP Internet Protocol

LCC Largest Connected Component

LMCC Largest Mutually Connected Component

MPLS Multiprotocol Label Switching

MTFR Minimum Total Failure Removal

NoN Network of Networks

NST Number of Spanning Trees

OESS Open Exchange Software Suite

OSS Operation Support Systems

PC Principal Component

PN Petri Net

PoP Point of Presence

QLRM QuaLitative Robustness Metric

QNRM QuaNtitative Robustness Metric

QoS Quality of Service

RCIC Random Coupling In Communities

RGG Random Geometric Graph

RID Random Inter Degree-degree

RoGER Robustness against Large-Scale Failures in Interdomain routing

RPCP Resilient Placement Controller Problem

SDN Software Defined Network

SF Scale-Free

SR Symmetry Ratio

SW Small-World

TGD Total Graph Diversity

VC Viral Conductance

VLAN Virtual Local Area Network

WMD Weapons of Mass Destruction

WS Weighted Spectrum

WWW World Wide Web

List of Tables

List of Figures

List of Publications

This research work has been published in the following international journals and proceedings of international conferences:

1 D. F. Rueda, E. Calle, X. Wang. and R. Kooij. ”Enhanced Interconnection Model in Geographical Interdependent Networks”. In: *International Journal of Computers Communications & Control*. 13.4 (Aug. 2018). pp. 537-549.

2 D. F. Rueda, E. Calle, and J. L. Marzo. ”Robustness Comparison of 15 Real Telecommunication Networks: Structural and Centrality Measurements”. In: *Journal of Network and Systems Management* 25.2 (Apr. 2017). pp. 269289.

3 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”. In: *International Journal of Critical Infrastructure Protection* 16 (Mar. 2017). pp. 312.

4 J. L. Marzo, E. Calle, S. Gómez-Cosgaya, D. F. Rueda and A. Mañosa, ”On selecting the relevant metrics of network robustness”. In: *Proceedings of the 2018 10th International Workshop on Resilient Networks Design and Modeling (RNDM)*. Longyearbyen, Norway: IEEE, Aug. 2018, pp. 1-7.

5 D. F. Rueda, E. Calle, and J. L. Marzo. ”Improving the Robustness to Targeted Attacks in Software Defined Networks (SDN)”. In: *Proceedings of the 2017 13th International Conference on Design of Reliable Communication Networks (DRCN)*. Munich, Germany: VDE VERLAG GMBH, Mar. 2017, pp. 78-85. ISBN: 978-3-8007-4383-4.

6 D. F. Rueda, E. Calle, F. A. Maldonado-Lopez, and Y. Donoso. ”Reducing the impact of targeted attacks in interdependent telecommunication networks”. In: *Proceedings of the 2016 23rd International Conference on Telecommunications (ICT)*. Thessaloniki, Greece: IEEE, May 2016, pp. 348352. ISBN: 978-1-5090-1990-8.

7 D. F. Rueda and E. Calle. ”Enhanced Interconnection Model in Geographical Interdependent Networks”. In: *Proceedings of the 3rd Delft - Girona Workshop on Robustness of Networks*. Conference with abstract only. Delft, The Netherlands, Jul. 2017.

8 D. F. Rueda and E. Calle. ”The Effect of Interdependency Matrices on Failure Spreading in Interdependent Critical Infrastructures that Involve Telecommunication Networks”. In: *Proceedings of the I Conference of Pre-Doctoral Researches of the UdG*. Conference with abstract only. Girona, Spain, Jun. 2017. ISBN: 978-84-8458-502-2.

9 D. F. Rueda, E. Calle, and J. L. Marzo. ”Detecting the most Relevant Robustness Parameters in Telecommunication Networks”. In: *Proceedings of the 1st Delft - Girona Workshop on Robustness of Networks*. Conference with abstract only. Girona, Spain, Jun. 2015.

Contents

Abstract

Telecommunication networks, power grids, water/gas networks, metro and rail systems are some examples of transportation networks where this thesis is focused. Nowadays, most of these are crucial to support our modern society way of life. These critical infrastructures are built to geographically distribute resources over a certain region. Single failures can occur in a network and most of them have been well investigated and can be dealt with and eliminated. However, multiple failures, which are irrelevant statistically, cause catastrophic consequences to the normal operation of these networks. Unlike single failures, multiple failures cannot be solved, but their consequences can be mitigated. In this sense, guaranteeing network robustness to avoid users and services being affected is essential. However, most critical infrastructures in the real world cannot be adequately depicted as single isolated networks and so have to be represented as two or more interdependent networks. In interdependent networks, node interactions are represented by connectivity links withing the networks (intralinks) and dependency links between the networks (interlinks).

The proper performance of interdependent networks depends on the normal operation of the networks that are interconnected. In order to study the robustness of interdependent networks, three factors should be considered: the network model, the interdependency model and the failure model. In interdependent networks, a small fraction of the nodes removed from one network may lead to a dynamic failure process involving both networks and cause severe consequences to the networks' operation. The aim of this thesis is to measure and analyze the robustness of different interdependent networks models under large-scale failures and, in particular, to consider interdependent networks where at least one of the networks is a telecommunication network. Both, the effects of different network models and the dynamic process of failure propagation between networks are considered. New interconnection strategies are proposed to improve the robustness of the interconnected networks. This thesis mainly focuses on two types of large-scale failures: targeted attacks and cascading failures.

Part of this thesis is also focused on analyzing and enhancing some previous work in both single and interdependent networks. Hence, the topological properties of

telecommunication networks that determine the sensitivity to random failures and targeted attacks are identified and compared with previous studies. Through this analysis the most relevant topological properties that can be used to group networks with similar robustness behavior are identified. In the case of interdependent networks, robustness under targeted attacks is analyzed for different interlink patterns between two networks. The identification of the critical nodes according to the most dangerous targeted attack in one network is used to interconnect networks with similar and dissimilar topological properties as a more real case. Results indicate that the interlink patterns can identify critical new parts in the networks and an attack in a network can change when it is spread to another network. Moreover, by selecting a suitable interlink pattern, the robustness level under targeted attacks can be improved.

Additionally, interdependent networks can help to study the interconnection of physical and logical layers in telecommunication networks (a more general vision of network multilayer research). Thus, as a study case a robust design of a Software Defined Network (SDN) is proposed by identifying the critical nodes of the physical network to find suitable placement for the controllers. By comparing previous proposals, the SDN network resulting from this new approach performs better in the case of targeted attacks. Finally, based on previous study, an enhanced region-based interconnection model is proposed by considering a limit to the number of interlinks between the interconnected nodes. The new interconnection model has yielded promising results in maintaining an acceptable level of network robustness under cascading failures with a limited number of interlinks.

Resumen

Las redes de telecomunicaciones, eléctricas, agua/gas, metros o ferroviarias son un ejemplo de redes de transporte. Actualmente, la mayoría de ellas con cruciales para soportar nuestro modo de vida de la sociedad moderna. Estas infraestructuras críticas están construidas para distribuir recursos geográficamente sobre ciertas zonas. Una falla individual puede ocurrir en una red y la mayoría de estas han sido bien investigadas y pueden enfrentadas y eliminadas. No obstante, las fallas múltiples, las cuales son irrelevantes estadísticamente, causan consecuencias catastróficas a la operación normal de estas redes. A diferencia de las fallas individuales, las fallas múltiples no pueden ser resueltas, pero sus consecuencias pueden ser mitigadas. Sin embargo, la mayoría de las infraestructuras críticas del mundo real no pueden ser descritas como redes independientes, por lo cual tienen que ser representadas como dos o más redes interdependientes. En las redes interdependientes, las interacciones entre nodos son representadas por enlaces de conectividad internos (*intralinks*) y enlaces de dependencia (*interlinks*).

El correcto funcionamiento de las redes interdependientes depende de la operación normal de las redes que están interconectadas. A la hora de estudiar la robustez de las redes interdependientes, tres factores han de ser considerados: el modelo de la red, el modelo de interdependencia y el modelo de falla. En las redes interdependientes, una pequeña fracción de nodos removidos de una red puede desencadenar un proceso de fallo dinámico que involucra ambas redes y causa consecuencias severas en la operación de las redes. El objetivo de esta tesis es medir y analizar la robustez de diferentes modelos de redes interdependientes bajo fallas de gran escala y, en particular, considerar redes interdependientes donde al menos una de las redes es una red de telecomunicaciones. Los efectos de diferentes modelos de red y procesos dinámicos de propagación de fallos entre redes son considerados. Nuevas estrategias de interconexión son propuestas para mejorar la robustez de las redes interconectadas. El principal tipo de fallas que se abarcan en esta tesis son las fallas a gran escala, cuando se producen tanto por ataques dirigidos como por fallas en cascada.

Parte de esta tesis también se enfoca en analizar y mejorar algunos trabajos previos

tanto en redes individuales como en redes interdependientes. En este caso, se identifican las propiedades topológicas de las redes de telecomunicaciones que determinan la sensibilidad a fallas aleatorias y ataques dirigidos y se comparan con estudios previos. Mediante este análisis se extraen las propiedades topológicas más relevantes que pueden ser usadas para agrupar redes con un comportamiento de robustez similar. En el caso de las redes interdependientes, la robustez bajo ataques dirigidos es analizada para diferentes patrones de enlaces de interdependencia (*interlinks*) entre dos redes. La identificación de los nodos críticos en el ataque dirigido más peligroso en una red es usada para interconectar redes con propiedades topológicas similares y disimilares como un caso más real. Los resultados indican que los patrones de enlaces de interdependencia pueden identificar nuevas partes críticas en la red y un ataque en una red puede cambiar cuando se propaga hacia la otra red. También, la adecuada selección del patrón de interdependencia puede mejorar el nivel de robustez bajo ataques dirigidos.

Adicionalmente, las redes interdependientes pueden ayudar al estudio de la interconexión de las capas física y lógica en las redes de telecomunicaciones (una visón más general de la investigación de redes multicapa). En este caso, se propone el diseño robusto de una red SDN considerando la identificación de los nodos críticos de la capa física para encontrar las ubicaciones adecuadas para los controladores. Comparando con propuestas previas, la red SDN resultante de esta nueva propuesta mejora el rendimiento frente a ataques dirigidos. Finalmente, teniendo en cuenta los estudios previos, se propone un modelo mejorado para la interconexión basada en regiones considerando un límite para el número de enlaces de interconexión entre las redes interconectadas. Los resultados presentados muestran que el nuevo modelo de interconexión mantiene unos niveles de robustez aceptables bajo fallas en cascada con un número limitado de enlaces de interdependencia (*interlinks*).

Resum

Les xarxes de telecomunicacions, alta tensió, aigua/gas, metro o ferrocarrils son un exemple de xarxes de transport. Actualment, la majoria d'elles son crucials per suportar el nostre mode de vida a la societat moderna. Aquestes infraestructures critiques estan construïdes distribuint els recursos en certes zones geogràficament localitzades. Una fallada individual o aïllada, que pot ocórrer a la xarxa, solen ser esdeveniments controlats i ben investigats per ser afrontades i/o eliminades. No obstant, les fallades múltiples, encara que estàticament menys importants, poden causar conseqüències catastròfiques al normal funcionament de la xarxa. A diferencia de les fallades individuals, les fallades múltiples no solen poder-se solucionar, però poden aplicar-se mètodes per mitigar les seves conseqüències. En aquest sentit, garantir la robustesa de la xarxa es essencial per preservar els serveis previstos als usuaris. No obstant, la majoria de les infraestructures critiques en el mon real no poden ser descrites con a xarxes independents, per tant han de ser representades com dos o més xarxes interdependents. En les xarxes interdependents, les interaccions son representades connectant enllaços de dependències (interlinks).

El correcte funcionament de les xarxes interdependents depèn del correcte mode d'operació de les xarxes que estan interconnectades. A l'hora d'estudiar la robustesa de les xarxes interdependents, tres aspectes s'han de considerar: el model de xarxa, el model d'interdependències i el model de fallades. En xarxes interdependents, una petita fracció de nodes eliminats en una xarxa pot desencadenar un procés de fallades dinàmiques entre les dues xarxes causant conseqüències severes a l'operativitat de la xarxa. L'objectiu d'aquesta tesis és mesurar i analitzar la robustesa de diferents models de xarxes interdependents sota fallades de gran abast i, en particular, considerant que almenys una de les xarxes analitzades sigui una xarxa de telecomunicacions. Els efectes dels models de xarxa i dels processos dinàmics de propagació de fallades entre les xarxes es tenen en compte. Proposem noves estratègies d'interconnexió per millorar la robustesa de la xarxes interconnectades. El principal tipus de fallades que cobrim en aquesta tesis, son les fallades de gran abast, quan es produeixen tan atacs dirigits com fallades en cascada.

Part d'aquesta tesis també es focalitza en analitzar i millorar algunes del les anteriors

propostes tan en xarxes úniques com en xarxes interdependents. En aquest cas, es proposa una comparació de propietats topològiques i com afecten al grau de robustesa front atacs dirigits en xarxes de telecomunicacions. A través d'aquest anàlisis, s'extreu quines son les propietats topològiques més rellevants per poder agrupar xarxes amb nivells similars de robustesa. En el cas de xarxes interdependents, la robustesa front atacs dirigits s'analitzen diferents patrons de interlinks per connectar les dues xarxes. La identificació dels nodes més crítics segons l'atac més incisiu en una xarxa s'utilitza com a model d'interconnexió entre topologies amb propietats topològiques similars o dispars. Els resultats indiquen que els patrons d'interconnexió poden identificar noves parts crítiques a la xarxa on un tipus d'atac pot canviar el seu comportament quan propaga a l'altre xarxa. La conclusió, és que un bon patró d'interconnexió pot elevar el nivell de robustesa d'avant atacs dirigits.

Addicionalment, les xarxes interdependents poden ajudar a l'estudi de les xarxes física i lògica d'una xarxa de telecomunicació (com a visió més general de l'estudi de xarxes multicapa). En aquest cas, s'ha realitzat l'estudi del disseny de xarxes SDN considerant la identificació dels nodes crítics de la capa física per triar el posicionament adequat dels controladors. Comparant amb propostes anteriors, la xarxa SDN resultant d'aquesta nova aproximació millora el rendiment front a atacs dirigits. Finalment, basant-nos en estudis previs, presentem un nou model d'interconnexió per regions considerant la limitació d'Inter enllaços entre xarxes. Els resultats presentats mostren el manteniment d'uns nivells acceptables de robustesa davant fallades en cascada amb número limitat d'*interlinks*.

Chapter 1

Introduction

1.1 Motivation

Transportation networks support most areas of daily life including fundamental systems and services that are indispensable to the security, economic, and social well-being of our countries and communities [1, 2]. Customers, businesses, governments and the military depend on telecommunication networks to satisfy, not only their communication needs, but also to access information, obtain products and services, manage finances, handle commerce transactions, respond to disasters, execute network centric operations and wage warfare [2]. Telecommunication networks, along with water supply systems, power grids, transportation systems, oil and gas pipelines, are critical infrastructure systems. Therefore, these infrastructures must have the ability to provide and maintain an acceptable level of service in the face of multiple failures and challenges to normal operation [2]. Network robustness, defined as the ability of a network to continue to operate when subjected to failures [3], can be evaluated by measuring the impact large-scale failures have in different scenarios.

Large-scale failures in critical infrastructures rarely occur, but when they do, their consequences are catastrophic and expensive. Failures in critical infrastructures imply service disruptions that can affect thousands of people, multiple communities, entire countries, or delimited geographical areas [4]. For instance, in 2014, a human error in configuring Time-Warner's Internet routers in the United States resulted in a failure that prevented 11.4 million clients from accessing broadband services for three hours [5]. Another well-studied large-scale example is the 2003 Northeast Blackout in the United States and Canada, where an overload in a transmission line resulted in 50 million people losing power for up to two days and an estimated cost of US$ 6 billion [6]. This blackout also affected essential provisioning services such as water supply, metro and mobile communication.

Failures have different origins. Sometimes an element of the network fails without any specific pattern (random failures), and other times are generated by targeted attacks on the most important network elements (sequential or simultaneous targeted attacks) [2]. Usually, natural disasters (hurricanes, earthquakes, tsunamis, tornadoes, floods or forest fires), man-made disasters (Electromagnetic Pulse (EMP), Weapons of Mass Destruction (WMD) or terrorist attacks), technology-related failures (power grid blackouts, hardware failures, dam failures or nuclear accidents), or cyber-attacks (viruses, worms or denial of services attacks) are responsible for large-scale failures in transportation networks [2, 7]. In some cases, failures can spread within the network or generate cascading failures. In the literature, a wide range of metrics for measuring the network robustness can been found [8–11]. These metrics are either based on the structural or centrality properties of networks, or can be measured from the networks' quality of service parameters of networks [9–11].

One of the lines of research the Broadband Communications and Distributed Systems (BCDS) research group at the University of Girona (Spain) has is the robustness analysis of transportation networks under multiple failures and several doctoral dissertations and research projects have been carried out by the BCDS research group in this area. In [12] the multi-layer survivability in routing schemes for GMPLS-based networks was studied. The robustness against large-scale failures in telecommunication networks was also analyzed in [13] and subsequently, new robustness evaluation mechanisms for complex networks were proposed in [8]. In addition to these doctoral dissertations, the BCDS research group has carried out the RoGER project [14], financed by the Spanish Ministry of Economy and Competitiveness. The RoGER project evaluates the robustness of interdomain routing networks to large-scale failures, develops new failure models and denes new robustness metrics [14]. As can be seen in Table 1.1, in these projects, network models failure models and robustness metrics have been considered as the main aspects with which to analyze the robustness in the case of isolated transportation networks.

However, many critical infrastructures are highly dependent and need to interact with another to produce and distribute the essential goods and services required for the proper functioning of society [1]. Therefore, recent years have seen the interest in robustness analysis research, not only for isolated complex networks, but also for interdependent networks [15]. In interdependent networks, node interactions are represented by connectivity (intralinks) and dependency links (interlinks). A critical infrastructure in which the nodes of two or more networks are interconnected by interlinks is known as an interdependent network. A key property of interdependent networks is that a node failure in one network can spread to nodes in the interconnected networks [16]. Hence, interdependencies between critical infrastructures mean that the behavior and reliability

Table 1.1: Aspects considered when studying the robustness of single networks

Topic	Description
Network model	Defines how the networks are modeled: • *Theoretical models*: random, scale free, small world, etc. • *Real networks*: power grids, rail and telecommunication networks
Failure model	Defines how the network elements are removed from the network: • Random failures • Targeted attacks: Sequential and simultaneous • Cascading failures • Virus and epidemics
Robustness metrics	Defines how the failure impact is measured: • Structural metrics • Centrality metrics • Functional metrics

of one network depend on the other networks [7, 16, 17].

In interdependent networks a small fraction of removed nodes in one network may lead to a dynamic failure process and cause severe consequences to the networks' operation [16, 17]. Previous studies have pointed out that there is a critical fraction of interdependent nodes above which a single node failure can lead to cascading failures collapsing the whole system, whereas below this critical dependency a failure of a few nodes causes very little damage to the network [16–19]. A good example of interdependent networks is the interconnection of a power grid and a telecommunication network, where the power grid relies on the telecommunication network for control and the telecommunication network relies on the power grid for electricity supply [20]. A well-studied real case of large-scale failures in interdependent networks was the 2003 Italy Blackout, where a single failure in the power grid resulted in failures that propagated over a telecommunication network, ultimately affecting more than 55 million people [16, 20].

As the added complexity of interdependent networks poses new challenges the interest to research in this area has likewise increased. [21]. Aspects, such as a network model of the topologies to be interconnected, an interdependency model between the interconnected networks and a failure model that affects the network, are decisive to

Table 1.2: Aspects to consider in interdependent network scenarios

Topic	Description
Network model	Interdependent networks should be represented by models that capture the topological properties of the transportation networks to be interconnected. These properties partially define the network's sensitivity to certain types of failure scenarios.
Interdependency model	Defines the properties of the interconnections between the nodes in the networks to be interconnected: • *Interdependency type*: Defines the relationship that exists between the interconnected nodes. This can be physical, cyber, geographical or logical interdependency [1]. • *Interlink type*: Defines the dependency between two interconnected nodes. Thus, an interlink can be unidirectional [16] or bidirectional [23]. • *Interconnection type*: Represents the number of nodes placed in the other network that are interconnected to a node. Thus, interconnection type can be one-to-one nodal correspondence [16] or one-to-multiple nodal correspondence [23]. • *Interlink pattern*: Defines if nodes are to be randomly interconnected or to follow a certain pattern [25]. • *Interconnection constraint*: This restrict which nodes can be interconnected, e.g., centrality (related to node importance in each network) [29], functionality (related to services to be offered) [25, 34] or distance (related to node location) [38].
Failure Model	Defines how the network elements are disconnected/removed. Network failures can be generated from random failures or targeted attacks on nodes or links, which lead t o dynamic failure processes such as: • Single affectation to its interconnected nodes • Cascading failure process

define the vulnerability and behavior of interdependent networks under multiple failures. Therefore, understanding and analyzing the interdependency between transportation networks is essential in order to design more robust interdependent networks. Most of the previous work is focused on analyzing the robustness of interdependent networks in the context of random failures and targeted attacks triggering a cascading failure process [16, 18, 19, 22–28]. Meanwhile, other studies are focused on identifying the influence intedependency types have on the propagation of failures between the interconnected networks [25, 29–37]. A summary of the aspects that have been considered when constructing scenarios to evaluate the interdependent network robustness is shown in Table 1.2.

The Geographically-constrained and Interdependent networks: RObustness indicatorS (GIROS) project, which is being carried out by the BCDS research group, is responding to these challenges by developing new robustness analysis models for interdependent networks [39]. This research thesis aims to contribute to the GIROS project by measuring and analyzing the robustness of different interdependent network models under large-scale failures, and with a particular focus on interdependent networks where at least one of the networks is a telecommunication network. The effects of different network topologies and the dynamic process of failure propagation between networks are also considered and new interconnection strategies are defined to improve the robustness of the interconnected networks. The case studies considered in this thesis capture the essential properties of interdependent networks, consequently they can be used by network administrators in real scenarios in order to identify critical points in their networks, to improve investment strategies and to assess the social and economic risks of the critical infrastructure in question. The four scenarios to be studied in this research work are as follows:

1. Two networks with similar topological properties being interconnected by bidirectional interlinks and one-to-one nodal correspondence. This scenario represents interconnection case of of two backbone telecommunication networks or the interlayer relations in telecommunication networks.

2. Two networks with different topological properties being interconnected by bidirectional interlinks and one-to-one nodal correspondence. This scenario represents, for instance, the case of a telecommunication network connected to a power grid, and vice versa.

3. A multilayer network represented by bidirectional interlinks and one-to-one nodal correspondence. This study depicts the case of a Software Defined Network (SDN) modeled as an interdependent network by considering two networks: 1) a physical network, and 2) a control network running over the physical network.

4. Two geographical networks being interconnected by bidirectional interlinks and one-to-multiple nodal correspondence. This scenario represents the case of two telecommunication networks being interconnected according to the proximity of the nodes.

In Scenarios 1 and 2, the impact targeted attacks have on the robustness of interdependent networks is analyzed for different interlinks patterns. The failure spreading of the most dangerous targeted attack in one network to its interconnected network is also studied. In Scenario 3, the critical parts of a physical network are identified and the best placements for controllers are found in order to improve the SDN network robustness against targeted attacks. In Scenario 4, an enhanced region-based interconnection model is proposed by considering a limit to the number of interlinks between the nodes. The influence of reducing the number of interlinks in the robustness of region-based interdependent networks is also analyzed under cascading failures.

1.2 Research Questions

The aim of this dissertation is to conduct a research on geographical robustness measures in interdependent transportation networks under large-scale failures, in particular, to consider interdependent networks where at least one of the networks is a telecommunication network. This thesis is dedicated to a better understanding of the following research questions:

1. What are the topological properties of networks that determine the sensitivity to a certain type of failure?
2. How can the impact of targeted attacks in interdependent networks be reduced?
3. What influence do interlink patterns have on targeted attacks spreading?
4. How can identifying the critical parts in a network influence or improve the network robustness in the case of targeted attacks?
5. How can a region-based interconnection model be enhanced by reducing the number of interlinks?
6. What impact does reducing the number of interlinks have on the robustness of interdependent networks under cascading failures?

1.3 Methodology

Figure 1.1 presents the methodology used to address the research questions, run the simulations and evaluate the results. The simulations are developed by using the igraph[a] package in R[b]. The following provides an explanation of each of the process the activities are described:

- *Network model*: The telecommunication networks, power grid and the SDN network are characterized by relationship between the network elements. Thus, networks to be interconnected are modeled from real topologies or graph models.

[a] http://igraph.org/r/
[b] https://www.r-project.org/

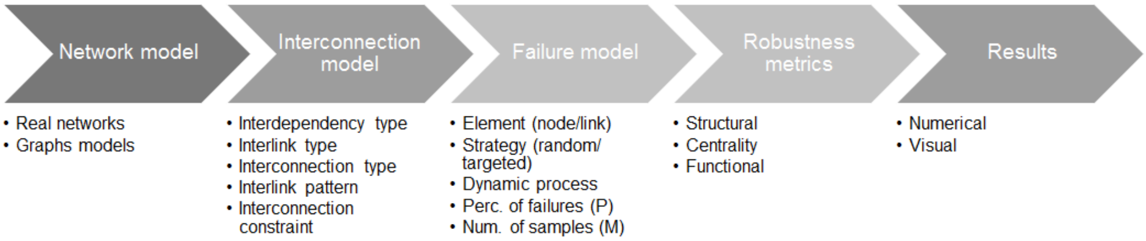


Figure 1.1: Methodology

- *Interconnection model*: This represents the interconnection strategy to be analyzed. Thus, networks are interconnected by following an interdependency type, interlink type, interconnection type, interlink pattern and interconnection constraint.

- *Failure model*: A failure in a network element (node or edge) is defined as the physical loss of this element. In interdependent networks, a failure is made by eliminating the given element of one network and generating a dynamic process between the interconnected networks.

- *Robustness metrics*: These are used to compare and quantify the impact failures have on the network. Three types of robustness metrics can be used: structural, centrality and functional.

- *Results*: The simulation results of a failure model on an interdependent network with a specific interconnection model are analyzed via numerical and visual representation. These results are validated through the publication of a paper in JCR indexed journals and its presentation at specied conferences.

1.4 Contributions

The main contributions of this thesis are the following:

- A structural and centrality robustness analysis of real telecommunication networks under multiple failures to detect the most relevant topological parameters of networks with similar robustness.

- An interconnection model to mitigate the impact of targeted attacks on network robustness. This model is based on the analysis of the vulnerability of the interconnected networks to targeted attacks. Thus, the most suitable interconnection model is identified in order to reduce the impact of targeted attacks and enhance the robustness of interdependent critical infrastructures.

- A more robust design for the control plane in a Software Defined Network is developed by what are the critical parts of physical topology are in order to place controllers in the case of targeted attacks.
- An enhanced region-based interconnection model to interconnect two geographical networks by decreasing the number of interlinks. This model is able to maintain an acceptable level of network robustness under cascading failures, while reducing the deployment and maintaining cost.

1.5 Outline of the document

This doctoral thesis is organized into chapters that present the contributions mentioned above:

- In Chapter 2, a review of the research efforts related to robustness measurements in single networks under multiple failure scenarios is presented. Moreover, a structural and centrality robustness comparison considering real telecommunication networks under random failures and targeted attacks is done. Through this analysis the common topological properties for grouping networks with similar robustness are identified. Thus, this chapter is focused on the first research question.
- In Chapter 3, a review of the most relevant research on the robustness measurements in interdependent networks based on network model, interdependency model and failure model is presented. Furthermore, an interconnection mechanism based on interdependency matrices is proposed to mitigate the impact of targeted attacks. The impact of targeted attacks on the network robustness is also analyzed in two case studies: 1) two interconnected telecommunication networks and 2) a power grid interconnected to a telecommunication network. Finally, the failure propagation between the interconnected networks is also studied. In this chapter the second and third research questions are addressed.
- In Chapter 4, a Software Defined Network (SDN) is considered as a case study in order to provide a robust design and to achieve SDN architecture that is more resilient to targeted attacks. The proposal is focused on identifying what the critical parts of physical topology are and finding the best controller placements to mitigate the damage from targeted attacks. Additionally, in order to show the performance of the proposed algorithm, the robustness of the SDN is analyzed when a targeted attack occurs in the switches of a real telecommunication network and compared with previous proposals. Thus, the fourth research question is covered in this chapter.

- In Chapter 5, a review of the most relevant research into robustness measurements in region-based interdependent networks is carried out and an enhanced interconnection model for region-based interdependent networks is presented. The model proposed introduces a new strategy for interconnecting nodes between two geographical networks by limiting the number of interlinks. Finally, the impact of limiting the number of interlinks on the robustness of region-based interdependent networks to cascading failures is discussed. Thus, this chapter addresses the fifth and sixth research questions.

- In Chapter 6, the main contributions of this doctoral dissertation are summarized and lines for future research are proposed.

Chapter 2

Robustness measurements in single networks: review and applications

Telecommunication networks, power grids, water/gas networks, metro and rail systems are some examples of transportation networks. These critical infrastructures are built to geographically distribute resources over a certain region. Multiple failures can have catastrophic consequences on the normal operation of networks. In this sense, guaranteeing network robustness to avoid users and services being affected is essential. A wide range of metrics have been proposed for measuring the network robustness. In this chapter a review of research efforts related to robustness measurements in single networks under multiple failure scenarios is carried out. Moreover, a structural and centrality robustness comparison taking as study case real telecommunication networks experiencing random failures and targeted attacks is made. Throughout this analysis the common topological properties for grouping networks with similar robustness can be identified.

2.1 Introduction

Transportation networks distribute flows of critical resources in different geographic regions [40]. Telecommunication networks, via optical fiber cables, electrical networks, via power lines, water/gas networks, pipelines, are some examples of critical infrastructures that provide our society with essential services [1, 40]. Therefore, it is of utmost importance that these networks are robust to avoid the interruption of services running on them in scenarios of multiple failures. This research particularly focus on the study of robustness measurements in telecommunication networks under random failures and targeted attacks. Telecommunication networks are crucial transportation infrastructures required to support a variety of human activities such as socialization, entertainment, information gathering, health and well-being, learning, transportation and emergency communications.

The consequences of multiple failures in telecommunication networks are dramatic as when they occur millions of users and services can be disconnected. Failures in telecommunication networks can be caused by fiber cuts, configuration errors, viruses and worms, cyber-attacks, terrorism or natural disasters [2]. For instance, in 2014, a human error in configuring TimeWarner's Internet routers in the United States resulted in a failure that prevented 11.4 million clients from accessing broadband services for three hours [5]. Therefore, robustness measuring in telecommunication networks is useful for network administrators to evaluate and reduce the impact of multiple failures in their networks. Robustness can be defined as network's ability to continue performing well when it is subject to failures [3].

Telecommunication networks are considered as complex according to their network topology. Through complex networks the structure of networks can be represented and overall network performance can be understood and predicted. [41]. A basic representation of a complex network is carried out by the nodes, links and dynamic processes that run over them. In telecommunication networks, the nodes represent routers or switches, links are the physical (or logical) interconnections between them and connections perform the dynamic processes [10]. In the field of complex networks, a large number of graph metrics have been studied to characterize the topological properties, structure and dynamics of networks [42–44]. However, a subset of these metrics is only representative for measuring the network robustness in static or multiple failure scenarios [9–11]. Thus, measuring the vulnerability of networks to potential failures is an important aspect for network planning in order to manage and mitigate service disruption.

Safeguarding networks against multiple failures requires an analysis of robustness measurements to detect the parts of the network that are highly vulnerable. Consequently, a set of appropriate robustness metrics should be considered to measure the consequences of such failures in the network performance. In this chapter, a review of the main research efforts related to robustness measurements in single networks under multiple failure scenarios is carried out. Moreover, a structural and centrality robustness analysis of real telecommunication networks under multiple failures (random and targeted) is carried out. Through this analysis the most relevant topological parameters to group networks with similar robustness are identified and compared with the results found in previous works.

This chapter is structured as follows. In Section 2.2, the basic notation and models in complex networks are introduced. A review of robustness metrics in transportation networks is presented in Section 2.3. Robustness measurements in single networks are reviewed in 2.4. In Section 2.5, the structural properties of the networks studied in this work are described, while the simulation results of structural and centrality robustness metrics under multiple failure scenarios are presented and analyzed in Section 2.6. Last, Section 2.7 provides a discussion and lessons learned.

2.2 Review of models in single networks

The characterization of the interactions between the network elements is carried out by concepts in the field of network science. Essentially, the mathematical graph theory can be applied to study complex networks in a wide range of disciplines. Traditionally, complex networks have been modelled as random graphs. As network science has continued to grow in importance and popularity, other complex network models have been developed [41]. The two most well-known examples of recently introduced complex network models are those of small-world and scale-free graphs [41]. In this section, the basic notation in single networks and models of complex networks are introduced.

2.2.1 Basic notation in single networks

Generally, complex networks are studied by applying methods developed in the field of mathematical graph theory. In the context of graph-theory, mathematical structures called graphs are used to model pairwise connections between components of a network [41]. A complete definition of a network must include both structural and behavioral information [45]. Graphs consist of nodes or components (vertices), links or connections (edges), and a mapping function that defines how nodes connect to one another [41].

Let $G(S,U)$ be an unweighted and undirected graph with a set of nodes S and a set of links U. Let us denote N as the number of nodes and L as the number of links. The adjacency matrix A of a graph G is an $N\times N$ symmetric matrix with elements a_{ij} that are either 1 or 0 depending on whether there is a link between nodes i and j or not. The Laplacian matrix Q of G is an $N\times N$ symmetric matrix $Q=\Delta-A$, where $\Delta=diag(d_i)$ is the $N\times N$ diagonal degree matrix with the elements $d_i=\sum_{j=1}^{N}a_{ij}$. Note that the degree of a node i (d_i) is the number of outgoing links from the node. Interested readers are referred to [45] for a detailed coverage of graph theory and its relevance to this research.

2.2.2 Random graph of Erdős-Rényi

The random graph of Erdős-Rényi (ER) is one of the most studied models of complex networks. Let us denote the random graph by $ER_p(N)$, where N is the number of nodes in the graph and p is the probability of having a link between any two nodes (or in short, the link probability). $ER_p(N)$ is the set of all such graphs in which a graph having L links appears with probability $p^L(1-p)^{L_{max}-L}$, where L_{max} is the maximum possible number of links. Many properties of the random graph are known analytically in the limit of large graph size N, as was shown by Erdős-Rényi in [46] and later by Bollobás [47]. Typically, for large graph size N, the degree distribution of the random graph model, which is a binomial distribution, can be replaced by a Poisson distribution [48]. The expected structure of the random graph varies depending on the value of p. most important point is that it possesses a phase transition: from a low link density or low p value for which there are few links and many small components to a high link density or high p value for which an extensive fraction of all the nodes are joined together in a single giant component [41].

2.2.3 Small-World graph of Watts-Strogatz

The Small-World (SW) model describes the fact that despite the large graph size, in most real-world networks there is a relatively short path between any two nodes [48]. The most studied SW model is the one proposed by Watts and Strogatz [49], which starts by building the ring R_N with N nodes and then joins each node to $2 \times s$ neighbors (s on either side of the ring) [48]. This results in the ring lattice R_{N_s} with $L = s \times N$ links. The SW graph is then created by moving, with probability p_r, one end of each link (connected to a clockwise neighbor) to a new node chosen uniformly in the ring lattice, except that no double links or loops are allowed [48]. The rewiring process allows the small-world model to interpolate between a regular lattice ($p_r = 0$) and something which is similar, though not identical, to a random graph ($p_r = 1$) [49]. For already small p_r, the small-world becomes a locally clustered network in which two arbitrary nodes are connected by a small number of intermediate links. This model is located between an ordered finite lattice and a random graph, presenting the small world property and the high clustering coefficient [44]. Watts and Strogatz [49] showed that small-world networks are common in a variety of realms ranging from the C-Elegans neuronal system to power grids.

2.2.4 Scale-Free graph of Barabási-Albert

The Scale-Free (SF) model has a power-law degree distribution which contrasts with that of random or small-world graphs. Barabási [50] showed that the growth and preferential attachment of nodes, which implies that the nodes with larger degrees are more likely candidates for the attachment of new nodes, give rise to a class of graphs with a power-law degree distribution. The Barabási-Albert model starts with a small number m_0 of fully-meshed nodes, followed at every step by a new node attached to $m \leq m_0 = 2 \times m + 1$ nodes already present in the system [48]. After t steps this procedure results in a graph with $N = t + m_0$ nodes and $L = \frac{m_0(m_0-1)}{2} + mt$ links [48]. The structure of the Internet and the World Wide Web (WWW), which consist of a small number of extremely popular nodes or sites called hubs and a large number of nodes or unpopular sites with few links, are examples of scale-free networks [45, 50].

2.3 Review of robustness metrics in single networks

In the field of complex networks a large number of graph metrics have been studied to characterize the topological properties, structure and dynamics of networks [42–44]. However, a subset of these metrics is only representative for measuring network robustness in static or multiple failure scenarios. To classify robustness metrics we consider a taxonomy based on structural properties, centrality measures and services supported by networks. A preliminary version of this taxonomy can be found in [10]. Figure 2.1 shows an extended taxonomy of robustness metrics. A brief description of these robustness metrics is presented in this section.

2.3.1 Structural metrics

Structural metrics are a well-known area in the conventional analysis of graphs. They are also used to explain stability - or the lack of it - in a network, and to determine how viruses spread through a network under node/link removal [45]. A preliminary robustness analysis in isolated networks is carried out by considering the following basic network properties: average nodal degree ($\langle k \rangle$), average shortest path length ($\langle l \rangle$), Diameter (D) and assortativity coefficient (r). Other metrics are based on these basic network properties such as heterogeneity (σ_k), efficiency (ε) and Graph Diversity (GD).

Vertex connectivity (κ_v) and edge connectivity (κ_e) are an extension of the classical connectivity (κ) measurement. In addition, structural metrics also use the Adjacency (A) and Laplacian (Q) matrices to abstract and calculate the robustness of the networks e.g., Symmetry Ratio (SR), largest eigenvalue (λ_1), algebraic connectivity (λ_2), natural connectivity ($\bar{\lambda}$), Effective Graph Resistance (EGR) and Weighted Spectrum (WS). Other metrics that have been used to measure the robustness in networks based on their structural properties are clustering coefficient ($\langle C \rangle$), percolation limit (ρ_c), Number of Spanning Trees (NST), Average Two-Terminal Reliability ($ATTR$) and Viral Conductance (VC). The key features of these structural metrics are described below.

2.3.1.1 Average nodal degree

Let d_i be the degree of node i in a network G with N nodes. The average nodal degree ($\langle k \rangle$) of G is defined as [51]:

- Structural
  - Average nodal degree ($\langle k \rangle$)
  - Average shortest path length ($\langle l \rangle$)
  - Diameter (D)
  - Assortativity coefficient (r)
  - Heterogeneity (σ_k)
  - Efficiency (ε)
  - Vertex connectivity (κ_v)
  - Edge connectivity (κ_e)
  - Cluster coefficient ($\langle C \rangle$)
  - Symmetry Ratio (SR)
  - Largest eigenvalue (λ_1)
  - Algebraic connectivity (λ_2)
  - Natural connectivity ($\bar{\lambda}$)
  - Effective Graph Resistance (EGR)
  - Graph Diversity (GD)
  - Weighted Spectrum (WS)
  - Percolation limit (ρ_c)
  - Number of Spanning Trees (NST)
  - Average Two-Terminal Reliability ($ATTR$)
  - Viral Conductance (VC)
- Centrality
  - Degree centrality (d_c)
  - Eigenvector centrality (e_c)
  - Closeness centrality (c_c)
  - Betweenness centrality (b_c)
  - Cross-clique centrality
  - Spreaders
- Functional
  - Elasticity (E)
  - QuaNtitative Robustness Metric ($QNRM$)
  - QuaLitative Robustness Metric ($QLRM$)
  - Endurance (ξ)
  - R-value
  - R^*-value (robustness surfaces (Ω))

Figure 2.1: Taxonomy of robustness metrics in single networks

$$\langle k \rangle = \frac{1}{N}\sum_{i=1}^{N} d_i \tag{2.1}$$

Networks with higher $\langle k \rangle$ are on average considered as better-connected and as a result are more likely robust (i.e., there are more chances to establish new connections) [10]. However, detailed topology characterization based only on the average degree is rather limited, since graphs with the same average node degree can have vastly different structures [52].

2.3.1.2 Average shortest path length

Regarding the average shortest path length ($\langle l \rangle$) this is calculated as an average of all the shortest paths between all the possible origindestination node pairs of the network [10]:

$$\langle l \rangle = \frac{2}{N(N-1)} \sum_{i=1}^{N} \sum_{j=i+1}^{N} l_{ij}, \tag{2.2}$$

where N is the number of nodes in the network and l_{ij} is the shortest path between nodes i and j in the network [11]. Values can take any number larger than or equal to 1, where $\langle l \rangle = 1$ means that all the nodes are directly connected to each other [11]. Therefore, a network is more robust if $\langle l \rangle$ is at its lowest as then it is likely to lose fewer connections [10].

2.3.1.3 Diameter

The Diameter (D), like the average nodal degree, is another coarse robustness metric of a network. The diameter D is the longest of all the shortest paths between pairs of nodes [53]:

$$D = max\left(l_{ij}\right), \tag{2.3}$$

where l_{ij} is the shortest path between nodes i and j in the network. Thus, one would want the diameter of networks to be low to achieve the higher robustness.

2.3.1.4 Assortativity coefficient

The assortativity coefficient (r) lies within the range $[-1,1]$ and it defines two types of networks. Disassortative networks with $r < 0$ have an excess of links connecting nodes of dissimilar degrees. Assortative networks with $r > 0$, which have an excess of links connecting nodes of similar degrees, have the opposite properties [52]. As can be found in [54], such networks exhibit greater vulnerability to certain types of targeted attacks.

2.3.1.5 Heterogeneity

Based on $\langle k \rangle$, the heterogeneity (σ_k) is a coefficient of variation of the connectivity and it is defined as [55]:

$$\sigma_k = \frac{StDev(\langle k \rangle)}{\langle k \rangle}, \tag{2.4}$$

where $StDev(\langle k \rangle)$ is the standard deviation of the average nodal degree and $\langle k \rangle$ is the average nodal degree. Lower σ_k values translate to higher network robustness [10].

2.3.1.6 Efficiency

Similar to the average shortest path length, the efficiency (ε) is calculated as the averaged sum of the reciprocal (multiplicative inverse) of the shortest paths [56]:

$$\varepsilon = \frac{2}{N(N-1)} \sum_{i=1}^{N} \sum_{j=i+1}^{N} \frac{1}{l_{ij}}, \tag{2.5}$$

where N is the number of nodes in the network and l_{ij} is the shortest path between nodes i and j in the network. The greater the ε value, the greater the network robustness is [11].

2.3.1.7 Vertex and edge connectivity

In addition to the classical connectivity measure κ, which distinguishes connected graphs ($\kappa = 1$) and unconnected graphs ($\kappa = 0$), two more connectivity measures have been defined: vertex and edge connectivity [57]. Vertex connectivity (κ_v) represents the smallest number of nodes that must be removed to disconnect the network. The same definition can be applied to edge connectivity (κ_e) when considering links instead of nodes.

2.3.1.8 Clustering coefficient

The clustering coefficient ($\langle C \rangle$) captures the presence of triangles formed by a set of three nodes and compares the number of triangles to the number of connected triples [49]. The clustering coefficient (C_i) of a node i is the portion of actual links between the nodes within its neighborhood divided by the maximal possible links between them [49]. Note that the neighborhood of node i includes all the nodes directly connected to it but excludes the node i itself. A larger C_i value means that the node has a more compact system of connections with its neighbors [58]. The clustering coefficient of a network is the average of all individual C_i's, calculated as [58]:

$$\langle C \rangle = \frac{1}{N} \sum_{i=1}^{N} C_i, \tag{2.6}$$

where N is the number of nodes in the network and C_i is the clustering coefficient of a node i. The higher the clustering coefficient is, the higher the network robustness is, because the number of alternative paths increases with the number of triangles in the presence of failure on a node or link [11]. The clustering coefficient ranges within the interval $[0,1]$, where $\langle C \rangle = 1$ indicates all the possible existing triangles due to the fact that all the nodes are interconnected.

2.3.1.9 Symmetry ratio

The Symmetry Ratio (SR) has been used for partially predicting the robustness of a network in the face of attacks [59]. The Symmetry Ratio SR for a network G is calculated as [59]:

$$SR = \frac{e}{D+1}, \tag{2.7}$$

where e is the number of distinct eigenvalues of the Adjacency matrix A and D is the diameter. Networks with low symmetry ratio values are considered more robust to random failures or targeted attacks [10].

2.3.1.10 Largest eigenvalue

The largest eigenvalue or spectral radius (λ_1) is the largest nonzero eigenvalue of the Adjacency matrix of a network [45]. Generally, networks with high values of λ_1 have a small D and higher node distinct paths. The λ_1 metric also provides information on network robustness [52] and captures the virus propagation properties of networks defining an epidemic threshold of node infection [60].

2.3.1.11 Algebraic connectivity

Algebraic connectivity (λ_2) is defined as the second smallest Laplacian eigenvalue [61]. Let us order the eigenvalues of the Laplacian matrix Q as $0 = \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_N$. Then, the algebraic connectivity is λ_2. Algebraic connectivity measures how difficult it is to break the network into different components is. If $\lambda_2 = 0$ the graph is disconnected, so higher λ_2 values indicate better network robustness [48]. Most λ_2 values are between zero and one, but can be equal to the number of nodes when all the nodes are interconnected [11].

2.3.1.12 Natural connectivity

Networks with identical algebraic connectivity (λ_2) can be compared using natural connectivity ($\bar{\lambda}$). The $\bar{\lambda}$ metric characterizes the redundancy of alternative paths by quantifying the weighted number of closed walks of all lengths [62]. In addition, $\bar{\lambda}$ is expressed as the average of the eigenvalues of the adjacency matrix [62]:

$$\bar{\lambda} = \ln\left(\frac{1}{N}\sum_{i=1}^{N} e^{\lambda_i}\right), \tag{2.8}$$

where N is the number of nodes in the network. A higher $\bar{\lambda}$ value indicates a more robust network [63].

2.3.1.13 Effective graph resistance

The Effective Graph Resistance (EGR) can be written as a function of nonzero Laplacian eigenvalues (λ_i). Let us order the eigenvalues of the Laplacian matrix Q as $0 = \lambda_N \leq \lambda_{N-1} \leq \cdots \leq \lambda_1$. Then, the Effective Graph Resistance EGR is calculated as [40]:

$$EGR = N\sum_{i=1}^{N-1} \frac{1}{\lambda_i}, \tag{2.9}$$

where N is the number of nodes in the network. Note that the second smallest eigenvalue $\lambda_{N-1} = \lambda_2$ is the algebraic connectivity defined previously. The effective graph resistance is the sum of the effective resistances over all pairs of nodes. Then, the EGR metric measures the number of paths between two nodes and their length. The smaller the EGR value is, the more robust the network [64]. Therefore, EGR strictly decreases if a link is added into a graph and strictly increases if a link is removed from a graph [40, 64, 65].

2.3.1.14 Graph diversity

The Graph Diversity (*GD*) is related to the number of nodes shared with the shortest path considering all the possible paths between two nodes. This metric is equal to one when the paths do not share any common point of failure (node or link). Total Graph Diversity (TGD) is the average of all the Effective Path Diversities (*EPDs*) over all the paths [66]. Consequently, calculating this metric requires significant computational resources. Larger TGD indicates greater robustness [66].

2.3.1.15 Weighted spectrum

The Weighted Spectrum (WS) metric is based on the eigenvalues (λ_i) of the normalized Laplacian matrix and the n-cycle of a graph. The Weighted Spectrum (WS) is given as the normalized sum of n-cycles [67]:

$$WS = N \sum_{i=1}^{N-1} (1-\lambda_i)^n, \tag{2.10}$$

where N is the number of nodes in the network. Different values of n indicate different topology properties to be analyzed e.g., $n = 3$ is associated with the clustering coefficient, while $n = 4$ is related to the number of disjoint paths in a network [67]. The network robustness is calculated as $W' - W$, where W denotes the default WS of the original graph and W' denotes the WS of the resulting network after link or nodal failures [68].

2.3.1.16 Percolation limit

The percolation limit or percolation threshold (ρ_c) returns the critical fraction of nodes that need to be removed before the network disintegrates [11]. Degree diversity (κ_0) is taken into account to calculate the percolation limit [69]. Hence, the higher the degree diversity, the higher the percolation limit. Then, a higher ρ_c indicates that the fraction of nodes that can be removed without disconnecting the network is higher, which means that the network is more robust [11]. According to [70], the percolation limit can be calculated as:

$$1 - \rho_c = \frac{1}{\kappa_0 - 1}, \tag{2.11}$$

where κ_0 is the degree diversity, also called the second-order average degree. In a network G with corresponding nodal degrees $d_1, d_2, \ldots, d_N$, the degree diversity (κ_0) is defined as [35]:

$$\langle k_0 \rangle = \frac{\sum_{i=1}^{N} d_i^2}{\sum_{i=1}^{N} d_i} \tag{2.12}$$

2.3.1.17 Number of spanning trees

The number of spanning trees (a spanning tree is a subgraph containing $N-1$ edges and no cycles [3]) as an indicator of network robustness has been suggested in [71]. The Number of Spanning Trees (NST) counts all the possible spanning trees that exist for a network. The NST in a network can be determined by Kirchhof's matrix-tree theorem [72]. However, it has been proven that the NST can be written as a function of the unweighted Laplacian eigenvalues [3]:

$$NST = \frac{1}{N} \prod_{i=2}^{N} \lambda_i \tag{2.13}$$

2.3.1.18 Average two-terminal reliability

The Average Two-Terminal Reliability ($ATTR$) measures the probability of a randomly-chosen pair of nodes being connected [73]. The two-terminal reliability between two nodes is equal to one if a path exists between them; otherwise, it is equal to zero [4]. Thus, when the network is fully connected, exactly one component exists and $ATTR = 1$. In another case [4], the $ATTR$ metric is calculated as the sum over the number of node pairs in each connected component and divided by the total number of node pairs in the network. The $ATTR$ is defined as [73]:

$$ATTR = \frac{\sum_{i=1}^{c} K_i(K_i - 1)}{N(N-1)}, \tag{2.14}$$

where c is the number of components, K_i is the number of nodes in component i and N is the number of nodes in the network. At failure scenarios, the higher the average two-terminal reliability is, the higher the robustness is [10, 73].

2.3.1.19 Viral conductance

The last structural metric is Viral Conductance (VC), where the robustness is measured with respect to virus spread [74]. This metric is measured by considering the area under the curve that provides the fraction of infected nodes in steady-state for a range of epidemic intensities [74]. The lower the VC in a network, the more robust with respect to virus spread it is. However, as this work is focused on random failures and targeted attacks, the VC metric is not evaluated.

2.3.2 Centrality metrics

This group of metrics attempts to identify which elements in a network are the most important or central [54]. Consequently, they could help disseminate information in the network faster, stopping epidemics and protecting the network from breaking. These metrics also define the network centralization as a measure of how central the most central node is in relation to how central all the other nodes are [75, 76]. Centralization, which is a key characteristic of a network, can be used to measure network robustness as the differences between the centrality of the most central node and that of all the others [75, 76]. In general, the most central network is the most robust i.e., if the network has more nodes with similar centrality values, there are then several spots to attack when centrality metrics are used to select the elements to be removed.

A large number of centrality metrics have been proposed to identify the most central nodes in networks. However, the following are the most common: degree centrality, eigenvector centrality, closeness centrality, betweenness centrality and spreaders. In degree and eigenvector centralities the importance of a node is given in terms of its neighbors, whereas in closeness and betweenness centralities the importance is related to the path lengths. A brief description of the most common centrality metrics is presented in this section.

2.3.2.1 Degree centrality

Degree centrality (d_c) is the simplest measure of nodal centrality and is determined by the number of neighbors connected to a node [77]. The larger the degree, the more important the node is. However, if a node with a high nodal degree fails, potentially higher numbers of connections are also prone to being affected. In many real networks only a small number of nodes have high degrees e.g., in social networks or citation networks the number of edges connected to a given vertex may often be a good measure of its importance. Thus, the degree centrality of a node i (d_c) is simply the degree of node i given by [54]:

$$d_c = \sum_{j=1}^{N} a_{ij}, \tag{2.15}$$

where N is the number of nodes in the network and a_{ij} is an entry of the adjacency matrix (A) of the network.

2.3.2.2 Eigenvalue centrality

Accordingly, eigenvalue centrality (e_c) is based on the notion that a node should be viewed as important if it is linked to other important nodes [78]. Thus, the eigenvalue centrality can take a large value either by the node being connected to many other nodes or by it being connected to a small number of important nodes. The eigenvalue centrality is proportional to the sum of the centrality scores of its neighbors, where the centrality corresponds to the largest eigenvector of the adjacency matrix. The eigenvalue centrality of a node i (e_c) is given by [78]:

$$e_c = \frac{1}{\gamma} \sum_{j=1}^{N} e_{cj}, \tag{2.16}$$

where γ is a constant and e_{cj} are the eigenvalue centralities of its neighboring nodes.

2.3.2.3 Closeness centrality

With closeness centrality (c_c) the nodal importance is measured by how close a node is to other nodes [77]. It is based on the length of the shortest path between a given node and all the other nodes in the network. An important node is typically close to the other node if it can reach the whole network more quickly than the non-close nodes. Consequently, a node with the highest closeness centrality has the shortest distance to the other nodes, on average. The closeness centrality of a node i (c_c) is given by [54]:

$$c_c = \frac{N}{\sum_{j=1}^{N} l_{ij}}, \tag{2.17}$$

where N is the number of nodes in the network and l_{ij} is the shortest path between nodes i and j in the network.

2.3.2.4 Betweenness centrality

Betweenness centrality (b_c) is when the number of shortest paths that pass through a given node is counted [75]. A node may have a high betweenness centrality while being connected to only a small number of other vertices (which are not necessarily important/central). This is due to the fact that nodes that act as bridges between groups of other nodes typically have high b_c. Thus, nodes with high b_c play a broker role in the network and are important in communication and information diffusion [77]. The betweenness centrality of a node i (b_c) is given by:

$$b_c = \sum_{j=1}^{N} \frac{g_{ij}(i)}{g_{ij}}, \tag{2.18}$$

where N is the number of nodes in the network, $g_{ij}(i)$ is the number of shortest paths between nodes i and j passing through node i and g_{ij} is the total number of shortest paths between nodes i and j. Similar to b_c, the link betweenness centrality (l_c) can also be calculated as the degree to which a link makes other connections possible.

2.3.2.5 Spreaders

Centrality metrics also take into account measures in epidemic scenarios where the best spreaders of an epidemic do not correspond to the most central nodes. Instead, the most efficient spreaders are those located within the core of the network according to a k-shell decomposition analysis [79]. This metric is not evaluated in this work as it is focused on random and targeted attacks.

2.3.3 Functional metrics

This set of metrics quantifies the variation of the performance of a network in response to multiple failures by focusing on the Quality of Service (QoS) parameters of the established connections. Thus, these metrics define key aspects of the services that run over a network. Services can be classified according to different QoS parameters, such as: throughput, delay, jitter, packet loss, etc. Some network failures, if not all, impact all these parameters resulting in a reduction of the QoS levels [80]. Moreover, from the perspective of the operator network, failures also affect the number of connections established and the future connection demands [80]. In this section a short description of functional robustness metrics is presented.

2.3.3.1 Elasticity

The concept of robustness considered by this metric is the ability of a network to maintain its total throughput under node and link removal [81]. The Elasticity (E) is the area under the curve of throughput (T_G) versus the percentage of nodes removed. Initially, $T_G(0) = 1$, which accounts for the normalized throughput. The elasticity decreases as the percentage of removed nodes is increased and thus this metric provides a measure of robustness at any point of node removal [81]. Therefore, when n nodes have been removed, E can be computed as [81]:

$$E\left(\frac{n}{N}\right) = \frac{1}{2N}\sum_{k=0}^{n}\left(T_G\left(\frac{k}{N}\right) + T_G\left(\frac{k+1}{N}\right)\right), \tag{2.19}$$

where N is the number of nodes in the network and $T_G(\frac{k}{N})$ is the throughput at each interval when k nodes are removed.

2.3.3.2 Quantitative robustness metric

The QuaNtitative Robustness Metric ($QNRM$) analyses how multiple failures affect the number of connections established in a network. In this metric, the number of Blocked Connections (BC) in each time step are analyzed. Let us define BC as a connection that should have been established at time t but could not be established as a consequence of nodal failures. The $QNRM$ in each time stamp t is defined as [80]:

$$QNRM[t] = \frac{BC(t)}{TTC(t)}, \tag{2.20}$$

where $BC(t)$ is the number of BC in a given time step and $TTC(t)$ is the number of total connections that should have been established in the same time step. Then, the average of all the values obtained during the interval of interest is computed as [80]:

$$QNRM = \frac{\sum_{t=0}^{Total} QNRM[t]}{Total}, \tag{2.21}$$

where $Total$ is the maximum number of time steps.

2.3.3.3 Qualitative robustness metric

The QuaLitative Robustness Metric (*QLRM*) analyses how the quality of service on a network varies when a failure occurs in the network. This metric measures the average shortest path length ($\langle l \rangle$) in each time step. In contrast to the *QNRM*, the *QLRM* evaluates the Established Connections (*EC*). In order to compare the *QLRM* for different topologies the values obtained from the average shortest path length are normalized. The *QLRM* is defined as [80]:

$$QLRM = \frac{U(\langle l \rangle)}{U(P)}, \tag{2.22}$$

where $U(\langle l \rangle)$ is the quotient of the standard deviation of the $\langle l \rangle$ of the topology and its $\langle l \rangle$ before a failure, and $U(P)$ is the same quotient, but calculated when a failure has affected a certain percentage of nodes (P) in the network.

2.3.3.4 *R*-value

Using the *R*-value, the network robustness is given by an arbitrary topological vector and a weight vector [82]. The topological vector ($\hat{t}$) components take into consideration one or more QoS parameters, network properties or any other structural robustness metric e.g., hop-count, average shortest path length ($\langle l \rangle$), maximum nodal degree (k_{max}) or algebraic connectivity (λ_2) [82]. The weight vector ($\hat{w}$) components reflect the importance of the topological vector for the network service [82]. The *R*-value of the network robustness is computed by a weighted, linear norm [82]:

$$R = \sum_{k=1}^{m} \hat{w}_k \hat{t}_k, \tag{2.23}$$

where $\hat{w}$ and $\hat{t}$ are the $m \times 1$ weight and the topology vectors, respectively. Thus, the *R*-value includes several graph metrics characterizing network robustness. The $R*$-value can take values in the interval [0, 1] where $R = 0$ is the absence of network robustness and $R = 1$ is perfect robustness [82].

2.3.3.5 Endurance

Endurance (ξ) is also calculated by one or more QoS parameters (e.g., delay) or topological metrics (e.g., size of the largest connected component). In contrast to the *R*-value, endurance places greater importance on perturbations affecting low percentages of elements in a network. Endurance is normalized to the interval [0, 1], where $\xi = 1$ denotes the non-existence of robustness, whereas $\xi = 0$ is correlated to the maximum possible degree of robustness [83].

2.3.3.6 R^*-value

The R^*-value is a functional metric, which is the *R*-value computed via a normalized eigenvector or Principal Component (*PC*). The *PC* gives each of the robustness metrics dimension and non-arbitrary weights [84]. The $R*$-value is defined as [84]:

$$R^* = \sum_{k=1}^{m} \hat{v}_k \hat{t}_k, \tag{2.24}$$

where $\hat{v}$ is the $m \times 1$ normalized eigenvector or Principal Component (*PC*) and $\hat{t}$ is the $m \times 1$ topology vector (set of robustness metrics). Without failures the R^*-value is set to one and can take values in the interval $[0, +\infty)$ when failures are considered [84]. Then, a greater R^*-value will mean better robustness. A graphical representation of the R^*-value is called the robustness surface (Ω) and and it enables a visual assessment of network robustness variability to be made [84].

The robustness surface allows the network performance variability for a given failure scenario to be visually assessed [84]. In fact, Ω is a matrix where the rows are the percentage of failures (*P*) and the columns are the distinct failure configurations (*m*). The list of percentage of failures *P* (e.g., $P = 1\%, 2\%, \ldots, 100\%$) denotes the range of failures for which the robustness is evaluated [84]. A failure configuration represents a realization of the failure process. The different failure configurations *m* depict the different subsets of elements that fail for a given percentage of failures, with each subset being distinct from one another [84]. The robustness value in $\Omega[p][i]$, where $p \in 1\%..|P|\%$ and $i \in 1 \ldots m$, is given by R^* (2.24) [84].

2.4 Review of robustness measurements in single networks under multiple failure scenarios

Failures on network elements (nodes or links) can affect the normal operation of networks due to their physical removal from the network. Removing a network element causes

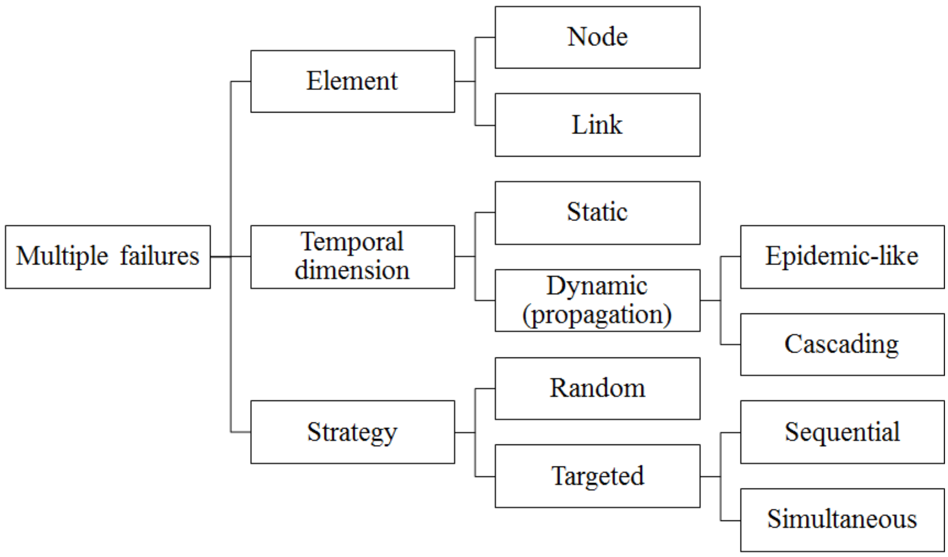


Figure 2.2: Taxonomy of multiple failures in single networks

a change in the topological structure of a network, which has consequences in terms of system performance, properties and architecture, such as transportation properties, information delivery efficiency and the reachability of network components (i.e., ability to go from one node of the network to another) [85, 86]. Therefore, services supported by a network and users connected to it may experience catastrophic consequences due to loss of connectivity. In order to protect networks against multiple failures, several works have focused on studying the vulnerability of single complex networks. In this section a classification of multiple failures and a review of robustness measurements in single networks are presented.

2.4.1 Types of multiple failures in single networks

Failures that affect critical infrastructures have several origins including natural disasters, man-made disasters, technology-related disasters or cyber-attacks [2, 7]. For instance, the geographical layout of the fiber optic infrastructure has a critical impact on the robustness of the network in the face of geographical physical failures such as earthquakes and Electromagnetic Pulse (*EMP*) attacks [4]. Figure 2.2 shows a general classification of multiple failures based on affected elements, temporal dimension and strategy used to remove the networks' elements. Interactions between network elements (node or links) are responsible for the correct functioning of a network. Thus, a failure on a node or link may cause service interruption due to decreased network performance [85]. Moreover, depending on the nodes or links that have been removed from the network, the impact of a failure can be catastrophic.

Regarding the temporal dimension, failure types can be either static or dynamic.

Static failures are essentially one-off failures that affect one or more elements at any given moment [10]. Dynamic failures have a temporal dimension [10] i.e., in a given time one or more network elements initially fail, but due to the dynamics of failure it spreads to other elements. Then, the initial failure causes other elements to also fail after a certain time. The spread of epidemic-like failures in telecommunication networks [87] and cascading failures in power grids [88] are some examples of dynamic failures in complex networks.

The strategy used to remove nodes or links plays a crucial role in triggering a failure and damaging a network. Thus, when an object that causes an attack knows and uses precise information about the network's topological structure, it is called an attack with white-information (targeted) [89]. However, when the attacker has little or no information, it is considered a black-information attack (random) [89]. The former would be more related to intentional failures, while the latter would be linked more with unintentional failures [10, 89]. The remainder of this section is focused on random and targeted attacks as the main failure scenarios in telecommunication networks.

2.4.1. Random failures

In a random (unintentional) failure, nodal or link failures occur selecting the elements at random [10, 70]. This type of failure is also called unintentional as they appear randomly. Human error, manufacturing defects, worn-out mechanical parts and natural disasters are some examples of random failures because a certain fraction of the network elements and their connections are removed randomly [4, 70, 90]. When a network is subject to random failures their integrity might be compromised [70]. Thus, the impact of such failures involves the affectation of large regions due to the geographical distribution of the network elements.

Random failure damages nodes (links) with uniform probability, which can be seen as a simple abstraction of the successive error in a complex network [91]. Random failures lead to a probabilistic measure with statistical independence due to the fact that the nature of the failure is unknown and it has occurred independently [90, 92]. Consequently, in the random failure model considered in this work, all the network elements have the same probability to fail and this does not depend on the failure of another. The probability of a network element (node or link) i becoming inactive due to random failure is given by [93]:

$$P_r a(i) = \frac{1}{|NE|}, \tag{2.25}$$

where $|NE|$ is the number of network elements. Therefore, if the elements that fail are nodes, then $|NE| = N$, whereas if the elements that fail are links, then $|NE| = L$. When a network is subjected to random failures, the availability of their elements (nodes or links) can be calculated in order to estimate the failure probability of the network. Let us define the binary-state of a network element NE as $S(NE_i)$, where $S(NE_i) = 1$ if the element is in up (failure free) state, and $S(NE_i) = 0$ is if the element is in down (failed) state [92]. Let us also consider the set of the failure states of the network $\mathbf{S} = S_n$ as a combination of the states of the network elements. Therefore, the probability of a network state S_n is $P_r(S_n)$ and is given by:

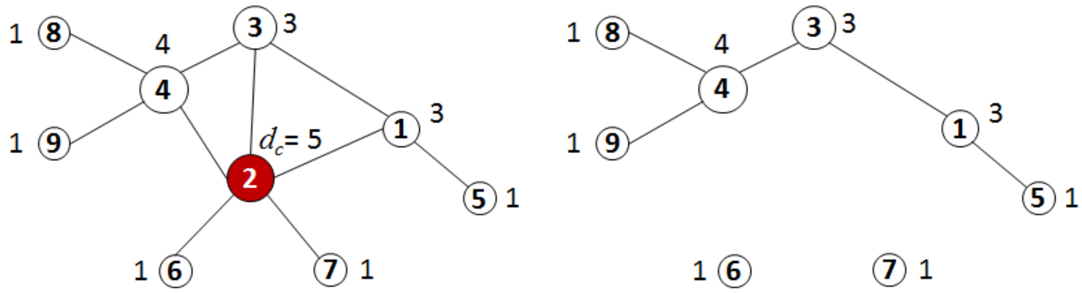
$$P_r(S_n) = \prod_{NE_i \in NE_{up}(S_n)} \Lambda(NE_i) \prod_{NE_i \in NE_{down}(S_n)} (1 - \Lambda(NE_i)), \tag{2.26}$$

where $NE_{up}(S_n)$ and $NE_{down}(S_n)$ denote the set of network elements being in the up and down states in network state S_n, respectively, and $\Lambda(NE_i)$ is the availability of network element NE_i. Availability is calculated as a function of the failure rate of the network elements, which can be defined from the historical data set of failures. Therefore, the probability of a network failing due to random failures depends on the failed network elements in the given network state. Knowing the failure probability of a network is relevant for network design and planning because network robustness can be measured when a fraction of random elements are removed from the network in order to assess the impact of failures and take actions to mitigate them.

2.4.1.2 Targeted failures

In targeted (intentional) failures, the network elements are removed with the express purpose of maximizing the damage done to a network [54, 91, 94]. In the literature, thses are known as targeted attacks where the most important nodes based on certain property are the first to be removed from the network. For instance, in backbone telecommunication networks the most vulnerable routers can be identified by the number of shortest paths passing through a given router or by the number of physical links from one router to others. Moreover, other real world features, such as the number of potentially affected users and socio-political and economic considerations, are also used to rank the nodes to be removed in a telecommunication networks [10]. Figure 2.3 shows that all the nodes in the network are ranked by their degree centrality (d_c) and the attack is triggered on node 2 because it has the highest degree centrality (so it is the most vulnerable). As can be seen, the network is fragmented in several components causing enormous damage to the network.

Targeted attacks, on the other hand, are not random and the attacker must have some knowledge about the network topology in order to trigger the attack on the most vulnerable (the most important) network elements [90, 91]. Centrality metrics (e.g.,



(a) Node vulnerability is calculated **(b)** Node 2 is the first to be attacked

Figure 2.3: Targeted attacks in single networks

degree, betweenness, closeness and eigenvector centrality) are widely used to identify the critical elements (nodes or links) in networks and to discern the probability that an element will be attacked initially and become inactive [40, 54, 85, 86, 90, 91, 93, 94]. The probability of a network element i (node or link) with a given property (e.g., centrality metric) value becoming inactive due to a targeted attack is given by [93]:

$$P_t a(w_i) = \frac{w_i}{\sum_{i=1}^{|NE|} w_i}, \tag{2.27}$$

where w_i is the property value selected to identify the importance of the network element and $|NE|$ is the number of network elements. Therefore, if the nodes fail, then $|NE| = N$ whereas if the links fail, then $|NE| = L$. Moreover, in contrast to random failures, in a targeted attack a network element has a different failure probability from the others, which is highest for the most important network elements. However, its failure probability does not depend on failure of the others. There are two major strategies for selecting which elements are attacked:

- **Simultaneous targeted attack**: in this type of targeted attack, first of all vulnerability is calculated for all the elements (node or link) in the network. Second, the elements are ranked once by the attacker from the most vulnerable (the most important) to the least vulnerable (the least important) [90]. Last, a specified fraction of the elements is removed based on this sorted list i.e., from the most vulnerable element to the least vulnerable element.

  In telecommunication networks, some failure scenarios can be modeled as simultaneous targeted attacks e.g., in an Ethernet switched network, the most vulnerable switches can be identified by the number of connected links. Thus, the attack can target the switches with the highest number of links in order to maximize the damage. Note that although other properties (role, traffic load, placement, etc.) can be considered to identify the most important switches in the network, the number of interlinks is the most illustrative example.

- **Sequential targeted attack**: vulnerability is calculated for all the elements (node or link) in the original network, and the element with the highest vulnerability is then removed. Next, the vulnerability of all the elements in the resulting network are recalculated and once again the highest ranked element is removed and so on [54, 85]. This process of recalculating the vulnerability of elements and removing the highest ranked element continues until the desired fraction of elements is reached.

  Sequential targeted attack may be used to describe certain types of failure scenarios in telecommunication networks e.g., the most vulnerable routers of a backbone network can be identified in order to protect the network's function. When a router fails, its functioning can be distributed to any one router in the network. Then, the failure of one router will affect the importance of the remaining ones. Therefore, the sequential targeted attack is appropriate to model the network vulnerability in such scenarios.

2.4.2 Robustness measurements in single networks

Robustness measurements in single networks become relevant when the goal is to protect the network against multiple failures [85, 91]. Moreover, the robustness analysis helps to learn how to construct failure-robust networks and also how to increase the robustness of critical infrastructures. Consequently, enormous interest and effort has been directed at studying the impact of node (link) removal in the normal functioning of critical infrastructures by means of several robustness metrics. In this section, a review of robustness measurements in single networks under multiple failures (random and targeted attacks) and the influence of their topological properties on network robustness is carried out, particularly emphasizing telecommunication networks.

The robustness of the Internet has been widely analyzed under random and targeted failures because of its importance to society and its particular topological structure. The Internet can be viewed as a special case of a random, Scale-Free (SF) network, where the probability of a node being connected to k other nodes follows a power-law: $P(k) \sim k^{-\alpha}$ ($\alpha \approx 2.5$) [70]. The Internet shows high robustness against random removal of nodes (for example, random failure of routers), but is relatively vulnerable, at least in terms of the fraction of nodes removed, to the specific removal of the most highly connected nodes (degree centrality) [95, 96]. The approach presented by Cohen et al. [70] based on the percolation theory has lead to a general condition for the critical fraction of nodes, ρ_c, that need to be removed before the network disintegrates. If a fraction P of the nodes is removed randomly, then for $\alpha > 3$ there exists a critical threshold, ρ_c, such that for $P > \rho_c$

the network disintegrates into smallest components [70].

However, the Internet is extremely vulnerable to attack when a few of the most important nodes for maintaining the network's connectivity are selected and removed first from the network (simultaneous targeted attacks) [96]. In [94] it was found that even networks with $\alpha \leq 3$ (such as the Internet), known to be resilient to the random removal of nodes, are highly sensitive to intentional attack on nodes with the highest connectivity (simultaneous targeted attacks). Such error tolerance and attack vulnerability are generic properties of communication networks because their connectivity depends on a small fraction of the highest-degree vertices [96]. Additionally, Holme et al. [85] have been studied the response of the Internet subject to attacks on nodes and links. It was found that removals by recalculated degrees and betweenness centralities (sequential targeted attacks) are often more harmful than attack strategies based on the initial network (simultaneous targeted attacks), suggesting that the network structure changes as important nodes or links are removed [85]. In [93] it was shown that few knowledge of the highly connected nodes in an intentional attack reduces the percolation threshold (ρ_c) drastically compared with the random case. This suggests that, for example, the Internet can be damaged efficiently when only a small fraction of hubs is known to the attacker [93].

Despite the fact that power-law node degree distribution is widely used for modeling telecommunication networks such as the Internet, other models can be used for modeling current structural of backbone core networks such as rings in fiber optical networks or random graphs in IP-Layer 3 networks. For the random graph of Erdős-Rényi (ER), the strategies based on recalculating the most important nodes (sequential targeted attacks) are, as expected more harmful than their counterparts based on the initial network [85]. The ER model, which lacks structural bias, is the most robust of the Small-World (SW) and Scale-Free (SF) models. Then, building a hub-less network would be very robust to attack. Even if the network connections were fixed in a random pattern this would lead to a tremendous increase in the attack-robustness of the network (as the ER model shows) [85].

The robustness of a set of real telecommunication networks against random and targeted attacks were studied in [10], and the most robust networks were identified by comparing the measurements of some classical and contemporary metrics in simulated scenarios. In [11] the robustness of real telecommunications networks and generic topologies (ER, SW and SF) in non-failure scenarios were compared. Both [10, 11] rank the best topologies based on their robustness metrics. In [11] it was shown that some the robustness measurements of a set of metrics present incompatibilities in detecting the most robust networks in a faultless scenario. The temporal evolution of the topological robustness of backbone telecommunication networks by identifying their trends was analyzed in [97]. Maniadakis et al. [97] have found that modifying the structure of networks over time does not guarantee a better robustness.

Trajanovski et al. [90] studied the robustness of random (ER, SF and SW) and real networks (power grid, railway and social collaboration network) under node removal, considering random node failure, as well as targeted node attacks based on network centrality measures (node degree, betweenness, closeness and eigenvector centrality). Their analysis suggest that that real-world networks are susceptible to rapid degradation under sequential targeted attacks. Therefore, centrality-based targeted attacks are sufficient for studying the worst-case behavior of real-world networks [90]. An analytical comparison of well-known robustness metrics in some model and empirical networks under random and targeted attacks is carried out by Iyer et al. [54]. They showed that for scale-free networks (SF) the node degree centrality (d_c) metric is the most effective strategy to remove nodes in simultaneous targeted attacks, whereas for sequential attacks it is betweenness centrality (b_c) [54].

In addition to the simultaneous and sequential targeted attacks based on centrality metrics, a combination of centrality metrics and other strategies have been studied. Nie et al. [91] have proposed two new attack strategies named IDB (Initial Degree and Betweenness) and RDB (Recalculated Degree and Betweenness). Experimental results indicate that the proposed strategies are more efficient than the traditional ID (Initial Degree distribution) and RD (Recalculated Degree distribution) strategies.The Small-World (SW) network in particular behaves more sensitively towards the proposed strategies [91]. In [98], the damage and behavior of both real networks and synthetic networks against attacks is analyzed. Empirical study has shown that for real networks in a wide range of domains there exists a critical-point before which damage attack is more destructive than degree attack. This is further explained by the fact that degree attack tends to produce networks with more heterogeneous damage distribution than damage attack [98].

The impact of geographical failures on network robustness has also been studied. Long et al. [99] measured the survivability of core backbone communication networks to geographic correlated failures and determined the most vulnerable geographic cuts or nodes in the network. Neumayer et al. [4, 73] analyzed network connectivity after a random geographic disaster. The random location of the disaster has modeled situations where the physical failures are not targeted attacks. In particular, disasters can take the form of a randomly located disk or line on a plane and their impact on network performance has been estimated using the Average Two-Terminal Reliability ($ATTR$) metric [4]. The effect of large scale disasters [100] and the identification of critical region vulnerability [33] have been modeled by geometric forms which have a certain geographical area of impact and consequently determine their damage on network elements that are located in such areas. Disasters can be circular to model solar Coronal Mass Ejections (*CME*) and Electromagnetic Pulse (*EMP*) weapons, polygonal to model power blackouts, or they may have movement to model hurricanes and typhoons [100].

In addition to the robustness analysis of a set of networks, some works have extracted the topological properties that make a network more vulnerable to a certain type of failure. In [81, 101, 102] the characteristics of network topologies that maintain a high level of throughput in spite of multiple attacks are studied. Topologies with high degree core nodes show robustness to random attacks, while topologies with low degree core nodes demonstrate robustness to targeted attacks by nodal degree centrality (d_c) [101] e.g., a random failure can break a random graph of Erdős-Rényi (ER) into several components, whereas a Scale-Free (SF) network is more robust in this failure scenario. However, SF networks are highly vulnerable to a targeted attack by nodal degree centrality (d_c) due to the presence of high degree core nodes (hubs) [93, 94, 96]. From [101] it can also be concluded that topologies with a small fraction of low degree core nodes show vulnerability to targeted attacks by nodal betweenness centrality (b_c).

Through the analysis of Internet AS-level topologies, Mahadevan et al. [103] studied the assortativity coefficient (r) which ranges in $[-1,1]$. In disassortative networks (with disassortative values i.e., $r < 0$) the majority of radial links connect nodes of different degrees, indicating that such networks are vulnerable to random failures, targeted attacks and faster virus spreading. The opposite properties apply to assortative networks (with assortative values i.e., $r > 0$), which have an excess of tangential links connecting nodes of similar degrees [103]. In [102] it was also showed that Internet topologies with negative r values have the highest performance against random failures. Conversely, low performing topologies have positive r values [102]. In [81] it was shown that, for a given network density, regular and semi-regular topologies can have higher degrees of robustness than heterogeneous topologies, and that link redundancy is a sufficient but not necessary condition for robustness. This is due to the almost constant degree for the semi-regular class results in high network performance. However, heterogeneous networks span a wide range of degrees and behave differently under attacks [81]

In disassortative networks ($r < 0$), a simultaneous targeted attack by degree is the most effective means of exposing the vulnerability of a network [54]. In contrast, for assortative networks ($r > 0$) a simultaneous targeted attack by node betweenness is the most effective method of degrading the network [54]. Additionally, networks exhibit greater vulnerability to a sequential attack based on any centrality metric (degree, betweenness, eigenvalue or closenness) than is the case under simultaneous attack [54]. In all cases of sequential attacks, networks are most effectively degraded by removing nodes in decreasing order of betweenness centrality, while removing nodes in reverse order of degree is the least effective method [54]. Additionally, in [90] it was suggested that by slightly increasing degree assortativity (through degree-preserving rewiring), networks become more resilient to targeted attacks, if somewhat less resilient to random attacks. On the other hand, networks whose assortativities are moderately minimized are more tolerant to random attacks (and less tolerant to targeted attacks) [90]. Additionally, in [40] it was proved that the links addition increases the network robustness but is not a sufficient design constraint of a network.

2.4.3 Summary and research direction

Telecommunication networks have become essential to many aspects of our society, and thus the consequences of network disruption are now dramatic and expensive. As can be seen in the previous section, telecommunication networks are not sufficiently robust under random and targeted attacks. Additionally, some topological properties of networks have defined the robustness behavior in certain failure scenarios. Table 2.1 is a summary of the relevant results from previous research. As can be seen, most of the works are focused on identifying the behavior of network robustness in the context of various network types when they are subject to failure. Other works are focused on identifying the relevant topological properties that define the robustness profiles based on a set of metrics. Thus, what follows is the research direction that will be taken in the remainder of this chapter:

- Several robustness metrics have been proposed to measure the network robustness, but some of these have given contradictory results in identifying the most robust networks. Thus, a set of structural and centrality metrics is analyzed in order to address a comprehensive study of topological parameters that define the network robustness to random and targeted failures. Through this analysis the most relevant topological parameters to group networks with similar robustness are identified.

- The study of robustness in real networks takes on importance due to the fact that their topological properties provide networks with different resistance levels to multiple failures. Moreover, some of their topological properties can not be emulated by classical graph models. Therefore, a structural and centrality robustness analysis of a set of real telecommunication networks under multiple failures (random and targeted) is carried out in order to understand the response of real telecommunication networks to such as failures.

- Determining what type of failure will cause the greatest damage to networks is relevant to designing and planning more robust networks. Consequently, the types of failures that causes major damage to networks are identified and are compared with the results of previous works

Table 2.1: Comparison of relevant results on robustness measurement in single networks

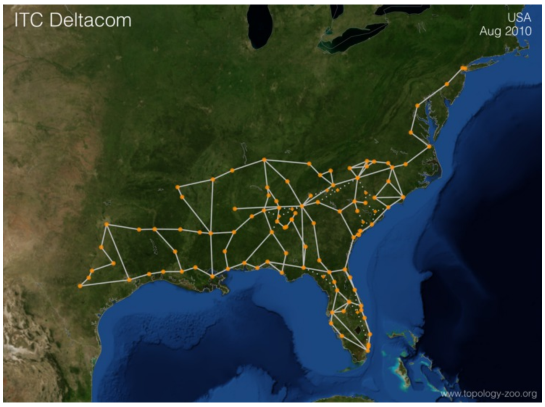
Author	**Network model**	**Failure model**	**Main result**	**Robustness metric**
Callaway et al. [95]	Internet (SF)	Random and targeted attacks on nodes	Fragility to removing the most highly connected nodes	Percolation threshold
Cohen et al. [70, 94]	Internet (SF)	Random and targeted attacks on nodes	High robustness to randomly removing of nodes and fragility to removing the most highly connected nodes	Percolation threshold
Albert et al. [96]	Internet (SF)	Targeted attacks on nodes	Highly sensitive to targeted attacks on nodes with the highest connectivity	Giant component
Cohen et al. [94]	Internet (SF)	Targeted attacks on nodes	Fragility to removing the most highly connected nodes	Percolation threshold
Holme et al.[85]	Internet (SF), ER and SW	Targeted attacks on nodes and links	Strategies with recalculated degree and betweenness are more harmful than the initial information strategies	Average shortest path length and giant component
Gallos et al. [93]	ER, BA, Internet (SF), and social	Targeted attacks on nodes	Little knowledge of the well-connected nodes is sufficient to greatly reduce ρ_c	Percolation threshold
Sydney et al. [81, 102]	ER, SW, BA, social and technological	Random and targeted attacks on nodes	The ability of a network to maintain its total throughput is reduced by increasing the removed nodes	Elasticity
Manzano et al. [10]	Real telecommunication networks	Random and targeted attacks on nodes	Ranking of the most robust networks by comparing some classical and contemporary metrics	Some structural and functional metrics
Van der Meer[11]	Real telecommunication networks	No failures	Relations between the robustness measurements of a set of metrics	Some structural and functional metrics

Continue on the next page

Table 2.1: Comparison of relevant results on robustness measurement in single networks

Author	**Network model**	**Failure model**	**Main result**	**Robustness metric**
Trajanovski et al. [90]	ER, SW, BA, social and technological	Random and targeted attacks on nodes	Real-world networks are susceptible to rapid degradation under sequential targeted attacks	R-value
Iyer et al. [54]	ER, SW, BA, social, biological and technological	Random and targeted attacks on nodes	Node degree centrality is the most effective metric to remove nodes in simultaneous targeted attacks, whereas for sequential attacks it is betweenness centrality (b_c)	V-index

(a) RENATER



(b) DELTACOM

Figure 2.4: Network layout of some telecommunication networks

2.5 Topological properties of real telecommunication networks

In this section the topological properties of real telecommunication networks are described. This set of networks have been selected through a careful search in specialized databases considering the number of times that they were used in relevant publications e.g., a preliminary robustness analysis of this set of topologies can be found in [10, 11, 97, 104]. The topologies are part of important telecommunication network repositories such as [105, 106]. Thus, the 15 real telecommunication networks serve as a standardized benchmark for testing, evaluating and comparing several network robustness metrics.

Some of these networks are backbone transport networks (representing real physical links), whereas others are logical networks (representing the IP layer). Then, the selected networks offer a wide range of topological properties which allow structural and centrality robustness analysis to be carried out. By comparing their network robustness, the common topological properties that can be used to group networks with similar robustness under random failures and targeted attacks are identified. Moreover, the analysis carried out allows for the possibility of identifying the type of failure that causes the highest damage on the network. Figure 2.4 shows the network layout of some of the telecommunication networks that are studied.

Each network topology is modeled by a graph $G(S,U)$, which is given by a vertex set $S = 1,2,\ldots,N$ and an edge set $U = 1,2,\ldots,L$. In telecommunication networks vertices (i.e., nodes) can be routers, switches, hosts or any telecommunication equipment, and edges (i.e., links) can be optical fiber cables, wired or wireless links (physical or virtual). The graph representation and topological map of the set of networks considered as study cases can be found in [105, 106]. Table 2.2 presents the main topological properties of

Table 2.2: Topological properties of the 15 real telecommunication networks

Network	N	L	$\langle k \rangle \pm StDev$	k_{max}	$\langle l \rangle$	D	r
ABILENE	11	14	2.55 ± 0.52	3	2.42	5	0.067
GEANT	40	61	3.05 ± 1.95	10	3.53	8	-0.204
RENATER	43	56	2.60 ± 1.70	10	3.93	9	-0.1544
GpENI_L2	51	61	2.39 ± 1.73	9	4.69	10	-0.232
TISCALI_L3	51	129	5.06 ± 5.42	22	2.43	5	-0.361
CESNET	52	63	2.42 ± 3.13	19	3.05	6	-0.374
GARR	61	89	2.92 ± 3.09	14	3.62	8	-0.258
CORONET_L1	100	136	2.72 ± 0.83	5	6.67	15	0.035
DELTACOM	113	183	3.24 ± 1.85	10	7.16	23	0.316
USCARRIER	158	189	2.39 ± 0.82	6	12.09	35	-0.095
COGENTCO	197	245	2.48 ± 1.06	9	10.51	28	0.02
SPRINT_L1	264	313	2.37 ± 0.81	6	14.7	37	-0.188
ATT_L1	383	488	2.55 ± 1.15	8	14.13	39	-0.062
US_MW	411	553	2.69 ± 1.13	7	13.65	42	0.112
KDL	754	899	2.38 ± 0.85	7	22.73	58	-0.096

the real telecommunication networks: number of nodes (N), number of links (L), average nodal degree ($\langle k \rangle$) $\pm$ standard deviation ($StDev$), maximum nodal degree (k_{max}), average shortest path length ($\langle l \rangle$), diameter (D) and assortativity coefficient (r). The networks are different sizes, ranging from 11 to 754 nodes and from 14 to 899 links. ABILENE is the smallest network with 11 nodes and 14 links, and the KDL network is the largest with 754 nodes and 899 links.

As can be seen in Table 2.2, the TISCALI_L3 and DELTACOM networks have higher $\langle k \rangle$ with 5.0588 and 3.2389, respectively. In contrast, SPRINT_L1 and KDL have the lowest $\langle k \rangle$ values, 2.3712 and 2.3846, respectively. According to k_{max}, TISCALI_L3 has the node with the highest number of connections (22), while ABILENE has the node with the lowest degree (3). In telecommunication networks, k_{max} is used to identify the most important node according to the number of links, because if the node with the highest nodal degree fails, a potentially higher number of connections are also prone to being affected.

In terms of $\langle l \rangle$ and D, ABILENE and TISCALI_L3 have the lowest values for these properties. The former has $\langle l \rangle = 2.4182$, while the latter has $\langle l \rangle = 2.4298$. Both networks have $D = 5$. Nonetheless, KDL and SPRINT_L1 with 22.727 and 14.705 have the highest values of $\langle l \rangle$, and KDL and US_MW have the highest D values, 58 and 42, respectively.

Last, Table 2.2 shows that most of the networks analyzed have a negative or near to zero value of r. DELTACOM (0.3158) is the most assortative network and CESNET (-0.3739) is the most disassortative. As explained in section 2.3.1, when $r < 0$ the network is said to be disassortative, meaning that it has an excess of links connecting nodes of dissimilar degrees, whereas assortative networks are when $r > 0$ indicating an excess of links connecting nodes of similar degrees.

2.6 Robustness measurements in telecommunication networks: structural and centrality analysis

In this section, first the measurement of structural and centrality robustness metrics in a static scenario are presented and a preliminary robustness comparison is carried out. Then, some simulation scenarios are set up to allow the robustness under random and targeted attacks to be evaluated and analyzed. Most of the metrics presented in Fig. 2.1 were simulated under multiple failure scenarios. However, in this work only the most relevant results are presented as the metrics analyzed allow the robustness behavior of the set of the real networks to be abstracted for grouping according to common topological properties.

Multiple failure scenarios were simulated for random and targeted attacks and in each of them a subset of the structural and centrality robustness metrics is analyzed. The nodes to be removed in the simultaneous targeted attacks were selected by their degree centrality (d_c), whereas for the sequential targeted attacks they were selected by their betweenness centrality (b_c). In all the scenarios, the percentage of nodes removed (P) ranged from 1% to 70 %. Twenty and ten runs were performed for random and targeted attacks, respectively. For each of the runs, different subsets of nodes were selected according to the failure scenario.

2.6.1 Robustness measurements in a static scenario

Table 2.3 shows the measures of structural and centrality robustness metrics for the defined set of real networks in a static scenario. The first and second columns in Table 2.3 show that ABILENE and CORONET_L1 have maximum vertex connectivity (κ) and edge connectivity (ρ), (two in each case), i.e., more than one element must be removed to break these networks. The clustering coefficient($\langle C \rangle$) shows that the TISCALI_L3 (0.3776) and GPENI_L2 (0.1847) networks are the most robust. Their nodes are more interconnected with their neighbors as there are many triangles (i.e., many alternative paths) in case of nodal or link failures. However, for the CORONET_L1 network $\langle C \rangle = 0$ as it does not have any triangles, as can be seen in its topological map available in [106]. As regards to the Symmetry Ratio (*SR*), the lowest value indicates high robustness. Thus, ABILENE and USCARRIER, with *SR* values equal to 2.2 and 4.5143, respectively, are the most robust networks. In consequence, *SR* suggests that the impact caused by removing a node does not depend on which node is removed [10].

With the largest eigenvalue (λ_1), TISCALI_L3 and DELTACOM are the most robust networks with values of 9.5895 and 6.0015, respectively. On the other hand, TISCALI_L3 and ABILENE have the highest values of the second smallest Laplacian, each one with 0.5255 and 0.3238. Therefore, according to the algebraic connectivity (λ_2), they are the most robust networks. Also, a similar robustness result can be concluded for the TISCALI_L3 and ABILENE networks from their low values of D and $\langle l \rangle$. Nonetheless, DELTACOM is one the most robust networks according to λ_1, with a low λ_2 value (0.0233) and high values of $\langle l \rangle$ (3.2389) and D (10), making its robustness results the opposite. In this case, a relevant conclusion about its robustness cannot be drawn as the λ_1 and λ_2 metrics rank the DELTACOM network in a different way.

Based on natural connectivity ($\bar{\lambda}$), TISCALI_L3 and GARR are the most robust networks as they have the highest values at 5.6718 and 2.3343, respectively. With Effective Graph Resistance (EGR), ABILENE and GEANT have the best robustness as they obtain the smallest values of EGR: 7.54E+01 and 1.31E+03, respectively. KDL and US_MW, , however, obtain the worst EGR (with values of 1.98E+06 and 3.48E+05, respectively). Weighted Spectrum (WS) was calculated with $N = 3$ and the most robust networks are GARR and ABILENE with values of 0.1990 and 0.3333, respectively.

Regarding percolation limit (ρ_c), TISCALI_L3 (0.8974) and CESNET (0.8142) have the highest values, indicating that these networks are more robust. With respect to Number of Spanning Trees (NST), in general, the larger the network, the higher the NST is. Therefore, NST must be compared in similar sized networks. By comparing the NST of the whole set of networks, KDL and US_MW are shown to be the most robust networks. However, by comparing the NST metric for networks with similar size, TISCALI_L3 is more robust than RENATER and CESNET because, as shown in Table 2.2, the first has more links than the others. Therefore, the number of spanning trees in the TISCALI_L3 network is higher. In the static scenario, the Average Two-Terminal Reliability ($ATTR$) for all the networks is one.

Table 2.3: Structural and centrality robustness metrics of telecommunication networks in a static scenario

Network	κ	ρ	$\langle C \rangle$	SR	λ_1	λ_2	$\bar{\lambda}$	EGR	ρ_c	WS	NST	d_c	e_c	c_c	b_c	l_c
ABILENE	2	2	0.15	2.2	2.68	0.33	1.1	7.5E+01	0.39	0.33	2.5E+02	0.05	0.35	0.24	0.2	0.09
GEANT	1	1	0.15	5	4.39	0.14	1.57	1.3E+03	0.69	0.7	6.9E+10	0.18	0.79	0.3	0.45	0.09
RENATER	1	1	0.17	4.78	3.88	0.14	1.28	1.8E+03	0.63	0.71	4.3E+08	0.17	0.83	0.22	0.4	0.09
GpENI_L2	1	1	0.18	5.1	3.74	0.054	1.22	4.5E+03	0.62	1.25	5.5E+05	0.13	0.81	0.21	0.42	0.21
TISCALI_L3	1	1	0.38	10.2	9.59	0.53	5.67	1.3E+03	0.89	0.77	1.9E+22	0.34	0.76	0.38	0.29	0.01
CESNET	1	1	0.08	8.67	4.97	0.14	1.65	2.8E+03	0.81	0.41	8.7E+05	0.33	0.87	0.46	0.69	0.24
GARR	1	1	0.05	7.63	5.79	0.12	2.33	3.8E+03	0.8	0.19	5.6E10	0.18	0.83	0.33	0.46	0.08
CORONET_L1	2	2	0	6.67	3.29	0.05	1.13	1.0E+04	0.49	0	1.5E+26	0.02	0.85	0.09	0.2	0.07
DELTACOM	1	1	0.09	4.91	6	0.02	2.29	1.8E+04	0.69	1.67	1.8E+33	0.06	0.94	0.15	0.4	0.05
USCARRIER	1	1	0.06	4.51	2.98	0.01	1.03	8.4E+04	0.4	1.78	4.6E+23	0.02	0.92	0.07	0.45	0.27
COGENTCO	1	1	0.01	7.04	3.79	0.01	1.09	9.4E+04	0.48	0.41	5.9E+34	0.03	0.94	0.09	0.34	0.15
SPRINT_L1	1	1	0.03	7.14	2.93	0.01	1.01	2.0E+05	0.39	1.42	7.6E+41	0.01	0.96	0.06	0.28	0.16
ATT_L1	1	1	0.04	9.82	3.71	0.01	1.14	3.3E+05	0.52	2.59	5.9E+74	0.01	0.97	0.05	0.19	0.1
US_MW	1	1	0.05	9.79	4.22	0.01	1.21	3.4E+05	0.54	3.44	2E+94	0.01	0.96	0.07	0.25	0.12

Continue on the next page

Table 2.3: Structural and centrality robustness metrics of telecommunication networks in a static scenario

Network	κ	ρ	$\langle C \rangle$	SR	λ_1	λ_2	$\bar{\lambda}$	EGR	ρ_c	WS	NST	d_c	e_c	c_c	b_c	l_c
KDL	1	1	0.03	13	3.17	0.01	1.03	1.9E+06	0.41	3.91	3E+120	0.01	0.98	0.03	0.23	0.14

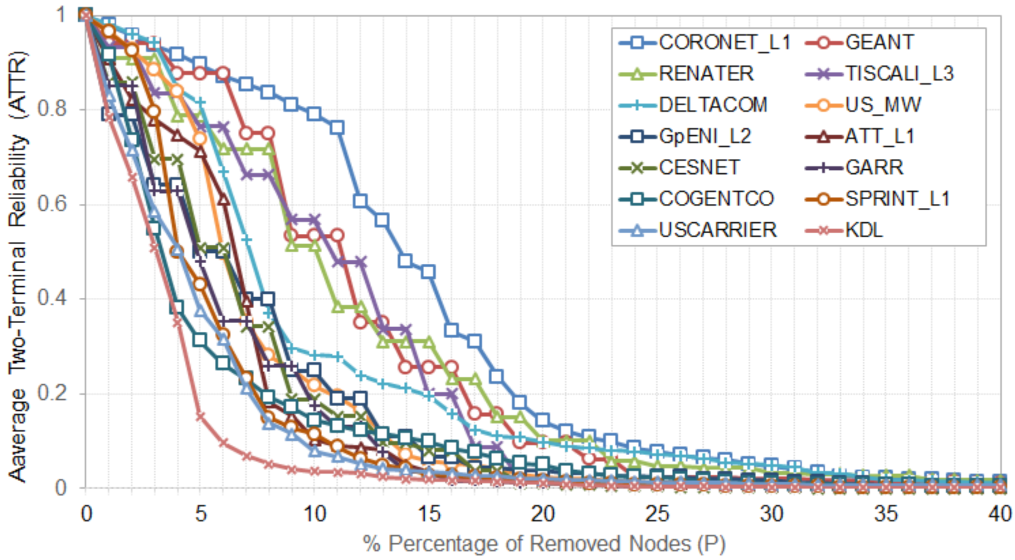
As regards centrality-based metrics, nodal degree centrality (d_c), nodal closeness centrality (c_c), nodal betweenness centrality (b_c) and link betweenness centrality (l_c) are considered to measure network centralization. As explained in section 2.3.2, network centralization is used to analyze network robustness based on these centrality metrics as the differences between the centrality of the most central node and that of all the others [76]. This indicates that those networks close to uniform centrality distributions are more robust in the case of targeted attacks on the most central nodes. In Table 2.3 it can be seen that the networks with the highest centralization values when considering d_c are TISCALI_L3 (0.3388) and CESNET (0.325); with e_c, the KDL (0.986) and ATT_L1 (0.9756) networks are the most central; based on c_c, the CESNET (0.4605) and TISCALI_L3 (0.3837) networks have the highest centralization values; the most central networks based on b_c are CESNET (0.6939) and GARR (0.4591), and last USCARRIER (0.27) and CESNET (0.24) have the highest network centralization based on l_c.

This preliminary robustness analysis (summarized in Table 2.3) shows that some metrics differ when identifying the most robust networks. Hence, taking just one metric into account is not sufficient to measure network robustness. Therefore, a set of significant metrics to calculate robustness and compare the results should be considered. In order to identify the relationships between network properties and their robustness, the behavior of this set of real telecommunication networks when multiple failures occur under targeted attacks and random failures must be considered.

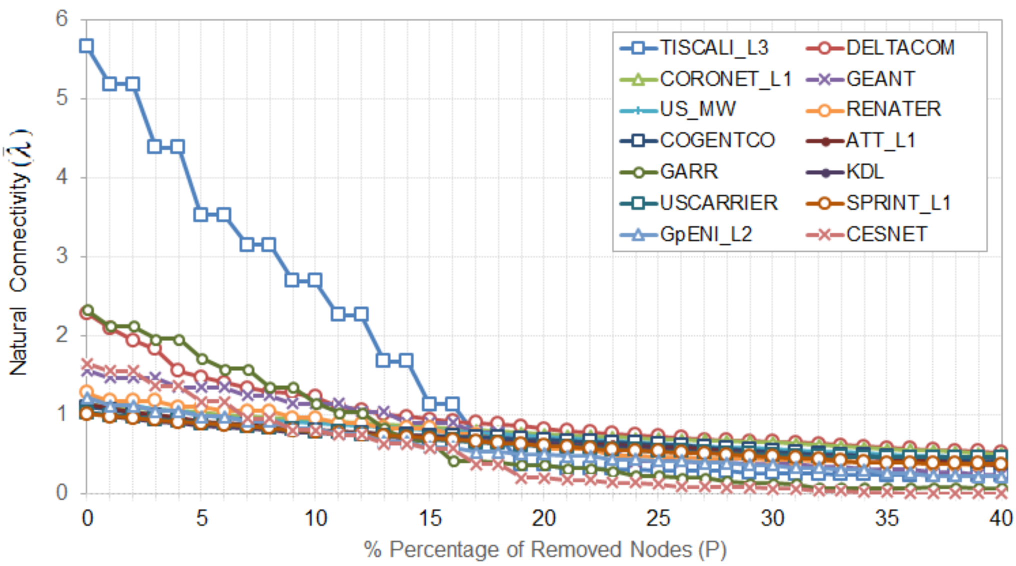
2.6.2 Robustness measurements under simultaneous targeted attacks

In this section, the robustness analysis of the real telecommunication networks when nodes are removed under the simultaneous targeted attack is presented. According to [54], the nodal degree centrality (d_c), which is a purely local centrality measure, is the most effective technique for removing nodes in the case of simultaneous targeted attacks. In Fig. 2.5(a) the robustness results using Average Two-Terminal Reliability ($ATTR$) metric are shown. When the network is fully connected, exactly one component exists and $ATTR$ is one. Successive removals of nodes or links will bring it closer to zero [73]. If failures affect two topologies in the same percentage of nodes or links, the one that takes longest to reach a given critical $ATTR$ can be considered as the more robust [73]. The $ATTR$ metric provides an approximation to measure the network connections and to group networks with similar robustness, as can be seen in Fig. 2.5(a). Then, for each subset of networks the common topological properties among them can be identified.

As can be observed in Fig. 2.5(a), it is possible to identify different affectation levels i.e., the number of lost connections when a given percentage of nodes are eliminated from



(a) Average Two-Terminal Reliability ($ATTR$) results



(b) Natural connectivity ($\bar{\lambda}$) results

Figure 2.5: Robustness analysis of telecommunication networks under simultaneous targeted attacks by degree centrality (d_c): Structural measurements

networks. The weak level is between 1 and 5 % of failures, where network connections can decrease dramatically to 60 %. When the percentage of nodes removed (P) is in the range of 5-20 %, networks have an intermediate affectation with a reduction of 70 % of connections. At 20 % or more of P, networks reduce their connection to $< 10\%$, so networks are near to being completely disconnected with a severe affectation. Therefore, making robustness comparisons for $P > 20\%$ is not relevant as these networks are close to being completely disconnected and the robustness metrics do not reflect real behavior.

For each P, the number of nodes removed from the ABILENE network does not vary substantially due to its small number of nodes and links. Consequently, ABILENE was not considered in the present analysis. The robustness analysis using the $ATTR$ metric (see Fig. 2.5(a)) shows that CORONET_L1 is the most robust network as its network connections are maintained at over 80 % when P is not more than 10 %. CORONET_L1 has a high value of average nodal degree ($\langle k \rangle$) (2.72), and low values of maximum nodal degree (k_{max}) (5) and average shortest path length ($\langle l \rangle$) (6.6741), which would explain this result. This network is also an assortative network with $r = 0.0357$. Nonetheless, the KDL network has the least robustness. For instance, in the range of 3 to 5 % of P, the connections of KDL are reduced to $< 15\%$. This is because KDL has the lowest value of $\langle k \rangle$ (2.3846) and the highest value of $\langle l \rangle$ (22.727), and it is also a disassortative network ($r = -0.096$).

In Fig. 2.5(a), it can be seen that the GEANT, RENATER and TISCALI_L3 networks have similar $ATTR$ behavior and that these networks remain in the top five of most robust networks. At 5 % of P their networks' connections are reduced to 80 %. This first set of networks has high values of $\langle k \rangle$ and low values of $\langle l \rangle$ and diameter (D). In contrast, the COGENTCO, SPRINT_L1 and USCARRIER networks lose more than 50 % of their connections after 5 % of P. This second set of networks is characterized by low values of $\langle k \rangle$ and high values of $\langle l \rangle$ and D.

In Fig. 2.5(b), the robustness results for natural connectivity ($\bar{\lambda}$) are presented. As can be seen, with $< 20\%$ of P it is possible to identify which networks are more robust than others and they can be grouped. Thus, the most robust networks are TISCALI_L3, DELTACOM and GARR, and the least robust are USCARRIER, SPRINT_L1 and KDL. Analogous robustness results for $\bar{\lambda}$ were obtained with the largest eigenvalue (λ_1) metric. Hence the structural metrics selected in this analysis agree in grouping the more and less robust networks. These sets of networks have similar topological properties, as can be seen in Table 2.3.

With respect to centrality-based metrics and comparing the structural robustness results, the networks with high centralization values are the most robust i.e., networks have more nodes with similar centrality values that can help to maintain network connections when the percentage of nodes removed increases according to targeted attacks. However, in simultaneous targeted attacks, the network centralization based on degree centrality (d_c) is the most appropriate metric to measure the network robustness owing to nodes being removed by their degree centrality values. Similar to structural metrics, centrality-based metrics allow network robustness to be compared to no more than 20 % of failures.

Figure 2.6 shows the robustness results of network centralization based on degree centrality (d_c). As can be seen, it is possible to identify three subsets of networks:

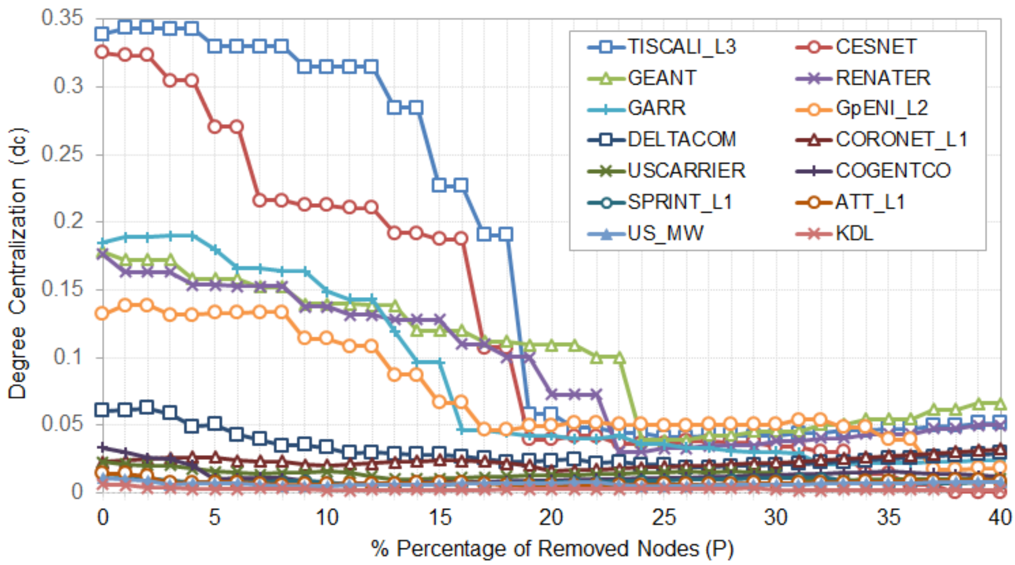


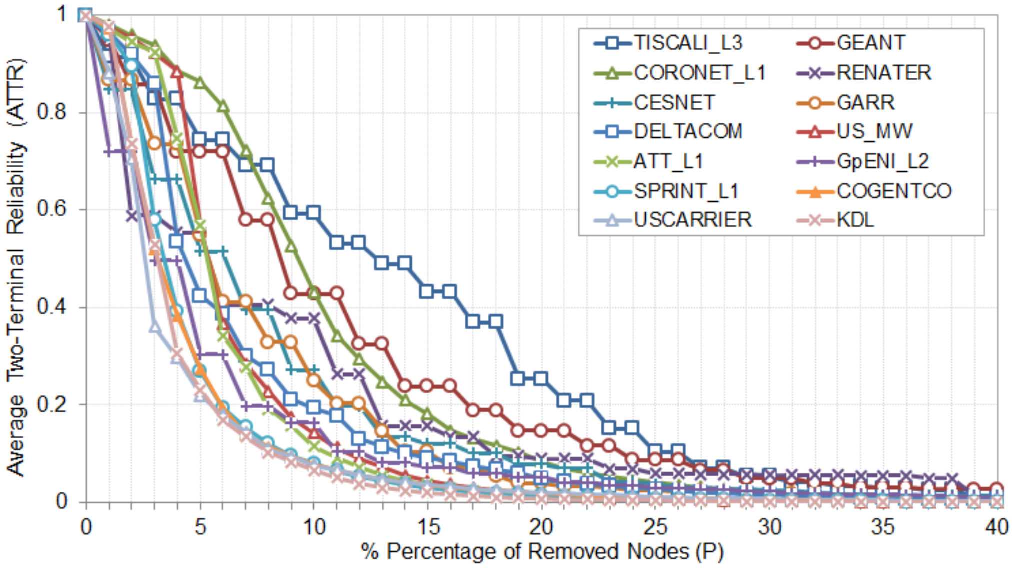
Figure 2.6: Robustness analysis of telecommunication networks under simultaneous targeted attacks by degree centrality (d_c): Centrality measurements

the first has two networks with the highest robustness (TISCALI_L3 and CESNET), the second has four networks with an intermediate robustness (GEANT, RENATER, GARR and GPENI_L2) and the third has the least robust networks e.g., SPRINT_L1, ATT_L1, US_MW and KDL. The topological properties of these subsets of networks are similar i.e., the most robust networks have high values of $\langle k \rangle$ and low values of $\langle l \rangle$ and D, whereas the least robust networks have low values of $\langle k \rangle$ and high values of $\langle l \rangle$ and D (see Table 2.3).

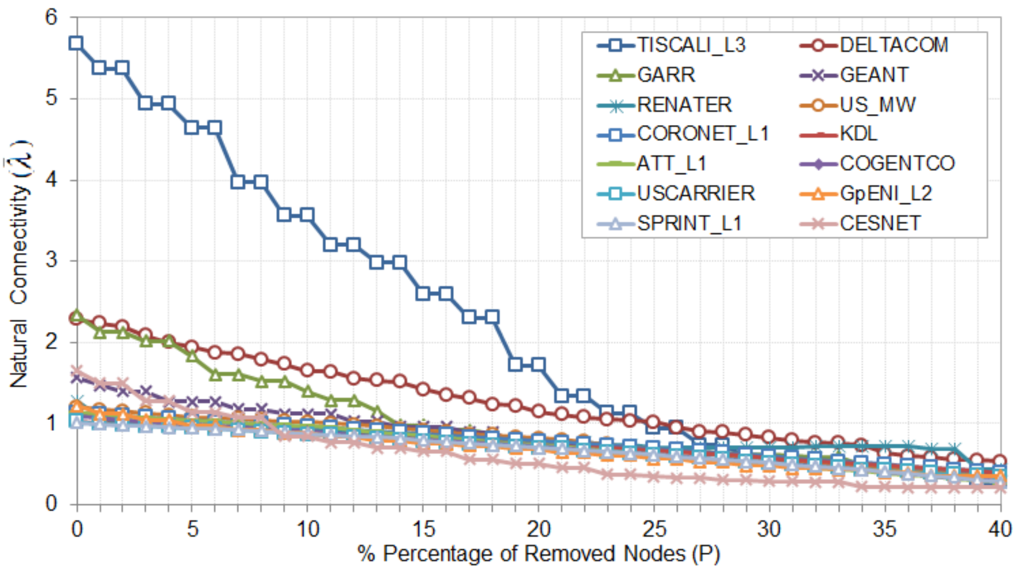
2.6.3 Robustness measurements under sequential targeted attacks

This section presents the robustness analysis of the real telecommunication networks when nodes are removed under the sequential targeted attack. In this scenario the most effective technique for removing nodes is nodal betweenness centrality (b_c) [54]. As more vertices are removed, the network structure changes, leading to the different distributions of the most important nodes from the initial ones [85]. As can be seen in Fig. 2.7(a), Average Two-Terminal Reliability ($ATTR$) results show that all the networks are more robust under sequential targeted attacks than when compared to simultaneous targeted attacks. A similar robustness behavior for both attacks can be found in [54, 85]. Figure 2.7(a) also shows that when the percentage of removed nodes (P) is between 1 and 5 %, 50 % of the network connections are lost. At 15 % of P, most of the networks reduce their connections to $< 20\%$ and, at 20 % or more, networks are near to being completely disconnected.

By comparing this robustness result with the robustness result in simultaneous



(a) Average Two-Terminal Reliability ($ATTR$) results



(b) Natural connectivity ($\bar{\lambda}$) results

Figure 2.7: Robustness analysis of telecommunication networks under sequential targeted attacks by betweenness centrality (b_c): Structural measurements

targeted attacks, in sequential targeted attacks the TISCALI_L1 network moves up from fourth to first place in the ranking of most robust networks, whereas CORONET_L1 goes down to eighth place. TISCALI_L1 has a high average nodal degree ($\langle k \rangle$) value (5.0588) and a low average shortest path length ($\langle l \rangle$) value (2.4298), which can explain this result. In contrast to the CORONET_L1 network, TISCALI_L3 is one of the most disassortative networks ($r = -0.3614$). This means that disassortative networks are less vulnerable to sequential targeted attacks by nodal betweenness centrality and assortative networks show more robustness under simultaneous targeted attacks by nodal degree centrality.

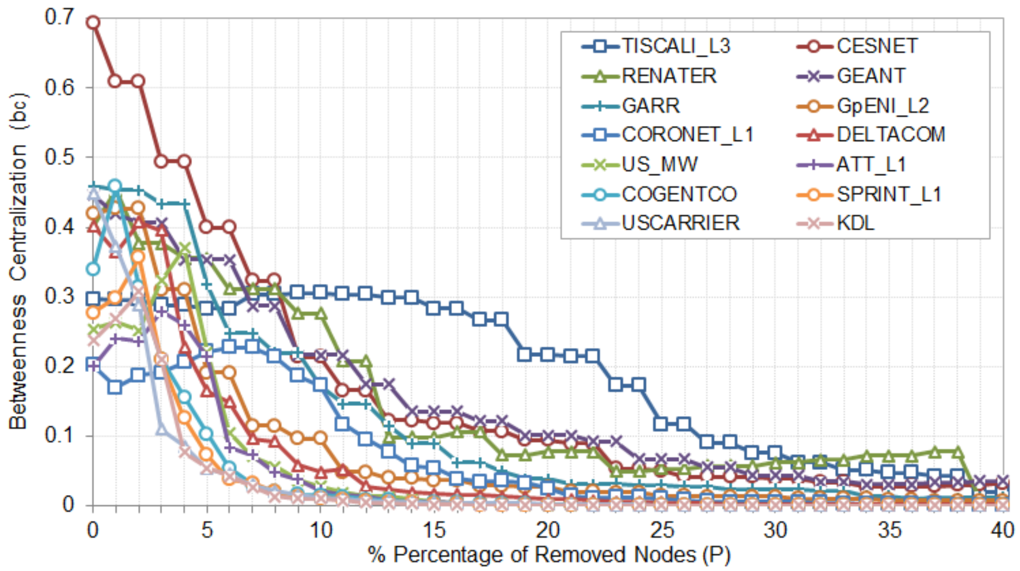


Figure 2.8: Robustness analysis of telecommunication networks under sequential targeted attacks by betweenness centrality (b_c): Centrality measurements

This result for assortativity coefficient (r) analysis is the same as that found in [54, 103]. In both targeted attacks, KDL is the least robust network.

In Fig. 2.7(b) the robustness results for the natural connectivity ($\bar{\lambda}$) metric are presented. The $\bar{\lambda}$ metric allows the networksthat are the most robust to $< 25\%$ of P to be identified. In this sense, TISCALI_L3 presents the best robustness and USCARRIER the poorest. The largest eigenvalue (λ_1) metric exhibits similar robustness behavior to $\bar{\lambda}$. In both cases, the robustness degradation is lower than the results found in the simultaneous targeted attacks.

For centrality-based metrics, the most robust networks are also those with high centralization values. In contrast to the simultaneous targeted attack results, for sequential targeted attacks these metrics allow network robustness to be compared to no more than 35 % of failures. In this failure scenario, network centralization based on nodal closeness centrality (c_c) and nodal betweenness centrality (b_c) are the most effective metrics to measure the network robustness in sequential targeted attacks due to the nodes being removed by their betweenness centrality values. As shown in Fig. 2.8, in the range of 1–10 % of P, the shortest paths are quickly lost and so the length of the shortest path between nodes quickly increases. Therefore, networks have fewer nodes with high values of betweenness or closeness centrality, which generates the increases in network centralization values.

Figure 2.8 shows the robustness results according to the network centralization based on b_c. As can be observed, in the range of 1-10 % of failures, it is not easy to identify which networks are most robust due to the high variability produced by the increase in

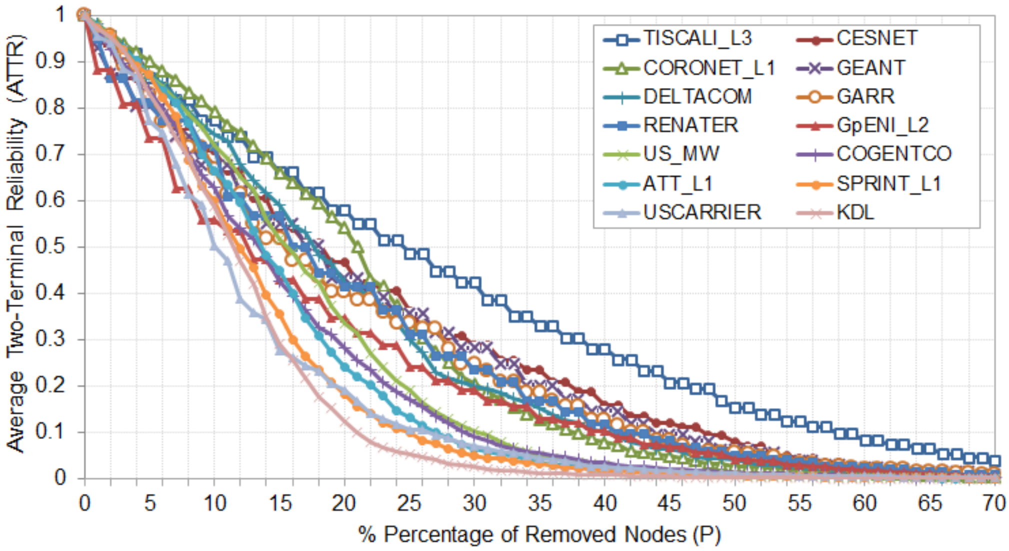


Figure 2.9: Robustness analysis of telecommunication networks under random failures: Structural measurements

$\langle l \rangle$. Nonetheless, when P is between 10 and 30 %, it can be seen that TISCALI_L3 is the most robust network, followed by the group including the CESNET, RENATER, GEANT and GARR networks and last by a set of least robust networks e.g., SPRINT_L1, USCARRIER and KDL. Like the robustness results presented in sequential targeted attacks, the most robust networks have high values of $\langle k \rangle$ and low values of $\langle l \rangle$ and D, whereas the least robust networks have low values of $\langle k \rangle$ and high values of $\langle l \rangle$ and D.

2.6.4 Robustness measurements under random failures

In this section, the robustness analysis of the set of real telecommunication networks, when nodes are removed under random failures is presented. Figure 2.9 shows the robustness results according to Average Two-Terminal Reliability ($ATTR$) for random node failures. As can be seen, all the networks are more robust under random failures as compared to both types of targeted attacks. This is because in random attacks most central nodes are less likely to be removed in first percentages of failures.

Figure 2.9 shows that network connections are over 50 % from 1 to 10 % of failures, whereas all of them reduce their connections to $< 50\%$ in the range of 10–25 % of P. At 68 % or more failures, all the networks have $< 5\%$ of connections. In this case, TISCALI_L3 is the most robust network and KDL is the least robust. The set of networks with high robustness to random node failures has low values of average shortest path length ($\langle l \rangle$) and diameter (D), and they are the most disassortative networks ($r < 0$). Furthermore, it can be observed that networks with high average nodal degree ($\langle k \rangle$) show robustness to random attacks, which is in line with the results found in [101, 102].

2.7 Discussion and lessons learned

In accordance with the results presented here, some conclusions can be drawn. First, the robustness analysis based on structural metrics shows that the subset of most robust real telecommunications networks under targeted attacks has high values of average nodal degree ($\langle k \rangle$) and low values of average shortest path length ($\langle l \rangle$) and Diameter (D), whereas the subset of least robust networks has the opposite results for $\langle k \rangle$, $\langle l \rangle$ and D. Similar to previous studies, for disassortative networks ($r < 0$) simultaneous targeted attacks by nodal degree centrality is the most effective method of degrading a network. However, in sequential targeted attacks by nodal betweenness centrality, assortative networks ($r > 0$) are more vulnerable. These results are a consequence of disassortative networks having an excess of links connecting nodes of dissimilar degrees, which in simultaneous targeted attacks are removed rapidly according to their degree centrality value.

The second round of conclusions is focused on the robustness comparison using the centrality-based metrics. The subset of real telecommunication networks with high values for the network centralization metrics based on nodal degree centrality (d_c), nodal closeness centrality (c_c) and nodal betweenness centrality (b_c) shows robustness under targeted attacks as more central nodes must be removed to affect network performance. Networks with low results in centralization metrics are less robust. Moreover, a robustness analysis according to centrality-based metrics can be carried out by selecting the appropriate metric to identify the impact of nodal failures. Hence, in simultaneous targeted attacks by nodal degree centrality, the centralization metric based on d_c should be used to measure the robustness. However, in the case of sequential targeted attacks by nodal betweenness centrality, network robustness should be measured by the centralization metric based on b_c.

As regards the results of nodal random failures, the subset of more robust real telecommunication networks has low values of average shortest path length ($\langle l \rangle$) and Diameter (D), and they are the most disassortative networks ($r < 0$). Similar to previous studies, topologies with high average nodal degree ($\langle k \rangle$) also show robustness to random failures as there are more nodes available to maintain connections. Additionally, in random failures the probability of affecting central nodes at first values of percentage of removed nodes (P) is low compared to targeted attacks. Therefore, a lot of nodes would have to be removed to degrade the network structure to the same affectation levels reached by targeted attacks.

Chapter 3

Robustness measurements in interdependent networks: review, new proposals and applications

Most of critical infrastructures in the real world cannot be described adequately as single isolated networks, but should be represented as interdependent networks. Consequently, the proper functioning of interdependent infrastructures depends on the normal operation of networks that are interconnected. In order to study the robustness of interdependent networks, three factors should be considered: the network model, the interdependency model and the failure model. In this chapter, a review of the most relevant research on robustness measurements in interdependent networks is presented. Moreover, as an application scenario, an interconnection mechanism based on interdependency matrices is proposed to mitigate the impact of targeted attacks, and the propagation of these attacks between interconnected networks is also studied.

3.1 Introduction

Critical infrastructures are not isolated, but interact with each other to provide the goods and services that are essential to modern society [107]. Transportation infrastructures provide many examples of interdependent networks. Power grid, water/gas networks, metro and rail systems rely on telecommunication networks for their control systems [21]. Particularly, in a power grid connected to a telecommunication network, and vice versa, each router receives power from a substation and every substation sends data and receives control signals to/from one router [20, 108, 109]. Another example is the case of power grids and water distribution networks, where their interdependencies are illustrated by the fact that pump stations, control units and storage tanks in water networks depend directly on substations in the power network to function well [25, 110]. These interdependent networks are characterized by connectivity links within each network and interdependency links between networks.

Interdependency between critical infrastructures is a crucial aspect to the normal operation of the whole system, but it increases these systems' vulnerability to failures because the behavior and reliability of one network then depends on the other networks [16]. If one network depends on and supports another network, a pair of networks are interdependent [111]. A fundamental property of interdependent networks is that a node failure in one network can spread to nodes in the other, leading to cascading failures and system collapse [16]. Moreover, the geographical distribution of network elements influences the susceptibility of networks to certain type of failures and their impact in network operation. For instance, in the case of an interdependent network formed by a power grid and a telecommunication network, electrical blackouts affect large regions and are usually the result of cascading failures due to interdependencies between the two networks [6, 16, 20, 108, 109]. Therefore, interdependent networks are more complex and vulnerable than isolated networks [21].

In previous research, interdependent networks have been generated by interconnecting at least two real transportation networks or artificial graphs following a certain interlink pattern and their robustness has been analyzed under distinct failure strategies [7, 107, 111, 112]. The robustness of these interdependent networks is mainly influenced by three aspects which can define their behavior and vulnerability to failures. First, there are the topological properties of networks that have to be interconnected, which partially define the network's sensitivity to certain types of failure. Second, there is the interdependency model between two networks, which defines the nodes that can be interconnected and how they interact. An interdependency model is determined by interdependency type (physical, cyber, geographic or logical), interlink type (unidirectional or bidirectional), interonnection type (one-to-one or one-to-multiple nodal correspondences), interlink pattern and constraints on interconnecting the nodes (distance, importance, risk, capacity or cost). Last, there is the failure model that defines how the network elements are disconnected. For instance, failures can originate from random or targeted attacks, which in interdependent networks can trigger a cascading failure process due to the interdependency between the interconnected networks.

Most previous studies have focused on measuring the impact of failures in interdependent networks and proposing strategies to reduce the damage they generate [107]. This chapter presents the relevant research on robustness measurements in interdependent networks based on network models of the topologies to be interconnected, interdependency models between the interconnected networks and failure models that affect the networks. In contrast to previous work, we have considered the impact of the most dangerous attack on a network to propose an interconnection mechanism, based on interdependency matrices, which mitigates the damage done to its interconnected network. This is because when a network interacts with another, the critical parts of the network may change due to a failure spreading between them. Therefore, it is interesting to identify changes in robustness in two interdependent network scenarios: 1) the interconnection of two networks with similar topological properties e.g., two interconnected backbone telecommunication networks and 2) the interconnection of two networks with different topological properties e.g., a power grid interconnected to a telecommunication network. Whether or not a failure spreads and generates a cascading failure is beyond the scope of this work. Instead, the focus is on protecting telecommunication and power grid networks from propagating failures. These interdependent networks also support the investigation of the effects of distinct interlink patterns on the propagation of targeted attacks between the two interconnected networks.

The remainder of this chapter is structured as follows. In Section 3.2, a review of aspects to consider in constructing interdependent network scenarios is presented. In Section 3.3, a review of robustness measurements in interdependent networks is carried out. The interlink patterns proposed for the three interdependency matrices are described in 3.4. In Section 3.5, the topological properties of networks to be interconnected are presented. The effect of the interdependency matrices to mitigate and propagate targeted attacks in the interdependent networks is provided in Section 3.6. Last, the results are discussed along with the lessons learned in Section 3.7.

3.2 Review of aspects to consider in interdependent network scenarios

In the literature, several approaches have been proposed for modeling and analyzing interdependent critical infrastructures [7]. These approaches are all useful for capturing interdependencies between transportation networks. Interdependent networks can be generated from the interconnection of at least two single transportation networks by interlinks. Moreover, this representation allows the robustness of interdependent networks to be measured by modeling failures in network elements and then simulating the failure process within a network and its propagation between the interconnected networks [7]. Consequently, network models of the topologies to be interconnected, interdependency models between the interconnected networks and failure models that affect the networks are three key factors that determine vulnerability and the behavior of interdependent networks under multiple failures. Figure 3.1 summarizes the factors that may be

- Network model
  - Network-based
    - Graphs
    - Interlinks
  - Other models
    - Hierarchical Holographic
    - High Level Architecture
    - Petri-Net
    - Bayesian Network
- Interdependency model
  - Interdependency type
    - Physical
    - Cyber
    - Goegraphic
    - Logical
  - Interlink type
    - Unidirectional
    - Bidirectional
  - Interconnection type
    - One-to-one
    - One-to-multiple
  - Interlink pattern
    - Randomly
    - Nodal property
    - Functionality
    - Vulnerability
  - Interconnection constraint
    - Distance
    - Importance
    - Risk
    - Capacity
    - Cost
- Failure model
  - Element removed
    - Link
    - Node
  - Dynamic process
    - Single affectation
    - Cascading failure
  - Triggered event
    - Random failure
    - Targeted attack

Figure 3.1: Factors to consider in interdependent network scenarios

considered in interdependent network scenarios to evaluate its robustness. In this section, these three factors to characterize interdependent network scenarios are introduced.

3.2.1 Network model: Network-based approach for interdependent networks

Interdependent networks should be represented by models that capture the topological properties of the transportation networks to be interconnected. Consequently, the characterization of the interactions between the nodes of these critical networks can be carried out according to concepts in the field of network science. In this work, interdependent critical infrastructures are modeled by using a network-based approach, where each infrastructure is modeled as a network (graph) and the interdependencies between the networks are expressed by interlinks. This representation describes the interdependencies between them because it captures the topological properties of transportation networks and the flow patterns within an interdependent critical infrastructure [7, 16, 18, 26, 31].

Let us consider two undirected networks $G_1(S,U)$ and $G_2(T,V)$, each with a set of nodes (S,T) and a set of links (U,V), respectively. Within network G_1, the nodes are randomly connected by L_1 links with degree distribution $P_1(k)$, while the nodes in network G_2 are randomly connected by L_2 links with degree distribution $P_2(k)$. When G_1 and G_2 interact, a set of bidirectional interlinks I joining the two networks is introduced. Consequently, an interdependent network is defined as $G = (S \cup T, U \cup V \cup I)$, where $S \cup T$ is the set of nodes in G and $U \cup V \cup I$ is the set of links in G [31]. Let us denote $N = N_1 + N_2$ as the number of nodes in G and $L = L_1 + L_2 + L_{12}$ as the number of links in G. Note that L_{12} is the number of interlinks between the G_1 and G_2 networks.

Interdependent networks can be generated from interconnecting at least two complex networks, generating some models that could be extended to real world systems. Thus, Erdős-Rényi (ER), Small-World (SW) and Scale-Free (SF) graphs can be considered to generate interdependent networks to address robustness studies. An interdependent network can be generated by interconnecting networks with similar or dissimilar topological properties such as nodal degree distributions [113]. The ER-ER coupled system represents the interconnection of two random graphs of Erdős-Rényi (ER) [46] and may model the interconnection of two backbone telecommunication networks. Other interdependent network models whose networks have similar degree distributions are the SW-SW coupled system, which represents the interconnection of two Small-World (SW) graphs of Watts-Strogatz [49], and the SF-SF coupled system, which correspond to interconnection of two Scale-Free (SF) graphs of Barabási-Albert [50]. Many modern networks, such as the Internet, scientific collaboration, telephone, power grids and airline networks, can be approximated by the SF graph [49], thus a SF-SF system can model the interconnection of these real networks [113]. Regarding the interconnection of networks with dissimilar properties there are combinations such as the ER-SF, ER-BA and SF-BA coupled systems. For instance, the interconnection of a telecommunication network and a power grid can be represented by an ER-SF interdependent network.

As in the case of simple networks, interdependent networks also have a matrix representation [31]. Let us define the Adjacency matrix A of an interdependent network G as the $N \times N$ matrix:

$$A_{N\times N} = \begin{pmatrix} A_1 & \alpha B_{12} \\ \alpha B_{12}^T & A_2 \end{pmatrix}, \tag{3.1}$$

where α represents the coupling strength of the interaction, A_1 is the $N_1 \times N_1$ Adjacency matrix of network G_1, A_2 is the $N_2 \times N_2$ Adjacency matrix of network G_2 and B_{12} is the $N_1 \times N_2$ interconnection matrix representing the interlinks between node i in network G_1 and node j in network G_2 [31]. Considering bidirectional interlinks, then $B_{21} = B_{12}^T$ [31]. Let b_{ij} denote as the (i, j) entry in the B_{12} matrix, where $b_{ij} = 1$ if the node i and node j are interconnected, and $b_{ij} = 0$ if they are not. The interdependency matrix (B) of the whole coupled system is given by [31]:

$$B_{N\times N} = \begin{pmatrix} 0 & B_{12} \\ B_{12}^T & 0 \end{pmatrix} \tag{3.2}$$

Similar to the adjacency matrix, let us introduce the Laplacian matrix Q of an interdependent network G as a $N \times N$ symmetric matrix given by [31]:

$$Q_{N\times N} = \begin{pmatrix} Q_1 + \alpha D_1 & -\alpha B_{12} \\ -\alpha B_{12}^T & Q_2 + \alpha D_2 \end{pmatrix}, \tag{3.3}$$

where Q_1 is the $N_1 \times N_1$ Laplacian matrix of adjacency matrix A_1 in network G_1 and Q_2 is the $N_2 \times N_2$ Laplacian matrix of adjacency matrix A_2 in network G_1, D_1 is the $N_1 \times N_2$ diagonal matrix of degrees in network G_1 and D_2 is the $N_2 \times N_1$ diagonal matrix of degrees in network G_2. The diagonal matrices of degrees D_1 and D_2 may be defined as [31]:

$$\begin{cases} (D_1)_{ii} = \sum_j (B_{12})_{ij}, \\ (D_2)_{jj} = \sum_j (B_{21})_{ij} = \sum_j (B_{12}^T)_{ij}; \end{cases} \tag{3.4}$$

Depending on the coupling weight α, different diffusion processes can be expressed in interdependent networks. When $\alpha = 0$, there are no interactions between the networks [31]. However, if $\alpha < \alpha^*$, then the two networks are structurally distinguishable. On the other hand, if $\alpha > \alpha^*$, the two networks behave as a whole unit [114]. The α^* value represents a structural transition point. For large α values, a superdiffusion process is observed, i.e., diffusion in the interconnected networks takes place faster than in either of the networks separately [115]. Superdiffusion is a synergistic phenomenon in an interconnected network that can occur for values of $\alpha < \alpha^*$, where the network components function distinctly [116]. Therefore, the consequences of a failure in one network on the other network depend on a diffusion process provided by the strengths of the interconnections between the nodes.

3.2.2 Other models for interdependent networks

In addition to the network-based model previously described, other approaches have been proposed in the literature for modeling and analyzing interdependent critical infrastructures, including empirical methods, agent-based methods, system-dynamics-based methods, economic-theory-based methods, Hierarchical Holographic Modeling (HHM) based methods, High Level Architecture (HLA) based methods, Petri Net (PN), dynamic control system theory and Bayesian Network (BN) [7, 117]. These approaches are all useful in capturing interdependencies between critical infrastructures. Interested readers are referred to [7, 117] for detailed descriptions and comparisons of the various modeling approaches. However, what follows is presented a brief description of some of the models that are based on graph representation:

- **Hierarchical Holographic Modeling (HHM) based method**: In this approach, the term hierarchical refers to an understanding of risks depending on different levels in a hierarchy [117]. The term holographic modeling refers to a multiview image of a critical infrastructure with regards to identifying vulnerabilities [117]. The basis of HHM is the overlap among various holographic models with respect to the objective functions, constraints, decision variables and input-output relationships of the critical infrastructure [117].

- **High Level Architecture (HLA) based method**: This approach breaks the entire interdependent network down into individual operating networks [117]. In the HLA-based interdependency modeling architecture, three levels can be identified: the low level includes the models of single critical infrastructures, the middle level covers the interaction model between critical infrastructures and the high level represents the global interdependent model [118].

- **Petri-Net (PN) based method**: The Petri-net (PN) can be represented by a four tuple: $PN = (P, T, I, O)$, where P stands for a set of places, T for transitions, I for input functions (a mapping from bags of places to transitions) and O for output functions (a mapping from transitions to bags of places) [7]. Places may contain any number of tokens. When a transition switches ("fires"), it consumes the tokens from its input places, performs some processing task and places a specified number of tokens into each of its output places [117].

- **Bayesian Network (BN) based method**: This approach represents the probabilistic relationship between system and component reliability. The BN consists of a directed acyclic graph where nodes represent random variables and directed links represent causal relationships between these nodes. A BN model requires conditional probabilities to model the dependencies among components, subsystems and systems to represent probabilistic failure relationships in a multilevel system configuration [119]. Moreover, the BN model is capable of combining information from multiple sources at multiple levels for system reliability prediction when the BN model is coupled with statistical Bayesian inference techniques [119].

3.2.3 Interdependency model

The fundamental property characterising interdependent networks is the existence of two different kinds of links: connectivity links (within a transportation network) and interdependency links (between separate transportation networks) [111]. In interdependent networks, how the state of a node influences on the functioning of its interconnected node is determined by the direction of the interlink [1]:

- **Unidirectional interlinks**: An interlink is unidirectional if the dependency is in one way i.e., the state of a node i in one network depends on the state of a node j in the other, but the state of node j does not necessarily depends on the state of the same node i [20].
- **Bidirectional interlinks**: An interlink is bidirectional if the dependency is in two-way i.e., the state of node i in a network depends on the state of node j in the other, and vice versa [1, 111].

Interdependency can be also defined as the bidirectional relationship between the nodes of two or more critical infrastructures, where a node's state in a network depends on least one node's state in other to continue functioning, and vice versa. There are several interdependency types, which have different characteristics and effects on the relationships between the interconnected networks. The following are the common interdependencies that can be evidenced between transportation networks:

- **Physical interdependency**: The state of an infrastructure is dependent on the material output(s) of the other [1] e.g., outages in power systems have caused traffic signals, water supply pumping station and automated teller machines to fail and businesses to close [7].

- **Cyber interdependency**: The state of an infrastructure depends on the information transmitted through the information infrastructure [1] e.g., failures on telecommunication networks affect the control system of power grid substations and cause their failure due to a lack of control from the central system [20].

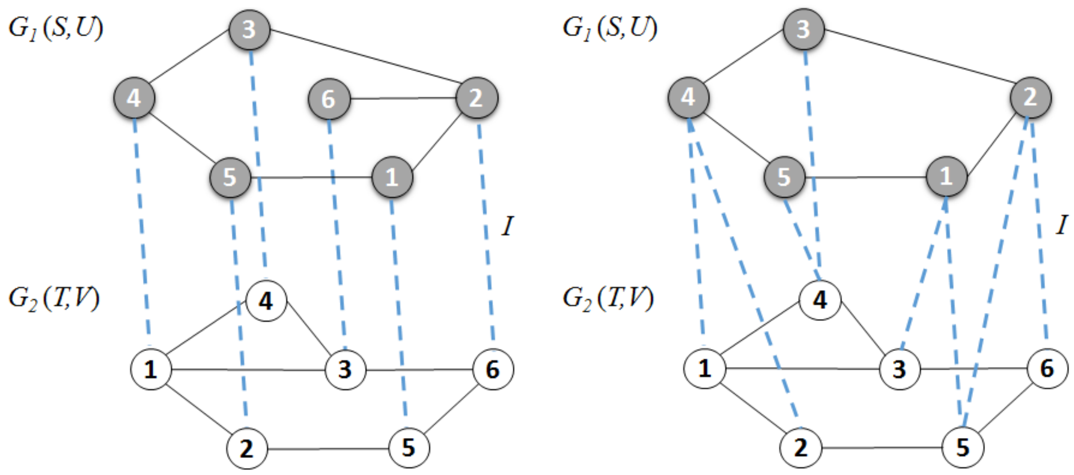
- **Geographic interdependency**: Infrastructures are geographically interdependent if a local environmental event can create state change in them all [1]. It also refers to interconnection based on the proximity between infrastructure systems [120] e.g., power grids provide power to infrastructures that are localized near to a distribution node. A failure in a power grid can cause the disruption of the interconnected networks (mobile networks, water and railway) and can affect large geographical regions [108].

- **Logical interdependency**: The state of an infrastructure depends on the state of the other via a mechanism that does not belong to the above types [1]. Logical interdependencies are usually caused by human decisions and actions undertaken in political or societal areas e.g the amount of oil and gas delivered is highly dependent on the political decisions of OPEC (Organization of the Petroleum Exporting Countries) members [117].

Interdependency links represent the idea that for a node to operate it requires support from a least one another node which, in general, is in another network [111]. According to the number of interlinks that are allocated to a node, the following interconnection types can be identified:

- **One-to-one nodal correspondence model**: Let us consider two undirected networks G_1 and G_2, each with the same number of nodes ($N_1 = N_2$). Then, in this model a node i in network G_1 is interconnected to one and only one node j in network G_2, and vice versa [16]. The one-to-one interconnection can be found in multilayer telecommunication networks where a node in a low layer provides services to a node in the upper layer [15, 121]. However, in practice not all network G_1 nodes depend on network G_2 nodes, and vice versa.

- **One-to-multiple nodal correspondence model**. Let us consider two undirected networks G_1 and G_2, each with a number of nodes N_1 and N_2, respectively. In this



(a) One-to-one correspondence **(b)** One-to-multiple correspondence

Figure 3.2: Interdependent networks representation

model a fraction of the q_1 nodes in G_1 depends on one or more than one node in network G_2 and a fraction of the q_2 nodes in G_2 depends on one or more than one node in network G_1 [18]. When q_1 and q_2 are large, a strong coupling between two networks is presented, whereas for small q_1 and q_2 values, the interdependent network shows a weak coupling [18]. The one-to-multiple interconnection can be found when a communication node provides control services to several nodes in a power grid, and a node in the power grid provides power to a several nodes in the communication network.

The two interconnection types in interdependent networks are illustrated in Fig. 3.2. Nodes in G_1 are represented with filled circles, whereas nodes in G_2 are represented with unfilled circles. The interlinks are represented by dashed lines between the nodes of the two networks. As can be seen in Fig. 3.2(a) each node has one and only one interlink, whereas in Fig. 3.2(b) nodes have one or more interlinks. In both cases, the interlink patterns are represented by an interdependency matrix B. Note that in Fig. 3.2(a) and Fig. 3.2(b) the interlinks between networks G_1 and G_2 follow a random pattern. However, in other cases, interlinks may be allocated following a specific pattern based on the properties, functionality or vulnerability of the nodes as can be seen in the next sections. In addition, constraints such as distance, importance, risk, capacity or cost can be considered to define which nodes will be interconnected.

3.2.4 Failure model: dynamic process in interdependent networks

Transportation networks operate in an environment subject to failures [25]. Failures can be caused by different events that affect the normal functioning of these critical infrastructures. A triggering event is caused by unintentional failures (such as natural disasters or configuration errors) or intentional failures (such as cyber-attacks or terrorism), which damage one network element or a fraction of them [2, 7, 10, 117]. However, the complexity of interdependent networks in which two or more single transportation networks are interconnected by interlinks, means that failures in a network are propagated to its interconnected networks with dramatic and expensive consequences [16].

From the topological properties of transportation networks it is possible to discern what failure type causes the greatest damage in each network. However, failures in interdependent networks present a dynamic process due to the interdependency and the functional properties of the networks to be interconnected. For instance, when a network is under random failures or targeted attacks, the balance of flows is broken causing overloads on some nodes, which may ultimately trigger cascading failures [32]. Therefore, identifying changes in the robustness of interdependent networks help us to understand the behavior of networks in the face of failures and to find strategies to reduce their impact through improving the interconnection patterns between the interconnected networks. Let us consider two networks G_1 and G_2, which are interconnected by bidirectional interlinks. In general, because of the failure propagation between the interconnected networks, when a fraction of P_1 of the nodes in network G_1 fail, a fraction of P_2 of the dependent nodes in network G_2 are removed. Thus, two cases can be considered to define the operational state of the nodes in interdependent networks [22, 120]:

1. A node i in network G_1 is functional if at least one of its interconnected nodes in network G_2 is operative. This condition can be presented in interdependent networks with one-to-one nodal correspondence or one-to-multiple nodal correspondence.

2. A node i in network G_1 is functional if all of its interconnected nodes in G_2 are operative. This case is presented in interdependent networks with one-to-multiple nodal correspondence.

In addition to both conditions, other constraints can be considered to define the operational state of a node. For instance, a node i in network G_1 is functional if the node i belongs to the giant component of the functional nodes in network G_1 [122]. Note that these constraints can define whether a cascading failure process between the interdependent networks is triggered or not. Therefore, the dynamic process of failures may have different implications that should be considered in order to protect interdependent networks from failures. The following are two failure processes on

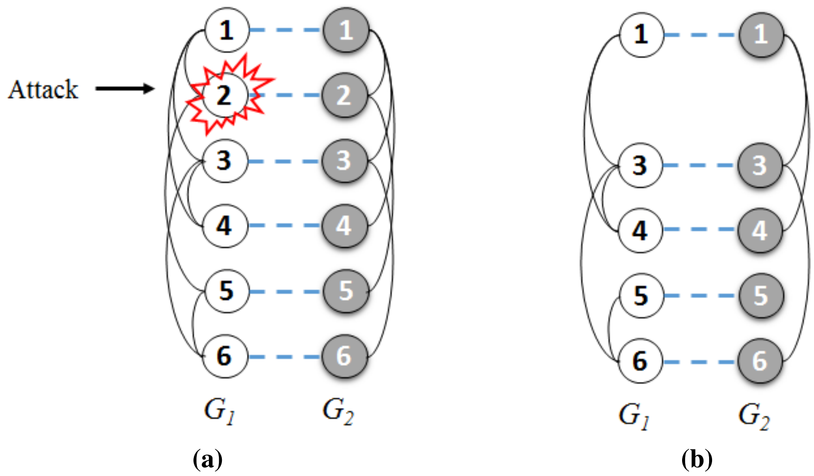


Figure 3.3: Dynamic process of single affectation on interdependent networks (a) Node 2 in G_1 is attacked (b) Node 2 in G_2 fails due to interdependency

interdependent networks which can be triggered by random failures or targeted attacks on one of the interconnected networks:

1. **Dynamic process of single affectation on interdependent networks** Let us consider an interdependent network G with one-to-one nodal correspondence and bidirectional interlinks. Let us also consider that each node i ($i = 1,2,\dots,N_1$) in network G_1 depends on one and only one node j ($j = 1,2,\dots,N_2$) in network G_2 to continue functioning, and vice versa. Thus, when a random failure or a targeted attack occurs on a node i in network G_1, the dependent node j in network G_2 is removed without allowing the attack to propagate to other nodes in network G_2, and vice versa. Figure 3.3 shows targeted attacks on two interdependent networks. Each node in network G_1 depends on one, and only one, node in network G_2, and vice versa. Bidirectional interlinks between the networks G_1 and G_2 are shown as dashed horizontal lines while U and V intralinks are shown as non-directed solid arcs. In Fig. 3.3(a), node 2 in network G_1 is attacked because it has the highest nodal degree. Then, as can be seen in Fig. 3.3(b), only dependent node 2 in network G_2 is removed.

2. **Dynamic process of cascading failures on interdependent networks** Let us consider two networks G_1 and G_2, which are partially dependent in the sense that only a fraction q_1 (q_2) of the nodes in network G_1 (G_2) are interdependent, the rest being autonomous [18, 112, 122]. When a fraction of the nodes in network G_1 fail, a cascading failure process is induced. Generally, node i in network G_1 is functional if a) at least one of its interconnected nodes in network G_2 is operative, and b) node i belongs to the giant component of the functional nodes in network

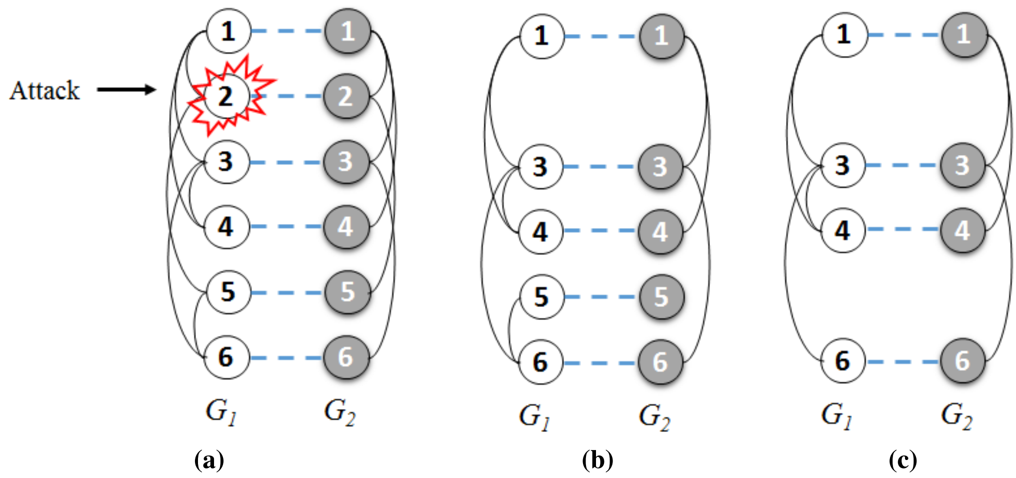


Figure 3.4: Dynamic process of cascading failures on interdependent networks (a) Node 2 in G_1 is attacked (b) Node 2 in G_2 fails due to interdependency (c) Node 5 in G_2 fails due to it not belonging to the giant connected component of G_2, causing the failure of node 5 in G_1 due to the interdependency

G_1 [122]. Thus, at each stage of a cascading failure, the nodes that depend on the initially attacked nodes are removed first. Next, the nodes that do not belong to the giant connected component of the network are removed [122]. Figure 3.4 shows the dynamic process of cascading failure on an interdependent network with one-to-one nodal correspondence and bidirectional interlinks. In Fig. 3.3(a), node 3 in network G_1 is attacked. Then, due to the interdependency, in Fig. 3.3(b) only dependent node 3 in network G_2 is removed. Node 5 in network G_2 also fails due to it not belonging to the Largest Connected Component (*LCC*) of network G_2, causing the failure of node 5 in network G_1 due to the interdependency.

3.2.5 Interdependent network scenarios in previous works

According to the three aspects presented in Fig. 3.1, a number of interdependent networks may be constructed to evaluate their robustness. Hence, a comparison of the previously studied interdependent network scenarios is presented in Table 3.1. As can be seen, the network models considered in these research works are both artificial and real networks, which have been interconnected by several types of interlinks (bidirectional or unidirectional), interconnections (one-to-one or one-to-multiple) and patterns (random, topological-based or geographical). Regarding the failure model, most of them have taken both random failures and targeted attacks triggering a cascading failure process into account. The relevant results of these works about the robustness of interdependent networks under multiple failures are presented in the following section.

Table 3.1: Comparison of the interdependent network scenarios considered in previous works

Author	**Network model**	**Interlink type**	**Interconnection type**	**Interlink pattern**	**Triggered event**
Buldyrev et al. [16], Parshani et al. [18] and Zhou et al. [19]	SF-SF and ER-ER	Bidirectional	One-to-one	Random	Random failure
Jian et al. [28]	SF-SF and ER-ER	Bidirectional	One-to-multiple	Random	Random failure
Shao et al. [22]	SF-SF and ER-ER	Unidirectional	One-to-multiple	Random	Random failure
Hu et al. [23]	ER-ER	Unidirectional and bidirectional	One-to-one and one-to-multiple	Random	Random failure
Gao et al. [24, 122, 123], Havlin et al. [124], Dong et al. [125]	NoN SF-SF and NoN ER-ER	Bidirectional	One-to-one and one-to-multiple	Random	Random failure
Huang et al. [126]	SF-SF	Bidirectional	One-to-one	Random	Targeted attacks
Dong et al. [127]	ER-ER	Bidirectional	One-to-multiple	Random	Targeted attacks
Zhang et al. [26]	SF-SF and ER-ER	Bidirectional	One-to-one	Random	Random and targeted attacks
Dong et al. [27]	NoN SF-SF and NoN ER-ER	Bidirectional	One-to-one and one-to-multiple	Random	Targeted attacks
Wang et al. [128] and Wu et al. [129]	Real and artificial networks	Bidirectional	One-to-one and one-to-multiple	Random and geographical	Targeted attacks: localized and terrorist
Wang et al. [25]	Power and water interdependent network	Bidirectional	One-to-one and one-to-multiple	Distance, betweenness, degree, and clustering coefficient	Random and targeted attacks

Continue on the next page

Table 3.1: Comparison of the interdependent network scenarios considered in previous works

Author	**Network model**	**Interlink type**	**Interconnection type**	**Interlink pattern**	**Triggered event**
Wang et al. [29]	SF-power grid and ER-power grid	Bidirectional	One-to-one	Assortative, disassortative and random	Random failure
Tan et al. [30] and Cheng et al.[33]	SF-SF	Bidirectional	One-to-one	Assortative, disassortative and random	Random and targeted attacks
Tian et al. [32]	SF-SF	Bidirectional	One-to-one	Communities-based on assortative, disassortative and random patterns	Random and targeted attacks
Golshan et al. [34]	Real power grid and communication network	Bidirectional	One-to-one	Assortative, disassortative and random	Random and targeted attacks
Fu et al [130]	SF-SF and ER-ER	Unidirectional and bidirectional	One-to-multiple	Random	Random and targeted attacks
Yagan et al [131]	ER-ER	Unidirectional and bidirectional	One-to-multiple	Random	Random failure
Li et al [35]	ER-ER, real power grid and communication network	Bidirectional	One-to-multiple	Random and cost-based	Random failure
Ji et al [36]	ER-ER, SF-SF and SW-SW	Bidirectional	One-to-multiple	Random and nodal properties-based	Random failure
Parandehgheibi et al.[20]	Real power grid and communication network	Unidirectional and bidirectional	One-to-one	Random	Random failure

Continue on the next page

Table 3.1: Comparison of the interdependent network scenarios considered in previous works

Author	Network model	Interlink type	Interconnection type	Interlink pattern	Triggered event
Tauch et al. [132, 133]	ER-ER	Bidirectional	One-to-multiple	Random	Random failure
Chai et al. [37]	Power grid-ER, power grid-SF and power grid-SW	Bidirectional	One-to-one	Assortative, disassortative and random	Random and targeted attacks
Martín-Hernández et al. [31]	ER-ER, SF-SF, SW-SW and Lattice	Bidirectional	One-to-multiple	Random and diagonal	
Shahrivar et al. [134]	Random k-partite networks and ER	Bidirectional	One-to-multiple	Bernoulli interconnections	

3.3 Review of robustness measurements in interdependent networks

Interdependencies between transportation networks pose new challenges and expose vulnerabilities that should be studied in order to protect these critical infrastructures against service disruption and increase network availability [21]. The robustness analysis of interdependent networks can be considered as a fundamental factor to find methods that contribute to improving their design and to mitigating the impact of failures. In this section, a review of relevant research on the robustness measurements of interdependent networks is carried out by considering the three factors described in previous section. Thus, the response of several interdependent network models to different failure models and the impact of the interdependency models on interconnected transportation networks are described.

3.3.1 Robustness measurements on interdependent networks under random failures

Previous research has focused on analyzing the robustness of interdependent networks to cascading failures resulting from random initial failures by using the percolation theory. The percolation theory helps identify the global connectivity of complex networks with critical threshold (ρ_c), which distinguishes between the connectivity phase and the fragmented phase of networks [107]. Percolation on a single network is an instantaneous process but on interdependent networks the removal of a random fraction of the nodes initiates a cascading failure [112]. When an initial node failure occurs in interdependent networks, a dynamic process of failure between the networks occurs. The most common cascading failure process was described in section 3.2.4, and this showed that there is a critical percolation threshold (ρ_c) above which a considerable fraction of the nodes in the two networks remain functional at a steady state [16]. However, if $\rho < \rho_c$, then both networks fragment completely and the entire system collapses [16].

Scale-Free interdependent networks (SF-SF) were surprisingly found to be more vulnerable to random attack than Erdős-Rényi interdependent networks (ER-ER) [16, 18]. This is because the hubs in one network, which are the source of the stability of single SF networks, can be dependent on low degree nodes in the other network and are thus vulnerable to random damage via dependency links [16]. Furthermore, the percolation threshold decreases with increasing assortativity and therefore assortative networks ($r > 0$) are more fragile in both the ER and SF cases even though in general, SF networks are less robust than ER interdependent pairs [19]. Interdependencies significantly increase the entire network's vulnerability to random failure [18, 23, 24, 123]. In the case of partially interdependent networks (ER-ER and SF-SF), for strong coupling (large values of q_1 and q_2) the networks exhibit a first-order transition, while for a weak coupling they exhibit a second-order phase transition. The first-order phase transition presented in interdependent networks is totally different from the second-order phase transition occurring in single networks [28]. Therefore, interdependence between networks can vastly increase the system's vulnerability, since node failure in one network may lead to the failure of dependent nodes in other networks, and this may happen recursively and lead to a cascade of failures and system collapse [107].

Interdependent networks reach the steady state when the cascade of failures ends [22]. For ER-ER networks with unidirectional interlinks the Largest Mutually Connected Component (*LMCC*) in the steady state follows a simple law, which is equivalent to the random percolation of a single network in the limit of a large number of support links [22]. The case where both connectivity (intralinks) and dependency (interlinks) links connect different networks in coupled ER-ER systems was studied in [23]. The connectivity links can increase the robustness of the system, while the dependency links can decrease its robustness [23]. In the cascading failure process considered by Hu et al. [23], those nodes that are part of the remaining smaller clusters become inoperative unless there is a path of connectivity links connecting these small clusters to the Largest Connected Component (*LCC*) of the other network. In ER-ER networks under this failure scenario, an unusual phase-transition phenomena including first- and second-order hybrid transition was found [23]. Moreover, an unusual discontinuous change from second-order to first-order transition as a function of the dependency coupling between the two networks was discovered[23].

Other interdependent networks are formed when more than two networks might interact with each other. Thus, the robustness of Network of Networks (NoN), which is an extension of coupled networks, is also studied [124]. In a NoN, each node is a network and pairs of networks are considered linked if dependency links exist between them [112]. The robustness of a network formed by n interdependent networks with a one-to-one correspondence of dependent nodes was analyzed by Gao et al. [24, 122, 123]. In this type of network, percolation properties were examined including the size of the *LCC* at each phase of the cascading failure, the size of the *LCC* at steady state and the percolation threshold (ρ_c), among others. For tree-like NoNs, the number of networks in the NoN (n) affects overall robustness, but the specific topology of the NoN does not [24, 122]. In contrast, for a random regular NoN the number of networks n does not affect robustness, but the degree of each network within the NoN does [122]. Moreover, the robustness of n interdependent networks with a partial support-dependence relationship was studied in [125]. When there is a strong interdependent coupling between the networks of a NoN, the percolation transition is discontinuous (it is a first-order transition), unlike the well-known continuous second-order transition in single isolated networks [124].

3.3.2 Robustness measurements on interdependent networks under targeted attacks

Although a random failure can expose the high vulnerability of interdependent networks, it causes less damage than a failure generated by a targeted attack. This is because in a targeted attack, the most important network elements (nodes or links) are the first to be removed [90, 91]. Several properties have been proposed to identify the critical network elements and to discern the probability that an element will be attacked initially and become inactive. Hence, several researchers have analyzed the robustness of interdependent networks in the context of different attack strategies such as targeted attack and localized attack. The robustness of interdependent SF networks under targeted attack on high or low degree nodes was studied in [126]. A general technique that maps the targeted attack problem in interdependent networks to a random attack problem was introduced. Furthermore, Huang et al. [126] found that when the highly-connected nodes are protected and have a lower probability of failure compared with single SF networks, then the coupled SF networks are more vulnerable with ρ_c values significantly greater than zero. Thus, interdependent networks are more difficult to defend using strategies such as protecting the high degree nodes, which have been found useful to significantly improve the robustness of single networks [126].

The percolation of partially ER-ER networks under targeted attack was studied in [127]. In the targeted attack considered by Dong et al. [127], the probability of each node failing is proportional to its degree and it also depends on a factor α. When $\alpha = 1$ the nodes with the highest degree have a greater probability of being attacked first, whereas if $\alpha = 0$ the nodes are removed randomly. For any value of α, in the case of weak coupling the system shows a second-order phase transition, and in the strong coupling the system shows a first-order phase transition. Moreover, in [127] it was found that when the high degree nodes have a greater probability of failing (α increases), the interdependent network becomes more vulnerable.

The robustness of interdependent transportation networks by considering network flows and different attack strategies was analyzed by Zhang et al. [26]. The interdependent networks had a one-to-one bidirectional nodal correspondence that was established randomly. Attack strategies removed nodes with the highest load or the largest degree and a dependent node failed due to overloading or loss of interdependency [26]. Under these scenarios, the robustness of interdependent SF networks (SF-SF) was smaller than single SF network or interdependent SF networks without flows. For interdependent ER networks (ER-ER), the robustness changed substantially possibly due to their narrow betweenness distribution [26]. Finally, Zhang et al. [26] showed that as the tolerance parameter β increased in each case, robustness was improved by increasing the capacities of nodes.

A wide range of possible coupling modes in terms of direction (unidirectional or bidirectional interlinks), redundancy (average of interlinks by node) and extent (fraction of network nodes that are dependent on another network) were evaluated in [130]. These coupling modes were tested in interdependent SF networks (SF-SF) and interdependent ER networks which generated a one-to-multiple nodal correspondence. Fu et al. [130] have shown that interdependent networks with unidirectional interlinks are less robust than those with bidirectional interlinks, and that the degree of redundancy can have a differential effect on robustness depending on the interlinks' directionality. Moreover, optimizing inter-network connections or hardening high degree nodes could help to reduce the vulnerability of an interdependent network to random or targeted attacks [130].

The robustness of a Network of Networks (NoN) under targeted attack on high- or low-degree nodes was studied in [27]. For any tree of n fully interdependent networks (ER-ER and SF-SF) under targeted attacks, the network becomes significantly more vulnerable when higher degree nodes have a greater probability of failing [27]. For different values of α, in [27] it was found that the LCC and the critical fraction p_c is a function of average nodal degree ($\langle k \rangle$) and n for ER and SF networks [27]. Furthermore, when α is increasing or decreasing, the network becomes more vulnerable or more robust, which coincides with the classic percolation of a single network to a targeted network [27]. The robustness of networks coupled by connectivity and dependency links under three types of targeted-attack strategies was analyzed by Du et al. [135]. The results showed that the system undergoes a second- to first-order phase transition as coupling strength increases [135]. Protecting nodes with high degrees of intralinks or interlinks can increase the robustness of the system. But also defending nodes whose sum of degrees of intralinks and interlinks is large can prevent the system from becoming vulnerable [135].

Additionally, interdependent networks may be affected by localized attacks, which are used to simulate the effect of natural disasters such as earthquakes or floods on critical infrastructures [136]. Generally, in a localized attack all the nodes placed in the influence area fail [137, 138], but in real cases the failure probability of nodes should decrease with the distance from the epicenter [128]. Real and artificial interdependent networks with one-to-one nodal correspondence have been considered to analyze robustness as a function of the largest mutually connected component [128]. Wang et al. [128] showed that the impact of the new localized attack on network robustness is relatively small compared with the impact generated by traditional localized attacks, random failures and targeted attacks. On the other hand, in [129] the robustness of a medium-sized energy system including an oil network and a power network was explored against cascading failures generated by terrorist attacks. Physical and geographical interdependencies were considered to generate the interdependent networks. Wi et al. [129] showed that interdependent networks collapse when only a small fraction of nodes were attacked and spatially localized attacks cause less vulnerability than equivalent random failures [138].

3.3.3 Robustness measurements on interdependent networks under different interlink patterns

Interlink patterns refer to those mechanisms whereby the interdependency links between the nodes of the interconnected networks are allocated. Most of the works presented above consider a random interconnection pattern to interconnect two or more networks. However, real interdependent networks are not usually randomly interdependent, but rather pairs of dependent nodes are coupled according to an interlink pattern [139]. Therefore, other research works have focused on studying the effects of various interlink patterns on the robustness of interdependent networks. Parshani et al. [139] showed that inter-similar coupled networks, i.e., coupled networks in which pairs are coupled according to kind of regularity rather than randomly, are significantly more robust to random failure. The interdependent networks ER-ER and SF-SF and the port-airport system were studied in [139]. In [131] was demonstrated that the regular allocation of bidirectional interlinks always yields stronger robustness than random strategy and unidirectional interlinks do.

The power and water systems were taken in [25] as an example to analyze the vulnerability of interdependent infrastructures with bidirectional interlinks. Random failures and degree-based and betweenness-based attacks were considered to generate cascading failures. Four interlink patterns based on distance, betweenness, degree and clustering coefficient were considered to analyze the robustness of interdependent networks to random failures and targeted attacks. Wang et al. [25] found that the random removal of nodes causes the network less damage, whereas the betweenness-based attack causes the largest performance losses. This is due the fact that the high-degree and high-betweenness nodes usually support more loads. Thus, when nodes with high loads are attacked and removed, other nodes are assigned more loads, which may exceed their maximum capacity causing more performance loss [25]. The distance-based coupling modes had low efficiency change trends under deliberate attacks, but were rather vulnerable to random attacks. The betweenness-based coupling and the clustering coupling strategies had relatively good performance, and the betweenness-based strategies had better tolerance to random events [25]. The degree-based strategy has intermediate efficiency drops for random disturbance.

The robustness of the interdependent networks' two artificial networks (ER and SF graphs) and the power grid were analyzed in [29]. Three coupled patterns with bidirectional interlinks and one-to-one nodal correspondence were considered. Wang et al. [29] showed that interlink patterns can dramatically improve the robustness of interdependent networks by preventing cascade propagation according to the load, the load redistribution and the node capacity. The results found in [29] indicate that SF networks play the important role in enhancing the performance of the interdependent networks. Therefore, for the smaller value node initial load the best coupling pattern to interconnect a power grid and an SF network is an assortative (”high-to-high” degree coupling) interlink pattern, while for larger node initial load the best is the disassortative (”high-to-low” degree coupling) interlink pattern [29].

The study of the effect of coupling preference on cascading failures in interdependent SF networks generated from initial targeted attacks was carried out under the two main failure factors: loss of interdependency and overloads [30, 140]. Thus, if one node in a network is removed, loads will be redistributed globally, leading to the failure of nodes within the network due to the overload factor, and the failed nodes in this network will cause the failure of their dependency counterparts in its interconnected network [30]. Tan et al. [30] found that an assortative interlink pattern (”high-to-high” load coupling) is more helpful to resist cascades compared to disassortative (”high-to-low” load coupling) or random interlink patterns. Chen et al. [140] found that a disassortative interlink pattern is more robust for sparse coupling, while assortative patterns performs better for dense coupling. For sparse coupling, enhancing the coupling probability can make interconnected networks more robust against intentional attacks, but keeping increasing the coupling probability has the opposite effect for dense coupling [30]. Moreover, increases in redundancy, average degree or network size can significantly improve assortative coupling robustness [140]. These results can be useful for the design and optimization of interconnected networks such as communication networks, power grids and transportation systems [30]. For instance, Golshan et al. [34] showed that assortative coupling (”high-to-high” degree interconection) is better at mitigating cascading failures in real power grids interconneceted to communication networks.

Additionally, the influences of community structure on cascading failures on interdependent SF networks with traffic loads was studied by Tian et al. [32]. Communities, also called clusters or modules, are groups of nodes which probably share common properties and/or play similar roles within the graph [141]. In [32] three mainly inter-community connections and coupling preferences were analyzed, i.e., Random

Coupling In Communities (RCIC), Assortative Coupling In Communities (ACIC) and Assortative Coupling With Communities (ACWC), where the ACIC model was shown to best resist cascading failures. For ACIC, cascading failures propagate mainly in a local community where the initial failure occurs [32]. Furthermore, increasing inter-community connections can enhance the robustness of interdependent modular SF networks for both inner attacks and hub attacks [32]. The addition of interlinks to interdependent networks was studied in [36]. Ji et al. [36] suggested that the low Inter Degree-Degree (IDD) difference addition strategy and the Random Inter Degree-degree (RID) difference addition strategy are superior to the four existing link addition strategies (random addition, low degree, low betweenness and algebraic connectivity based) in improving the robustness of interdependent networks with high average inter degree-degree difference. In addition, the weighted allocation of interdependency links under a limited budget to obtain a more robust interdependent cyber-physical network was studied by Li et al. [35]. If weights of dependency links are identical, node degree distribution is critical to network robustness, but if weights of dependency links are not identical, choosing dependency link strategies under a limited budget affects network robustness [35].

3.3.4 Robustness metrics in interdependent networks

Most research in the robustness of interdependent networks under multiple failures has been carried out using the tools of the percolation theory. However, to quantify the impact of failures on interdependent networks, new robustness metrics have been proposed and some metrics used in robustness analysis of single networks have been extended. One of the first robustness metrics was the Largest Mutually Connected Component ($LMCC$), which measures the level of connectivity of a network [16, 126]. In a cascading failure, clusters of nodes that are disconnected from the network core (giant component) become non-functional and are removed. The $LMCC$ measures the number of nodes that remain functional after a cascading failure process in interdependent networks [16]. The larger the $LMCC$, the more robust the networks. Therefore, the $LMCC$ is of special interest since it is the only functional part of an interdependent network [16].

Modiano et al. [20] proposed the Minimum Total Failure Removal ($MTFR$) as a new metric to evaluate the robustness of interdependent networks. The $MTFR$ metric quantifies the minimum number of network elements that should be removed from two interconnected networks for all the nodes in the networks to fail after the ensuing cascades [20]. Thus, the larger the $MTFR$ is, the more robust are the networks. In [34], the final failure size of two interdependent networks was measured after a cascading failure process to estimate the impact of an initial failure. A number of vulnerability metrics used to measure the disaster impact in multilayer communication networks was presented by Habib et al. [142]. Disaster failures can cause multidomain multilayer failures and damage large portions of communication networks [142]. Thus, most reviewed metrics in [142] have focused on quantifying network connectivity, the amount of disrupted traffic, the probabilistic number of failed components and the economic loss due to disaster failures.

Other researchers have used algebraic connectivity (λ_2) to analyze the robustness of interdependent networks [31, 132, 134]. In [31] the critical number of interlinks beyond which any further inclusion does not enhance the algebraic connectivity was analysed; this phase transition depends on the topology of the graph model and it was discovered that the transition point also increases with assortativity. In [132] the algebraic connectivity was evaluated as a robustness metric and was used to rewire interlinks. A tight asymptotic growth rate on the algebraic connectivity of random interdependent networks for certain ranges of interlink formation probabilities (again, regardless of the intra-layer topologies) was provided, showing the importance of the interdependencies between networks to information diffusion dynamics [134].

Effective Graph Resistance (EGR) as a robustness metric for interdependent networks by considering the Laplacian matrix of interdependent networks was analyzed in [133]. The results via EGR analysis showed that an interdependent network is more robust when more interlinks are added to the interdependent network [133]. Relative size, which is defined as a quotient between the number of nodes in the giant component after and before a cascading failure was also used to quantify the damage done to an interdependent network [32]. To understand how communication functionality is degraded, Chai et al. [37] selected Efficiency (E) [56] to estimate the impact of cascading failures on interdependent communication and power distribution networks. Centrality metrics (degree, betweenness, closeness and eigenvalue) were used to rank the nodes based on their importance and the attacks on the interdependent networks in descending order. The results showed that for all three coupling networks (Power-ER, power-SF and power-SW) the different targeted attacks were more effective in reducing their robustness than random failures [37]. However, power grids coupled with an SF communication network were the least robust against cascading failures, but they were the most robust when they depended on a SW communication network [37]. Last, it was found that higher link density in sparse networks (i.e., at low density region) provides better robustness for the same type of network model [37].

3.3.5 Summary and research direction

The distinction between internal connectivity links within transportation networks (intralinks) and interdependent links between these critical infrastructures (interlinks) has posed new challenges in interdependent networks, increasing the interest in research in this area [21]. Because of the interdependency between interconnected networks, random failures or targeted attacks in one network are propagated to the others with severe consequences for the operation of the networks. Factors such as the network model of the topologies to be interconnected, the interdependency model between the interconnected networks and the failure model that affect the network have been decisive in defining vulnerability and the behavior of interdependent networks under multiple failures. Therefore, understanding and analyzing interdependency between transportation networks is essential for designing more robust interdependent networks.

The main objective of failure vulnerability studies is to identify the critical parts of networks to improve their robustness to multiple failures. In order to protect networks, the most important nodes (links) that cause the whole network to malfunction should be identified. Therefore, one can learn how to build attack-robust networks and also how to increase the robustness of interdependent networks [85]. A comparison of the relevant results of previous works about robustness measurement in interdependent networks is presented in Table 3.2. As can be seen, most of the works are focused on identifying the network robustness behaviour in the context of random failures and targeted attacks which trigger a cascading failure process based on a some metrics. Other works are focused on identifying the influence of interdependency types on the propagation of failures between the interconnected networks. Therefore, what follows are the research objectives that will be covered in the remainder of this chapter:

- Interdependencies between transportation networks have severe consequences for their operation due to the fact that a failure in one network is propagated to its interconnected network, even causing full service disruption. Previous research has shown that interdependency links that follow a pattern different from random coupling may enhance the robustness of interdependent networks to failures. Targeted attacks in particular have been shown to be the most aggressive trigger of dynamic failures on interdependent networks. Therefore, three interlink patterns based on a vulnerability analysis of each transportation network to be interconnected are proposed. Moreover, we focus on measuring the robustness of interdependent networks for those interlink patterns to identify the best coupling strategy for mitigating the impact of targeted attacks.

- From the results presented in Chapter 2, when the topological structure of a transportation network is taken into account, it is possible to determine which failure type will produce the greatest damage. In such a scenario, the elements that could have serious impacts on the robustness of a transportation networks can be discerned. However, when one transportation network interacts with another, the network's critical parts may change due to failure propagation between them. Thus, it is interesting to identify changes in robustness when two transportation networks with similar or dissimilar topological properties interact. In this chapter a study of targeted attacks propagation between interdependent networks is addressed for the three proposed interlink patterns.

- The main objective of vulnerability studies is to protect networks against failures and build more robust networks. Most previous work has focused on analyzing the robustness of whole interdependent systems by using different metrics such as percolation threshold, *LMCC*, algebraic connectivity and *EGR*, among others. In this research, however, we are interested in individually measuring the robustness of networks that are interconnected to analyze the response of one network due to failures in its interconnected network. Hence, a study of connectivity loss within each network is carried out to identify changes in the robustness of individual networks for the three proposed interlink patterns.

Table 3.2: Comparison of relevant results on robustness measurements in interdependent networks

Author	**Results**	**Robustness metric**
Buldyrev et al. [16], Parshani et al. [18] and Zhou et al. [19]	In interdependent network scenarios, SF networks are more vulnerable to random attack compared to ER networks. In addition, the larger the LMCC is, the more robust are the networks.	Percolation threshold and LMCC
Jian et al. [28] and Zhang et al. [26]	Under random and targeted attacks, partially interdependent networks (ER-ER and SF-SF), percolation exhibits a first-order transition for strong coupling , while a second-order phase transition is exhibited by a weak coupling	Percolation threshold and LMCC
Shao et al. [22]	In interdepedent ER networks with unidirectional interlinks, the largest mutually connected component (*LMCC*) in the steady state follows a simple law	Percolation threshold and LMCC
Hu et al. [23]	The interconnectivity links (intralinks) can increase the robustness of the system, while the interdependency links (interlinks) can decrease its robustness	Percolation threshold and LCC
Gao et al. [24, 122, 123], Havlin et al. [124], Dong et al. [27, 125]	The number of networks that are interconnected and their topology influence in the robustness of NoN. Targeted attacks increase the vulnerability of NoN due to failures on higher degree nodes.	Percolation threshold and LCC
Huang et al. [126]	Protecting interdependent SF networks against targeted attacks is more difficult than for single SF networks.	Percolation threshold and LMCC
Zhang et al. [26]	The robustness of interdependent networks (ER-ER and SF-SF) with flows is improved when tolerance parameter β increases due to the nodes supporting more load.	Percolation threshold and LCC
Wang et al. [128] and Wu et al. [129]	Localized attacks have a relatively small impact compared to random failures or targted attacks	Percolation threshold and LCC
Parshani et al. [139]	Coupled networks in which pairs are coupled according to some kind of regularity rather than randomly are significantly more robust to random failure	Percolation threshold and LCC

Continue on the next page

Table 3.2: Comparison of relevant results on robustness measurements in interdependent networks

Author	**Results**	**Robustness metric**
Wang et al. [25]	Random failures cause interdependent networks less damage, whereas betweenness-based attacks cause the largest performance losses	Percolation threshold and LCC
Wang et al. [29]	Interlink patterns can dramatically improve the robustness of interdependent networks by preventing cascade propagation	Percolation threshold and LCC
Tan et al. [30] and Cheng et al.[33]	An assortative interlink pattern (”high-to-high” load coupling) is more helpful to resist the cascades in SF-SF networks. Moreover, a disassortative interlink pattern (”high-to-low” load coupling) is more robust for sparse coupling, while assortative patterns performs better for dense coupling.	LCC
Tian et al. [32]	Assortative coupling in communities (ACIC) been shown to be the most effective in resisting cascading failures	Relative size of giant component
Golshan et al. [34]	Assortative coupling (”high-to-high” degree interconnection) is better at mitigating cascading failures in real power grids interconnected to communication networks	Failure finally size
Fu et al [130] and Yagan et al. [131]	Interdependent networks with unidirectional interlinks are less robust than those with bidirectional interlinks.	Percolation threshold and LCC
Li et al [35]	The robustness of interdependent networks is influenced when weighted allocation of interdependency links under limited budget is considered	Percolation threshold and LCC
Ji et al [36]	The low Inter Deree–Degree difference addition strategy (IDD) and the Random Inter Degree–degree difference addition strategy (RID) are better at improving the robustness of interdependent networks	LMCC
Parandehgheibi et al.[20]	The larger the minimum total failure removal ($MTFR$), the more robust the networks	Minimum total failure removal

Continue on the next page

Table 3.2: Comparison of relevant results on robustness measurements in interdependent networks

Author	**Results**	**Robustness metric**
Tauch et al. [133]	Results via *EGR* analysis showed that an interdependent network is more robust when more interlinks are added to the interdependent network	Effective graph resistance
Chai et al. [37]	For all three coupling networks (Power-ER, power-SF and power-SW) the different targeted attacks were more effective to reduce their robustness than random failures	Efficiency and LCC
Martín-Hernández et al. [31], Shahrivar et al. [134] and Tauch et al. [132]	There is a critical number of interlinks beyond which any further inclusion does not enhance the algebraic connectivity ($_2$). In failure scenarios, higher λ_2 values indicate better network robustness.	Algebraic connectivity

3.4 Interlink patterns for interdependent networks based on node vulnerability

In the network-based approach considered in this research, an interlink pattern to interconnect two transportation networks is modeled via an interdependency matrix B (see equation 3.2). Let us consider two undirected networks G_1 and G_2, each with the same number of nodes $N_1 = N_2$. Let B_{12} be the $N_1 \times N_2$ interconnection matrix representing the bidirectional interlinks between node i in network G_1 and node j in network G_2, and vice versa. In order to interconnect the nodes i and j through an interlink b_{ij}, our proposal suggests that the vulnerability of nodes in each network to targeted attacks must be quantified. For simplicity, centrality metrics based on the graph theory are used to rank the nodes that are more vulnerable to targeted attacks. However, any other property can be used to quantify the vulnerability of nodes in each network.

Let m_i denote a centrality value of node $i \in G_1$. Then, nodes $i \in G_1$ are ordered from the highest to the lowest value of m_i, i.e., $m_1 \geq m_2 \geq \cdots \geq m_{i-1} \geq m_i \geq m_{i+1} \geq \cdots \geq m_{N_1-1} \geq m_{N_1}$. Similarly, let n_j denote a centrality value of node $j \in G_2$. Then, nodes $j \in G_2$ are ordered according to n_j, i.e., $n_1 \geq n_2 \geq \cdots \geq n_{j-1} \geq n_j \geq n_{j+1} \geq \cdots \geq n_{N_2-1} \geq n_{N_2}$. In both cases, if some nodes have the same centrality measure, then they are labeled randomly. Based on [34], the three interdependency matrices based on node vulnerability that can be generated to interconnect two transportation networks are the following:

- **High Centrality Interdependecy Matrix** (B_{HC}): denoted as a dependency by an interlink $n_i \leftrightarrow m_i$ which defines a one-to-one correspondence between nodes i and j in G_1 and G_2 networks, respectively, i.e., high-centrality (low-centrality) nodes in G_1 are connected to high-centrality (low-centrality) nodes in G_2.

- **Low Centrality Interdependecy Matrix** (B_{LC}): denoted as a dependency by an interlink $m_i \leftrightarrow n_{N_2-j+1}$ which defines a one-to-one correspondence between nodes i and j in networks G_1 and G_2, respectively, i.e., high-centrality nodes in G_1 are connected to low-centrality nodes in G_2, and vice versa.

- **Random Interdependency Matrix** (B_{RA}): denoted as a dependency by a randomly allocated interlink $i \leftrightarrow j$ which defines a one-to-one correspondence between nodes i and j in networks G_1 and G_2, respectively, i.e., nodes between the networks G_1 and G_2 are connected without their centrality measures being considered.

The interlink patterns between two transportation networks can be conditioned by a coupling weight $\alpha > 0$ which affects interdependency strength. Although the impact of a

Table 3.3: Interdependent network scenarios to be studied

Aspect	Scenario 1	Scenario 1
Network model	ER-ER	ER-Power grid
Interlink type	Bidirectional	Bidirectional
Interconnection type	One-to-one	One-to-one
Interlink pattern	B_{HC}, B_{LC} and B_{RA}	B_{HC}, B_{LC} and B_{RA}
Triggered event	Targeted attacks	Targeted attacks

network failure on other networks could be weighted by the coupling coefficient α, this chapter focuses on a scenario where a failure in one node of a network leads to a failure in the dependent node in the other network. Thus, the α value does not condition the failure propagation between the nodes of the interconnected networks and does not limit the evaluation of the three interdependency matrices to mitigate the impacts of targeted attacks. The analysis of the effects of α on failure propagation should be considered as a topic for future research.

As application contexts for the three interlink patterns, the B_{HC} matrix may be used when the most important telecommunication and power grid nodes serve each other, such as in a large city where the nodes in a telecommunication network and a power grid depend on population density. The B_{LC} matrix may be used when the most vulnerable power nodes serve the least critical telecommunication nodes, and vice versa. For example, a telecommunication operator can identify zones where blackouts frequently occur; thus, any of the most critical telecommunication nodes can be located at these points. In contrast, the B_{RA} matrix connects nodes randomly without considering their centrality values; this is the case with telecommunication networks and power grids in non-urban or rural areas. These scenarios show the interlink patterns proposed can be apply in real-life interdependent networks. However, in the practice the BRA matrix may be the most common interlink pattern as the interconnection between networks is generally carried out by considering the function that nodes perform without consider other factors. Thus, the proper selection of one of these interconnection models depends on type of networks to be interconnected and the information available of the vulnerability of the network nodes.

Table 3.4: Topological properties of networks in Scenario 1

Network	N_i	L_i	$\langle k \rangle$	k_{max}	$\langle l \rangle$	D	r
G_1	500	677	2.71	10	6.78	19	0.031
G_2	500	978	3.91	12	4.73	10	0.021

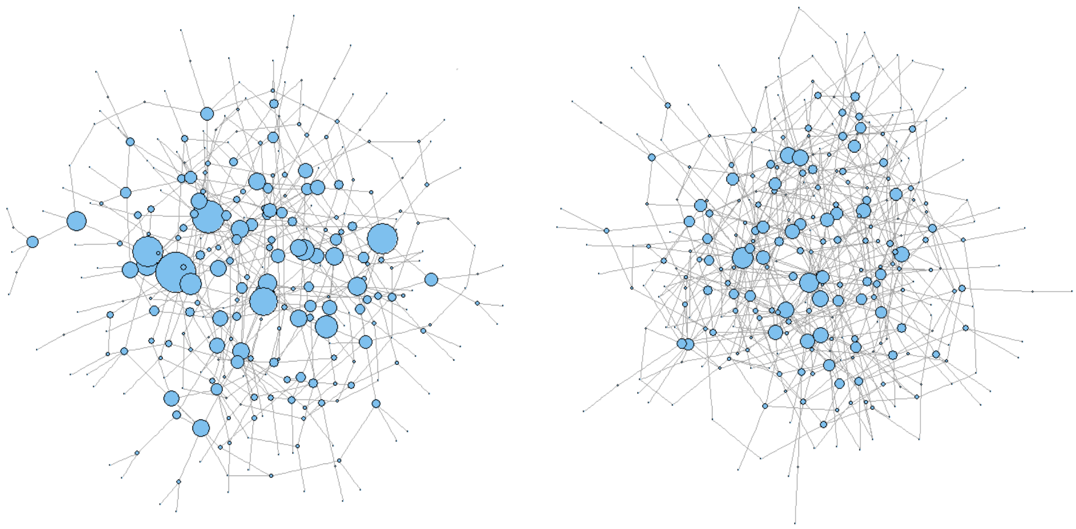
3.5 Interdependent network scenarios: topological properties of transportation networks

In this research, transportation networks to be interconnected are modeled as graphs to catch the main topological properties of the networks, and interlinks are modeled through interdependency matrices to represent the interdependencies between the nodes. In Table 3.3 the interdependent network scenarios to be studied are presented. As can be seen, the scenarios considered to analyze the impact of the proposed interlink patterns on the robustness of interdependent networks are 1) the interconnection of two backbone telecommunication modeled as an ER-ER interdependent network, and 2) an ER telecommunication network connected to a power grid. In this section, the topological properties of networks considered as study cases are described.

3.5.1 Scenario 1: The interconnection of networks with similar topological properties

As the first scenario, two backbone telecommunication networks with similar topological properties are interconnected. The random connection property of a backbone telecommunication network is modeled using an Erdős-Rényi (ER) random graph with a Poisson nodal degree distribution. This indicates that most nodes have approximately the same number of links close to the average nodal degree [46]. Although Scale-Free (SF) or other graph models can also be used to model telecommunication networks, these are more associated with large networks (such as multi-autonomous systems networks). Moreover, some current backbone topologies are also scaling to other models which are out of the scope of this work.

The ER-ER topology is the interconnection of two single network topologies generated from an *ER* graph model with the same number of nodes ($N_1 = N_2 = 500$), a different number of links $L_1 = 978$ and $L_2 = 677$. In order to interconnect the nodes between the two telecommunication networks, interlink patterns are based on the vulnerability of nodes in the most dangerous attack for these networks. Hence, for the high centrality (B_{HC}) and low centrality (B_{LC}) interdependency matrices, the



(a) ER_1 **(b)** ER_2

Figure 3.5: Graph representation for the backbone telecommunication networks (ER_1 and ER_2) of Scenario 2

interconnection is carried out with the centrality metric used to rank the nodes in that targeted attack. Whereas in a random interdependency matrix (B_{RA}), the nodes between the networks are interconnected randomly.

Table 3.4 presents the main topological properties of the two telecommunication networks: number of nodes (N), number of links (L), average nodal degree ($\langle k \rangle$), maximum nodal degree (k_{max}), average shortest path length ($\langle l \rangle$), diameter (D) and assortativity coefficient (r). As can be observed, both networks exhibit assortative values close to zero (0.021 for G_1 and 0.031 for G_2) and have low values of $\langle k \rangle$ (3.91 for G_1 and 2.71 for G_2) and high values of $\langle l \rangle$ (4.73 for G_1 and 6.78 for G_2) and D (10 for G_1 and 19 for G_2).

3.5.2 Scenario 2: The interconnection of networks with different topological properties

As the second scenario, the case of a power grid interconnected to a telecommunication network is considered. The power grid will be interconnected to two ER telecommunication networks, each with different susceptibilities to targeted attacks. Figure 3.5 shows the topologies of the backbone telecommunication networks ER_1 and ER_2 such that the larger the nodes, the higher their betweenness centrality values. Note that ER_2 has more nodes with similar betweenness centrality values than does G_1. Hence, for targeted attacks based on betweenness centrality, G_2 is able to maintain network connections for larger numbers of removed nodes than ER_1.

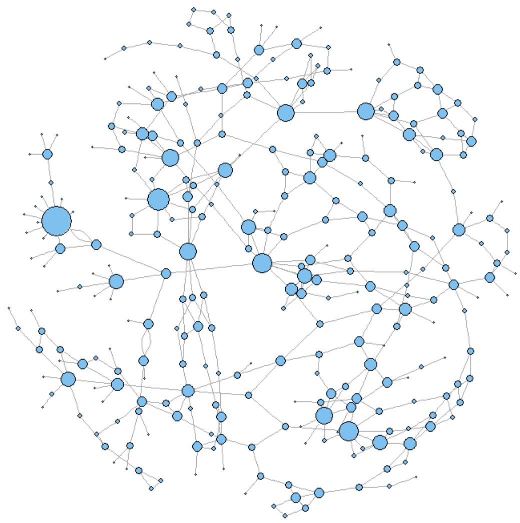


Figure 3.6: Graph representation of the IEEE_300 power grid of Scenario 2

The power grid can be modeled as a Small-World (SW) graph. A Small-World graph is a regular graph with increased randomness; thus, it exhibits the high clustering property of a regular graph and the short characteristic path length of a random graph [49]. However, in order to capture the topological properties of a power grid, the IEEE_300 real network [143] used by several researchers (see, e.g., [144]) was selected. Figure 3.6 shows the topology of the IEEE_300 power grid, where the larger nodes have higher degree centrality values.

For simplicity, the ER_1 and ER_2 backbone telecommunication networks and the IEEE_300 power grid have the same number of nodes $N = 300$, but different numbers of links (L) 437, 549 and 411, respectively. As shown in Table 3.5, the ER_1 and ER_2 networks have assortative values (r) close to zero, 0.0134 and 0.0093, respectively; and the IEEE_300 has a disassortative value (-0.2137). The three networks have low values of $\langle k \rangle$ (2.91 for ER_1, 3.66 for ER_2 and 2.74 for IEEE_300) and high values of $\langle l \rangle$ (5.57 for ER_1, 4.57 for ER_2 and 9.94 for IEEE_300) and diameter D (12 for ER_1, 10 for ER_2 and 24 for IEEE_300).

Because telecommunication networks and power grids are more vulnerable to different types of attacks, the nodes in each network should be weighted using different centrality metrics. Therefore, the high centrality (B_{HC}) and low centrality (B_{LC}) interdependency matrices interconnect the two types of networks with a one-to-one correspondence between the nodes of the networks according to the centrality metric used to rank the nodes in each targeted attack. Whereas in a random interdependency matrix (B_{RA}), the nodes between the networks are interconnected randomly.

Table 3.5: Topological properties of networks in Scenario 2

Network	N_i	L_i	$\langle k \rangle$	k_{max}	$\langle l \rangle$	D	r
ER_1	300	437	2.91	9	5.57	12	0.0134
ER_2	300	549	3.66	8	4.57	10	0.0093
IEEE_300	300	411	2.74	12	9.94	24	-0.2137

3.6 Impact of interlink patterns to mitigate targeted attacks in interdependent networks

In order to analyze the impact of the proposed interlink patterns to mitigate targeted attacks in interdependent networks, the robustness of each network is measured individually. Although several metrics have been proposed for assessing the network robustness (see Section 2.3), Average Two-Terminal Reliability ($ATTR$) [73] is selected as the network robustness metric. This metric has been used widely in previous work [4, 73, 145, 146] because it provides a good approximation and sensitivity to quantifying network connectivity under failure scenarios. Furthermore, $ATTR$ can be used to compare network robustness under various failure scenarios, so it supports analyses of the effects of the three interlink patterns with regards to the propagation of targeted attacks in the interdependent critical infrastructures. The $ATTR$ metric is calculated from equation 2.14 [73].

In the failure scenarios considered in this section, the percentage P of nodes removed ranged from 1% to 70%. Ten runs were conducted and, based on whether the targeted attacks were simultaneous or sequential, different subsets of nodes were selected for removal. The next section analyzes the robustness of the networks presented in Table 3.4 and Table 3.5 in the single network scenario. Thus, the most dangerous targeted attack for each network is detected. Following this, the three interdependency matrices (B_{HC}, B_{LC} and B_{RA}) are analyzed in terms of their ability to mitigate targeted attacks in the interdependent networks resulting from Scenario 1 and Scenario 2.

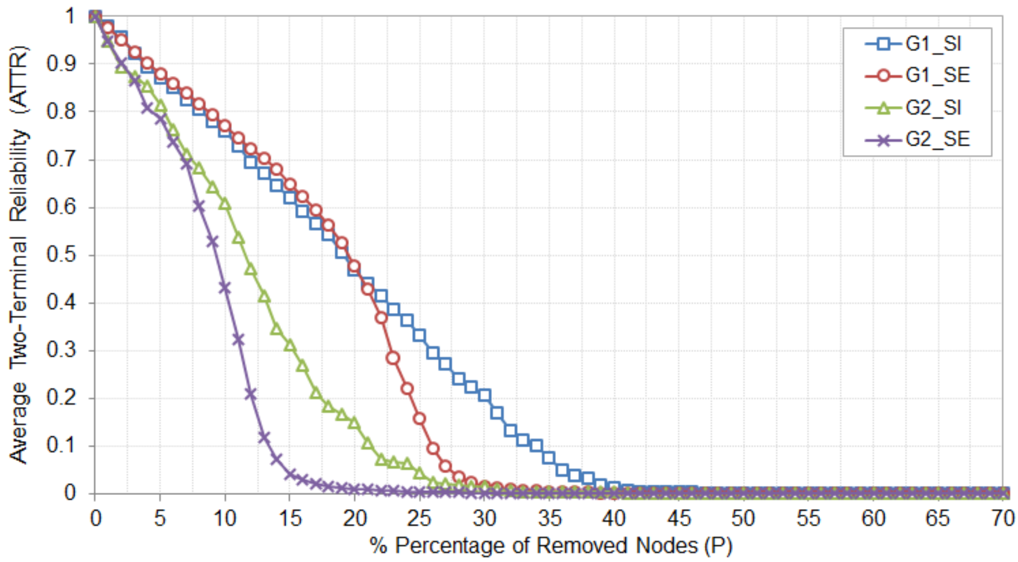
3.6.1 Robustness analysis in the single network scenario

The critical parts of an isolated transportation network are identified by considering a robustness analysis under a certain type of failure. In backbone telecommunication networks the most vulnerable routers can be identified by the number of shortest paths passing through a given router. Generally, this behavior is characterized by measuring the betweenness centrality (b_c) in each node. Therefore, the nodes to be attacked first are ranked according to their b_c values. For the two telecommunication networks in Table 3.4, a robustness comparison under targeted attacks is presented in Fig. 3.7(a). The $G1\_SE$ and $G2\_SE$ curves present the results of $ATTR$ measurements for G_1 and G_2 networks, respectively, under the sequential targeted attack based on b_c, while the $G1\_SI$ and $G2\_SI$ curves present the results of $ATTR$ measures for G_1 and G_2, respectively, under simultaneous targeted attacks by b_c.

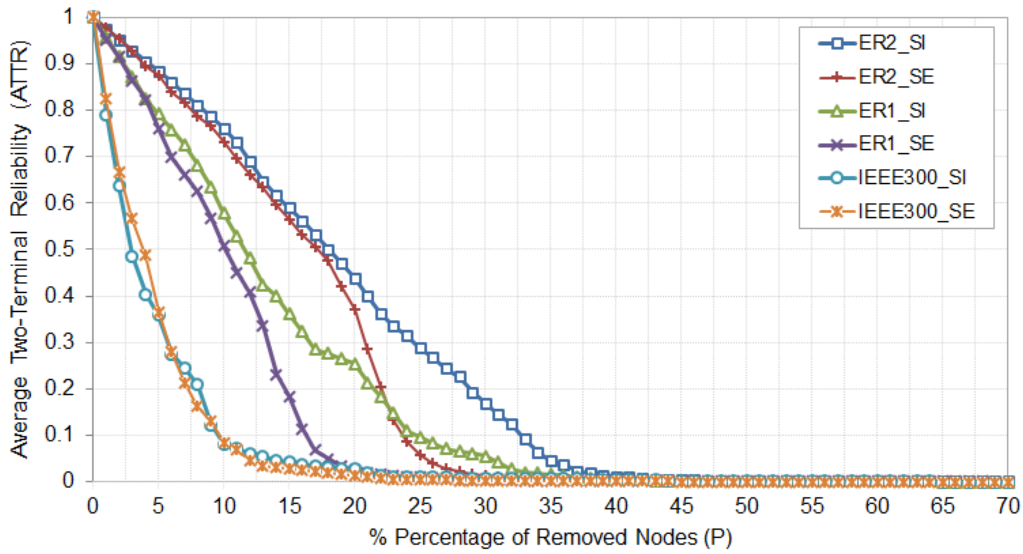
As can be seen in Fig. 3.7(a), G_2 is more vulnerable to a sequential targeted attack by b_c than G_1. This result is due to G_2 having a smaller $\langle k \rangle$ and higher values of $\langle l \rangle$ and D than G_1 does, as can be seen in Table 3.4. So, in the range of 1% and 5% of P, the network connections in G_2 are reduced to 80%, whereas the network connections in G_1 are reduced to 90%. For $P > 5\%$, the network connections in G_2 decrease dramatically until it is completely disconnected when P reaches 20%. In contrast, the network connections in G_1 are close to 0% when P is approximately equal to 30%. Furthermore, Fig. 3.7(a) shows that G_1 and G_2 are highly vulnerable under sequential targeted attacks by b_c than under simultaneous targeted attacks by b_c.

Regarding to the robustness comparison of networks presented in Table 3.5, Fig. 3.7(b) shows the $ATTR$ measures in a single network scenario for the ER_1 and ER_2 telecommunication networks and the IEEE_300 power grid under targeted attacks. The graphs show that ER_1 is more vulnerable to a targeted attack than ER_2; this is because ER_1 has lower $\langle k \rangle$ and higher $\langle l \rangle$ and D values than ER_2. Moreover, both telecommunication networks are more vulnerable to sequential targeted attacks based on betweenness centrality (curves ER1_SE and ER2_SE in Fig. 3.7(b)) than to simultaneous targeted attacks based on betweenness centrality (curves ER1_SI and ER2_SI in Fig. 3.7(b)); this is because the assortative values are close to zero. The high vulnerability of Erdős-Rényi random networks to sequential targeted attacks based on betweenness centrality is reported in [54].

In analyzing the robustness of the ER_1 and ER_2 telecommunication networks, the two attacks produce similar damage for specific percentage ranges of nodes removed (P). For ER_1, this range is between 1% and 5%, where the network connections are reduced to 76%; in the case of ER_2, the range is between 1% and 18%, where the network connections are reduced to 47%. For the remaining P values, the robustness behaviors of ER_1 and ER_2 differ for the two attacks. Thus, under a sequential targeted attack based on betweenness centrality, the network connections of ER_1 (curve ER1_SE in Fig. 3.7(b)) and ER_2 (curve ER2_SE in Fig. 3.7(b)) are close to 0% when the P values are approximately equal to 20% and 25%, respectively. In contrast, under a simultaneous targeted attack based on betweenness centrality, the network connections of ER_1 (curve ER1_SI in Fig. 3.7(b)) and ER_2 (curve ER2_SI in Fig. 3.7(b)) are close to 0% when the P



(a) Robustness of telecommunication networks (G_1 and G_2) under targeted attacks



(b) Robustnes of telecommunication networks (ER_1 and ER_2) and power grid ($IEEE\_300$) under targeted attacks

Figure 3.7: Robustness analysis of isolated networks under targeted attacks

reaches 30% and 37%, respectively.

Regarding to the IEEE_300 power grid, it is more vulnerable to targeted attacks than the ER_1 and ER_2 networks, which is expected because of the Small-World characteristics of the IEEE_300 network. As can be seen in Fig. 3.7(b), the robustness of the IEEE_300 power grid is similar for simultaneous and sequential targeted attacks based on degree centrality (curves IEEE300_SI and IEEE300_SE). Specifically, for P ranging from 1% to 5%, the network connections in the IEEE_300 network dramatically decrease to 36% and the network is completely disconnected when P reaches 10%. However, the average for the $ATTR$ values of the IEEE_00 network against a sequential target attack is greater than the average for the $ATTR$ values against a simultaneous target attack. Thus, the IEEE_300 network is more vulnerable to simultaneous targeted attacks based on degree centrality (curve IEEE300_SI) than to sequential targeted attacks based on degree centrality (curve IEEE300_SE).

In summary, the robustness analysis addressed in this section reveals that the G_1, G_2, ER_1 and ER_2 telecommunication networks are more vulnerable to a sequential targeted attack based on betweenness centrality, while the IEEE_300 power grid is more vulnerable to a simultaneous targeted attack based on degree centrality. This is a significant result to generate the interdependent networks in both Scenarios 1 and 2 because in the case of the B_{HC} and B_{LC} interlink patterns the nodes will be interconnected according to the centrality metric used in the most dangerous targeted attack in each network, i.e., nodes in the telecommunication networks are ranked by betweenness centrality, while nodes in the power grid are ranked by degree centrality. In the case of the random interdependency matrix B_{RA}, however, the nodes of two networks will be interconnected randomly without considering any centrality metrics.

3.6.2 Mitigation of targeted attacks on interdependent networks with similar topological properties

In the interdependent network of Scenario 1, dependent nodes in the G_1 telecommunication network are only removed as a result of nodal failures in the G_2 telecommunication network, and vice versa. In this scenario, the nodes to be removed are weighted by their betweenness centrality (b_c) values because the G_1 and G_2 telecommunication networks are highly vulnerable to sequential targeted attacks based on b_c (see Section 3.6.1). A sequential targeted attack may be used to describe certain types of failure scenarios in telecommunication networks e.g., the most vulnerable routers of a backbone network can be identified in order to protect the network's function. When a router fails, its functioning can be distributed to any one router in the network. Then, the failure of one router will affect the importance of the remaining ones. So, the sequential targeted attack is appropriate to model the network vulnerability.

In order to measure the robustness of the resulting ER-ER interdependent telecommunication network under this failure model, for each interdependency matrix, the G_2 network is initially attacked via a sequential targeted attack based on nodal b_c. Following this, the robustness of G_1 network is measured via $ATTR$. Next, the G_1 network is assaulted with a sequential targeted attack based on b_c and the robustness of the G_2 network is measured by using the $ATTR$ metric.

In Fig. 3.8, the robustness of G_1 when a sequential targeted attack by b_c occurs

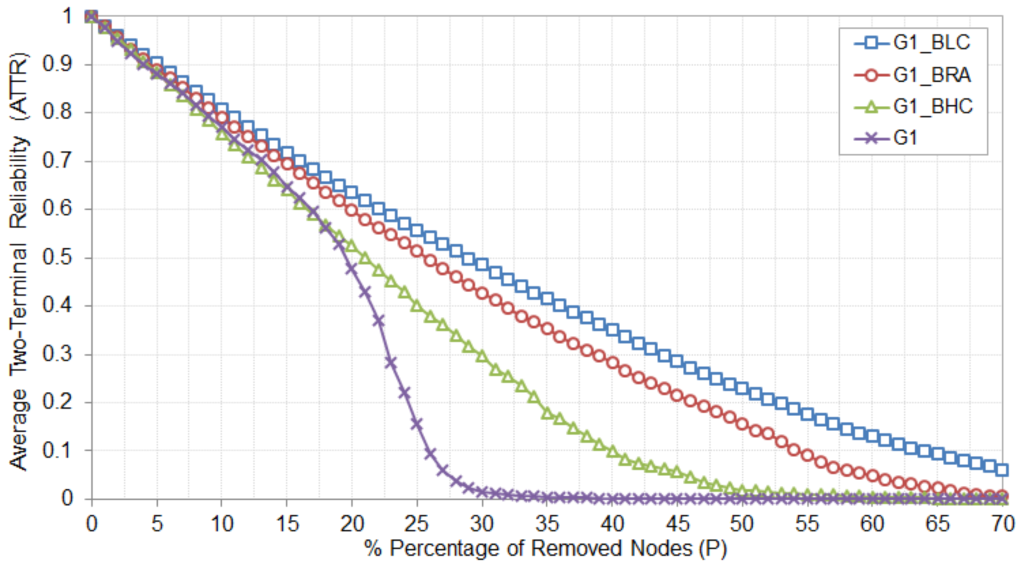


Figure 3.8: Robustness of G_1 network when a sequential targeted attack based on betweenness centrality occurs in the G_2 network

in G_2 is shown. For the three interdependency matrices, when P is between 1% and 10%, the robustness of G_1 has a similar degradation level as in the case of the single network scenario (compare the G1 curve with the other curves in Fig. 3.8). In this range, there is a reduction of up to 22% of connections. This degradation behavior is only maintained by the high centrality dependency matrix (B_{HC}) until P is equal to 18% (see G1_HC curve in Fig. 3.8). Furthermore, when P is larger than 11%, the B_{HC} matrix has a greater impact on G_1 robustness than do the low centrality (B_{LC}) and random (B_{RA}) interdependency matrices. However, the impact of the B_{LC} and B_{RA} matrices on the robustness of G_1 is similar for the rest of the P values (see G1_LC and G1_RA curves in Fig. 3.8, respectively). Therefore, a robustness analysis beyond 20% of P is not relevant as the network is close to being completely disconnected. As expected with the B_{LC} matrix, the nodes with the lowest b_c values in G_1 are the first to be removed when a sequential targeted attack occurs in G_2. Thus, the lowest impact in the robustness of G_1 is produced by the B_{LC} matrix. In the case of the B_{RA} matrix, a sequential targeted attack in G_2 produces a random failure in G_1 and generates an intermediate impact on its robustness.

The robustness of G_2 when a sequential targeted attack by b_c occurs in G_1 is shown in Fig. 3.9. As it can be seen, when P is between 1% and 7%, the B_{HC} matrix only achieves a similar level of degradation in G_2 to the case of the single network scenario (compare G2_SE and G2_HC curves in Fig. 3.9). In this range, up to 30% of the connections in G_2 are reduced. Therefore, for low P values in the ER-ER topology, the least vulnerable network to a sequential targeted attack by b_c exhibits a similar robustness

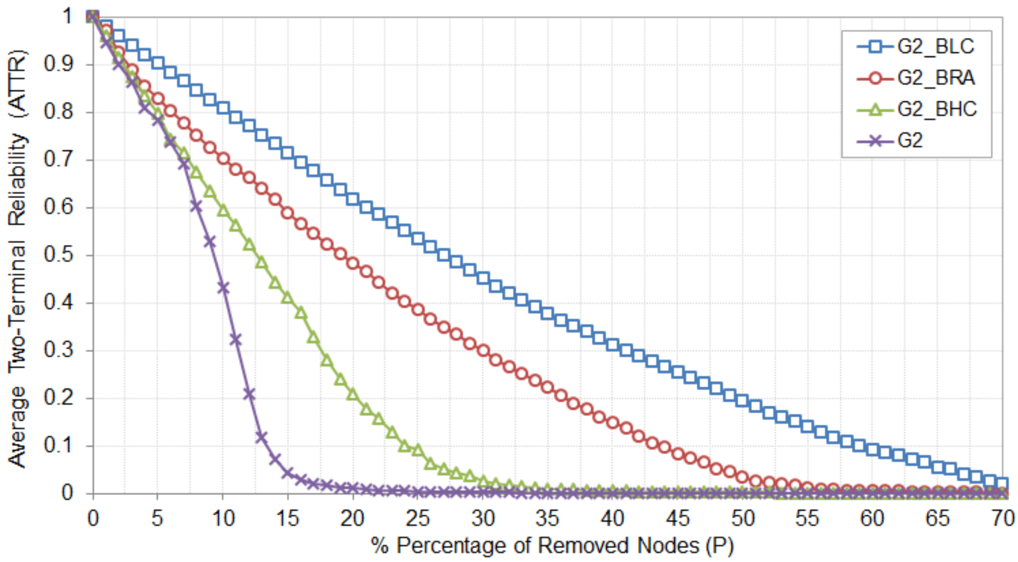


Figure 3.9: Robustness of the G_2 network when a sequential targeted attack based on betweenness centrality occurs in the G_1 network

behavior for the three interdependency matrices as the single network scenario does, whereas, the most vulnerable network does the opposite. Additionally, when P increases, the impact of the matrix B_{HC} (see G2_HC curve in Fig. 3.9) on G_2's robustness is worse than that of the B_{LC} and B_{RA} interdependency matrices (see G2_LC and G2_RA curves in Fig. 3.9, respectively). This is because the critical parts of two networks are interconnected. Consequently, in order to reduce the impact of sequential targeted attacks by b_c, it is recommended that two telecommunication networks are connected by using a low centrality B_{LC} link pattern model. Thus, the most critical parts of one network are interconnected to the least critical parts of the other network.

Moreover, in the failure scenario considered in this chapter and when networks G_1 and G_2 are connected by the B_{HC} matrix, the impact of a sequential targeted attack by b_c in G_2 can be approximated to a simultaneous targeted attack by b_c in G_1 (compare G1_SI in Fig. 3.7(a) and G1_HC in Fig. 3.8). This interesting result is because with the B_{HC} matrix the highest b_c nodes in G_1 are removed first when the attack occurs in G_2. An analogous result can be found for the robustness of G_2 when a sequential targeted attack by b_c occurs in G_1 (compare G2_SI in Fig. 3.7(a) and G2_HC in Fig. 3.9).

3.6.3 Mitigation of targeted attacks on interdependent networks with different topological properties

A simple functional model is used to express the failure dependencies between a power grid and backbone telecommunication networks. The power grid incorporates generators and substations that are connected to power lines. Similarly, the backbone telecommunication network incorporates routers connected by communications links. Each router receives power from a substation and every substation sends data and receives control signals to/from one router [20]. In this model, a substation continues to operate if it is connected to a router and a router continues to operate if it is connected to a substation. Thus, an attack on a power grid node causes the failure of a dependent node in the telecommunication network, and vice versa.

In the interdependent networks considered in Scenario 2, dependent nodes in the ER_1 or ER_2 telecommunication networks are only removed as a result of nodal failures in the IEEE_300 network, and vice versa. According to the results presented in Section 3.6.1, the ER_1 and ER_2 telecommunication networks are highly vulnerable to sequential targeted attacks by betweenness (b_c). Therefore, the telecommunication nodes to be removed are ranked by their betweenness centrality values. In a real scenario, the betweenness metric could represent the number of shortest paths passing through a router.

In the case of a power grid, the nodes to be removed are ranked by their degree centrality (d_c) values. This is because power grid functionality depends on nodes with high degree centrality (i.e., generators and substations). Based on the results presented in Section 3.6.1, a simultaneous targeted attack on the power grid based on degree centrality is considered to eliminate the nodes from the IEEE 300 power grid. In power grids an element failure may trigger cascading failures across the network and lead to a large blackout [6, 108]. Power outages are consequences of perturbations that overload the entire system by spreading flows across the network [108, 147, 148]. However, in this work it is assumed that the electrical properties of the power grid elements are extended. Therefore, when a node in the IEEE_300 grid is attacked, the load is distributed to other nodes without leading to cascading failures. Although this failure model in power grids is not completely realistic, it captures the essential properties required in order to study the effect of interdependency matrices for mitigating a targeted attack into interdependent critical infrastructures. This section analyzes the robustness of two interdependent networks (ER_1-IEEE_300 and ER_2-IEEE_300) under targeted attacks.

3.6.3.1 The case of the ER_1 telecommunication network and the IEEE_300 power grid

Figure 3.10 shows the robustness of the ER_1 backbone telecommunication network when a simultaneous targeted attack based on degree centrality is launched against the IEEE_300 power grid. When the ER_1 and IEEE_300 networks are interconnected by a high centrality interdependency matrix B_{HC}, a simultaneous targeted attack based on degree centrality on the IEEE_300 network causes exactly the same damage to the ER_1 network as a simultaneous targeted attack based on betweenness centrality does to the

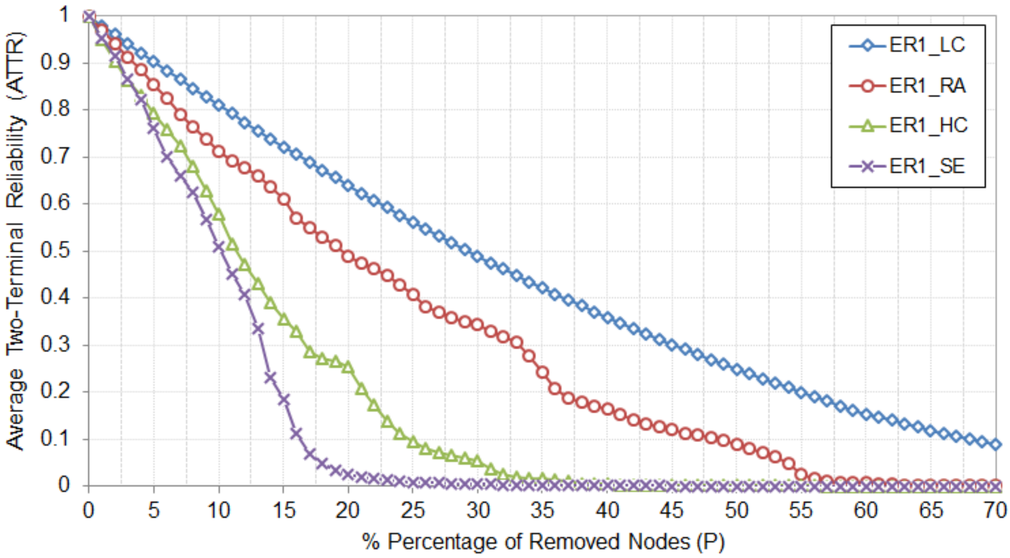


Figure 3.10: Robustness of the ER_1 network when a simultaneous targeted attack based on degree centrality occurs in the IEEE_300 network

ER_1 in the single network scenario. This is because in the case of the B_{HC} matrix, nodes in ER_1 with the highest betweenness centrality values are removed first when an attack is launched against the IEEE_300 power grid. This interesting result can be seen by comparing curves ER1_SI in Fig. 3.7(b) and ER1_HC in Fig. 3.10. Additionally, the greatest impact on ER_1 network robustness occurs when the networks are interconnected by a link model based on the B_{HC} interdependency matrix (curve ER1_HC in Fig. 3.10).

For the low centrality (B_{LC}) and random (B_{RA}) interdependency matrices, the ER_1 network is more robust to a simultaneous targeted attack based on degree centrality on the IEEE_300 power grid. As expected, in the case of the B_{LC} matrix, nodes in ER_1 with the lowest betweenness centrality values are the first to be removed when the IEEE_300 is attacked, generating the lowest impact on the robustness of ER_1 (curve ER1_LC in Fig. 3.10). In the case of the B_{RA} matrix, a simultaneous targeted attack based on degree centrality on the IEEE_300 power grid produces a random failure in the ER_1 network (curve ER1_RA in Fig. 3.10) and generates an intermediate impact on its robustness. In the case of the B_{LC} and BRA matrices, when the percentages of nodes removed (P) are between 1% and 10%, network connections are reduced by 20% and 30%, respectively. In the case of the B_{RA} matrix, network connections in ER_1 reach 0% when P is approximately 57%, whereas for the B_{LC} matrix P may be greater than 70% to reach 0% network connections.

The robustness of the IEEE_300 power grid when a sequential targeted attack based on betweenness centrality is launched against the ER_1 backbone telecommunication network is presented in Fig. 3.11. When P is between 1% and 7%, the robustness in

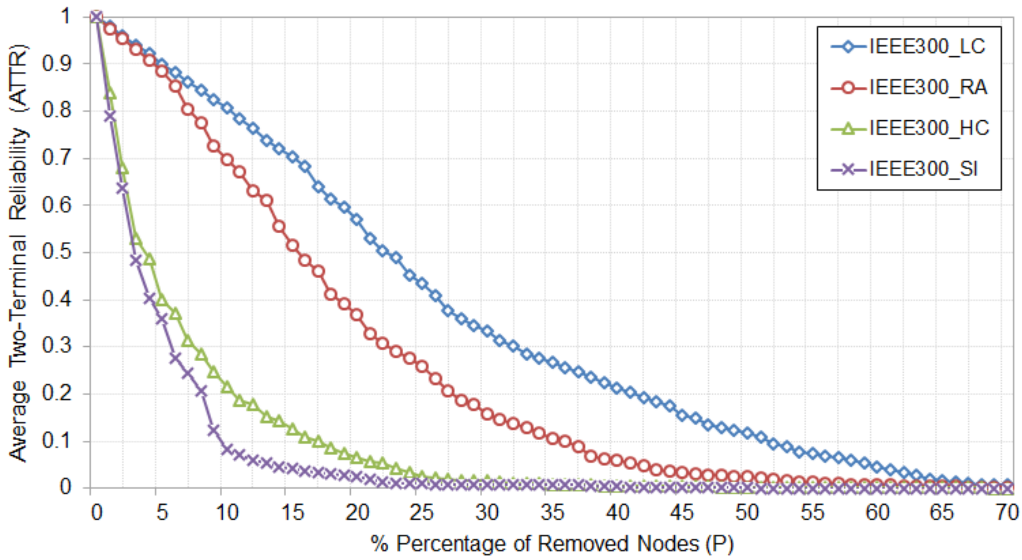


Figure 3.11: Robustness of the IEEE_300 network when a sequential targeted attack based on betweeness centrality occurs in the ER_1 network

the case of the B_{HC} matrix (curve IEEE300_HC in Fig. 3.11) is approximated by the degradation level produced by a simultaneous targeted attack based on degree centrality on the IEEE_300 power grid (curve IEEE300_SI in Fig. 3.7(b)). For this range of P values, there is a 65% reduction of network connections in the IEEE_300 power grid. When P is increased, the B_{HC} matrix (curve IEEE300_HC in Fig. 3.11) produces worse IEEE_300 network robustness compared with the B_{LC} and B_{RA} matrices (see curves IEEE300_LC and IEEE300_RA in Fig. 3.11, respectively).

In the case of the B_{HC} matrix, the IEEE_300 network connections dramatically decrease until they reach 0% when P is about 30% (curve IEEE300_HC in Fig. 3.11). In the case of the B_{LC} and B_{RA} matrices, the network connections reach 0% when the P values are about 55% and 65%, respectively (curves IEEE300_LC and IEEE300_RA in Fig. 3.11, respectively). In the case of the B_{RA} matrix, a sequential targeted attack based on betweenness centrality on the ER_1 network causes a random failure in the IEEE_300 power grid and generates an intermediate impact on its robustness (curve IEEE300_RA in Fig. 3.11) compared with the B_{HC} and B_{LC} interdependency matrices. Consequently, in order to mitigate the impacts of the targeted attacks considered in this scenario, it is recommended that an Erdős-Rényi backbone telecommunication network and a power grid should be connected using an interdependency matrix based on the B_{LC} link pattern model.

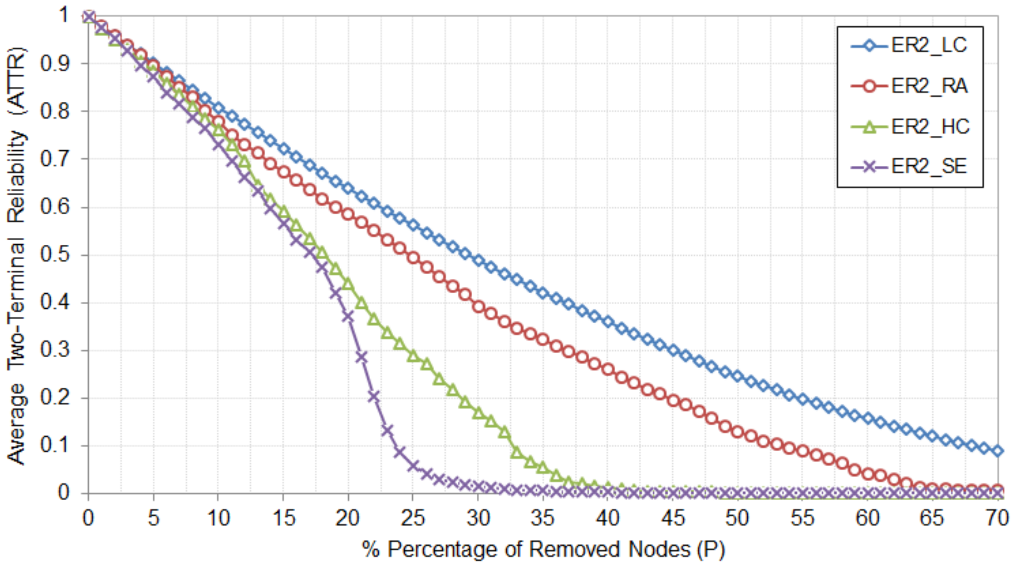


Figure 3.12: Robustness of the ER_2 network when a simultaneous targeted attack based on degree centrality occurs in the IEEE_300 network

3.6.3.2 The case of the ER_2 telecommunication network and IEEE_300 power grid

The robustness of the ER_2 backbone telecommunication network when a simultaneous targeted attack based on degree centrality is launched against the IEEE_300 power grid is shown in Fig. 3.12. In fact, the results are similar to those obtained for the ER_1 network. The greatest impact on ER_2 network robustness is seen with the B_{HC} interdependency matrix (curve ER2_HC in Fig. 3.12) while intermediate impact is seen with the B_{RA} interdependency matrix (curve ER2_RA in Fig. 3.12) and the least impact is seen with the B_{LC} interdependency matrix (curve ER2_LC in Fig. 3.12).

However, in this interdependency scenario and for the failure model considered in this chapter, the ER_2 network is more robust than the ER_1 for increasing values of P. In the range 1% to 7%, the robustness behavior produced by the three matrices is similar for ER_2 with a reduction to 20% network connections. ER_2 network connections reach 0% when P is 40% for B_{HC} and 67% for B_{RA} (curves ER2_HC and ER2_RA in Fig. 3.12, respectively), whereas for B_{LC}, P may be greater than 70% (curve ER2_LC in Fig. 3.12). Again, when the ER_2 and IEEE_300 networks are interconnected by a B_{HC} matrix, a simultaneous targeted attack based on degree centrality on the IEEE_300 power grid causes exactly the same damage to the ER_2 network as a simultaneous targeted attack based on betweenness centrality on the ER_2 in the single network scenario (curves ER2_SI in Fig. 3.7(b) and ER2_HC in Fig. 3.12).

Figure 3.13 shows the robustness of the IEEE_300 power grid when a sequential targeted attack based on betweenness centrality is launched against the ER_2 backbone telecommunication network (which is more robust than the ER_1 network). Comparison

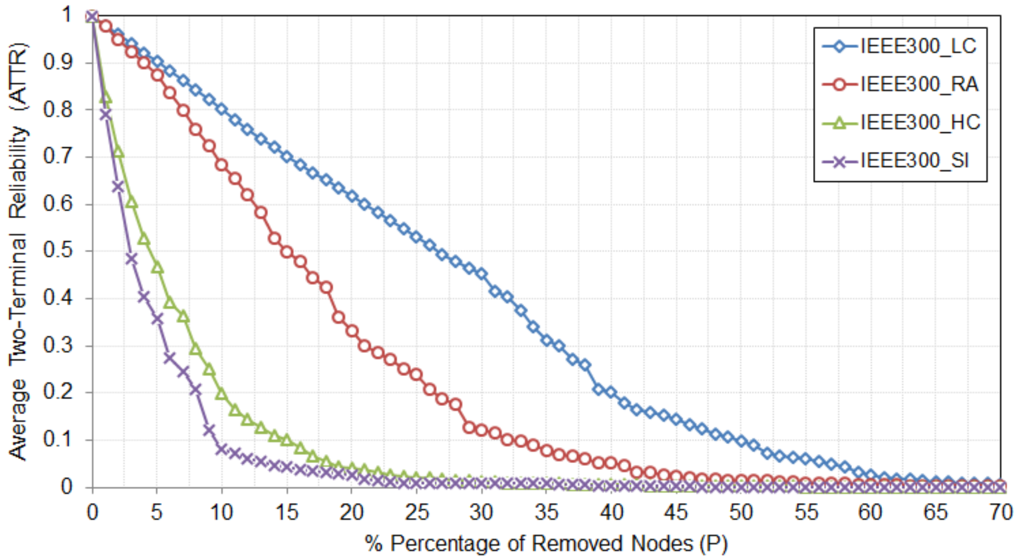


Figure 3.13: Robustness of the IEEE_300 network when a sequential targeted attack based on betweeness centrality occurs in the ER_2 network

of Figs. 3.11 and 3.13 shows a slight improvement in IEEE_300 network robustness when it is interconnected with the ER_2 by the B_{HC} and B_{LC} interdependency matrices. For example, when P is in the range 1% to 5% for the IEEE_300 power grid connected to ER_2 by the B_{HC} matrix (curve IEEE300_HC in Fig. 3.13), the IEEE_300 network connections decrease to 47%; on the other hand, when the IEEE_300 power grid is connected to the ER_1, its network connections dramatically decrease to 35% (curve IEEE300_HC in Fig. 3.11). For P equal to 15%, when the IEEE_300 power grid is connected to ER_2 by the B_{LC} matrix, the network connections are 71% (curve IEEE300_LC in Fig. 3.13), whereas when it is connected to the ER_1, the network connections are 70% (curve IEEE300_LC in Fig. 3.11).

3.7 Discussion and lessons learned

Table 3.6 summarizes the effects of the three interdependency matrices in mitigating targeted attacks on the interdependent networks. The table shows that each matrix produces a different impact in terms of propagating targeted attacks on the interconnected networks. This is because the three interdependency matrices considered as study cases provide different link patterns for interconnecting interdependent networks based on the centrality metrics used to rank nodes in the networks (b_c: betweenness centrality, d_c: degree centrality and random). However, it is important to remember that different metrics can be used to rank the most vulnerable nodes in a network.

Table 3.6: Effects of the B_{HC}, B_{LC} and B_{RA} interdependency matrices to propagate targeted attacks and impact on network robustness

Type of Interdependent Network	Type of Attack on First Network	Interdependency Matrix (Centrality Metrics)	Resulting Attack on Second Network	Impact on Network Robustness
ER-ER	Sequential by b_c	B_{LC} (b_c,b_c)	-	Lowest
ER-ER	Sequential by b_c	B_{RA} (b_c,b_c)	Random failure	Intermediate
ER-Power Grid	Sequential by b_c	B_{HC} (b_c,d_c)	Approximately equal to simultaneous by d_c	Highest
ER-Power Grid	Sequential by b_c	B_{LC} (b_c,d_c)	-	Lowest
ER-Power Grid	Sequential by b_c	B_{RA} (b_c,d_c)	Random failure	Intermediate
Power Grid-ER	Simultaneous by d_c	B_{HC} (d_c,b_c)	Exactly equal to simultaneous by b_c	Highest
Power Grid-ER	Simultaneous by d_c	B_{LC} (d_c,b_c)	-	Lowest
Power Grid-ER	Simultaneous by d_c	B_{RA} (d_c,b_c)	Random failure	Intermediate

The numerical results presented in the previous section can be used to identify the interdependency matrices that best mitigate targeted attacks on the Scenario 1 and 2 networks. Specifically, the low centrality interdependency matrix (B_{LC}) reduces the impact on a certain type of network when a targeted attack is launched against the other, and vice versa. This is because when a targeted attack occurs in one network the nodes that are less important are the first to be removed in the other network and the lowest impact on network robustness is achieved. However, the high centrality interdependency matrix (B_{HC}) produces the greatest impact on the robustness of each network. This is because the most important nodes are the first to be removed in both networks. For the random interdependency matrix (B_{RA}), a targeted attack on a network produces a random failure in the other network with an intermediate impact on network robustness.

With regard to the propagation of targeted attacks between the two networks, an interesting result is that in the case of a link model based on the high centrality interdependency matrix B_{HC}, a simultaneous targeted attack based on degree centrality on the power grid causes exactly the same damage to the Erdős-Rényi telecommunication networks as does a simultaneous targeted attack based on betweenness centrality in a single network scenario. This is due to for the B_{HC} matrix the nodes with the highest betweenness centrality in an Erdős-Rényi telecommunication network are the first to be removed when a simultaneous attack based on degree centrality occurs on the power grid. In contrast, when two networks with similar topological characteristics are connected by a B_{HC} matrix, the impact of a sequential targeted attack based on betweenness centrality in one of the networks generates an impact that approximates to that of a simultaneous targeted attack based on betweenness centrality on the other network.

This research also assesses the effects of interconnecting the power grid with different telecommunication networks, each with different susceptibilities to targeted attacks. The numerical results reveal that connecting a power grid via B_{HC} and B_{LC} interdependency matrices to a telecommunication network that is less vulnerable to targeted attacks yields a slight improvement in the robustness of the power grid. This is because in the interdependency scenario considered in this work (one-to-one nodal interconnections), a sequential targeted attack based on betweenness centrality on any of the telecommunication networks propagates to the same nodes in the power grid. Thus, approximately the same impact on network robustness is observed.

Chapter 4

Robustness measurements in multilayer networks: design of robust networks

Telecommunication networks are considered as multilayer transportation networks that can be modeled as the interconnection of single layers. Therefore, interdependent networks can help to study physical and logical layer interconnection in order to design more robust telecommunication networks. In this chapter, Software Defined Network (SDN) is considered as study case to provide a robust design and make that SDN architecture more resilient to attacks. The proposal is focused on identifying what the critical parts of physical topology are and finding the best controllers placement to mitigate the damage done by targeted attacks. Moreover, to show the efficacy of the proposed algorithm, SDN robustness is analyzed when a targeted attack occurs in the switches of a real telecommunication network and compared with previous proposals.

4.1 Introduction

The multilayer interconnection present in telecommunication networks is partly due to the fact that protocols interact at multiple levels and in part because of the ways in which players operate, provide and use the services of those networks [15, 121]. Robustness analysis in multilayer networks can be carried out at the bottom layer, the upper layer or both layers, depending on network designer's interest [149]. For instance, the robustness of the Internet can be examined at the physical, Multiprotocol Label Switching (MPLS), Internet Protocol (IP), Point of Presence (PoP) and Autonomous System (AS) levels from a topological point of view. In multilayer telecommunication networks, the interconnection between networks in each layer is carried out through logical or physical interlinks [15]. Hence, a failure in a physical network node (e.g., a fiber optical node or a switch) results in the failure of multiple upper-layer networks (Ethernet, IP, MPLS, etc.)

[142].

Given the high complexity and scale of telecommunication networks, multiple correlated failures can have catastrophic consequences on connectivity, which in turn can cause the collapse and disruption of the provided services [142]. Therefore, understanding the vulnerability of physical networks to failures is crucial to design multilayer networks that better resist failures [15]. In this chapter, we are interested in designing a more robust Software Defined Network (SDN) as a particular case of multilayer networks. An SDN architecture separates the network's control logic from the data forwarding devices (routers and switches), providing the network with a centralized control plane, the functions of which move from network devices to dedicated controller instances running on software [150]. However, the centralized control plane proposed by SDN poses a great challenge for network robustness because of the new vulnerable parts that are introduced [151].

In this chapter, a robust SDN control plane design in order to maintain the proper network operation in the presence of failures is proposed. Our proposal is focused on identifying what the critical parts of physical network are and finding the best placements for controllers to improve SDN robustness against targeted attacks. As shown in Chapter 2, when the topological structure of the networks is taken into account, the type of attack producing the greatest damage can be determined. In addition, network operators can detect the most vulnerable areas where failures frequently occur due to natural disasters (hurricanes, earthquakes, tsunami, tornados, floods or forest fires) or technology-related disasters (power grid blackouts, hardware failures, dam failures or nuclear accidents). Therefore, in the physical network, a subset of less vulnerable switches C has a high probability of being selected to place κ controllers. Moreover, we consider that the subset of switches to be managed by each controller c is determined by a maximum distance δ between switches and controllers.

In this work, the SDN architecture is modeled as an interdependent network, where each control plane node is directly connected to a given physical switch by a bidirectional link. Additionally, in-band controller-switch communication via single shortest path is assumed i.e., the control traffic from controllers to switches is delivered via the same physical links [152, 153]. Thus, one-to-one dependence relation between data and control plane nodes is performed. Due to this correspondence, a targeted attack in one physical switch can lead to cascading failure in SDN architectures. To show the efficacy of the proposed algorithm to design a control plane layer (G_{CS}), the robustness of three SDN architectures is analyzed when a targeted attack takes place in the switches of a real telecommunication network.

The remainder of this chapter is structured as follows: Section 4.2 contains a review of previous work. A mathematical model for SDN interdependent networks and the failure process in SDN are defined in Section 4.3. In Section 4.4, a mechanism for the robust design of control planes in SDN architectures is proposed. The resulting SDN topology from a physical network and the impact analysis of a targeted attack on network robustness are provided in Section 4.5. Finally, discussion and lessons learned are presented in Section 4.6.

4.2 Review of controller placement problem for SDN architectures

Software Defined Network (SDN) is an emerging networking paradigm that breaks the vertical integration of current network infrastructures by separating the control plane from the data plane [150]. With this separation, the physical network elements (routers and switches) become simple data forwarding devices and SDN controllers take the centralized control logic [150]. For instance, the controllers can send the switch configuration to adapt to traffic demands and can take decisions to mitigate the failures in the physical network [154]. However, the SDN control plane cannot be fully physically centralized due to responsiveness, reliability, and scalability metrics [150]. Hence, distributed controllers can be used to control different subsets of switches in order to reduce the processing capacity of each controller and decrease the switch-to-controller latency [150].

An SDN architecture can be modeled as an interdependent network where the switch-switch network (G_{SS}) for data forwarding and the controller-switch network (G_{CS}) for network control, are interconnected by bidirectional interlinks [152]. In SDN, failures can take place in the physical network, where a switch or link fails, or in the domain of the controllers, where the controller fails. The interdependency introduced in SDN architectures and their sophisticated supported services make this type of network more vulnerable to failures. This growing reliance in telecommunication networks is translated into increased disruption consequence, and increased disruption consequences leads to networks becoming more attractive for target attacks [2]. One SDN node failure (switches or controllers) can lead to cascading failures due to the nodal mutual dependence [152]. Therefore, SDN robustness depends on the proper operation of these interdependent networks.

From the perspective of security and reliability, an SDN architecture exhibits new vulnerable parts in both the data plane and the control plane. For instance, the most vulnerable physical network elements can be identified by the number of shortest paths that pass through a given router or by the number of physical links from one switch to others. In SDN architectures, controllers introduce a centralized point of failure [151]. Controller failures are usually caused by software malfunctioning or cyber-attacks e.g., a Denial of Service (DoS) attack in one controller can generate the disconnection of the dependent subset of switches [155]. The consequences of this type of failure are dramatic as the SDN can even become disconnected. Therefore, designing fault-tolerant SDN architecture that is robust to targeted attacks poses several challenges as the controllers can be physically distributed along the network and connected to different switches.

One of the critical challenges in SDN is the control plane layer design where defining the best controller locations has several repercussions on robustness. The Controller Placement Problem (CPP) refers to how to select the best switches in the physical network for placing κ controllers to maximize an objective function such as inter-controller latency, switch-controller latency, links load, controllers load or resilience [152, 153]. Previous work has addressed CPP as a key issue to improve the performance and resilience of SDN. Performance improvement was studied in [156]. Heller et al. [156] decided on the number of controllers and their placements to minimize the latency from nodes to their assigned controller. Bari et al. [157] solved the Dynamic Controller Provisioning Problem (DCPP) to dynamically adapt the number of controllers and their placements with changing network conditions due to traffic patterns or bandwidth demands.

Regarding the Resilient Placement Controller Problem (RPCP), a greedy algorithm was used by Hu et al. [158] to provide placement decisions to maximize the reliability of SDN networks. In [152], the controller placement problem for improving the SDN resilience was analyzed by using interdependent network modeling and a new metric to measure the impact of cascading failures was proposed. RPCP in large scale SDN networks with respect to latencies constraints, resilience against node and link failures, and load balancing in the control plane was also studied under heuristic approaches by Lange et al. [153]. In [159], the minimum number of controllers for building a scalable, robust and balanced control layer was identified. The proposed k-Critical algorithm also satisfied a target communication between controller and switches such as delay, latency or convergence time [159].

Additionally, the Fault Tolerant Controller Placement (FTCP) problem was solved by Ros et al. [160]. This proposal considers the fact that in a given topology there is a set of facilities where controllers can be deployed, and it also requires that each node is effectively connected to at least one controller with high reliability. Thus, a reasonable number of controllers and their placements to achieve very high reliability in the SDN network are identified. Mattos et al. [161] proposed a distributed control architecture with optimized controller placement and assurance of network resilience. This controller architecture establishes control areas with distributed control. The global network view is achieved by applying a designated controller, which is an area controller that assumes the role of maintaining the consistency of the entire network [161].

In contrast to previous studies, a novel algorithm to improve robustness to targeted attacks in SDN networks with distributed controllers is proposed. Our approach is based on analyzing the critical parts of the physical network most vulnerable to targeted attacks in order to define the best placements for controllers. As constraints of the SDN control layer design (G_{CS}), our method requires three input parameters: 1) a switch-switch network (G_{SS}), 2) the number of controllers (κ) and 3) the maximum distance between controllers and switches (δ). The values for κ and δ are design parameters that could be defined from the particular requirements of the network operator. For instance, in large-scale networks the distance δ has practical implications for the control layer design in SDN, affecting availability and convergence time. The distance δ can also be defined by the geographical proximity between controllers and switches. However, we are not focused on finding optimal minimum-latency placements to reduce the delay in controllers-to-switches communication [156], but rather on presenting an initial analysis of G_{SS} network vulnerability to certain types of targeted attacks as a fundamental aspect to solve the resilient controller placement problem.

4.3 Modeling interdependency and failure processes in multilayer networks: The case of SDN architectures

In multilayer networks, each layer can be represented as a graph and the interaction between layers as interlink patterns. For the case of an SDN architecture, two layers - a physical layer and a logical layer - are interconnected through bidirectional interlinks and one-to-one nodal correspondence. Therefore, in this study an SDN architecture is constructed by the interconnection of switch (physical layer) and control (logical layer) topologies. Given the interdependency between switches and controllers the failure of a node in an SDN layer can have a devastating impact on topological connectivity, which in turn can cause cascading failures and the collapse of the whole network. Based on [152] and [29], a mathematical model of an interdependent SDN architecture and a failure model in SDN networks are defined in this section.

4.3.1 Interdependent model for SDN architectures

In an effort to further understand the structure of an SDN architecture, a network-based model for studying SDN networks is employed. Consider the switch-switch network as an undirected graph $G_{SS}(S,U)$, and the controller-switch network as an undirected

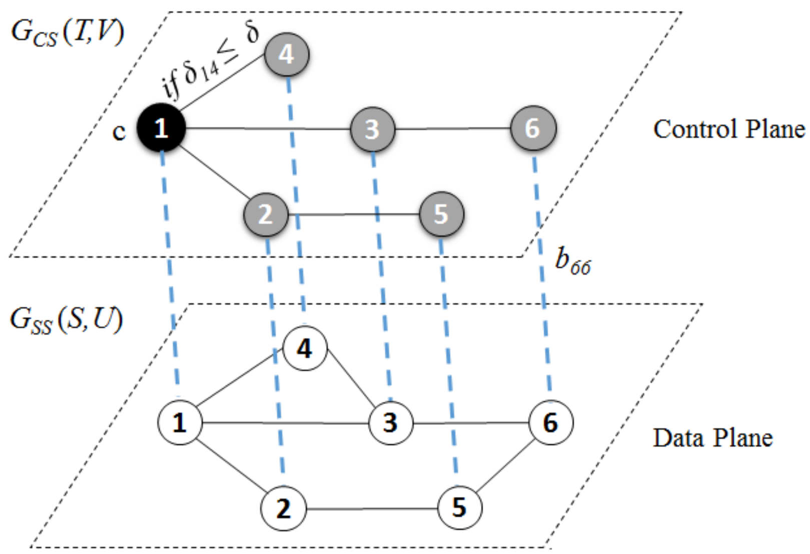


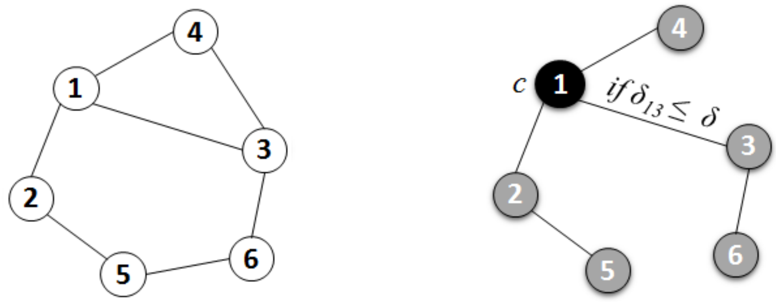
Figure 4.1: Interdependent network modeling of an SDN architecture

graph $G_{CS}(T,V)$, each with a set of nodes (S,T) and a set of links (U,V), respectively. The nodes in G_{SS} consist of the physical switches randomly connected by a set of U intralinks with degree distribution $P_{SS}(k)$. Analogously, the nodes in G_{CS} consist of the controllers and switches connected by a set of V intralinks with degree distribution $P_{CS}(k)$. Moreover, in-band controller-switch communication via single shortest path is assumed, and one-to-one correspondence between a node i in network G_{SS} and node j in network G_{CS} is considered. Thus, the interdependent SDN network resulting from the connection of these two networks is a graph G with $S \cup T$ nodes and $U \cup V$ intralinks, plus a set of bidirectional interlinks I joining the two networks Consequently, the SDN graph is defined as $G(N,L) = (S \cup T, U \cup V \cup I)$.

Let B_{12} be a $N_1 \times N_2$ interconnection matrix representing the interlinks between a node i in network G_{SS} and a node j in network G_{CS}. Because we consider bidirectional interlinks, it follows that $B_{21} = B_{12}^T$ [31]. Let b_{ij} denote as the (i,j) entry in the B_{12} matrix, where $b_{ij} = 1$ if the entry belongs to the main diagonal, and $b_{ij} = 0$ otherwise. The interdependency matrix (B) of the whole system G is given by the equation 3.2.

In the G_{CS} network, the switches are limited to a maximum distance δ_{cs} from their assigned controller c. Therefore, if the distance δ_{cs} between switches $i = \{1,2,\ldots,N_1\}$ and controller c is less than or equal to the maximum distance ($\delta_{cs} \leq \delta$), switches i belong to the subnetwork controlled by controller c. Distance δ can represent a design constraint such as delay propagation or latency, physical distance of links or the number of hops. Distance δ also has implications in the availability and convergence time of the SDN architecture. Figure 4.1 shows an SDN architecture modeled as an interdependent network.

As an illustrative example of an interdependent SDN network, Fig. 4.2(a) shows



(a) G_{SS} network

(b) G_{CS} network

Figure 4.2: Generating the G_{CS} network for an interdependent SDN network (a) in the G_{SS} network controller c is placed on switch 1 (b) in the G_{CS} network a switch i belongs to the subnetwork controlled by controller c if $\delta_{cs} \leq \delta$

a physical network (G_{SS}) as a random graph and Fig. 4.2(b) shows the controller-switch network (G_{CS}) as a shortest path routing tree for in-band controller-switch communication on G_{CS} [152]. In Fig. 4.2(a) nodes i are the physical switches, whereas in Fig. 4.2(b) switch 1 is controller c (placed on the switch 1) and the other nodes are the switches controlled by it.

4.3.2 Cascading failures in SDN architectures

Due to the fact that the SDN architecture could be modeled as an interdependent network, SDN robustness depends on the proper functioning of both G_{SS} and G_{CS} networks. When interconnecting the G_{SS} and G_{CS} networks by bidirectional interlinks, we consider that each node $i = \{1,2,\ldots,N_1\}$ in network G_{SS} depends on one, and only one, node $j = \{1,2,\ldots,N_2\}$ in G_{CS} to continue functioning, and vice versa. Furthermore, a subset of nodes in network G_{CS} depends on communication whit a particular controller $c \in \{1,2,\ldots,\kappa\}$ to maintain proper functioning.

In SDN architectures, a targeted attack in one physical switch could lead to cascading failure. When a node i in G_{SS} is attacked, the dependent node j in G_{CS} is removed. Therefore, if a subset of nodes in G_{CS} is disconnected from a controller c due to the failure of switch i, by mutual dependence the same subset of nodes in G_{SS} also fails. Similarly, if one controller c is attacked, the subset of dependent nodes in G_{CS} fails and this failure will spread to the same subset of nodes in G_{SS}.

In Fig. 4.3, each node in G_{SS} depends on one, and only one, node in G_{CS}, and vice versa. Bidirectional interlinks I are shown as dashed horizontal lines, and U and V intralinks are shown as undirected solid arcs. To illustrate the cascading failure model in SDN networks, Fig. 4.3(a) shows that node 3 is attacked in G_{SS}. Then, due to dependence, node 3 in G_{CS} fails (see Fig. 4.3(b)). As a consequence of the failure of node 3 in G_{CS},

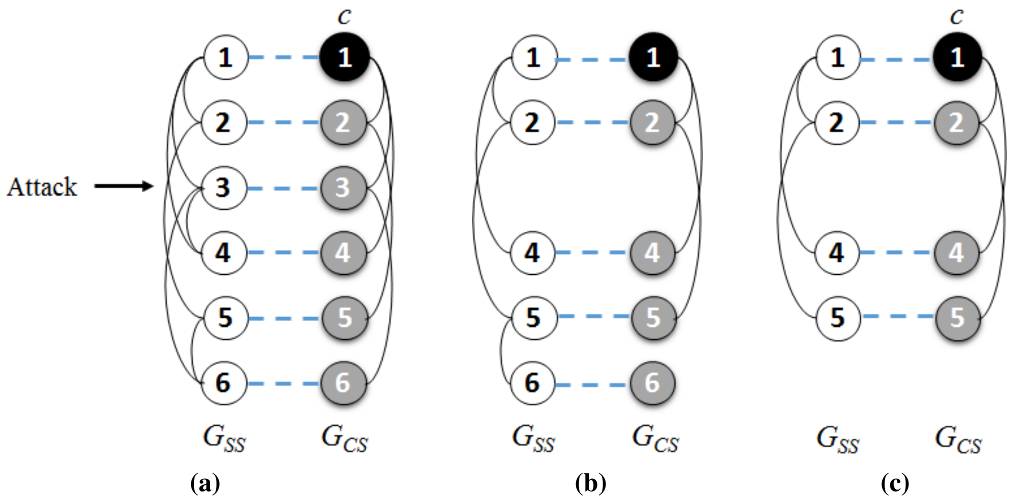


Figure 4.3: Cascading failures in SDN networks (a) node 3 in G_{SS} is attacked (b) node 3 in G_{CS} also fails (c) nodes 6 in G_{SS} and in G_{CS} also fail because they are disconnected from controller c

node 6 in G_{CS} also fails because it is disconnected from the controller located in node 1. Finally, by mutual dependence, the failure spreads to node 6 in G_{SS} (see Fig. 4.3(c)).

In targeted attacks the network elements are removed with the purpose of maximizing the impact of the attack on the network. As explained in Chapter 2, the targeted attack that will produce the greatest damage can be determined from the topological structure of networks. Hence, it is crucial to understand the vulnerability of physical switch-to-switch network to targeted attacks and define the appropriate placement for controllers. In this chapter, the topological properties of the G_{SS} network are considered to select the most important nodes for network connectivity i.e., a centrality metric is measured to rank the nodes to be removed first in the targeted attack. Therefore, the critical parts of one physical topology to certain types of attack can be identified and the best placements for controller to reduce the impact of targeted attacks can be determined.

4.4 Robust design of multilayer networks: finding the best placements for controllers in SDN architectures

Algorithm 1 provides a procedure to find the best placements for controllers in order to improve the SDN network robustness. *Algorithm 1* requires as input three parameters: 1) a switch-switch network (G_{SS}), 2) the number of controllers (κ) and 3) the maximum distance between controllers and switches (δ). As output, *Algorithm 1* generates an array C containing the best placements for controllers. In the first step in *Algorithm 1* (line 1),

---

Algorithm 1: Robust control plane design: finding the best placements for controllers in SDN architectures

---

Data: a switch-switch network (G_{SS}), the number of controllers (κ) and the maximum distance between controllers and switches (δ)

Result: an array C containing the best placements for controllers to improve SDN network robustness

1 $attack\_strategy \leftarrow getMostDangerousAttackStrategy(G_{SS})$
2 $C \leftarrow getLeastCriticalNodes(G_{SS}, \kappa, attack\_strategy)$
3 **for** *all* $c \in C$ **do**
4   **for** *all* $s \in S$ **do**
5   **if** $\delta_{cs} \leq \delta$ **then**
6             $s \in G_{T_c}$
7   **end**
8   **end**
9 **end**
10 $G_{CS} = (G_{T_1}, G_{T_2}, \ldots, G_{T_c}), c = \{1, 2, \ldots, \kappa\}$
11 $G \leftarrow getInterdepentSDNGraph(G_{SS}, G_{CS})$
12 **return** C

---

the targeted attack strategy that produces the greatest damage in G_{SS} is identified through analyzing topological structure of the networks or identifying the areas where failures frequently occur. Based on the number of controllers κ and the type of attack identified to be the most dangerous, a subset of less vulnerable switches can be selected as the possible controllers locations (C) (line 2). Note that the subset C is an array with κ nodes, which is contained in the set of nodes S of the G_{SS} network.

Then, for each controller $c \in C$, the *Algorithm 1* generates a hierarchical tree graph (G_{T_c}) via single shortest path, which contains a subset of G_{SS} nodes to be controlled by controller c (lines 3 to 9). Each tree graph G_{T_c} has as diameter $D_{T_c} \leq \delta$ and controller c as the root. If the distance $\delta_{cs} \leq \delta$, switch i will be part of the subnetwork managed by controller c. For simplicity, we consider δ_{cs} as the shortest path between controller c and switches $i = \{1, 2, \ldots, N_1\}$. In the G_{T_c} graph, controller c is connected to the switches by using the physical links of G_{SS} (as shown in Fig. 4.2(b)). Furthermore, to achieve a load balancing among controllers, the number of nodes of each G_{T_c} is expected to be the same and is given by the fraction between the number of nodes of G_{SS} (N_1) and the number of controllers (κ).

In line 10, the controller-switch network (G_{CS}) is generated by the interconnection of the κ tree graphs G_{T_c} with an in-band controller-switch communication strategy, i.e., the control traffic from controllers to switches is delivered via the physical links of G_{SS}. Thus, controller-controller communications are not direct. Finally, the interdependent SDN graph $G(N, L)$ is obtained by the interconnection of $G_{SS}(S, U)$ and $G_{CS}(U, V)$ with a one-to-one correspondence between node i in G_{SS} and node j in G_{CS} (line 11). Therefore, a subset of switches C as the best locations to place the κ controllers are identified (line 12).

As can be seen, the proposed algorithm takes the robustness of the physical network (G_{SS}) to a given targeted attack into account in order to generate the control plane network (G_{CS}) of the SDN architecture. Consequently, based on the critical parts of the physical network, the best placements for controllers to improve SDN network robustness are identified. The number of controllers (κ) could be defined by the network operator in order to balance the load of controllers, reduce the deployment cost or limit the geographical location of data centers. In addition, in this chapter the control plane network is defined in function of a maximum distance δ based on the number of hops. Other definitions to δ such as latency (a key aspect in data center locations [162]) or the distance of physical links (an important design criteria in large-scale networks) could be considered in the algorithm.

4.5 Robustness measurements in multilayer networks: robust design of the control plane in SDN architectures

In order to provide a practical use case for the robust design of multilayer networks, this section covers the control plane problem in SDN architectures to improve network robustness to targeted attacks. Initially, the topological properties of a real switch-to-switch network (G_{SS}) are described and a robustness analysis of this G_{SS} network under simultaneous and sequential targeted attacks is carried out. Through this study case, the most dangerous targeted attack in the single network scenario of G_{SS} is identified. Then, by executing *Algorithm 1*, an SDN interdependent network is obtained from the G_{SS} network, a number of controllers (κ) and a maximum distance (δ). Therefore, a subset of switches C as the best locations to place the κ controllers are identified. Last, the network robustness of this SDN network is studied in the cascading failure model (presented above in section 4.3.2), when a percentage of nodes (P) are removed from the G_{SS} based on the most dangerous targeted attack.

4.5.1 Topological properties of the physical network

Internet2 was selected for this study case because it supports SDN networking and it has also been studied as an SDN network in previous works [153]. Internet2's Advanced Layer 2 Service (AL2S) provides an effective and efficient wide area 100 gigabit Ethernet

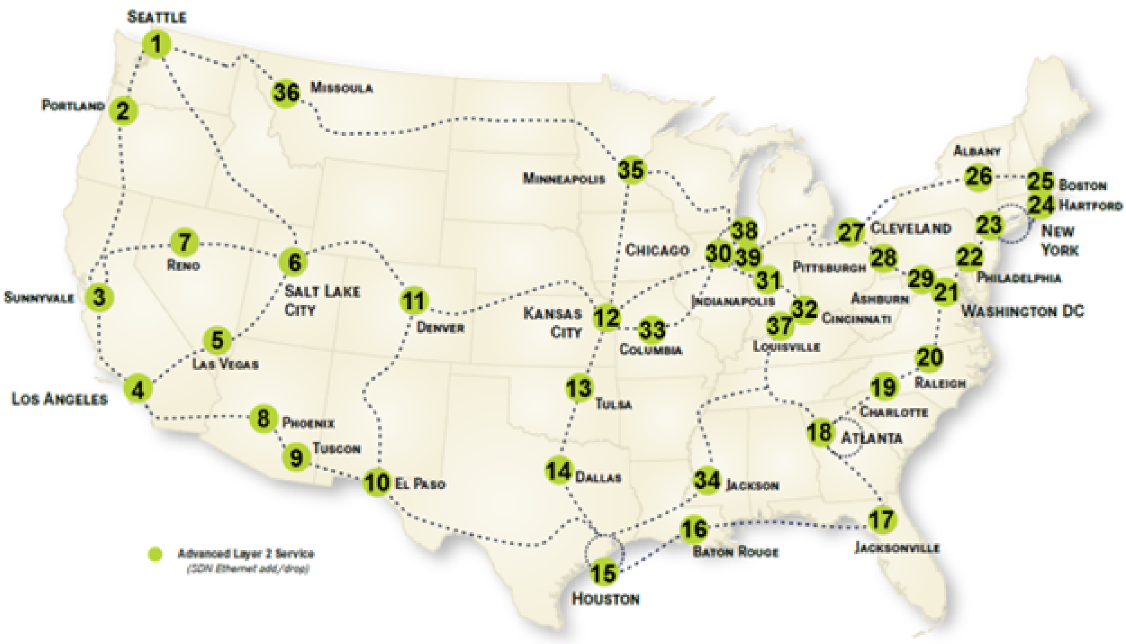


Figure 4.4: Internet2 AL2S network's topology map

technology [163]. The AL2S layer allows for building Layer 2 circuits (VLAN, Virtual Local Area Network) on the Internet2 AL2S backbone. Open Exchange Software Suite (OESS) is a set of software used to configure and control dynamic (user-controlled) VLAN networks on OpenFlow enabled switches [163]. Figure 4.4 shows the Internet2 Network Advanced Layer 2 Service topology map, where each switch has SDN Ethernet add/drop capabilities [163].

In this chapter, the Internet2 AL2S backbone is considered as the switch-switch network (G_{SS}). Table 4.1 presents the main topological properties of this network: number of nodes (N_1), number of links (L_1), average nodal degree ($\langle k \rangle$), maximum degree (k_{max}), average shortest path length ($\langle l \rangle$), Diameter (D) and assortativity coefficient (r). As can be observed in Table 4.1, the network exhibits an assortative (r) value close to zero (-0.128) and has a low value of $\langle k \rangle$ (2.62), and high values of $\langle l \rangle$ (4.65) and D (11).

4.5.2 Robustness measurements in the physical network under targeted attacks

The Average Two-Terminal Reliability ($ATTR$) is selected as the robustness metric to be analyzed in the SDN interdependent network under targeted attacks. Figure 4.5 shows the robustness comparison for the Internet2 AL2S network under targeted attacks in the single network scenario. The INTERNET2_SI_Dc and INTER-NET2_SI_Bc curves present the results of $ATTR$ measures for the Internet2 AL2S network under simultaneous

Table 4.1: Topological properties of the Internet2 AL2S network

Network	N_1	L_1	$\langle k \rangle$	k_{max}	$\langle l \rangle$	D	r
Internet2	39	51	2.62	5	4.65	11	-0.128

targeted attacks based on nodal degree centrality (d_c) and nodal betweenness centrality (b_c), respectively, while INTERNET2_SE_Dc and INTERNET2_SE_Bc curves present the results of $ATTR$ measures for the Internet2 AL2S network under the sequential targeted attack based on d_c and b_c, respectively. In the failure model, the percentage of nodes removed (P) ranges from 1% to 70%. Ten runs were carried out and, in accordance with each targeted attack, different subsets of nodes were removed.

As can be seen in Fig. 4.5, the Internet2 AL2S network is more vulnerable to sequential targeted attacks (see curves INTERNET2_SE_Dc and INTERNET2_SE_Bc) than to simultaneous targeted attacks (see curves INTERNET2_SI_Dc and INTERNET2_SI_Bc). This result can be explained due to the Internet2 AL2S network presenting a small value of $\langle k \rangle$ and high values of $\langle l \rangle$ and D. In Fig. 4.5, in the range of 1% and 5% of P network connections of the Internet2 AL2S topology are reduced to 70% in a sequential targeted attack by b_c (see curve INTERNET2_SE_Bc) and to 66% in a sequential targeted attack by d_c (see curve INTERNET2_SE_Dc). When P ranges from 6% to 15%, in both sequential targeted attacks the network connections dramatically decrease to 21%. For $P > 15\%$, the network connections in the sequential targeted attacks begin to exhibit similar behavior, and the Internet2 AL2S network is almost completely disconnected when P reaches 40%.

In the case of a simultaneous targeted attack, the network connections are reduced to 87% when nodes are removed by their dc (see curve INTERNET2_SI_Dc) and to 85% when nodes are removed by their b_c (see curve IN-TERNET2_SI_Bc). However, for simultaneous targeted attacks there are 22% of network connections when P reaches 20% of removed of nodes. For $P > 20\%$, the Internet2 AL2S topology shows more robustness to simultaneous targeted attacks by b_c than to simultaneous targeted attacks by d_c. The network connections of Inter-net2 are approximately 0% when P reaches 45%.

The robustness analysis presented in this section shows that the Internet2 AL2S network is more vulnerable to a sequential targeted attack by betweenness centrality (b_c) (see curve INTERNET2_SE_Bc in Fig. 4.5). This is an important result due to in the first step in the *Algorithm 1* (line 1), the targeted attack strategy that produces the greatest damage in G_{SS} must be identified. Therefore, based on the strategy explained in the section 4.4 (line 2 in the *Algorithm 1*), the sequential targeted attack by b_c will select as the critical parts of the network those nodes with the highest betweenness centrality for each of the resulting networks after removing the desired fraction of nodes (P).

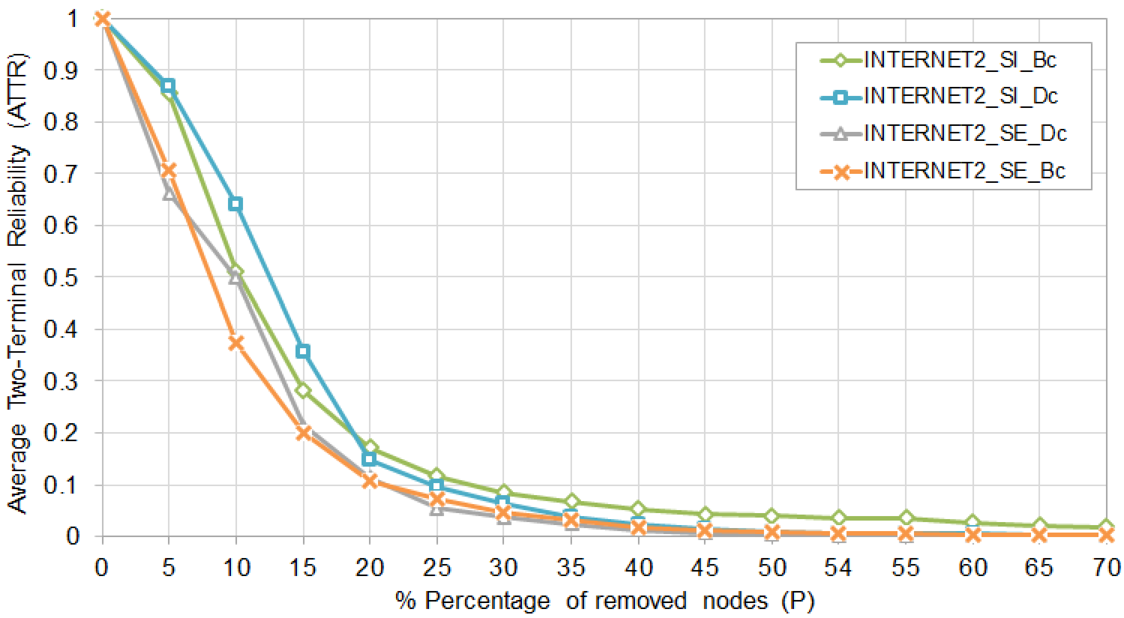


Figure 4.5: Robustness analysis of Internet2 AL2S under targeted attacks in the single network scenario

4.5.3 Robust design of the control plane in SDN architectures to mitigate the impact of targeted attacks

The input parameters to *Algorithm 1* are defined as follows. The Internet ASL2 network is considered as G_{SS}. The number of controllers κ is equal to 5 because according to [160], 8 controllers or less are enough to reach high availability. The distance δ is equal to 6 and it is defined in function of the diameter (D) of network G_{SS}, i.e., $\delta = round(D/2)$. For the switch-to-switch topology considered as study case, the *Algorithm 1* selects as best placements for controllers the switches that are the least vulnerable to a sequential targeted attack based on betweenness centrality (b_c). This prevents the controllers from being removed in the first percentages of attacked nodes. Therefore, the best placements for controllers for the resulting SDN architecture (GA1) after executing *Algorithm 1* (with $\kappa = 5$ controllers and a distance $\delta = 6$) are $C_{A1} = \{32, 34, 35, 37, 38\}$. The subsets of switches (S_T) managed by each controller $c \in C_{A1}$, the number of switches (N_T) in each tree graph of the controller-to-switch network (G_{CS}) and their diameter (D_T) are presented in Table 4.2.

Similarly, we have generated two SDN topologies from the Internet AL2S network in order to compare their robustness with the robustness of the SDN topology generated from the *Algorithm 1* (GA1). The former is the GLBc network, where the nodes for placing κ controllers are selected as those having the lowest betweenness centrality (b_c), i.e., the controllers will be placed on the switches that are less vulnerable to simultaneous targeted

Table 4.2: Subsets of switches managed by each controller in the SDN topologies

Network	C	S_T	N_T	D
GA1	32	{32,12,21,22,33,36}	6	2
	34	{34,25,24,30}	4	2
	35	{35,1,2,5,7,8,9,14,15,17,26,27,29,39}	14	6
	37	{37,3,4,6,13,16,18,19,23,28,31}	11	6
	38	{38,11,10,20}	4	2
GLBc	10	{10,7,8,17,20,24,38}	7	3
	18	{18,3,4,6,11,16,19,23}	8	3
	32	{32,12,13,25,33,34}	6	3
	36	{36,21,22,28,30,37}	6	3
	35	{35,1,2,5,9,14,15,26,27,29,31,39}	12	6
GHCc	20	{20,10,11,38}	4	2
	7	{7,3,6,8,17,18,19,23,35}	9	5
	12	{12,4,13,16,21,22,28,32,33,37}	10	3
	24	{24,25,25,30,34,36}	6	4
	14	{14,1,2,5,15,26,27,29,31,39}	10	5

attacks by b_c. The latter is the GHCc network, where κ controllers are placed in nodes with the minimum distance to switches, i.e., controllers will be placed in switches with the highest values of closeness centrality (c_c) [152]. Therefore, the $\kappa = 5$ controllers for the GLBc network are placed in the subset of nodes $C_{LBc} = \{10, 18, 32, 36, 35\}$, whereas for the GHCc network they are located in the subset of nodes $C_{HCc} = \{20, 7, 12, 24, 14\}$. The subsets of switches managed by each controller c in C_{LBc} and C_{HCc} are presented in Table 4.2. Note in Table 4.2 how the GHCc network has a lowest distance (i.e., the lowest diameter D) among the controllers and switches than the GA1 and GLBc networks.

The placements for controllers for each of the three SDN architectures considered in this chapter are graphically illustrated in Fig. 4.6. As *Algorithm 1* does not take the geographical location of nodes and the physical distance between them into account, the controllers can be placed near each other (see Fig. 4.6(a)) and the shortest path between controllers and switches can be overlapped. Hence, there are some controllers that manages high loads and the diameter of their tree networks are greater than the others e.g., the tree subnetwork created by controller 35 in GA1 manages 14 switches and its diameter is 6, whereas controller 34 only manages 4 switches and the tree subnetwork has a diameter equal to 2 (see Table 4.2). Similar results were found for the placement for controllers for the GLBc and GHCc SDN topologies (Fig. 4.6(b) and Fig. 4.6(c),

(a) GA1

(b) GLBc

(c) GHCc

Figure 4.6: Controllers placement for Internet2 AL2S in each SDN topology

respectively) where the controllers are also geographically close and are unbalanced.

In the SDN modeling proposed in this work, the load balancing is not considered as a mandatory constraint. Thus, in the resulting SDN models it is assumed that each controller must have enough capacity to handle the loads introduced by the switches managed. The unbalanced controllers may have influence in the control plane latency underlying the generation of control messages and the execution of control operations [164]. It is important to note the control plane latency not only depends of the controllers load, but also depends on other factors such as the physical distance between a controller and the switches, the communication protocols and the congestion of the physical links that interconnects controllers and switches. Although the models studied are not fully realistic, they capture other essential constraints in the design of the SDN networks such as the number of controllers and the switch-to-controller distance.

4.5.4 Robustness measurements in SDN architectures under targeted attacks

In this section, the network robustness of the resulting SDN architecture (GA1) after executing *Algorithm 1* is studied in the cascading failure model explained in Section 4.3.2. In order to show the efficacy of the proposed algorithm to improve the robustness of SDN architectures under targeted attacks, the robustness of GA1 is compared with the robustness of the GLBc and GHCc networks. In the failure model, the percentage of nodes removed (P) from the G_{SS} network ranges from 1% to 20% based on a sequential targeted attack by betweenness centrality (b_c). Figure 4.7 illustrates the robustness analysis of the three SDN architectures under a sequential targeted attack by b_c.

In Fig. 4.7 it can be seen that the GA1 SDN network (see curve GA1) is more robust to sequential targeted attacks by b_c than the GLBc and GHCc networks (see curves GLBc and GHCc, respectively). This result is because the GA1 controllers are the last to be attacked, whereas the GLBc and GHCc controllers has a great probability to be removed in the first percentages of failures. In the range of 1% and 3% of P, network connections of GA1 (see curve GA1 in Fig. 4.7) are dramatically reduced to 54% and for the GLBc and GHCc networks to 51% (see curves GLBc and GHCc in Fig. 4.7). When P ranges from 3% to 8%, the network robustness of GA1 is better than the robustness of the GLBc and GHCc networks for approximately 3% plus of network connections.

For $P \geq 9\%$, the network connections for the three SDN topologies are reduced to 10% and the robustness of the GA1 and GLBc networks begin to exhibit a similar behavior. Moreover, in Fig. 4.7 it can be seen that GLBc is more robust than GHCc when P is between 6% and 15% (see curves GLBc and GHCc, respectively). For $P > 15\%$, the robustness of the three SDN topologies are similar and the networks are completely

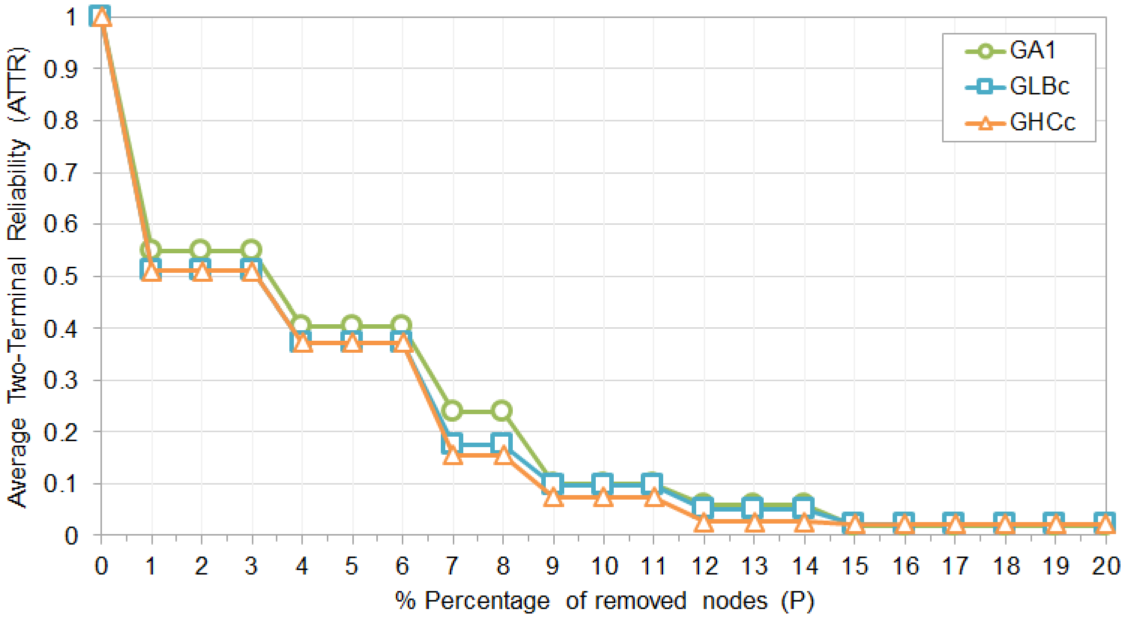


Figure 4.7: Robustness analysis of SDN architectures under targeted attacks

disconnected when P reaches 20%. Therefore, Fig. 4.7 illustrates how the robustness of an SDN network generated by *Algorithm 1* is improved when the most dangerous targeted attack in their switch-to-switch network occurs.

Another interesting result can be found by comparing the robustness of the Internet2 ASL2 network in the single network scenario (see curve INTERNET2_SE_Bc in Fig. 4.5) and the SDN scenario (see curve GA1 in Fig. 4.7). Internet2 ASL2 always is more robust in the single network scenario for different values of P. This result is because in the simulated failure model, an attack on the nodes that support the SDN controllers can cause a higher loss of connections.

4.6 Discussion and lessons learned

The results demonstrate how *Algorithm 1* provides a procedure to mitigate the impact of targeted attacks in SDN networks. It requires three input parameters: 1) a switch-switch network (G_{SS}), 2) the number of controllers (κ), and 3) the maximum distance between controllers and switches (δ). Based on the critical parts of a switch-switch network (G_{SS}) to a targeted attack, *Algorithm 1* selects as best placements for controllers the switches that are the least vulnerable to attack, i.e., those nodes with the lowest probability of being selected in the first percentage of failures of the targeted attack.

By comparing the robustness of the SDN network resulting from executing *Algorithm 1* (GA1) with the two SDN topologies selected as study case (GLBc and GHCc), the GA1 network is the most robust. Hence, for the most dangerous targeted attack, the vulnerability of an SDN network can be reduced when *Algorithm 1* is used to generate a SDN topology. This is because the least vulnerable nodes where controllers are placed are removed in the last percentages of failures. Thus, the GA1 network maintains more network connections than other SDN topologies by increasing of the percentage of removed nodes (P).

Chapter 5

Robustness measurements in region-based interdependent networks: review and new proposals

In region-based interdependent networks, interconnection between critical infrastructures usually is established through nodes that are spatially close, generating a geographical interdependency. Previous work has shown that in general, region-based interdependent networks are more robust with respect to cascading failures when the interconnection radius (r) is large. However, to obtain a more realistic model, the allocation of interlinks of a region-based interconnected model should consider other factors. In this chapter, an enhanced interconnection model for region-based interdependent networks is presented. The model proposed introduces a new strategy for interconnecting nodes between two geographical networks by limiting the number of interlinks. Preliminary simulation results have shown that the model yields promising results to maintain an acceptable level in network robustness under cascading failures with a decrease in the number of interlinks.

5.1 Introduction

Nodes and links that characterize transportation networks are embedded either in two-dimensional or in three-dimensional space [137, 165, 166]. For example, telecommunication networks, water supply, transportation networks, power grids, and oil and gas distribution networks are embedded in the two-dimensional surface of the earth [166], i.e., each node in the networks has a spatial coordinate given by longitude and latitude. Usually, these critical infrastructures are referred to as spatially embedded networks or geographical networks where the spatial distribution of nodes is relevant in order to establish a connection between pairs [165, 166]. Consequently, the geographical location of nodes influences both the cost associated with the length of links as well as the topological structure of these networks [165]. Thus, geographical constraints have a significant impact on network properties and must be considered when modeling real transportation networks [167].

However, many modern critical infrastructure networks depend on one another to function [16]. For instance, telecommunication networks play a vital role in supporting the control, monitoring, connectivity and data transportation services of a number of critical infrastructures. Thus, the interconnection between the nodes of these critical infrastructures and telecommunication networks is usually carried out under geographical constraint, i.e., the spatial proximity between nodes to be interconnected. This region-based interconnection model generates a geographical interdependency [1], where two nodes, i and j, located in two separate networks are interconnected if the distance (d_{ij}) between them is less than or equal to a given radius (r) [38, 120, 168, 169]. Due to such interconnections, failures that occur in one infrastructure can directly or indirectly affect the other and impact large regions with catastrophic consequences [2, 4]. Therefore, network topologies, the geographic locations of nodes and their interdependency relationships have a huge impact on how robust interdependent networks are designed and maintained.

In contrast to the one-to-one interconnection studied in previous work [16], region-based interdependent networks exhibit a one-to-multiple nodal correspondence, i.e., one node in one network can depend on an arbitrary number of nodes in the other network [120]. In [120] it has been shown that in terms of the functional Largest Mutually Connected Component (*LMCC*), a region-based interdependent network is more robust with respect to cascading failures when r is large. This is because with the increase of r, a node tends to have more interconnection nodes which, in turn, will decrease the probability of that node failing as result of the failures of its interconnection nodes. However, the region-interconnection models proposed in [38, 120, 137, 168, 170, 171] only consider the distance between nodes to establish the interlink, whereas in most real scenarios, interlink allocation in region-based interdependent networks should be controlled with additional factors in order to mitigate other issues introduced by the large number of interlinks in each r for example, high deployment cost of interdependent networks or exceeding the capabilities of the nodes to be interconnected.

In [31] the critical number of interlinks beyond which any further inclusion does not enhance the algebraic connectivity (λ_2) of an interdependent network is highlighted. Therefore, controlling the number of interlinks in geographically interdependent networks is likely a valuable design feature in order to reduce the deployment cost and not to exceed node capabilities. Unlike prior efforts, the major contributions of this chapter are: 1) proposing a new strategy for interconnecting nodes between two geographical networks by limiting the number of interlinks and 2) analyzing the impact of limiting the number of interlinks has on the robustness of region-based interdependent networks against cascading failures. As a study case, we focused on interdependent telecommunication networks because they can represent the interconnection of two network operators or can refer to multilayer telecommunication networks which is a particular interdependent network [121]. Moreover, in this chapter we consider the vulnerability analysis of each network to a certain type of targeted attack to determine the influence the new region-based interconnection model has on the robustness of the resulting interdependent network.

The remainder of this chapter is organized as follows: Section 5.2 presents the relevant research in robustness of region-based interdependent networks. Section 5.3 describes the proposed interconnection model for region-based interdependent networks and cascading failure process in interdependent networks. Section 5.4 presents the topologies of the networks to be interconnected and discusses the impact limiting the number of interlinks has on the robustness of region-based interdependent networks to cascading failures. Finally, Section 5.5 provides discussion and lessons learned.

5.2 Review of robustness measurements in region-based interconnected networks

In the literature, most of the studies about robustness of interdependent networks have been focused on real or artificial networks in which geographical constraints are not considered (see Table 3.1). However, critical infrastructures are embedded either in two-dimensional or three-dimensional space, and the nodes in each network might be interdependent with nodes in other networks [168]. These interconnected networks are referred to as interdependent spatially embedded networks, but when the geographical distance between nodes to be interconnected is considered as a constraint, these can also be called region-based interdependent networks. An example of region-based interdependent networks are the routers in a backbone telecommunication network that are distributed among different regions of a country and dependent on regional power grids for power supply. In the same way, every substation in a power grid sends data and receives control signals to/from the nearest router [108]. Due to the interdependency between these critical infrastructures, a random failure or a targeted attack can lead to cascading failures which imply service disruptions that affect thousands of people, multiple communities, entire countries, or just one company [4, 16].

The vulnerability of interdependent networks modeled as the interconnection of two embedded lattice network have been studied in [17]. Bashan et al. [17] have found that in embedded lattice systems, as opposed to non-embedded systems, there is no critical dependency and any small fraction of interdependent nodes q leads to an abrupt collapse as a result of cascading failures. The parameter q represents the fraction of nodes in one network that depend on nodes in the other network [17]. If there is no restriction on the length of the dependency links, then any fraction of dependency leads to a first-order transition ($q_c = 0$). Therefore, the extreme vulnerability of very weakly coupled lattices is a consequence of the critical exponent describing the percolation transition of a single lattice [17]. However, the length of interlinks is considered to be a relevant aspect to interconnect the nodes located in two separate transportation networks. Thus, in other studies a geographical constraint, which is based on the spatial proximity between the nodes, has been considered to interconnect networks [38, 120, 168, 169].

In [168] cascading failures when two square lattice networks placed on the same Cartesian plane are interconnected have been studied. In this interdependent network, each node in a network is connected with one, and only one, node in the other network, randomly chosen within a certain radius r from the corresponding node in each network, thus generating full dependency ($q = 1$). The parameter r represents the maximum distance a node in one network receives support from a node in another network. Li et al. [168] have shown the existence of a phase transition phenomena when the length of the dependency links r changes, i.e., the critical percolation threshold ρ_c increases linearly with r to reach a maximum for $r = r_c$ and is characterized by a second-order transition [168]. Furthermore, interdependent networks embedded in Cartesian space become most vulnerable when the distance between interconnected nodes is in the intermediate range, which is much smaller than the size of the system [168].

In the more realistic cases, region-based interdependent networks have partial dependency ($0 < q \leq 1$). In [38] the relationship between r_c and q on the specific dynamics of cascading failures in such systems has been studied. In [38] a similar result to [168] was found for any finite value of q with a larger r_c as q decreases. Danziger et al. [38] have also studied the dynamics at the percolation threshold p_c for varying r and q. Below r_c the system undergoes a continuous transition similar to standard percolation [38], while above r_c there are two distinct first-order transitions for finite or infinite r, respectively [38]. The transition for finite r is characterized by node failures spreading through the system while the infinite r corresponds to a non-spatial cascading failure similar to the case of random networks [38].

The robustness of interdependent networks modeled as a Random Geometric Graph (RGG) [172] has been studied by Zhang et al. [171] and Wang et al. [120]. In this model, the networks to be interconnected are spatially embedded on the same two-dimensional space, i.e., nodes are geographically distributed. Then, a node in one network will be interconnected with all the nodes in the other network within the radius r, thus, generating a one-to-multiple interconnection. On one hand, Zhang et al. [171] have obtained analytical upper bounds on the percolation thresholds of the interdependent RGGs, above which a positive fraction of nodes are functioning. Moreover, if the node densities are above any upper bound on the percolation thresholds, then the interdependent RGGs remain percolated after a geographical attack [171]. On the other hand, Wang et al. [120] have not only studied interdependent RGGs but have also considered a relative neighborhood graph as the interconnection model. Results have shown that as a function of the Largest Mutually Connected Component (*LMCC*), an interdependent network is more robust by increasing the interconnection radius r. In addition, in [120] the derivative of the *LMCC* as a new robust metric has been proposed. This metric quantifies the damage to networks that is triggered by a small fraction of failures, significantly smaller than the fraction at the critical threshold, and corresponds to the collapse of the whole network [120].

The percolation of a Network of Networks (NoN) made up of interdependent spatially embedded networks has been analyzed in [170]. This work considers both dependency links restricted to a maximum Euclidean length r and unconstrained dependency links ($r = \infty$). Shekhtman et al. [170] have found that for treelike networks of networks (composed of n networks) r_c significantly decreases as n increases and rapidly ($n \geq 11$) reaches its limiting value of 1. For cases where the dependencies form loops, such as in random regular networks, there is a certain fraction of dependent nodes, q_{max}, above which the entire network structure collapses even if a single node is removed [170]. The value of q_{max} decreases quickly with m, the degree of the random regular network of networks. Results have also shown the extreme sensitivity coupled geographical networks have and emphasize their susceptibility to sudden collapse [170].

In [173] interdependent networks in which each node has links in multiple networks and requires connectivity in each layer to function has been studied. Furthermore, the connectivity links in each layer have lengths exponentially distributed with the characteristic length ζ [173]. Thus, high values of ζ reflect weak spatiality and low values reflect strong spatiality. In this region-based interdependent model, percolation exhibits first or second-order transitions, depending on the characteristic length of the connectivity links. Thus, longer links make a multilayer network more vulnerable, which contrasts with the increase in robustness in a single-layer for larger connectivity links [173]. When ζ is longer than a certain critical value, ζ_c, abrupt, discontinuous transitions take place, while for $\zeta < \zeta_c$ the transition is continuous, indicating that the risk of abrupt collapse can be eliminated if the typical link length is shorter than ζ_c [173].

Region-based interdependent networks are also vulnerable to geographical localized attacks, such as terrorist attacks or natural catastrophes, which damage all nodes within a given radius r_h from a random location in the network [137, 174]. Berezin et al. [137] have studied the impact localized attacks have on interdependent networks in which a node in one network is interconnected with one, and only one, node randomly chosen in the other network if they are within the radius r. Results have shown that a localized attack can cause substantially more damage than an equivalent random attack in interdependent square lattices networks [137]. Furthermore, for a broad range of parameters (average nodal degree $\langle k \rangle$ and r), interdependent networks are metastable and are qualitatively different from the stable and unstable phases known to percolation theory [137]. In metastable systems, there is a critical damage size with radius r_h^c defining the potential risk of localized attacks on spatially embedded networks. Thus, if the interdependent network if subjected to a localized attack larger than a critical size, a cascading failure emerges which, in turn, leads to a complete system collapse [137]. The robustness of interdependent networks against localized attacks where dependency links are no longer than connectivity links has been analyzed in [174]. Vaknin et al. [174] have found a metastable zone where a localized attack larger than a critical size r_h^c induces a nucleation transition as a cascade of failures spreads throughout the system, leading to its collapse. Moreover, localized attacks in these multiplex systems can induce a previously unobserved combination of random and spatial cascades [174].

In summary, although most previous studies have focused on measuring the robustness of independent networks against multiple failures, only a small number of them addressed geographic constraints. Table 5.1 presents a comparison of the relevant results concerning robustness measurements in region-based interdependent networks. As can be seen in most of the previous work, the interconnection model for spatially embedded or geographical networks considers the distance of interlinks as being important design constraint and the *LMCC* as the robustness metric. Moreover, these works are focused on identifying the behavior of the percolation threshold in the context of cascading failures generated by random failures or localized attacks. Therefore, the following research objectives will be covered in the remainder of this chapter:

- The region-interconnection models proposed in previous studies only consider the distance between nodes to establish interlinks. However, interlink allocation in region-based interdependent networks should be controlled with additional factors in order to mitigate other issues produced by the large number of interlinks in each radius r. Thus, controlling the number of interlinks in region-based interdependent networks is likely a valuable design feature in order to reduce the deployment cost of interdependent networks and not to exceed the capabilities of the nodes to be interconnected. Unlike previous research, a new strategy for limiting the number of interlinks between two geographical networks is proposed.

- Region-based interdependent networks have exhibited high vulnerability to cascading failures due to the elimination of a small fraction of nodes in one network may lead to catastrophic consequences for the whole system. Hence, in this work the impact limiting the number of interlinks has on the robustness of region-based interdependent networks against cascading failures is also analyzed. As a study case, we focused on interdependent telecommunication networks in which nodes are placed in a two dimensional space, i.e., nodes are geographically distributed. Furthermore, in this chapter we consider the vulnerability analysis of each network to a certain type of targeted attack to determine the influence the new region-based interconnection model has on the robustness of the resulting interdependent network.

Table 5.1: Comparison of relevant results about robustness measurement in region-based interdependent networks

Author	Network model	Interconnection type	Triggered event	Results
Bashan et al. [17]	Interconnected spatially embedded lattice networks	One-to-multiple	Random failure	Any small fraction of interdependent nodes q leads to an abrupt collapse resulting from cascading failures.
Li et al. [168]	Interconnected spatially embedded square lattice networks	One-to-one	Random failure	The critical percolation threshold ρ_c increases linearly with r to reach a maximum for $r = r_c$ and is characterized by a second-order transition.
Danziger et al. [38]	Interconnected spatially embedded square lattice networks	One-to-multiple	Random failure	The transition phase of percolation for finite r is characterized by node failures spreading through the system while the infinite r corresponds to a non-spatial cascading failure similar to the case of random networks.
Zhang et al [171]	Random Geometric Graphs (RGG) for interdependent spatially embedded networks	One-to-multiple	Random failure	Above the upper bounds of the percolation thresholds in interdependent EGGs, a positive fraction of nodes are functioning.
Wang et al [120]	ER-ER network through RGG and relative neighborhood graph	One-to-multiple	Random failure	As a function of the Largest Mutually Connected Component (*LMCC*), an interdependent network becomes more robust by increasing in the interconnection radius r. The *LMCC*, as a new robust metric, quantifies the damage of networks that is triggered by a small fraction of failures.
Shekhtman et al. [170]	Network made up of interdependent spatially embedded networks	One-to-multiple	Random failure	The r_c significantly decreases as n increases and for a certain fraction of dependent nodes the entire network structure collapses even if only a single node is removed.

Continue on the next page

Table 5.1: Comparison of relevant results about robustness measurement in region-based interdependent networks

Author	**Network model**	**Interconnection type**	**Triggered event**	**Results**
Danziger et al. [173]	Multilayer interdependent networks	One-to-multiple	Random failure	Percolation threshold exhibits first or second-order transitions, depending on the characteristic length of the connectivity links. Moreover, longer links make a multilayer network more vulnerable to cascading failures.
Berezin et al. [137]	Interconnected spatially embedded square lattice networks	One-to-one	Random failure and localized attack	A localized attack can cause substantially more damage than an equivalent random attack in interdependent square lattices networks.
Vakin et al. [174]	Interconnected spatially embedded square lattice networks	One-to-multiple	Localized attack	There is a metastable region in which only attacks with a radius larger than r_h^c are propagated, through cascading failures, in the entire system rendering it non-functional.

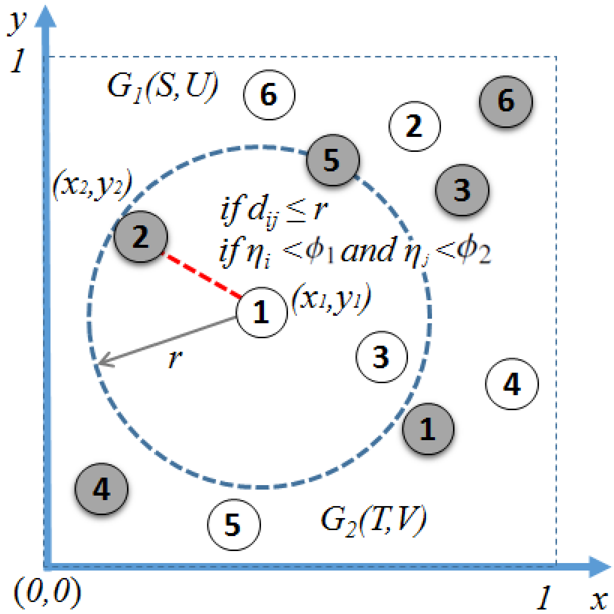


Figure 5.1: Enhanced interconnection model in region-based interdependent networks

5.3 Enhanced region-based interconnection model and failure model

In order to generate an enhanced region-based interconnection model, interlink allocation should be controlled by considering factors additional to the geographical constraint. This chapter proposes a new region-based interconnection model in which a node i in network G_1 and a node j in network G_2 can be interconnected if 1) the distance d_{ij} between them is less than or equal to a given radius r and 2) the number of interlinks for nodes i and j do not exceed a given percentage for limiting the number of interlinks (ϕ_1 and ϕ_2, respectively). Our new strategy for interlink allocation is based on dividing the nodes in both networks into subsets in accordance with a certain nodal property. Thus, the model prevents ϕ_1 and ϕ_2 being exceeded for any node in G_1 and G_2, respectively.

The proposed region-based interconnection model is illustrated in Fig. 5.1, where the nodes in G_1 are represented by filled circles and the nodes in G_2 are represented by unfilled circles. For each node i in G_1, there is a set of nodes in G_2 that can be interconnected if the conditions 1) and 2) are satisfied. Consequently, in contrast to [120], an enhanced interconnection model for limiting the number of interlinks in region-based interdependent networks is generated. The remainder of this section presents the proposed region-based interconnection model in detail and describes the failure model involving cascading failures.

5.3.1 Interconnection model for limiting number of interlinks in region-based interdependent networks

Consider two undirected networks $G_1\,(S,U)$ and $G_2\,(T,V)$, each with a set of nodes (S,T) and a set of links (U,V) respectively. Denote N_1 and N_2 as the number of nodes in G_1 and G_2, respectively, and L_1 and L_1 as the number of links in G_1 and G_2, respectively. When G_1 and G_2 interact, a set of bidirectional interlinks I joining the two networks is introduced. Consequently, an interdependent network is defined as $G(N,L) = (S\cup T, U\cup V\cup I)$ [31].

In the region-based interconnection model previously proposed in [120], the entry b_{ij} in the interconnection matrix B_{12} is determined by the geographical location of nodes of G_1 and G_2 networks. Let (x_i,y_i) and (x_j,y_j) denote the spatial coordinates for nodes i and j, then, b_{ij}= 1 if the Euclidean distance d_{ij} between node i in G_1 and node j in G_2 is smaller than a given threshold r, otherwise b_{ij} = 0. This link pattern generates a random geometric graph with a one-to-multiple interdependency model [120]. The Euclidean distances d_{ij} is given by:

$$d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{5.1}$$

In the random geometric graph, a node i in G_1 can depend on an arbitrary number of nodes in G_2 that is no greater than N_2, and vice versa [120, 171, 172]. When the distance between two nodes is considered as the unique interconnection constraint, some issues are evidenced. Specifically, the nodes in one network can have many interlinks from the other network, thus incurring high deployment cost. Note that the cost can be related to the economic investment required to construct an interlink. For instance, in the case of interdependent networks constructed by power grids and telecommunication networks, a new interlink has an associated deployment cost as a function of the cable length. Additionally, nodes in each network have limited capabilities to interconnect to a fixed number of nodes, and so the network's extension requires additional investments. Therefore, limiting the number of interlinks between the nodes in two networks contributes to keeping the deployment cost under control and adjusting to the operator's budget.

Let us define the new factor to be considered to limit the number of interlinks in region-based interdependent networks. For G_1, this factor is denoted as ϕ_1 and is given by:

$$\phi_1 = \frac{\eta_1}{N_2} \times 100\%, \tag{5.2}$$

where $\eta_1 \leq N_2$ is the maximum number of nodes from G_2 that each node in G_1 can interconnect to and N_2 is the number of nodes in G_2. Analogously, the limit of interlinks (ϕ_2) for nodes in G_2 can be calculated analogous to (5.2). Therefore, the maximum number of interlinks that each node in G_1 and G_2 can interconnect to is controlled by ϕ_1 and ϕ_2.

As part of our proposal, the nodes in G_1 (G_2) are divided into μ_1 (μ_2) subsets of nodes, each with a maximum of η_1 (η_2) nodes. Subsets of nodes are a key aspect to controlling the allocation of a specific number of interlinks to each node. The number of nodes in a subset is directly related to the capacity of the nodes and the functionality performed by nodes in each network. For instance, in a fixed broadband access architecture, a subset of nodes in the access network can be interconnected to a subset of nodes in the core network. Moreover, a core network can support the interconnection of a limited number of access nodes. Without loss of generality, a subset of nodes in a network can group nodes with similar properties or randomly. Then, the nodes of a subset in G_1 will be interconnected to the nodes of a subset in G_2 if the distance is less than or equal to the radius (r). As the number of nodes in each subset is limited, the number of interlinks in each node can be kept under control.

Let us consider that the nodes in G_1 are divided into μ_1 subsets of nodes, where μ_1 is given by:

$$\mu_1 = \begin{cases} round(\frac{N_2}{\eta_1}), & \text{if } \phi_1 < 50\% \\ 2, & \text{if } \phi_1 \geq 50\% \end{cases} \tag{5.3}$$

Similarly, the nodes in G_2 are divided into μ_2 subset of nodes, where μ_2 is given by:

$$\mu_2 = \begin{cases} round(\frac{N_1}{\eta_2}), & \text{if } \phi_2 < 50\% \\ 2, & \text{if } \phi_2 \geq 50\% \end{cases} \tag{5.4}$$

Let a_i denote the property value of node $i \in G_1$. Then, nodes in G_1 are ordered according to a_i, i.e., $a_1 \geq a_2 \geq ... \geq a_{i-1} \geq a_i \geq a_{i+1} \geq ... \geq a_{N_1-1} \geq a_{N_1}$. Moreover, let Γ_{S_g} denote the ordered set of nodes previously defined in G_1. If $\Gamma_{S_1}, \Gamma_{S_2}, ..., \Gamma_{S_{\mu_1}}$ represent the subsets of Γ_S, then, $\Gamma_S = \bigcup_{g=1}^{\mu_1} \Gamma_{S_g}$, and Γ_{S_g} is given by:

$$\Gamma_{S_g} = \begin{cases} \{i : (g-1) \times \eta_2 < i \leq g \times \eta_2\}, & \text{if } g < \mu_1 \\ \{i : (g-1) \times \eta_2 < i \leq N_1\}, & \text{if } g = \mu_1 \end{cases}, \tag{5.5}$$

where i represents the $i-th$ element in Γ_{S_g} and $g \in \{1, 2, ..., \mu_1\}$. Similarly, let c_j denote the property value of node $j \in G_2$. Then, nodes $j \in G_2$ are ordered according to c_j, i.e., $c_1 \geq c_2 \geq ... \geq c_{j-1} \geq c_j \geq c_{j+1} \geq ... \geq c_{N_2-1} \geq c_{N_2}$. Additionally, let Γ_{T_h} denote the ordered set of nodes previously defined in G_2. If $\Gamma_{T_1}, \Gamma_{T_2}, ..., \Gamma_{T_{\mu_2}}$ are subsets of Γ_T, then,

$\Gamma_T = \bigcup_{H=1}^{\mu_2} \Gamma_{T_h}$, and Γ_{T_h} is given by:

$$\Gamma_{T_h} = \begin{cases} \{j : (h-1) \times \eta_1 < j \leq h \times \eta_1\}, & \text{if } h < \mu_2 \\ \{j : (h-1) \times \eta_1 < j \leq N_2\}, & \text{if } h = \mu_2 \end{cases}, \tag{5.6}$$

where j represents the $j-th$ element in Γ_{T_h} and $h \in \{1, 2, ..., \mu_2\}$

Let us define B_ϕ as an $N_1 \times N_2$ interconnection matrix, whose entries or elements are $b_{\phi_{ij}} = 1$ if nodes in the subset Γ_{S_g} are connected to nodes in the subset Γ_{T_h} for $g = h$, otherwise $b_{\phi_{ij}} = 0$. Accordingly, the B_ϕ matrix defines which nodes in the networks can be interconnected and establishes the limit for the number of interlinks that each node in the networks can handle. Thus, each node in G_1 or G_2 will have a maximum of η_1 or η_2 interconnected nodes, respectively.

Finally, let us redefine the dependency matrix B_{12}, whose entries are $b_{ji} = 1$ if $d_{ij} \leq r$ and $b_{\phi_{ij}} = 1$, otherwise $b_{ij} = 0$. Note that the new B_{12} matrix captures the interconnection conditions 1) and 2) proposed in this chapter and thus the new interdependency matrix B, which is given by the equation (3.2), can be generated. Therefore, the nodes in each geographical or spatial network will interconnect with a limited number of interlinks, consequently improving the model defined in [120]. For simplicity, in this chapter we consider that G_1 and G_2 have the same number of nodes ($N_1 = N_2$) and that all the nodes in the interdependent network have the same limit of interlinks ($\phi_1 = \phi_2$). Therefore, each network has $\mu_1 = \mu_2$ subsets of nodes with a maximum number of nodes $\eta_1 = \eta_2$.

Figure 5.2 presents two geographical networks being interconnected by employing the interconnection proposal described in this section. As can be seen in Fig. 5.2, both networks have $N_1 = N_2 = 9$ nodes and each node in G_1 and G_2 can support until $\phi_1 = \phi_2 = 30\%$ of nodes from the other. According to what has been described above, nodes in both networks are divided into $\mu_1 = \mu_2 = 3$ subsets, each one with a maximum of $\eta_1 = \eta_2 = 3$ nodes. Then, the B_ϕ matrix is generated with the subsets Γ_{S_g} and Γ_{T_h}. Finally, the interlinks between the nodes from G_1 and G_2 (dashed lines) are established if $d_{ij} \leq r$ and $b_{\phi_{ij}} = 1$.

The percentage to limit the number of interlinks (ϕ) can be tuned by network administrators according to capabilities of nodes (i.e.,maximum number of clients per server) or budgets constraints. In practice, these features are important factors to define the number of interlinks that a node can interconnect. Moreover, in the design of interdependent critical infrastructures with geographical constraints (i.e.,radius r), limiting the number of interlinks have high value in order to maintain the network performance under control due to the interconnections between networks do not exceed the capacity of the nodes.

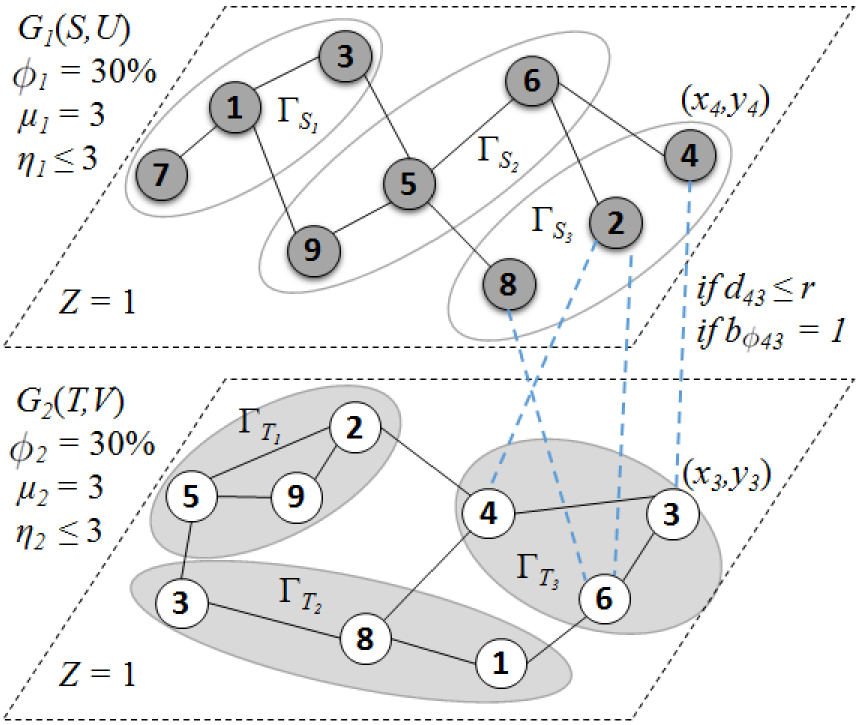


Figure 5.2: Subsets for limiting the number of interlinks in region-based interdependent networks

5.3.2 Algorithm description for enhancing a region-based interconnection model

Algorithm 2 summarizes the interconnection model proposed to limit the number of interlinks in region-based interdependent networks. *Algorithm 2* requires two networks (G_1 and G_2) to be interconnected, the percentage for limiting the number of interlinks (ϕ_1 and ϕ_2) and the radius (r). The output of *Algorithm 2* is a dependency matrix B_{12} with the conditions 1) and 2) previously described. As can be seen, *Algorithm 2* calculates the maximum number of nodes that a node can interconnect to (Lines 1 and 2) and the number of subsets (Lines 3 and 4). Then, the nodes are grouped in subsets according to one property (Lines 5 and 6). The interconnection matrix ($B_{\phi_{12}}$), in which each node in G_1 (G_2) has a maximum of η_1 (η_2) interconnected nodes (Line 7) is generated. Finally, the interdependency matrix B_{12} is generated by considering the distance constraint for a given r and the B_ϕ matrix (Lines 8 to 19). Thus, an enhanced region-based interconnection model is defined for interconnecting the G_1 and G_2 networks and the interdependency matrix B, which is given by the equation (3.2), can be generated from the resulting B_{12} matrix.

Algorithm 2: Interconnection model for limiting the number of interlinks in region-based interdependent networks

Data: two geographical networks (G_1 and G_2), limit for number of interlinks (ϕ_1 and ϕ_2) and radius (r)

Result: dependency matrix B_{12}

$\eta_1 = round(\phi_1 N_2/100)$
$\eta_2 = round(\phi_2 N_1/100)$
$\mu_1 = round(N_1/\eta_2)$
$\mu_2 = round(N_2/\eta_1)$
$\Gamma_{S_g} \leftarrow getSubsetNodes(S, \mu_1, \eta_2, nodal\_property)$
$\Gamma_{T_h} \leftarrow getSubsetNodes(T, \mu_2, \eta_1, nodal\_property)$
$B_\phi \leftarrow getB_\phi Matrix(\Gamma_{S_g}, \Gamma_{T_h}, \eta_1, \eta_2, \mu_1, \mu_2)$
for *all* $i \in S$ **do**
    for *all* $j \in T$ **do**
        $d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$
        if $d_{ij} \leq r$ *and* $b_{\phi_{ij}} == 1$ **then**
            $b_{ij} = 1$
        end
        else
            $b_{ij} = 0$
        end
    end
end
return B_{12}

5.3.3 Cascading failure process in interdependent networks

Consider a region-based interdependent network G generated from the model proposed in this chapter. When a random fraction of the nodes in G_1 fails, a cascading failure process is induced. We assume the node i in network G_1 is functional if *a*) at least one of its interconnected nodes in network G_2 is operative, and *b*) the node i belongs to the giant component of the functional nodes in network G_1 [122]. Due to interdependency, the failed nodes in G_1 spread failures in G_2. As the assumptions *a*) and *b*) are also applied to the node j in network G_2, the failed nodes in G_2 spread failures back into G_1, and so on. The cascading failures continue until no more nodes fail. The remaining set of functional nodes is referred to as the Largest Mutually Connected Component (*LMCC*):

$$LMCC = \frac{n_1 + n_2}{N_1 + N_2}, \tag{5.7}$$

where n_1 and n_2 are the number of nodes that belong to the giant component of the functional nodes in G_1 and G_2, respectively, when the assumptions *a*) and *b*) are satisfied. The cascading failures described in this section can occur in real scenarios such as power grid blackouts [108] and disruptions in economic networks [175]. Note that [120] also considered the case in which a node in G_1 is functional if all of its interconnected nodes in G_2 are operational. Under that condition, in some cases, having more interconnected links makes the region-based interdependent network less robust. However, this case is outside the scope of this chapter. Algorithm 3, based on the model proposed by [19], is used to simulate a cascading failure process from an initial failure:

Algorithm 3: Cascading failure process in region-based interdependent networks

Data: two geographical networks (G_1 and G_2) and an interconnection matrix B_{12}
Result: functional largest connected components in G_1 and G_2 networks

1 Remove the fraction p of initial failed nodes in network G_1
2 Identify the largest component n_1 in G_1
3 Remove the s nodes in G_1 not in n_1
4 Remove the t nodes in G_2 not linked to n_1
5 Identify the largest component n_2 in G_2
6 Remove the s nodes in G_2 not in n_2
7 Remove the t nodes in G_1 not linked to n_2
8 If $s > 0$ then repeat from line 2
9 **return** The final functional largest components n_1 and n_2

Table 5.2: Nodes distribution in G_1 and G_2 according to interlink limits

$\phi_1 = \phi_2$	$\mu_1 = \mu_2$	$\eta_1 = \eta_2$
10%	10	5
25%	4	12
50%	2	25
75%	2	37
100%	1	50

5.4 Simulation results and discussion

In this section, the topologies to be interconnected according to the proposed region-based interconnection model are described. Moreover, the impact limiting the number of interlinks has on the robustness of region-based interdependent network is analyzed.

5.4.1 Topologies for region-based independent networks

The region-based interdependent networks considered as the study case represent two backbone telecommunication networks being interconnected with bidirectional interlinks. The random connection property of a backbone telecommunications network is modeled using an Erdös-Rényi (ER) random graph with a Poisson nodal degree distribution. This indicates that most nodes have approximately the same number of links close to the average nodal degree [46].

In order to analyze the impact the model proposed has on the robustness of interdependent networks against cascading failures, the Largest Mutually Connected Component (*LMCC*) is measured in 100 interdependent telecommunication networks. Each backbone telecommunication network to be interconnected is modeled as an *ER* random graph with $N_1 = N_2 = 50$ nodes and the average nodal degree ($\langle k \rangle$) equal to 6. The nodes in each network are placed uniformly in a two-dimensional square of the size $Z = 1$ i.e., each node in the G_1 and G_2 networks has as spatial coordinates (x, y), where $0 \leq x \leq 1$ and $0 \leq y \leq 1$. The interconnection link pattern between a pair of ER graphs is conditioned by a given radius r, i.e., a geographical constraint. The number of interlinks in each node is limited by a given percentage ϕ.

The number of subset (μ_1, μ_2) and the maximum number of nodes that a node in G_1 and G_2 can interconnect with (η_1, η_2) are presented in Table 5.2. For instance, when $\phi = 25\%$, this is considered as the design constraint and, as such, the nodes in each network are divided into $\mu_1 = \mu_2 = 4$ subsets. Then, for a given radius r, it is expected that each node in G_1 and G_2 will have a maximum of 12 interlinks. Note that from the initial percentages, ϕ_1 and ϕ_2, the number of subsets (μ_1 and μ_2) can be calculated. Thus, from the number of subset, a network administrator is able to control nodes capacity in function of the number of interlinks that they can interconnect. Other relation can be found when the network administrator knows the maximum number of interlinks (η_1 and η_2) that nodes in each network can support. In consequence, the number of subsets can be estimated in order to apply the model proposed in this paper. However, this last consideration requires that the execution of the *Algorithm 2* starts from Line 5.

As was described in subsection 5.3.1, a nodal property is also required to define how nodes in each network can be grouped. In the study case considered in this chapter, node vulnerability to failures is selected as the property with which to group the nodes into subsets. In most real scenarios, the vulnerability of nodes to failures can be estimated from the historical failure database of their Operation Support Systems (OSS). However, given the difficulty of obtaining access to real data, centrality metrics could be used to measure the importance of nodes for the network connectivity under some failure scenarios [54]. Previous analysis has revealed that backbone telecommunication networks modeled as *ER* are highly vulnerable to a sequential targeted attack based on nodal betweenness centrality (b_c) (see Chapter 3).

Figure 5.3 depicts a robustness analysis of the backbone telecommunication networks under targeted attacks when networks are not connected to other. The networks' robustness is quantified as a function of the Average Two-Terminal Reliability ($ATTR$) metric [4]. As can be seen in Fig. 5.3, the telecommunication networks considered in this work exhibit high vulnerability to a sequential targeted attack by b_c. Whereas, the networks are more robust to a simultaneous targeted attack by b_c and sequential or simultaneous targeted attacks based on degree centrality (d_c). Consequently, node vulnerability in each *ER* network could be quantified by their b_c values i.e., the higher the betweenness centrality of node is, the higher the node's vulnerability is.

5.4.2 Analyzing the impact limiting the number of interlinks has on the robustness of region-based interdependent networks

To investigate the impact the region-based interconnection model has on the robustness of interdependent networks against cascading failures, the Largest Mutually Connected Component (*LMCC*) metric is measured when a fraction of nodes is removed. In the failure scenario considered in this chapter, nodes in the network G_1 are removed (according to their vulnerability to a sequential targeted attack by b_c) until the percentage of removed nodes (P) is reached. Removing the nodes in G_1 leads to a cascading failure process as described in Section 5.3.3.

Although several region-based interdependent networks can be generated by varying

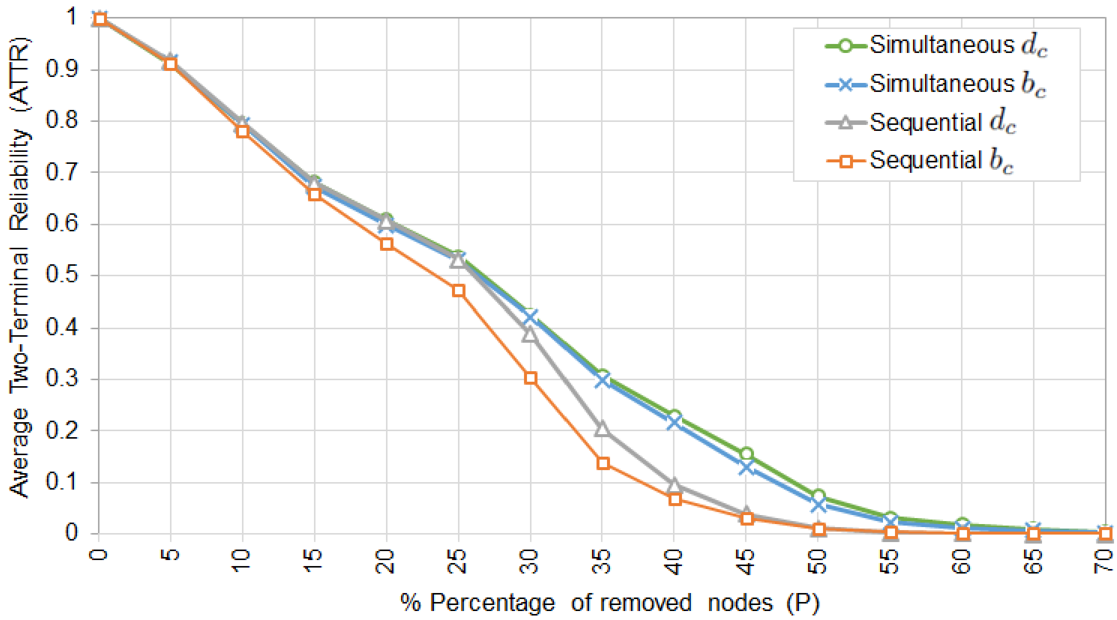


Figure 5.3: Robustness analysis of backbone telecommunication networks ($N_1 = 50$ and $\langle k \rangle = 6$) in a single scenario.

the radius and the limit of number of the interlinks, the two scenarios considered as case studies are:

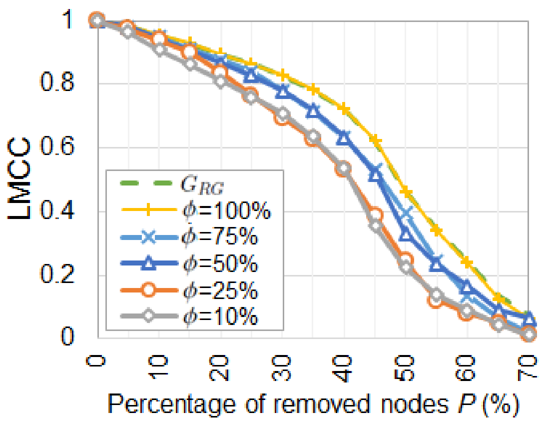
- Scenario 1: The radius (r) is fixed to 0.2 and the limit for the number of interlinks (ϕ) ranges from 25% to 100%. This scenario can represent a real situation in which a telecommunication network operator has a geographical area limited by a radius r and is interested in controlling the number of interlinks to other infrastructures.

- Scenario 2: The number of interlinks is limited to 25% and r is varied from 0.1 to $\sqrt{2}$. This scenario can be used by a telecommunication network operator who has a certain capacity in their network, but wants to restrict its coverage area to a certain radius r to interconnect to fewer number of nodes from other infrastructures.

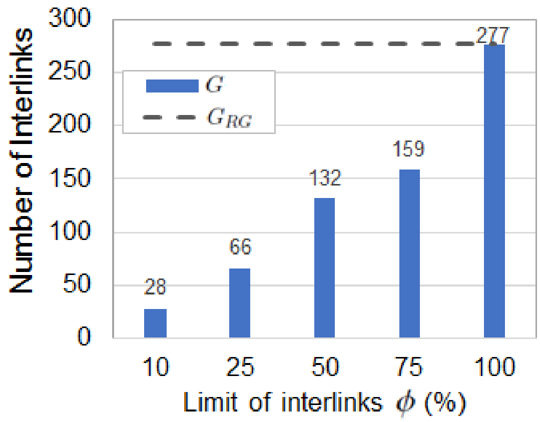
Both scenarios are replicated in 100 interdependent networks. The robustness analysis presented in this section is the average of the *LMCC* results measured in these interdependent networks.

5.4.2.1 Scenario 1: Robustness analysis in region-based interdependent networks against variations in the limit of interlinks (ϕ)

In this scenario, the radius (r) to interconnect the G_1 and G_2 networks is fixed to 0.2. Then, for a given limit in the number of interlinks (ϕ), the *LMCC* of an interdependent network is measured when a fraction of nodes (P) is removed in the G_1 network. Figure



(a)



(b)

Figure 5.4: Robustness analysis in region-based interdependent networks (r = 0.2) versus variations in the limit of interlinks (ϕ) a) Largest Mutually Connected Component (*LMCC*) as a function of the removed nodes (P) b) number of interlinks as a function of ϕ.

5.4(a) depicts that for a given ϕ the *LMCC* first decreases almost linearly with the increase of the fraction of removed nodes ($P \leq 35\%$). Later, the *LMCC* dramatically decreases until the networks are completely disconnected. Networks with the highest slope in their *LMCC* curves are those that have less ϕ. This is because with the decrease of ϕ, nodes in the G_1 and G_2 networks are divided into more subsets (μ_1 and μ_2, respectively) which decreases the probability for interconnecting a large number of nodes. Consequently, a node has fewer interconnected nodes and its failure probability is increased thanks to the failures of its interconnected nodes.

Also note that in Fig. 5.4(a) there is a zone ($P \leq 20\%$) in which the robustness of interdependent networks for a given ϕ is similar to the robustness reached by a network modeled according to [120] with $r = 0.2$ and without limiting the number of interlinks (G_{RG}). Moreover, in this zone all networks exhibit a high level of robustness against cascading failures ($LMCC > 0.8$). For example, when 20% of the nodes are removed from G_1 and after the cascading failure process, $LMCC = 0.89$ for $\phi = 100\%$ and 0.81 for $\phi = 10\%$. However, for $P > 20\%$, there are more differences between the *LMCC* values reached by the networks with $\phi \leq 25\%$ and the network G_{RG}. However, in the case of networks with $\phi \geq 50\%$, their robustness remains near to that achieved by G_{RG} until $P \leq 40\%$. Therefore, for some P values, our model is able to maintain the *LMCC* in values near those achieved by [120] when the number of interlinks is limited to a certain value of ϕ. In Table 5.4 is presented the numerical values for the average and standard deviation ($avg \pm StDev$) of the *LMCC* measurements in region-based interdependent networks (r = 0.2) versus variations in the limit of interlinks (ϕ). These values allow to determine

Table 5.3: *LMCC* measurements in region-based interdependent networks (r = 0.2) versus variations in the limit of interlinks (ϕ)

P [%]	$\phi = 10\%$	$\phi = 25\%$	$\phi = 50\%$	$\phi = 75\%$	$\phi = 100\%$
0	1 ± 0	1 ± 0	1 ± 0	1 ± 0	1 ± 0
5	0.963 ± 0.01	0.973 ± 0.009	0.981 ± 0.008	0.978 ± 0.007	0.982 ± 0.007
10	0.909 ± 0.016	0.939 ± 0.01	0.944 ± 0.013	0.949 ± 0.009	0.954 ± 0.01
15	0.862 ± 0.016	0.9 ± 0.014	0.908 ± 0.01	0.912 ± 0.015	0.923 ± 0.009
20	0.81 ± 0.019	0.835 ± 0.02	0.867 ± 0.013	0.875 ± 0.009	0.894 ± 0.008
25	0.761 ± 0.013	0.765 ± 0.024	0.827 ± 0.013	0.84 ± 0.012	0.864 ± 0.011
30	0.709 ± 0.02	0.695 ± 0.016	0.781 ± 0.016	0.781 ± 0.02	0.828 ± 0.012
35	0.637 ± 0.028	0.63 ± 0.024	0.72 ± 0.021	0.714 ± 0.024	0.785 ± 0.015
40	0.537 ± 0.044	0.532 ± 0.037	0.633 ± 0.039	0.632 ± 0.03	0.725 ± 0.03
45	0.354 ± 0.054	0.387 ± 0.051	0.519 ± 0.032	0.532 ± 0.044	0.645 ± 0.023
50	0.226 ± 0.03	0.244 ± 0.033	0.332 ± 0.043	0.394 ± 0.047	0.48 ± 0.041
55	0.14 ± 0.023	0.122 ± 0.031	0.235 ± 0.017	0.244 ± 0.05	0.374 ± 0.026
60	0.09 ± 0.016	0.082 ± 0.01	0.167 ± 0.033	0.136 ± 0.024	0.283 ± 0.041
65	0.047 ± 0.017	0.051 ± 0.014	0.092 ± 0.013	0.065 ± 0.024	0.168 ± 0.026
70	0.012 ± 0.006	0.013 ± 0.013	0.065 ± 0.01	0.023 ± 0.006	0.11 ± 0.018

confidence intervals from the *LMCC* measurements in the 100 interdependent networks.

On other hand, as can be seen in Fig. 5.4(b), the number of interlinks is under the maximum number of interlinks reached by the G_{RG} network for $\phi < 100\%$ (compare the dashed line G_{RG} and the blue bars G). This result is due to the strategy proposed in this chapter whereby the nodes in the G_1 and G_2 networks are divided into subsets, with a maximum number of nodes η_1 and η_2, respectively. Thus, our new region-based interconnection model guarantees that the number of interlinks in region-based interdependent networks is maintained below the limit ϕ. For instance, when $\phi = 75\%$, the maximum number of interlinks in the interdependent networks is 159. Although this value is not exactly 75% of the maximum number of interlinks, it is below the limit of interlinks considered to be a design constraint.

5.4.2.2 Scenario 2: Robustness analysis in region-based interdependent networks against variations in radius (r)

In this scenario, the interdependent telecommunication networks are the result of interconnecting the G_1 and G_2 networks by limiting the interlinks (ϕ) to 25% and varying the radius (r). The Largest Mutually Connected Component (*LMCC*) as a function of the

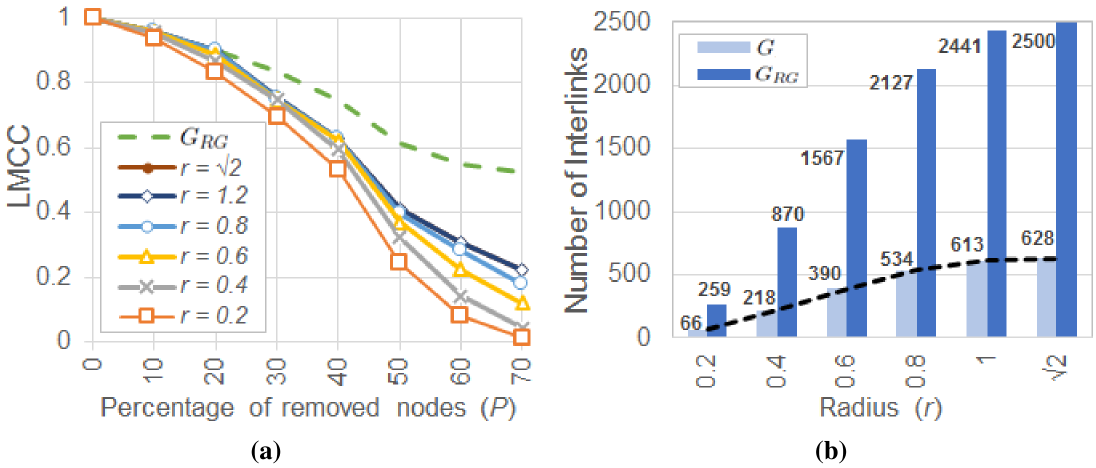


Figure 5.5: Robustness analysis in region-based interdependent networks (ϕ = 25%) versus variations in radius (r) a) Largest Mutually Connected Component (*LMCC*) as a function of removed nodes (P) b) number of interlinks as a function of r.

fraction of removed nodes from the G_1 network is shown in Fig. 5.5(a). Although the number of interlinks is limited to 25%, Fig.5.5(a) shows that region-based interdependent networks better resist cascading failures because of a major number of interlinks when the r is large. This result is to be expected as the nodes in the G_1 and G_2 networks tend to be more probable to interconnect to a greater number of nodes as a wide geographical area is defined by a larger radius r. For example, when 20% of the nodes are removed from G_1 and after the cascading failure process, $LMCC = 0.90$ for $r = 1.2$ and 0.83 for $r = 0.2$.

Additionally, Fig. 5.5(a) depicts a zone ($P \leq 20\%$) in which the robustness of region-based interdependent networks for a given radius r remains near to the robustness of a network modeled according to [120] where $r = \sqrt{2}$ and the number of interlinks is not limited (G_{RG}). In this zone, all region-based interdependent networks have the $LMCC > 0.8$. As the percentage of removed nodes in G_1 increases, the networks modeled with our new proposal maintain similar robustness levels until $P \leq 40\%$. Consequently, limiting the number of interlinks to a certain percentage ϕ tends to control interlink allocation against increases in radius r. Thus, our proposal based on subsets is effective in limiting the number of interlinks in region-based interdependent networks. Table 5.4 shows the numerical values for the average and standard deviation ($avg \pm StDev$) of the *LMCC* measurements in region-based interdependent networks (ϕ = 25%) versus variations in radius (r). With these values it is possible to determine confidence intervals from the *LMCC* measurements in the 100 interdependent networks.

Regarding the number of interlinks, Fig. 5.5(b) shows that for a given radius r our model generates interdependent networks where the interlinks are around 25% of the

Table 5.4: *LMCC* measurements in region-based interdependent networks (ϕ = 25%) versus variations in radius (r)

P [%]	$r = 0.2$	$r = 0.4$	$r = 0.6$	$r = 0.8$	$r = 1$	$r = \sqrt{2}$
0	1 ± 0	1 ± 0	1 ± 0	1 ± 0	1 ± 0	1 ± 0
5	0.973 ± 0.019	0.984 ± 0.007	0.984 ± 0.004	0.985 ± 0.003	0.985 ± 0.003	0.985 ± 0.003
10	0.939 ± 0.025	0.957 ± 0.011	0.959 ± 0.005	0.96 ± 0.004	0.96 ± 0.004	0.96 ± 0.004
15	0.9 ± 0.033	0.924 ± 0.014	0.93 ± 0.009	0.933 ± 0.005	0.934 ± 0.005	0.934 ± 0.005
20	0.835 ± 0.036	0.868 ± 0.022	0.886 ± 0.016	0.899 ± 0.01	0.903 ± 0.006	0.903 ± 0.006
25	0.765 ± 0.038	0.781 ± 0.022	0.795 ± 0.022	0.811 ± 0.018	0.82 ± 0.013	0.821 ± 0.011
30	0.695 ± 0.032	0.719 ± 0.017	0.718 ± 0.017	0.718 ± 0.017	0.718 ± 0.017	0.718 ± 0.017
35	0.63 ± 0.056	0.67 ± 0.028	0.678 ± 0.03	0.68 ± 0.03	0.68 ± 0.03	0.68 ± 0.03
40	0.532 ± 0.078	0.596 ± 0.046	0.623 ± 0.043	0.629 ± 0.044	0.629 ± 0.044	0.629 ± 0.044
45	0.387 ± 0.132	0.47 ± 0.1	0.526 ± 0.073	0.546 ± 0.057	0.553 ± 0.052	0.556 ± 0.052
50	0.244 ± 0.139	0.322 ± 0.11	0.369 ± 0.082	0.396 ± 0.06	0.408 ± 0.055	0.412 ± 0.055
55	0.122 ± 0.126	0.207 ± 0.1	0.275 ± 0.068	0.313 ± 0.042	0.326 ± 0.031	0.33 ± 0.028
60	0.082 ± 0.101	0.141 ± 0.098	0.223 ± 0.079	0.281 ± 0.045	0.303 ± 0.025	0.308 ± 0.018
65	0.051 ± 0.081	0.098 ± 0.077	0.191 ± 0.074	0.251 ± 0.054	0.282 ± 0.032	0.291 ± 0.025
70	0.013 ± 0.026	0.043 ± 0.049	0.121 ± 0.071	0.18 ± 0.061	0.213 ± 0.06	0.224 ± 0.055

maximum reached by each network G_{RG} (compare light blue and dark blue bars).The reason is because, independent of the selected radius (r), the model proposed in this chapter restricts the number of nodes that a node in the G_1 and G_2 networks can interconnect with to η_1 and η_2, respectively. For example, when $r = 0.6$, the maximum number of interlinks in the interdependent networks is 390, and the number of interlinks per node is 4 on average. Consequently, for some P values our model yields promising results for maintaining network robustness under cascading failures by reducing the number of interlinks.

5.5 Discussion and lessons learned

The interconnection strategy proposed in this chapter has proven to be effective in guaranteeing the number of interlinks in region-based interdependent networks is maintained under a certain limit ϕ. This is due to the fact for a given ϕ the nodes to be interconnected have been divided into subsets (μ_1, μ_2), each with a maximum number of nodes (η_1, η_2). Results indicate that in some scenarios ($P \leq 20\%$) the robustness for a given ϕ has been maintained at levels close to those reached by [120] ($LMCC \geq 0.80$).

This is a relevant outcome because compared to the critical threshold at which *LMCC* equals zero, quantifying the impact of a small percentage of node failures (P) is essential for network providers to prevent networks from collapsing.

The two scenarios that have been analyzed in this chapter represent some situations in which the model proposed can be applied by network providers. Results have shown the robustness behaviour for region-based interdependent networks under cascading failures. In the first case, by limiting the coverage area to a certain radius r and varying the number of interlinks (ϕ), a region-based interdependent networks is more robust against cascading failures when ϕ is increased. Meanwhile, in the second case, by limiting the number of interlinks to a certain ϕ and varying the radius r, the robustness increases for large values of r. In both cases, the results are because with the increase in the number of interlinks, a node tends to be less likely to fail from the failures of its interconnection nodes.

Chapter 6

Conclusions and future work

This chapter summarizes the main contributions of this doctoral dissertation, discusses the main issues and proposes the research lines for future work.

6.1 Summary and conclusions

- In Chapter 2, a robustness analysis of 15 real telecommunication networks under multiple failure scenarios (random and targeted attacks) was carried out. Through this analysis the common topological properties that can be used to group networks with similar robustness behavior were identified. Results have shown that the subset of real telecommunication networks more robust under targeted attacks have high values of average nodal degree ($\langle k \rangle$), low values of average shortest path length ($\langle l \rangle$) and diameter (D), while the subset of the least robust networks have the opposite results for $\langle k \rangle$, $\langle l \rangle$ and D. Similar to previous studies, for disassortative networks ($r < 0$) simultaneous targeted attacks by nodal degree centrality is the most effective method of degrading a network. However, we have also demonstrated that in sequential targeted attacks by nodal betweenness centrality, assortative networks ($r > 0$) are more vulnerable.

- Chapter 3 analyzed the performance of interdependency matrices in mitigating the propagation of targeted attacks in interdependent networks; specifically, the interconnection of two telecommunication networks, and a power grid connected to a telecommunications network. Through this analysis, novel methods to interconnect different interdependent networks in order to improve their robustness levels under target attacks have been presented. The interlink patterns are based on the vulnerability of nodes in the case of the most dangerous targeted attack for each of these networks. To achieve the least impact on one network when the most dangerous targeted attack is launched on the interconnected network, it is recommended to interconnect the two networks using the low centrality interdependency matrix (B_{LC}). Furthermore, interconnecting networks via high centrality interdependency matrix (B_{HC}) or random interdependency matrix (B_{RA}) is not recommended because of high impact targeted attacks have on networks. These results may help network administrators to identify the vulnerabilities of interdependent networks in order to plan and design more robust critical infrastructures.

- The scenarios studied in Chapter 3 yield interesting insights with regard to the propagation of targeted attacks in the interdependent networks. An interesting result is when the two networks are interconnected by a link model based on the B_{HC} matrix, a simultaneous targeted attack based on degree centrality on the power grid causes exactly the same damage to the telecommunications network as a simultaneous targeted attack based on betweenness centrality in a single network scenario. However, when the two infrastructures are interconnected via the B_{RA} matrix, a targeted attack on one of the networks propagates randomly in the other network. Whereas in the case of interconnection of two telecommunication networks by a B_{HC} matrix, the impact of a sequential targeted attack by betweeneess centrality in one of the networks generates an effect similar to a simultaneous targeted attack by betweeneess centrality in the other.

- In Chapter 4, a Software Defined Network (SDN) was considered as a multilayer telecommunication network. Through this approach, a robust design of SDN architecture to maintain an acceptable level of service in the face of targeted attacks has been presented. This new proposal has been focused on identifying exactly what the critical parts of the physical network are to find the best controller placements. By comparing the robustness of the SDN network resulting from our proposal with the robustness of two SDN topologies generated in previous works, our proposal has shown a better performance in the case of targeted attacks. These results have shown the importance of identifying the critical parts of networks in order to design more robust networks and mitigate the impact targeted attacks in SDN have.

- In Chapter 5, an enhanced interconnection model in region-based interdependent networks was proposed. In contrast to previous work, a new strategy based on subsets of nodes has been proposed to limit the number of interlinks in interdependent networks. The proposed region-based interconnection model has considered a percentage to limit the number of interlinks (ϕ) as a new key factor for interconnecting two geographically distributed networks. Moreover, the impact limiting the number of interlinks has on the robustness of region-based interdependent networks against cascading failures has been evaluated. Results have shown that for a given radius r, an interdependent network is more robust against cascading failures when ϕ is increased. Furthermore, for a given ϕ, a region-based interdependent network is more robust for large values of r. These results are due to the nodes have more interconnected nodes that reduce their probability to fail in a cascading failure process.

6.2 Future work

There are several research lines for future work as a result of this thesis:

- A more in-depth study focused on the relationship between robustness metrics under multiple failure scenarios. This would allow to identify those properties of the networks which must be strengthened to maintain desirable network robustness to be identified.

- The most important nodes in the power grid can be identified and ranked based on their electrical properties that lead to large-scale failures. Then, their network robustness can be evaluated based on this new metric. Research would also study other strategies for mitigating the impacts of targeted attacks on the robustness of interdependent networks.

- In the design of SDN topologies, the geographical placement of nodes and the physical distance between them can be taken into account to distribute the controller placements over the network. Thus, the controller load and the physical distance controller-switch can be reduced. Furthermore, *Algorithm 1* can be analyzed in others scenarios where finding the best locations in a network is a key design aspect to improving the network robustness. For example data centers placement or hierarchical controller placement.

- The proposed region-based interconnection model can be studied in other interdependent networks and validated with real-world data. Moreover, an in-depth cost-benefit analysis of limiting the number of interlinks in region-based interdependent networks can be carried out.

- Optimization strategies to limit the number of interlinks can be considered in order to interconnect two geographical networks and maximize network robustness. Additionally, the heuristic algorithm (*Algorithm 2*) presented in this thesis can be improved by including other constraints such as the cost and capacity of interlinks.

Bibliography

[1] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. "Identifying, Understanding, and Analyzing Critical Infrastructure Dependencies". In: *IEEE Control Systems Magazine* 21.6 (2001), pp. 11–23.

[2] J. P. G. Sterbenz et al. "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines". In: *Computer Networks* 54.8 (2010), 1245–1265.

[3] W. Ellens. "Effective Resistance and Other Graph Measures for Network Robustness". MA thesis. Leiden, The Netherlands: Mathematical Institute, Leiden Universty, Apr. 2011.

[4] S. Neumayer and E. Modiano. "Network reliability under geographically correlated line and disk failure models". In: *Computer Networks* 94 (2016), 14–28.

[5] D. Talbot. *Massive Internet outage points to flaws in policy and technology*. `https://www.technologyreview.com/s/530431/massive-internet-outage-points-to-flaws-in-policy-and-technology/`. [Online; accessed 19-July-2015]. 2014.

[6] J. R. Minkel. *The 2003 Northeast Blackout–Five Years Later*. `https://www.scientificamerican.com/article/2003-blackout-five-years-later/`. [Online; accessed 23-July-2017]. 2008.

[7] M. Ouyang. "Review on modeling and simulation of interdependent critical infrastructure systems". In: *Reliability Engineering and System Safety* 121 (2014), 43–60.

[8] M. Manzano. "New Robustness Evaluation Mechanisms for Complex Networks". PhD thesis. Girona, Spain: Dept. of Arch. and Comp. Tech., University of Girona, Nov. 2014.

[9] P. van Mieghem. “Robustness of Large Networks”. In: *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*. Waikoloa, Hawaii, Oct. 2005, pp. 2372–2377.

[10] M. Manzano, J. L. Marzo, E. Calle, and A. Manolova. “Robustness analysis of real network topologies under multiple failure scenarios”. In: *Proceedings of the 17th European Conference on Networks and Optical Communications (NOC 2012)*. Vilanova i la Geltru, Spain, July 2012, pp. 1–6.

[11] E. V. der Meer. *Comparing Measures of Network Robustness*. Research Paper Business Analytics. Amsterdam, The Netherlands: Faculty of Sciences, VU University Amsterdam. June 2010.

[12] A. Urra. “Multi-Layer Survivability: Routing Schemes for GMPLS-based Networks”. PhD thesis. Girona, Spain: Dept. of Arch. and Comp. Tech., University of Girona, July 2006.

[13] J. Segovia. “Robustness against Large-Scale Failures in Communications Networks”. PhD thesis. Girona, Spain: Dept. of Arch. and Comp. Tech., University of Girona, Dec. 2011.

[14] *RoGER Project: Robustness against Large-Scale Failures in Interdomain routing (TEC 2012-32336)*. `https://bcds.udg.edu/index.php/component/bcds/?view=projects&Itemid=111`. 2015.

[15] J. Rak et al. “Future research directions in design of reliable communication systems”. In: *Telecommunication Systems* 60.4 (2015), pp. 423–450.

[16] S. Buldyrev, R. Parshani, H. S. G. Paul, and S. Havlin. “Catastrophic cascade of failures in interdependent networks”. In: *Nature* 464.7291 (Apr. 2010), pp. 1025–1028.

[17] A. Bashan, Y. Berezin, S. V. Buldyrev, and S. Havlin. “The extreme vulnerability of interdependent spatially embedded networks”. In: *Nature Physics* 9.1 (2013), pp. 667–672.

[18] 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”. In: *Physical Review Letters* 105.4 (2010), p. 048701.

[19] D. Zhou, H. E. Stanley, G. D’Agostino, and A. Scala. “Assortativity decreases the robustness of interdependent networks”. In: *Physical Review E* 86.6 (2012), p. 066103.

[20] M. Parandehgheibi and E. Modiano. “Robustness of interdependent networks: The case of communications networks and the power grid”. In: *Proceeding of the 2013 IEEE Global Communications Conference (GLOBECOM)*. Atlanta, GA, USA, Dec. 2013, pp. 2164–2169.

[21] M. A. D. Muroa et al. “Recovery of Interdependent Networks”. In: *Scientific Reports* 6 (2016), p. 22834.

[22] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley. “Cascade of failures in coupled network systems with multiple support-dependence relations”. In: *Physical Review E* 83.3 (2011), p. 036116.

[23] Y. Hu, B. Ksherim, R. Cohen, and S. Havlin. “Percolation in interdependent and interconnected networks: Abrupt change from second- to first-order transitions”. In: *Physical Review E* 84.6 (2010), p. 066116.

[24] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley. “Robustness of a Network of Networks”. In: *Physical Review Letters* 107.19 (2011), p. 195701.

[25] S. Wang, L. Hong, and X. Chen. “Vulnerability analysis of interdependent infrastructure systems: A methodological framework”. In: *Physica A: Statistical Mechanics and its Applications* 391.11 (2012), 33233335.

[26] P. Zhang et al. “The robustness of interdependent transportation networks under targeted attack”. In: *EPL (Europhysics Letters)* 103.6 (Oct. 2013), p. 68005.

[27] G. Dong et al. “Robustness of network of networks under targeted attack”. In: *Physical Review E* 87.5 (2013), p. 052804.

[28] J. Jiang, W. Li, and X. Cai. “The effect of interdependence on the percolation of interdependent networks”. In: *Physica A: Statistical Mechanics and its Applications* 410.Supplement C (2014), pp. 573 –581.

[29] J. Wang, C. Jiang, and J. Qian. “Robustness of interdependent networks with different link patterns against cascading failures”. In: *Physica A: Statistical Mechanics and its Applications* 393 (2014), 535–541.

[30] F. Tan, Y. Xia, W. Zhang, and X. Jin. “Cascading failures of loads in interconnected networks under intentional attack”. In: *EPL (Europhysics Letters)* 102.2 (2013), p. 28009.

[31] J. Martín-Hernández, H. Wang, P. van Mieghem, and G. DAgostino. “Algebraic connectivity of interdependent networks”. In: *Physica A: Statistical Mechanics and its Applications* 404 (June 2014), 92–105.

[32] M. Tian et al. “Cascading failures of interdependent modular scale-free networks with different coupling preferences”. In: *EPL (Europhysics Letters)* 111.1 (2015), p. 18007.

[33] Y. Cheng and J. P. G. Sterbenz. “Critical region identification and geodiverse routing protocol under massive challenges”. In: *Proceedings of the 2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*. Munich, Germany, Oct. 2015, pp. 14–20.

[34] G. Golshan and Z. Zhang. “The effect of different couplings on mitigating failure cascades in interdependent networks”. In: *Proceedings of the 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. Hong Kong, China, Aug. 2015, 677–682.

[35] X. Li, H. Wu, C. Scoglio, and D. Gruenbacher. “Robust allocation of weighted dependency links in cyberphysical networks”. In: *Physica A: Statistical Mechanics and its Applications* 433 (2015), 316–327.

[36] X. Ji et al. “Improving interdependent networks robustness by adding connectivity links”. In: *Physica A: Statistical Mechanics and its Applications* 444 (2016), 9–19.

[37] W. K. Chai, V. Kyritsis, K. V. Katsaros, and G. Pavlou. “Resilience of interdependent communication and power distribution networks against cascading failures”. In: *Proceedings of the 2016 IFIP Networking Conference (IFIP Networking) and Workshops*. Vienna, Austria, May 2016, pp. 37–45.

[38] 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 on Signal-Image Technology Internet-Based Systems*. Kyoto, Japan, Dec. 2013, pp. 619–625.

[39] *GIROS Project: Geographically-constrained and Interdependent networks: RObustness indicatorS (TEC 2015-66412-R))*. 2016.

[40] X. Wang, E. Pournaras, R. E. Kooij, and P. van Mieghem. “Improving robustness of complex networks via the effective graph resistance”. In: *The European Physical Journal B* 87.9 (Sept. 2014), p. 221.

[41] A. Jamaković. “Characterization of Complex Networks: Application to Robustness Analysis”. PhD thesis. Delft, The Netherlands: Fac. Elect. Eng., Math. and Comp. Sci., Technische Universiteit Delft, Oct. 2008.

[42] S. N. Dorogovtsev and J. F. F. Mendes. “Evolution of networks”. In: *Advances in Physics* 51.4 (2007), pp. 1079–1187.

[43] S. Boccaletti et al. “Complex networks: structure and dynamics”. In: *Physics Reports* 424.4–5 (2006), 175–308.

[44] L. da F. Costa, F. Rodrigues, G. Travieso, and P. V. Boas. “Characterization of complex networks: A survey of measurements”. In: *Advances in Physics* 56.1 (2007), pp. 167–242.

[45] T. Lewis. *Network Science: Theory and Applications*. Hoboken, New Jersey: John Wiley and Sons, 2009.

[46] P. Erdős and A. Rényi. “On the evolution of random graphs”. In: *Publication of the Mathematical Institute of the Hungarian Academy of Sciences* 5 (1960), 17–61.

[47] B. Bollobás. *Random graphs*. Cambridge: Cambridge University Press, 2001.

[48] A. Jamaković and S. Uhlig. “Influence of the network structure on robustness”. In: *Proceedings of the 15th IEEE International Conference on Networks*. Adelaide, SA, Australia, Nov. 2007, pp. 278–283.

[49] D. Watts and S. Strogatz. “Collective dynamics of small-world networks”. In: *Nature* 393.6684 (1998), 440–442.

[50] A. L. Barabási and R. Albert. “Emergence of scaling in random networks”. In: *Science* 286 (1999), pp. 509–512.

[51] M. P. Damas, L. Markenzon, and N. M.M. D. Abreu. “New concepts and results on the average degree of a graph”. In: *Applicable Analysis and Discrete Mathematics* 1.1 (2007), pp. 284–292.

[52] P. Mahadevan et al. “The internet AS-level topology: three data sources and one definitive metric”. In: *ACM SIGCOMM Computer Communication Review* 36.1 (2006), 17–26.

[53] C. Shannon and D. Moore. “The spread of the witty worm”. In: *IEEE Security and Privacy* 2 (2004), 46–50.

[54] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang. “Attack robustness and centrality of complex networks”. In: *PLoS ONE* 8.4 (2013), e59613.

[55] J. Dong and S. Horvath. “Understanding Network Concepts in Modules”. In: *BMC Systems Biology* 1.1 (2007), pp. 1–24.

[56] V. Latora and M. Marchiori. “A measure of centrality based on network efficiency”. In: *New Journal of Physics* 9.6 (2007), p. 188.

[57] R. Diestel. *Graph theory, volume 173 of Graduate Texts in Mathematics*. Heidelberg: Springer-Verlag, 2010.

[58] J. Wang, H. Mo, F. Wang, and F. Jin. “Exploring the network structure and nodal centrality of Chinas air transport network: A complex network approach”. In: *Journal of Transport Geography* 19.4 (2011), pp. 712–721.

[59] A. H. Dekker and B. Colbert. “The symmetry ratio of a network”. In: *Proceedings of the 2005 Australasian symposium on Theory of computing - Volume 41*. Newcastle, Australia, Jan. 2005, 13–20.

[60] Y. Wang, C. Wang, C. Faloutsos, and D. Chakrabarti. “Epidemic spreading in real networks: an eigenvalue viewpoint”. In: *Proceedings of the 22nd International Symposium on Reliable Distributed Systems*. Florence, Italy, Oct. 2003, pp. 25–34.

[61] M. Fiedler. “Algebraic connectivity of graphs”. In: *Czechoslovak Mathematical Journal* 23.98 (1973), pp. 298–305.

[62] J. Wu, M. Barahona, Y. J. Tan, and H. Z. Deng. “Spectral Measure of Structural Robustness in Complex Networks”. In: *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 41.6 (2011), pp. 1244–1252.

[63] X.-K. Zhang et al. “Structural robustness of weighted complex networks based on natural connectivity”. In: *Chinese Physics Letters* 30.10 (2013), p. 108901.

[64] W. Ellens et al. “Effective graph resistance”. In: *Linear Algebra and its Applications* 10.435 (2011), pp. 2491–2506.

[65] R. Grone, R. Merris, and V. S. Sunder. “The laplacian spectrum of a graph”. In: *SIAM Journal on Matrix Analysis and Applications* 11.2 (1990), pp. 218–238.

[66] J. P. Rohrer and J. P. G. Sterbenz. “Predicting topology survivability using path diversity”. In: *Proceedings of the 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. Budapest, Hungary, Oct. 2011, pp. 1–7.

[67] D. Fay et al. “Weighted spectral distribution for internet topology analysis: theory and applications”. In: *IEEE/ACM Transactions on Networking* 18.1 (2010), pp. 164–176.

[68] X. Long, D. Tipper, and T. Gomes. “Measuring the survivability of networks to geographic correlated failures”. In: *Optical Switching and Networking* 14.2 (2014), pp. 117–133.

[69] C. Li et al. “The correlation of metrics in complex networks with applications in functional brain networks”. In: *Journal of Statistical Mechanics: Theory and Experiment* 115 (2011), p. 11018.

[70] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin. "Resilience of the Internet to random breakdowns". In: *Physical Review Letters* 85.21 (2000), pp. 4626–4628.

[71] J. S. Baras and P. Hovareshti. "Efficient and robust communication topologies for distributed decision making in networked systems". In: *Proceedings of the 48th IEEE Conference on Decision and Control (CDC)*. Shanghai, China, Dec. 2013, pp. 3751–3756.

[72] C. Godsil and G. Royle. *Algebraic graph theory*. New York: Springer Graduate texts in Mathematics, 2009.

[73] S. Neumayer and E. Modiano. "Network reliability with geographically correlated failures". In: *Proceedings of the 2010 IEEE INFOCOM*. San Diego, CA, USA, May 2010, pp. 1–9.

[74] M. Youssef, R. E. Kooij, and C. Scoglio. "Viral conductance: quantifying the robustness of networks with respect to spread of epidemics". In: *Journal of Computational Science* 2.3 (2011), pp. 286–298.

[75] L. C. Freeman. "A set of measures of centrality based on betweenness". In: *Sociometry* 40.1 (1977), pp. 35–41.

[76] L. C. Freeman. "Centrality in social networks conceptual clarification". In: *Social Networks* 1.3 (1978), pp. 215–239.

[77] L. Tang and H. Liu. *Community Detection and Mining in Social Media*. San Rafael: Morgan and Claypool, 2010.

[78] M. E. J. Newman. "Mathematics of networks," in: *The New Palgrave Encyclopedia of Economics*. Ed. by L. E. Blume and S. N. Durlauf. Basingstoke: Palgrave Macmillan, 2008, pp. 1–12.

[79] M. Kitsak et al. "Identification of influential spreaders in complex networks". In: *Nature Physics* 6.11 (2010), pp. 888–893.

[80] M. Manzano, E. Calle, and D. Harle. "Quantitative and qualitative network robustness analysis under different multiple failure scenarios". In: *Proceedings of the 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT 2011)*. Budapest, Hungary, Oct. 2011, pp. 1–7.

[81] A. Sydney, C. Scoglio, M. Youssef, and P. Schumm. "Characterising the robustness of complex networks". In: *Int. J. Internet Technology and Secured Transactions* 2.3/4 (Dec. 2010), 291–320.

[82] P. van Mieghem et al. *A Framework for Computing Topological Network Robustness*. Technical Report 20101218, Networks Architectures and Services, Delft University of Technology. Dec. 2010.

[83] M. Manzano et al. “Endurance: a new robustness measure for complex networks under multiple failure scenarios”. In: *Computer Networks* 57.17 (Dec. 2013), pp. 3641–3653.

[84] M. Manzano et al. “Robustness surfaces of complex networks”. In: *Scientific Reports* 4 (Sept. 2014), p. 6133.

[85] P. Holme, B. Kim, C. Yoon, and S. Han. “Attack vulnerability of complex networks”. In: *Physical Review E* 65 (2002), p. 056109.

[86] M. Bellingeri, D. Cassi, and S. Vincenzi. “Efficiency of attack strategies on complex model and real-world networks”. In: *Physica A: Statistical Mechanics and its Applications* 414 (2014), pp. 174 –180.

[87] J. Ripoll, M. Manzano, and E. Calle. “Spread of epidemic-like failures in telecommunication networks”. In: *Physica A: Statistical Mechanics and its Applications* 410 (2014), pp. 457–469.

[88] J. Wang. “Robustness of complex networks with the local protection strategy against cascading failures”. In: *Safety Science* 53 (2013), pp. 219–225.

[89] Y. Shang. “Shang, Robustness of scale-free networks under attack with tunable grey information”. In: *EPL (Europhysics Letters)* 95.2 (2011), p. 28005.

[90] S. Trajanovski, J. Martín-Hernández, W. Winterbach, and P. van Mieghem. “Robustness envelopes of networks”. In: *Journal of Complex Networks* 1.1 (June 2013), 44–62.

[91] T. Nie, Z. Guo, K. Zhao, and Z.-M. Lu. “New attack strategies for complex networks”. In: *Physica A: Statistical Mechanics and its Applications* 424 (2015), pp. 248–253.

[92] C. J. Colbourn. “Reliability Issues In Telecommunications Network Planning”. In: *Telecommunications Network Planning*. Ed. by B. Sansò and P. Soriano. Boston, MA: Springer US, 1999, pp. 135–146.

[93] L. K. Gallos et al. “Stability and Topology of Scale-Free Networks under Attack and Defense Strategies”. In: *Physical Review Letters* 94 (18 2005), p. 188701.

[94] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin. “Breakdown of the Internet under Intentional Attack”. In: *Physical Review Letters* 86.16 (2001), pp. 3682–3685.

[95] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts. “Network robustness and fragility: percolation on random graphs”. In: *Physical Review Letters* 85.25 (2000), pp. 5468–5471.

[96] R. Albert, H. Jeong, and A. L. Barabási. "Error and attack tolerance of complex networks". In: *Nature* 406 (2000), p. 378.

[97] D. Maniadakis, A. Balmpakakis, and D. Varoutas. "On the temporal evolution of backbone topological robustness". In: *Proceeding of the 18th European Conference on Networks and Optical Communications (NOC 2013)*. Graz, Austria, July 2013, pp. 129–136.

[98] H. Wang, J. Huang, X. Xu, and Y. Xiao. "Damage attack on complex networks". In: *Physica A: Statistical Mechanics and its Applications* 408 (2014), pp. 134–148.

[99] X. Long, D. Tipper, and T. Gomes. "Evaluating geographic topological vulnerabilities". In: *Proceedings of the 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. Almaty, Kazakhstan, Sept. 2013, pp. 54–61.

[100] J. P. G. Sterbenz et al. "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation". In: *Telecommunication Systems* 52.2 (2013), pp. 705–736.

[101] C. Scoglio et al. "Metrics for Robustness in Complex Networks". In: *Proceedings of the Complex Systems Conference*. Irvine, CA, USA, Nov. 2008.

[102] A. Sydney, C. Scoglio, P. Schumm, and R. E. Kooij. "Elasticity: topological characterization of robustness in complex networks". In: *Proceedings of the 3rd international conference on bio-inspired models of network, information, and computing systems (BIONETICS 2008)*. Hyogo, Japan, Nov. 2008, pp. 1–8.

[103] P. Mahadevan et al. *Lessons from Three Views of the Internet Topology: Technical Report*. Technical Report 200502, Cooperative Association for Internet Data Analysis (CAIDA). June 2005.

[104] E. K. Çetinkaya et al. "A comparative analysis of geometric graph models for modelling backbone networks". In: *Optical Switching and Networking* 14.Part 2 (2014), pp. 95–106.

[105] *The Internet Topology Zoo*. `http://www.topology-zoo.org`. [Online; accessed 29-Mar-2015]. 2013.

[106] *U-Topview Network Topology Tool*. `http://www.ittc.ku.edu/resilinets/maps`. [Online; accessed 3-Mar-2015]. 2010.

[107] J. Gao, X. Liu, D. Li, and S. Havlin. "Recent Progress on the Resilience of Complex Networks". In: *Energies* 8.10 (2015), pp. 12187–12210.

[108] G. Andersson and et. al. "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance". In: *IEEE Transactions on Power Systems* 20.4 (2005), pp. 1922–1928.

[109] L. Martins et al. "Interdependence between Power Grids and Communication Networks: A Resilience Perspective". In: *Proceedings of the 2017 13th International Conference on Design of Reliable Communication Networks (DRCN)*. Munich, Germany, Mar. 2017, 154–162.

[110] Y. Zhang, N. Yang, and U. Lall. "Modeling and simulation of the vulnerability of interdependent power-water infrastructure networks to cascading failures". In: *Journal of Systems Science and Systems Engineering* 25.1 (Mar. 2016), pp. 102–118.

[111] M. M. Danziger et al. "An Introduction to Interdependent Networks". In: *Nonlinear Dynamics of Electronic Systems*. Ed. by V. M. Mladenov and P. C. Ivanov. Cham: Springer, 2014, pp. 189–202.

[112] M. M. Danziger et al. "Vulnerability of Interdependent Networks and Networks of Networks". In: *Interconnected Networks*. Ed. by A. Garas. Cham: Springer International Publishing, 2016, pp. 79–99.

[113] M. Gong, L. Ma, Q. Cai, and L. Jiao. "Enhancing robustness of coupled networks under targeted recoveries". In: *Scientific Reports* 5 (2015), p. 8439.

[114] F. Radicchi and A. Arenas. "Abrupt transition in the structural formation of interconnected networks". In: *Nature Physics* 9.11 (2013), 717–720.

[115] S. Gomez et al. "Diffusion dynamics in multiplex networks". In: *Physical Review Letters* 110 (2013), p. 028701.

[116] F. Sahneh, C. Scoglio, and P. van Mieghem. "Exact coupling threshold for structural transition reveals diversified behaviors in interconnected networks". In: *Physical Review E: Statistical, Nonlinear and Soft Matter Physics* 92.4 (2015), p. 040801.

[117] I. Eusgeld, D. Henzi, and W. Kroger. *Comparative evaluation of modeling and simulation techniques for interdependent critical infrastructures*. Scientific report, ETH Zurich. June 2008.

[118] I. Eusgeld, C. Nan, and S. Dietz. "System-of systems approach for interdependent critical infrastructures". In: *Reliability Engineering and System Safety* 96 (2011), pp. 679–686.

[119] P. Yontay and R. Pan. “A computational Bayesian approach to dependency assessment in system reliability”. In: *Reliability Engineering and System Safety* 152 (2016), pp. 104–114.

[120] X. Wang, R. E. Kooij, and P. van Mieghem. “Modeling region-based interconnection for interdependent networks”. In: *Phys. Rev. E.* 94 (2016), p. 042315.

[121] E. K. Çetinkaya et al. “Multilevel resilience analysis of transportation and communication networks”. In: *Telecommunication Systems* 60.4 (2014), 515–537.

[122] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin. “Networks formed from interdependent networks”. In: *Nature Physics* 8 (2012), pp. 40–48.

[123] 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”. In: *Physical Review E* 85.6 (2012), p. 066134.

[124] D. Y. Kenett et al. “Network of Interdependent Networks: Overview of Theory and Applications”. In: *Networks of Networks: The Last Frontier of Complexity*. Ed. by G. D’Agostino and A. Scala. Cham: Springer International Publishing, 2014, pp. 3–36.

[125] G. Dong et al. “Robustness of n interdependent networks with partial support-dependence relationship”. In: *EPL (Europhysics Letters)* 102.6 (2013), p. 68004.

[126] X. Huang et al. “Robustness of interdependent networks under targeted attack”. In: *Physical Review E* 83.6 (June 2011), p. 065101.

[127] G. Dong et al. “Percolation of partially interdependent networks under targeted attack”. In: *Physical Review E* 85.1 (2012), p. 016112.

[128] J. Wang et al. “Research on the Robustness of Interdependent Networks under Localized Attack”. In: *Applied Sciences* 7 (2017), p. 597.

[129] B. Wu, A. Tang, and J. Wu. “Modeling cascading failures in interdependent infrastructures under terrorist attacks”. In: *Reliability Engineering System Safety* 147 (2016), pp. 1–8.

[130] G. Fu, R. Dawson, M. Khoury, and S. Bullock. “Interdependent networks: vulnerability analysis and strategies to limit cascading failure”. In: *The European Physical Journal B* 87.7 (2014), p. 148.

[131] O. Yagan, D. Qian, J. Zhang, and D. Cochran. "Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness". In: *IEEE Transactions on Parallel and Distributed Systems* 23.9 (2012), 1708–1720.

[132] S. Tauch, W. Liu, and R. Pears. "Evaluating the cascade effect in interdependent networks via algebraic connectivity". In: *International Journal of Information, Communication Technology and Applications* 1.1 (Mar. 2015), 55–68.

[133] S. Tauch, W. Liu, and R. Pears. "Measuring cascade effects in interdependent networks by using effective graph resistance". In: *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. Hong Kong, China, Aug. 2015, 683–688.

[134] E. M. Shahrivar, M. Pirani, and S. Sundaram. "Robustness and Algebraic Connectivity of Random Interdependent Networks". In: *IFAC-PapersOnLine* 48.22 (2015). 5th IFAC Workshop on Distributed Estimation and Control in Networked Systems NecSys 2015, pp. 252 –257.

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

[136] S. Shao, X. Huang, H. E. Stanley, and S. Havlin. "Percolation of localized attack on complex networks". In: *New Journal of Physics* 17.2 (2015), p. 023049.

[137] Y. Berezin et al. "Localized attacks on spatially embedded networks with dependencies". In: *Scientific Reports* 5 (2015), p. 8934.

[138] M. Ouyang. "Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks". In: *Reliability Engineering and System Safety* 154 (2016), pp. 106–116.

[139] R. Parshani et al. "Inter-similarity between coupled networks". In: *EPL (Europhysics Letters)* 92.6 (2010), p. 68002.

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

[141] S. Fortunato. "Community detection in graphs". In: *Physics Reports* 486.3 (2010), pp. 75 –174.

[142] M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee. "Disaster survivability in optical communication networks". In: *Computer Communications* 36.6 (2013), pp. 630 –644.

[143] *Power Systems Test Case Archive*. `www2.ee.washington.edu/research/pstca`. [Online; accessed 15-Apr-2016]. 1999.

[144] Z. Wang and R. Thomas. "On bus type assignments in random topology power grid models". In: *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS)*. Kauai, HI, USA, Jan. 2015, 2671–2679.

[145] W. Peng, Z. Li, Y. Liu, and J. Su. "Assessing the vulnerability of network topologies under large-scale regional failures". In: *Journal of Communications and Networks* 14.4 (2012), 451–460.

[146] M. Manzano, K. Bilal, E. Calle, and S. Khan. "On the connectivity of data center networks". In: *IEEE Communications Letters* 17.11 (2013), 2172–2175.

[147] P. Hines and S. Talukdar. "Controlling cascading failures with cooperative autonomous agents". In: *International Journal on Critical Infrastructures* 3.1/2 (2007), pp. 192–220.

[148] T. Verma. "Vulnerability of Power Grids to Cascading Failures". MA thesis. Delft, The Netherlands: Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, June 2012.

[149] J.-P. Vasseur, M. Pickavet, and P. Demeester. *Network Recovery: Protection and Restoration of Optical, SONETSDH, IP, and MPLS*. San Francisco: Morgan Kaufmann Publishers, 2004.

[150] D. Kreutz et al. "Software-Defined Networking: A Comprehensive Survey". In: *Proceedings of the IEEE* 103.1 (2015), pp. 14–76.

[151] S. Scott-Hayward. "Design and deployment of secure, robust, and resilient SDN controllers". In: *Proceedings of the 1st IEEE Conference on Network Softwarization (NetSoft)*. London, UK, Sept. 2015, pp. 1–5.

[152] M. Guo and P. Bhattacharya. "Controller Placement for Improving Resilience of Software-Defined Networks". In: *Proceedings of the 4th International Conference on Networking and Distributed Computing*. Los Angeles, CA, USA, Dec. 2013, pp. 23–27.

[153] S. Lange et al. "Heuristic Approaches to the Controller Placement Problem in Large Scale SDN Networks". In: *IEEE Transactions on Network and Service Management* 12.1 (2015), pp. 4–17.

[154] M. Katta, H. Zhang, M. Freedman, and J. Rexford. "Ravana: Controller Fault-tolerance in Software-defined Networking". In: *Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research*. Santa Clara, CA, USA, June 2015, 4:1–4:12.

[155] Q. Yan and F. R. Yu. "Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing". In: *IEEE Communications Magazine* 53.4 (2015), pp. 52–59.

[156] B. Heller, R. Sherwood, and N. McKeown. "The Controller Placement Problem". In: *Proceedings of the 1st Workshop on Hot Topics in Software Defined Networks (HotSDN)*. Helsinki, Finland, Aug. 2012, pp. 7–12.

[157] M. F. Bari et al. "Dynamic Controller Provisioning in Software Defined Networks". In: *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*. Zurich, Switzerland, Oct. 2013, pp. 18–25.

[158] Y. Hu et al. "On the placement of controllers in software-defined networks". In: *The Journal of China Universities of Posts and Telecommunications* 19.2 (2012), 92–97.

[159] Y. Jiménez, C. Cervelló-Pastor, and A. J. García. "On the controller placement for designing a distributed SDN control layer". In: *Proceedings of the 2014 IFIP Networking Conference*. Trondheim, Norway, June 2014, pp. 1–9.

[160] F. J. Ros and P. M. Ruiz. "On reliable controller placements in Software-Defined Networks". In: *Computer Communications* 77.Supplement C (2016), 41–51.

[161] D. M. F. Mattos, O. C.M. B. Duarte, and G. Pujolle. "A Resilient Distributed Controller for Software Defined Networking". In: *Proceedings of the 2016 IEEE International Conference on Communications (ICC)*. Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[162] R. Goścień and K. Walkowiak. "A Resilient Distributed Controller for Software Defined Networking". In: *Proceedings of the 2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*. Munich, Germany, Oct. 2015, pp. 48–55.

[163] *Internet2*. `www.internet2.edu`. [Online; accessed 3-March-2016]. 2015.

[164] K. He et al. "Measuring control plane latency in SDN-enabled switches". In: *Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research*. Santa Clara, California, US, June 2015, pp. 1–6.

[165] M. Barthélemy. "Spatial networks". In: *Physics Reports* 499.1 (2011), pp. 1–101.

[166] D. Li, K. Kosmidis, A. Bunde, and S. Havlin. "Dimension of spatially embedded networks". In: *Nature Physics* 7 (6 2011), pp. 481–484.

[167] K. Kosmidis, S. Havlin, and A. Bunde. "Structural properties of spatially embedded networks". In: *EPL (Europhysics Letters)* 82 (4 2008), p. 48005.

[168] W. Li et al. “Cascading Failures in Interdependent Lattice Networks: The Critical Role of the Length of Dependency Links”. In: *Physical Review Letters* 108 (22 2012), p. 228702.

[169] A. Asztalos, S. Sreenivasan, B. K. Szymanski, and G. Korniss. “Cascading Failures in Spatially-Embedded Random Networks”. In: *PLOS ONE* 9.1 (2014), e84563.

[170] L. M. Shekhtman, Y. Berezin, M. M. Danziger., and S. Havlin. “Robustness of a network formed of spatially embedded networks”. In: *Physical Review E* 90 (1 2014), p. 012809.

[171] J. Zhang, E. Yeh, and E. Modiano. “Robustness of interdependent random geometric networks”. In: *Proceedings of the 2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. Monticello, IL, USA, Sept. 2016, pp. 172–179.

[172] J. Dall and M. Christensen. “Random geometric graphs”. In: *Physical Review E* 66 (1 2002), p. 016121.

[173] M. M. Danziger, L. M. Shekhtman, Y. Berezin, and S. Havlin. “The effect of spatiality on multiplex networks”. In: *EPL (Europhysics Letters)* 115 (3 2016), p. 36002.

[174] D. Vaknin, M. M. Danziger, and S. Havlin. “Spreading of localized attacks in spatial multiplex networks”. In: *New Journal of Physics* 19 (2017), p. 073037.

[175] F. Schweitzer et al. “Economic Networks: The New Challenges”. In: *Science* 325.5939 (2009), pp. 422–425.