UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

METHODS BASED ON INTERDEPENDENT NETWORKS TO ANALYZE THE ROBUSTNESS OF THE INTERNET

TESIS PARA OPTAR AL GRADO DE DOCTORA EN COMPUTACIÓN

IVANA FRANCISCA BACHMANN ESPINOZA

PROFESOR GUÍA:
BENJAMÍN BUSTOS CÁRDENAS

PROFESOR CO-GUÍA:
JAVIER BUSTOS JIMÉNEZ

MIEMBROS DE LA COMISIÓN:
SANDRA CÉSPEDES UMAÑA
MICHAEL DANZIGER
LUIS MATEU BRÛLÉ
WALTER WILLINGER

Este trabajo ha sido parcialmente financiado por NIC Chile Research Labs y CONICYT/ANID Doctorado Nacional 21170165

SANTIAGO DE CHILE
2022

Resumen

MÉTODOS BASADOS EN REDES INTERDEPENDIENTES PARA ANALIZAR LA ROBUSTEZ DE INTERNET

El Internet nos permite comunicarnos, acceder a educación online, comercio online, etc. Su relevancia se ha vuelto aún más evidente en los últimos tiempos, pues se ha visto la necesidad de depender más de comunicación y servicios online. Para garantizar su correcto funcionamiento durante eventos adversos, se debe estudiar y comprender la robustez de Internet. Hay una variedad de formas de estudiar la robustez de Internet dependiendo del área desde la cual se aborde. Aquí, este problema se aborda desde el área de redes complejas.

Esta tesis presenta y evalúa un nuevo modelo físico-lógico de redes interdependientes inspirado en el Internet actual. Este modelo considera una red lógica inspirada en la red lógica de Internet (red a nivel de Sistemas Autónomos), una red física inspirada en la red física de Internet (Backbone de Internet), y las interdependencias entre ambas. Se propone una medida de robustez para evaluar la robustez del modelo, y esta es usada para probar el efecto que diferentes tipos de ataques físicos pueden tener sobre el sistema. Además, se propone una forma novedosa de atacar redes complejas para representar mejor el efecto que catástrofes naturales, como terremotos, podrían tener sobre la robustez de Internet.

Los principales aportes de este trabajo de tesis son: (1) el desarrollo de una red interdependiente físico-lógica inspirada en el Internet y su caracterización bajo diferentes tipos de daño físico. (2) El hallazgo de "nodos puente" en la red lógica, su efecto sobre la robustez de redes interdependientes físico-lógicas y su relación con los hubs en Scale-Free networks. Los resultados muestran que encontrar y proteger nodos puente puede mejorar drásticamente la robustez de un sistema. (3) El análisis del efecto que tiene la adición de enlaces a la red física sobre la robustez del modelo de redes interdependientes presentado. (4) El desarrollo de una nueva forma de atacar redes complejas: Ataques localizados con fallas probabilísticas (LAPF por su sigla en inglés). Estos ataques dañan elementos de la red siguiendo una distribución de probabilidad F y pueden ser usados para modelar el daño causado por catástrofes naturales. En este trabajo se muestra cómo se pueden utilizar estos LAPF para modelar el daño causado por terremotos y estos ataques son probados sobre el modelo de red interdependiente físico-lógico propuesto.

Según el análisis presentado, al estudiar la robustez de redes interdependientes físico-lógicas como las presentadas en este trabajo, debemos prestar especial atención a la presencia de "nodos puente" ya que estos nodos se relacionan con eventos que pueden dañar gran parte del sistema, llegando incluso a producir un fallo total del sistema. Los resultados muestran que agregar más enlaces a la red física puede ser útil para reducir el impacto de los nodos de puente. Sin embargo, estos resultados también muestran que la adición de enlaces físicos no es suficiente y que agregar más enlaces de interdependencia espacialmente separados entre sí puede ser una mejor solución.

Abstract

The Internet allows us to communicate, access online education, commerce, etc. Its relevance has become even more apparent in recent times as we have seen the need to rely more on online communication and services. In order to ensure its proper functioning during adverse events we must study and understand the Internet's robustness. There are different ways to study this, depending on the field of study approaching the subject. Here, we use a complex networks approach.

In this work we present and evaluate a newly proposed physical-logical interdependent network model inspired by today's Internet. This model considers a logical network inspired by the Internet network (Autonomous System level network), a physical network inspired by the physical Internet network (Internet backbone), and the interactions and dependencies between both networks. We propose a robustness measure to assess the model's robustness, and use it to test the effect that different types of physical attacks can have over such a system. Furthermore, we propose a novel way to attack complex networks that could allow us to better represent the effect that natural catastrophes, such as earthquakes, could have over the Internet's robustness.

The main contributions of this thesis work are: (1) the development of a physical-logical interdependent network inspired by the Internet, and its characterization under different types of physical damage. (2) The finding of "bridge nodes" in the logical network, their effect on the overall robustness of the physical-logical interdependent networks tested, and their relation with hubs in Scale-Free networks. Our results show that finding and protecting bridge nodes can dramatically improve the robustness of a system. (3) The analysis of the effect that adding links to the physical network has over the robustness of the presented interdependent network model. (4) The development of a novel way to attack complex networks: Localized Attacks with Probabilistic Failures (LAPF). These attacks damage network elements following a probability distribution F, and can be used to model the damage caused by natural catastrophes. In this work we show how LAPF can be used to model the damage caused by earthquakes, and test these attacks over the physical-logical interdependent network model proposed.

Our analysis shows that when studying the robustness physical-logical interdependent networks such as the one presented here, we must pay especial attention to the presence of "bridge nodes" as these nodes are related to events that can damage a great part of the system, even resulting in total system failure. Our results show that adding more links to the physical network can be useful to reduce the impact of bridge nodes. However, these results also show that physical link addition is not enough and adding more interlinks far apart from each other may be a better solution.

Para quienes no pudieron acompañarme pero habrían querido estar aquí.

Acknowledgements

I want to start by thanking Felipe for *everything*. He listened to me over and over again whenever I needed to voice my thoughts in order to continue. He helped deal with servers to run my experiments. He kept me well fed during the busiest moments, and celebrated each of my tiny victories. He cheered me with the cutest cheers, and hugged me whenever I felt lost. As if that weren't enough, he brewed most of the coffee that fueled this work. You did so much for me I cannot fit everything in here. I firmly believe that I could not have finished this thesis without your love and support.

I want to thank my family, especially my mom, who never really learned that 'rule' about 'not asking when someone will finish their thesis'. Thank you for asking and letting me vent. I want to thank my friends, especially to those that started their Ph.D around the same time as I started mine. Amanda, Dr.Ferrada, thank you. Thank you for the laughs, the talks, and good moments. I am truly happy to have shared this journey with both of you. I also want to thank Bella the senior cat, Gwen the hedgehog, and Flora the super senior cat. I know, they can't really read (and if they could they would *probably* read Spanish). These little creatures filled my days and nights with hairs, spikes, scratches and love. Thank you.

I want to thank my advisers, Javier and Benjamin. I want to thank you for your guidance and support. I remember when Javier told me that he would be there mostly for "emotional support" purposes, to guide me through my own ideas, to untangle them. It was true, thank you for everything. I would also like to thank those who allowed me to do this while being able to pay rent. I want to thank NIC Chile Research Labs, and ANID scholarship for the funding, and the NLHPC (ECM-02) for the computing resources.

Thank you all, and thanks to those I could not fit in here.

"Last but not least, I wanna thank me. I wanna thank me for believing in me. I wanna thank me for doing all this hard work. [...] I wanna thank me for never quitting." –Snoop Dogg [34]

Table of content

List of Tables

List of Figures

Chapter 1

Introduction

The Internet is a critical infrastructure that allows us to communicate, access online education and commerce, maintain other critical infrastructures, etc. Its relevance has become even more apparent in recent times as we have seen the need to rely more on online communication and services. Given its importance it is of special interest to maintain the Internet's proper functioning, especially during adverse events. To do this we must study the Internet's robustness. Several different sets of tools and methods can be used to try to understand and/or test the Internet's robustness, depending on the field of study approaching the subject. One of these fields is the complex networks area.

Within the complex networks area, interdependent networks studies observe the emerging behavior that arise when two or more networks interact with one another. In the context of complex networks, robustness is the ability of a network to resist perturbations or failures. Methods based on interdependent networks are particularly useful to study infrastructures that naturally present interactions between two or more systems such as the power grid [83, 53, 61], transportation networks [124], supply chains [104], etc. As a multi-layered system, the Internet contains several different layers or networks that interact and depend on one another, however few methods based on interdependent networks have been applied to the Internet and its interactions with other infrastructures [27]. Furthermore, there is a lack of methods that consider the interactions and dependencies among the different network layers that compose the Internet.

In this thesis we intend to contribute to the theory of complex networks by presenting and evaluating a newly proposed physical-logical interdependent network model inspired by today's Internet. Here, we develop and test a set of methods or tools based on interdependent networks that allow us to analyze the robustness of the proposed model. We are particularly

interested in studying its robustness against natural catastrophes. To do this we start by proposing a physical-logical interdependent network inspired by today's Internet. This model considers a logical network inspired by the Autonomous System level network, a physical network inspired by the Internet backbone, and the interactions and dependencies between both networks. Then we propose a robustness metric and use it to assess the robustness of the proposed physical-logical interdependent network. Using the tools developed, we simulate the effect that different types of attacks can have over such a system, and use this to analyze its behavior under different adverse scenarios and constraints. Finally, we propose a new way to attack complex networks that allow us to better represent the effect that natural catastrophes, such as earthquakes, could have over the Internet's robustness. Since this thesis focuses on developing a theoretical framework within the field of complex networks, we must note that this thesis makes no claims about the practical relevance of the proposed model or of the reported model-based findings on aspects of the actual Internet such as its robustness with respect to the considered failure/attack scenarios.

Please note that this thesis has been organized to be read in order as each chapter references previous chapters to build the concepts and results.

1.1 Motivation

The Internet's robustness has been commonly studied considering the Internet as an isolated network, such as the Border Gateway Protocol (BGP) network, or the physical Internet network [116]. However, the Internet is a multi-layered system with each layer being a different network. These networks have dependencies with one another that create a complex system whose robustness can not be properly understood by studying a single isolated network. Thus, in order to better understand what would happen to the Internet under different failure scenarios we should study its robustness using interdependent network methods.

Dependencies between networks are known to affect the robustness of interdependent systems [21]. In the past, cases of critical infrastructures such as power grids suffering massive blackouts due to the interdependencies between the power grid and its communication network [29, 91] have motivated the study of complex systems as interdependent networks.

In the current literature, multiple problems have been studied using methods based on interdependent networks. Among these we can find methods to study power grids [22, 49, 52, 75], spatially constrained networks [4, 17, 31], geographically interdependent networks [111, 92], etc. However, within the literature reviewed for this thesis it was found that almost none of these methods referred to the case of the Internet robustness [27]. This means that most of the methods developed to analyze the Internet robustness assume that the Internet can be represented without considering interaction between networks. This

approach oversimplifies the way in which the Internet works and omits the interactions between networks that influence the Internet's behavior under adverse scenarios such as the interactions between the BGP network and the Internet Backbone, the interactions between the Internet and the power grid network, etc. Indeed, this type of approach has been criticized in the past for not being able to capture the Internet's complex behavior [116].

When studying the Internet we want to focus on different sets of networks depending on the way we want to measure the robustness. An interesting approach is the one that measures the effect that physical catastrophic events can have over the user's ability to access the Internet through an Internet Service Provider (ISP). To measure if users have Internet access we can use the Autonomous Systems level network or the *logical Internet network*. By measuring if a logical node has access to the Internet through an ISP we can estimate the user's ability to access the rest of the Internet. However, we cannot directly map logical nodes into physical nodes since the existence of a physical link does not guarantee communication between two physical nodes. Indeed, if a pair of physical nodes are connected through a physical link but they do not host logical nodes (Autonomous Systems) that directly exchange traffic with one another in the logical network, they will not communicate through the shared physical link. Hence, to measure the effect that physical catastrophic events could have over the user's ability to access the Internet, we should consider both the physical Internet network and the logical Internet network, along with their interactions with each other.

In this thesis work we propose a physical-logical interdependent network model inspired by today's Internet, and a set of methods or tools that allow us to analyze its robustness. Here, we develop and test a physical-logical interdependent network model inspired by the Internet, a simple but useful way to measure its robustness, and a new way to test the robustness of physical networks.

1.2 Hypothesis and Goals

Hypothesis: It is possible to increase the expressiveness of complex network's models oriented to study the Internet robustness using interdependent networks to model the interactions of the different elements that compose the Internet. Here we consider the expressiveness of such a model is measured by the number of characteristics and/or behaviors of the object being modeled that it captures.

General goal: The general goal of the proposed thesis is to generate an interdependent networks model to **approximate** the behavior of the Internet, and a set of methods to study the robustness of the proposed model.

Specific goals: The following specific goals will allow us to develop an interdependent network model, and a set of methods inspired by the Internet. These specific goals increase the overall expressiveness by progressively adding characteristics and/or behaviors associated to the Internet.

(A) Perform a survey of the study of the robustness of interdependent networks. This will allow us to find current interdependent network models that intend to approximate characteristics and/or behaviors of the Internet, and measure its robustness.

(B) Generate an initial model that captures some of the characteristics and behaviors of the Internet, considering the interactions between the Internet Backbone and the BGP network.

(C) Establish indexes or measures to capture the robustness of the generated model.

(D) Generate a set of tests that include failures and attacks to test the behavior of the proposed model against adverse events.

(E) Perform tests to measure the robustness of the proposed model, and analyze its behavior under different adverse scenarios.

(F) Establish and generate a refined version of the initial model that captures more characteristics of the Internet's behavior.

(G) Refine the robustness measurement tests to simulate events that are closer to real world failure scenarios.

(H) Test the refined model using the refined tests.

1.3 Methodology

In this section we present the general methodologies used to accomplish this work's objective. Since the main objective is to generate analysis methods, we used an iterative methodology that allows incremental development. This methodology was used on all specific objectives with the exception of objective (A). For objective (A), the Kitchenham protocol [60] was followed. This protocol establishes a specific methodology to develop systematic reviews.

1.3.1 Iterative methodology

This methodology consists of four stages which are repeated on a cycle until the desired development level is reached. These stages are: Observation, research, selection, and appli-

cation.

1. Observation: Here the characteristics of what we want to develop are observed and identified.

2. Research: In this stage related literature is studied to look for information that helps reach a solution.

3. Selection: Given the characteristics observed in the observation stage, useful data obtained in the research stage is selected to be used or applied to reach a solution.

4. Application: In this stage the information collected is applied as a modification to the current solution.

1.4 Contributions

Our first contribution is the development of a physical-logical interdependent network model inspired by the Internet, and its characterization under different adverse scenarios. Here we test two existing types of physical attacks: physical random attacks, and localized attacks. We also test a third type of physical attack developed in this thesis work: seismic attacks. The model developed uses complex networks concepts to specifically represent the interactions between a logical network inspired by the logical Internet network, and a physical network inspired by the physical Internet network. To the best of our knowledge no other interdependent network models have been developed before with the goal of capturing Internet characteristics this way.

Our second contribution corresponds to the finding of "bridge nodes" in the logical network, their effect on the overall robustness of the physical-logical interdependent networks tested, and their relation with hubs in Scale-Free networks. We have found that bridge nodes play an important role in characterizing the robustness of our model, as finding and protecting bridge nodes can dramatically improve the robustness of a system. Furthermore we found that "bridge nodes" whose removal results in a higher damage level are likely to be hub nodes, although not all bridge nodes are hubs.

Our third contribution is the analysis of the effect that adding links to the physical network has over the robustness of the physical-logical interdependent networks tested. Here, we test simple strategies to add links to the physical network while maintaining the logical network and the interdependencies between the networks unchanged. During the literature review we found that few works have addressed the effect of link addition within a single network of an interdependent system [55, 112, 59]. However, none of these works have been oriented to the

case of interdependent networks intended to represent the Internet network. Similarly, we found that for the specific case of communication networks the addition of physical links has been used before to enhance the network's robustness, and improve the recovery process after failure [105, 5, 78], however these works have not considered the systems as interdependent networks.

Finally, we develop a novel way to attack complex networks: Localized Attacks with Probabilistic Failures (LAPF). These attacks damage network elements following a given probability distribution F. Here, we show how LAPF could be used to model the damage caused by earthquakes, and test these attacks over the interdependent networks tested throughout this work. To the best of our knowledge these types of attacks have not been presented before. The attack most closely related to the presented LAPF corresponds to Localized Attacks (LA) [101, 17]. Localized attacks damage or remove all the nodes within the affected areas. Unlike localized attacks, LAPF consider probabilistic damage, that is, nodes within the area affected by a LAPF may or may not be damaged. Furthermore, two LAPF with the same initial conditions may result in different outcomes.

1.4.1 Publications

In this section we provide a list of all the accepted papers related to this thesis since the beginning of the program.

- Ivana Bachmann, Javier Bustos-Jiménez. "Improving the Chilean Internet Robustness: Increase the Interdependencies or Change the Shape of the Country?" International Workshop on Complex Networks and their Applications. Springer, Cham, 2017. [8]

- Ivana Bachmann, Felipe Espinoza. "Modelling the interactions between the Internet backbone and the BGP network." 2018. [11]

- Ivana Bachmann, Javier Bustos-Jiménez, Benjamin Bustos. "A Survey on Frameworks used for Robustness Analysis on Interdependent Networks". Hindawi Complexity Journal, 2020. [10]

- Ivana Bachmann, Francisco Sanhueza, Javier Bustos-Jiménez. "Space Geometry Effect over the Internet as a Physical-Logical Interdependent Network". International Conference on Network Science. Springer, Cham, 2020. [12]

- Ivana Bachmann, Valeria Valdés, Javier Bustos-Jiménez, Benjamin Bustos. "Effect of adding physical links on the robustness of the Internet modeled as a physical-logical interdependent network using simple strategies". International Journal of Critical Infrastructure Protection, 2021. [13]

- Ivana Bachmann, Javier Bustos-Jiménez. "Using Localized Attacks with Probabilistic Failures to Model Seismic Events over Physical-Logical Interdependent Networks". International Conference on Network Science. Springer, Cham. [9]

1.5 Work structure

This thesis has been organized in an incremental fashion. Each chapter in this work uses data, concepts, and/or results obtained in previous chapters. References to previous chapters are clearly pointed out. However, we recommend the reader to follow this work in the intended order.

This thesis is organized as follows:

- In Chapter 2 we present definitions of the main concepts used throughout the thesis work, and provide relevant related work.

- In Chapter 3 we present a physical-logical interdependent network model inspired by today's Internet. In this chapter we also provide a robustness definition, and a robustness index to measure the Internet's robustness. Finally, we test our model robustness against physical random attacks using the robustness index proposed.

- In Chapter 4 we analyze the interplay between the logical network of our model and the interlinks. In this chapter we introduce the concept of "bridge nodes".

- Chapter 5 tests the effect of adding links to the physical network using four link addition strategies. We compare the cost of adding these links, and their effect over the system robustness against physical random attacks.

- In Chapter 6 we test the effect of using localized attacks instead of physical random attacks, and compare the effect of both types of attacks. In this chapter we test the robustness of all the physical-logical interdependent networks tested in previous Chapters, including systems with extra physical links added.

- In Chapter 7 we define "Localized Attacks with Probabilistic Failures" (LAPF), and use them to define "seismic attacks". We then test the effect that seismic attacks have over the robustness of all the physical-logical interdependent networks tested in previous chapters, and compare its effect with the effect of localized attacks.

- Finally, in Chapter 8 we present the conclusion of this work and discuss possible future research lines for the project.

Chapter 2

Background

In this chapter we present the definitions of the main concepts used throughout this work, and review related work relevant for this thesis.

2.1 General concepts

- **Definition 1** ***(Complex network):*** A complex network corresponds to a network that exhibits a non-trivial topology. Thus, these networks can be distinguished from graphs generated at random. These systems emerge when several single element units or individuals interact in such a way that the behavior of the system cannot be explained just as a combination of the units' behavior [64].

- **Definition 2** ***(Interdependent networks):*** Within the complex networks field, interdependent networks refer to systems that consider complex networks that interact with one another. On these systems each network exhibits its own internal behavior, and two interdependent networks may present vastly different behaviors. Interdependent networks use special links between nodes from different networks to encode the interactions between networks [18]. Here, we refer to these types of systems as 'interdependent networks' or 'interdependent systems' interchangeably.

- **Definition 3** ***(Interdependent link, interlink or interconnection):*** An interdependent link, interlink or interconnection corresponds to a link that connects nodes belonging to different networks within an interdependent networks system. These links encode the nature of the interactions between nodes, and may carry varying levels of dependence.

- **Definition 4** ***(Coupling):*** In the context of interdependent networks, coupling refers to the way in which two different networks interact with each other [84, 125]. Thus, the term coupling can be understood as the way in which the interlink set is allocated between networks.

- **Definition 5** ***(Attacks or failures):*** An attack or failure corresponds to the damage experienced by a network. This damage can be targeted to specific nodes or links, or random [114, 25]. Elements damaged by attacks or failures are usually considered to have been removed from the network. If a node is removed by an attack it is assumed that all its associated links and interlinks are also removed.

- **Definition 6** ***(Cascading failure):*** Cascading failures refer to failures that propagate back and forth between interdependent networks. These types of failures frequently appear on interdependent networks due to the dependencies between nodes of different networks [18].

- **Definition 7** ***(Percolation):*** In the context of complex networks percolation theory is used as a theoretical framework to study failure propagation or cascading failures [102]. In the context of percolation studies, $(1-p)$ is the probability that a node gets disconnected from its network (i.e. fails). The **percolation threshold**, typically denoted by p_c, represents the critical value at which if $p < p_c$, then it is not possible to identify a giant connected component on the system. Here, the lower the p_c value, the more robust the system is considered to be, as this implies a higher $(1-p_c)$ value. The robustness interpretation of this metric is that a lower p_c means that it is possible to disconnect a larger amount of nodes before reaching the system's collapsing point. When studying the percolation of an interdependent system, first and second order phase transitions may occur. **Second order phase transitions** represent a continuous decay of the system where no abrupt collapse can be detected. Second order phase transitions are characteristic of single or isolated networks. **First order phase transitions** represent an abrupt collapse of the system as $(1-p)$ increases. First order phase transitions usually appear on interdependent networks systems.

- **Definition 8** ***(Proximity graphs):*** Given a set of points or nodes V allocated in a space such that there is a distance measure $\mathrm{d} : V \times V \longrightarrow \mathbb{R}$, and $\mathrm{d}(u, v)$ is defined for any pair $u, v \in V$, a proximity graph is a graph $G = (V, E(V))$ where a link (u, v) belongs to the link set $E(V)$ if and only if nodes $u, v \in V$ meet some previously defined proximity requirement. [74].

- **Definition 9** ***(Autonomous System)*****:** Autonomous Systems (AS) [1] are IP networks that manage their own internal routing. That is, each AS contains several IP

addresses that communicate with one another through an internal routing protocol chosen by the AS. Different autonomous systems might have different sizes, and might use different internal routing protocols to suit their needs. ASes are managed by organizations or administrative entities such as companies, universities, Internet Service Providers, etc. Furthermore, a single organization can have more than one AS. Although each AS manages its own internal routing, they communicate with one another through external routing according to the Border Gateway Protocol (BGP) [2].

- **Definition 10** ***(Border Gateway Protocol)*****:** The Border Gateway Protocol (BGP) [2] is the routing protocol used to handle the traffic routing between different autonomous systems or external routing. BGP handles the routing and reachability among autonomous systems taking into consideration internal AS policies, and paths available. We must note that BGP can be also used as an internal routing protocol.

- **Definition 11** ***(AS traffic exchange)*****:** The traffic exchange between autonomous systems is largely determined by business relationships between the organizations behind each AS. These relations influence the BGP routing policies. Relationships between ASes can be grouped in three categories: Customer–to–Provider (c2p), where an AS pays a better connected AS to transit its traffic to the rest of the Internet. Peer–to–Peer (p2p), where two ASes agree to bilateral free transit between their networks or their customers. Sibling–to–Sibling (s2s), where two ASes under the same administrative entity exchange traffic without any cost or routing limitations [47]. Thus, relationships between autonomous systems are not intrinsically bidirectional. For example, if an AS_1 is a customer of AS_2 and AS_3 then AS_1 can send its traffic through both AS_2 and AS_3. However, AS_2 will not be able to send traffic to AS_3 through AS_1, since AS_1 is its customer and does not transit traffic from AS_2..

- **Definition 12** ***(Shared Risk Link Group)*****:** In the physical network, a single fiber or physical link can be shared by more than one logical link. Shared Risk Link Groups (SRLG) denote links that share a fiber or physical attribute. Links in the same SRLG share risk, that is, if a link in the SRLG fails, other links in the group might fail as well. The concept of SRLG can be used to find backup paths such that the backup path uses links that do not belong to SRLGs present in the path being protected.

2.2 Interdependent network robustness

To ensure the proper functioning of these systems we must understand how networks work, what their vulnerabilities are, and how these vulnerabilities can be corrected. Real world networks do not exist in isolation, but rather interact with other networks. Particularly, network vulnerabilities are affected by the interactions that networks have with other network systems. These interaction can induce new vulnerabilities that are not present in single networks [21]. Big failures due to the interactions of networks have already occurred in the past, such as the Italy blackout of 2003, where a large portion of the country lost power supply, generating further degradation of services such as the railway networks, communication networks, healthcare systems, etc. [91].

To analyze the vulnerabilities induced by the interactions and dependencies between networks, we need to study the robustness using interdependent networks methods. Thus, we need to define what it means to be a robust interdependent network, and how the robustness should be measured given the nature of the system. Several frameworks have been developed to study the robustness of interdependent networks systems. The development of this type of frameworks is relatively new, starting in 2010 with the work of Buldyrev et al. [21], and has slowly grown over the past years. Since then, several types of frameworks have been created to represent different systems and scenarios. These frameworks go from simple and general frameworks, to more complex and specific ones. Some examples of these frameworks include representations of power grid networks interacting with their control network [83, 53, 61, 22], transportation networks where the bus network interacts with the subway network [124], interdependent cyber-physical supply chain networks [104], etc.

Having specific frameworks for the interdependent networks' case has become more and more relevant, as they allow us to describe scenarios that would not occur when studying the robustness of single isolated networks. Frameworks also allow us to simplify the analysis process by providing a systematic way to study the robustness of interdependent networks. In our previous work [10] we identified four main aspects that characterize frameworks used to study the robustness of interdependent networks: the interdependent network model, the robustness metric, the studies performed by the framework, and the data used to test the framework. In this section we will give a brief summary of the most important aspects for the work presented in this thesis.

2.2.1 Interdependent network model

As identified in our previous work [10], one of the defining aspects of these types of frameworks is the interdependent network model used. These models must define the interactions and dependencies among the networks that compose the interdependent network. These

models are not restricted to only modeling the interactions, and can include information about the internal functioning of the networks within the system. The interactions between two networks can be defined between nodes, edges, or both. These interactions may differ among different interdependent networks to represent the networks' specific behaviors, and the nature of their interactions.

Among the frameworks developed to study the robustness of interdependent networks, we can find different models and robustness measures depending on what is being modeled, and how the robustness of the system is defined [10]. The seminal work of Buldyrev et al. [21] proposed the "one to one" model, which considers two interacting networks where each node depends on exactly one node in the other network with mutual dependency, meaning that if a node fails, then necessarily its interdependent neighbor will also fail. Several other interdependent models have been developed since then. Some of them are variations of the "one to one" model [51, 59, 87, 95, 114, 126], whereas other models are entirely different. We can find models that focus on specific networks such as power grids [22, 49, 52, 75], the Internet [27], spatially constrained networks [4, 17, 31], and models with "many to many" interdependencies where each node may be interconnected to 0 or more nodes in the other network [99, 35, 80, 85, 90, 26, 120]. For "many to many" models the type of dependency between nodes must be clearly established. In some models, a node will fail if any of its interlinks fail [120]. Whereas in other models, a node will fail only if all of its interlinks fail [99, 35, 80, 85, 90, 26].

2.2.2 Robustness measures

Another defining aspect of these types of frameworks corresponds to the way in which the robustness of the system is measured [10]. The robustness of a network can be measured using one or more robustness metrics that focus on relevant characteristics to assess the robustness of the system.

The robustness of interdependent networks can be measured in several different ways. One of the most common robustness measures is the size of the Giant Connected Component (GCC) or Giant Mutually Connected Component [10]. The GCC measures the fraction of nodes contained in the largest connected component after an attack [84, 126, 70, 107, 128, 122]. Here, a node is considered to be functional if (1) it meets the dependency criteria established by the interdependent model, and (2) it is connected to the largest mutually connected component.

Another relevant robustness measure is the percolation threshold p_c that can be used to identify the maximum fraction of nodes that can be removed before the system collapses [21, 51, 68, 45, 46, 50, 125, 56, 114, 100, 119, 87, 72]. The generalized k-core percola-

tion can be considered as a variation of the classic percolation threshold [118, 82]. The k-core percolation measures the fraction of nodes within the k-core, the subgraph obtained by recursively removing nodes with degree lower than k (or k-leaves) along all nearest neighbors and incident links, as well as nodes that do not meet the functionality criteria established by the interdependent model. The resulting subgraph can be viewed as a generalization of the k-core, which is the maximum subgraph containing nodes with degree at least k [98].

Other measures include the average avalanche size induced by an attack measure the average amount of nodes removed during the cascading failure induced by the attack [65, 71, 110], the number of iterations that a cascading failure takes [50, 31, 16, 127, 35, 28, 65], and the cost of increasing the robustness of the interdependent network [86, 85, 121].

In the present work, we will be specially interested in measuring the fraction of functional nodes, where the node functionality conditions do not require a node to be connected to the largest connected component. However, to the best of the author's knowledge, few articles use this approach. One of these articles being our own work published in 2017 [8], and another being the more recently presented work of Dong et al. [36]. Both of these articles use the work previously presented by Schneider et al. [94], which defines the robustness measure R index that represents the fraction of nodes contained in the largest connected component after node failure.

2.2.3 Robustness testing

In order to test the robustness of a network we need to simulate possible adverse scenarios. This is usually done in the form of *attacks*. There are many ways to damage a system to test its robustness, however we can classify attacks on three main categories:

- **Random attacks:** Random attacks, also referred in literature as random failures, randomly select a set of network elements that are simultaneously removed during the attack [21, 126, 26, 81, 62]. These attacks are commonly used as the baseline to test complex networks robustness.

- **Targeted attacks:** Targeted attacks select the nodes to be removed using some criteria such as the node degree, node load, etc. [80, 114, 103, 38, 59].

- **Localized attacks:** Localized attacks damage all the nodes within a specific area [101, 119, 17, 97, 96]. Usually these attacks affect a circular area of radius r centered at some point c within the space in which the network is embedded.

2.3 Internet robustness

The Internet has been mostly studied as the Autonomous System level network (Border Gateway Protocol network or Internet's logical layer). However, many more layers interact and affect the Internet's logical layer. Each of these layers corresponds to a network with its own set of nodes and edges. The interactions among these layers generate dependencies that affect one another in ways that can lead to cascading failures on the system. Even more, dependencies between networks are known to affect the robustness of the whole system in ways that can not be understood by studying each network in isolation [21]. Cases of massive power grid blackouts in the past due to interdependencies between the power grid and its communication network [29, 91], have motivated the study and analysis of complex systems as interdependent networks. However, as of the writing of this thesis, we only found one interdependent network model including a direct reference to the Internet [27].

It has been stated before that in order to understand the Internet's behavior we must first understand the underlying structures that compose it, and how they affect one another. Previously, Willinger and Roughan have mentioned the need for a way of modeling the Internet that considers real-world AS-connection policies, multiple links, and geographic location among others, instead of considering just the AS-level Internet in isolation as a simple connected di-graph [116].

On the one hand, there is the *logical Internet network* composed of autonomous systems (AS) [1]. Autonomous Systems are IP networks that manage their own internal routing. ASes communicate with one another through external routing according to the Border Gateway Protocol (BGP) [2]. The routes between autonomous systems are in part determined by the business relationships between the entities behind the AS. These relationships dictate whether an AS will transit traffic from other ASes to go through it so the traffic can reach its destination (see section 2.1).

On the other hand, there is the *physical Internet network* comprising cables, antennas, routers, etc. This network is usually represented by Points-of-Presence (PoP) [116]. A single PoP may represent a group of buildings containing equipment in a relatively close area, a neighborhood, an isolated infrastructure that is relevant enough to be represented as a single node, among others. In case of a physical catastrophic event the physical Internet network would be directly damaged by it.

The physical Internet network and the logical Internet network interact with one another, and damage on one network may affect the other. Physical damage, such as physical node failure, can damage the information flow between Internet consumers or customers, and Internet Service Providers (ISPs). Damaging this flow can leave users without Internet

access as they stop being able to send their traffic towards its destination. The negative effects of this damage over the system can end up disrupting the user's ability to access the Internet. Severe damage to the Internet's functionality due to natural catastrophes has been observed before: after the 8.8 Mw earthquake in Chile in 2010 a one day Internet outage was reported [88]. Whereas damage to the logical network can affect the proper functioning of the physical network.

The Facebook outage of October 2021 [3] was an example of how damaging the BGP can disrupt communications, despite the physical equipment being functional. During this incident the Facebook's DNS servers were operational, however since the BGP network considered Facebook's nodes to be non-existent, these DNS servers became unreachable. This in turn rendered these servers unreachable for the physical network too, as they could not answer any request from other physical nodes. Although in this example the Internet as a whole was not affected, it shows how damaging the logical Internet network results in users not being able to access online services, despite physical equipment being fully functional.

As for modeling the Internet as an interdependent network system, few models have been found where the Internet is explicitly part of an interdependent system. An example can be observed in the work of Chen et al. where the AS-level Internet is coupled with a power-grid [27]. However, to the best of our knowledge there have not been other works, aside from the work presented here, that attempt to create an interdependent network model entirely inspired by the Internet.

Chapter 3

Initial interdependent model

We start this chapter by defining what we consider to be a *robust Internet network*. According to this definition we identify the minimal set of components that an interdependent model should have to capture characteristics from the Internet network, and allow the measurement of its robustness. We then propose an interdependent network model inspired by the Internet, and define the robustness measure accordingly.

Here, we propose to use road network models to represent the physical Internet network. More specifically, we use Relative Neighborhood Graphs [106] since they have been proven useful for modeling roads networks [123, 32]. To model the logical Internet network we use Scale-Free networks as they have been widely used to model BGP networks [42].

Finally, we test the robustness of the proposed model against physical random attacks. In this chapter we test the coupling effect over the Internet's robustness, as well as the effect of the physical space shape in which we build the physical network.

3.1 Robustness definition

In this thesis, we consider the Internet to be robust if after a failure, most of their users still have access to the rest of the network, that is, they still have access to the Internet and retain most of their speed and throughput. Here, we consider that a user has Internet access if it is able to reach an Internet Service Provider (ISP) that can transit its traffic. In particular, if several users are connected to each other but none of them is an ISP, then we do not consider them as having access to the Internet. Thus, in this work we propose the following Internet robustness definition:

Definition 13 ***(Internet robustness):*** We consider the Internet to be robust against failures if most of its users still have Internet access after a failure.

3.2 Proposed model

The proposed model aims to capture the interactions and dependencies of a logical network inspired by the AS-level network, and a physical network inspired by the physical Internet network. To do this, we define a physical-logical interdependent network model.

3.2.1 Model requirements

Given the proposed Internet robustness definition in section 3.1, and considering the objective of this thesis, we can identify the minimal set of components that our interdependent model should have. Here we list the identified components. For each component, we explain the reason why they should be considered within the proposed model.

- **Provider and consumer nodes:** To be able to measure whether users have Internet access or not, we must first be able to distinguish users from ISPs. Thus, our model must consider nodes that provide the Internet service, and user nodes that consume the Internet service. The former are referred to as 'provider nodes', and the latter are referred to as 'consumer nodes'. Here, we consider a node to provide "Internet service" if it is associated with an ISP and transits consumer or customer traffic to the rest of the Internet. If a logical network only contains nodes associated to a single country or region, its provider nodes must be able to transit traffic outside of the country or region.

- **Logical Internet network:** Given the proposed robustness definition, we need to be able to measure the number of users that have access to the Internet after a failure. We could estimate how many users have Internet access by observing the BGP network, that is, the logical Internet network. In this network the nodes represent Autonomous Systems (AS), while the links represent BGP routes between different AS. Within this network there are nodes that correspond to Internet Service providers. Thus, we can estimate the number of logical nodes that have access to the Internet by observing if they have a path to an ISP node or not. In this work, we use a logical network inspired by the logical Internet network to capture this behavior.

- **Physical Internet network:** In this work we want to measure the effect that events, such as natural catastrophes, might have over our model's robustness. To test this, we must measure the effect of physical failures over the robustness. Physical failures directly affect the physical Internet network, which in turn may affect the logical net-

work. Thus, to measure the effect of physical failures over the Internet's robustness we must consider the physical Internet network in our model. To do this, we use a physical network inspired by the physical Internet network.

- **Physical-logical coupling:** To understand the effects that physical failures would have over nodes in the logical network, we must model the interactions and dependencies between them. Here, we model these interactions considering broad characteristics of the interactions between the physical Internet network and the logical Internet network.

3.2.2 General definition

Consider $P = (V_P, E_P)$ the physical network where V_P is the set of physical nodes, and E_P the set of physical links, and $L = (V_L, E_L)$ the logical network where V_L is the set of logical nodes, and E_L is the set of logical links. The physical network has a total of $|V_P| = N_P$ nodes, and the logical network has a total of $|V_L| = N_L$ nodes. The logical network is inspired by the Autonomous System level network, and the physical network is inspired by the physical Internet network. Thus, in this model no restrictions are imposed regarding the number of nodes in each network, thus N_P may differ from N_L. The interactions between both of these networks are modeled as a set I of bidirectional interlinks. The physical-logical interdependent network is described by the tuple (P, L, I) where P is the physical network, L is the logical network, and $I = \{(u, v) : u \in V_L, v \in V_P, u \text{ and } v \text{ are interdependent}\}$ is the set of interlinks between both networks.

In our model we do not specify the topology that each network should have. Thus, any network topology can be used to model each network (physical or logical). In order to test physical attacks, the physical network must be spatially embedded, that is, each physical node $v \in V_P$ must be allocated into a physical space. Therefore each physical node $v \in V_P$ has an associated set of coordinates (x_v, y_v) to represent its allocation in space. For the case of the logical network the nodes are not allocated into space as the logical network is inspired by the Autonomous System level network.

We must note that the logical network is considered to be a snapshot in time of the state of the network in a given moment. Thus, the logical network does not incorporate the ability to re-route or recover of the logical Internet network. In particular, in this model the logical network does not make use of Shared Risk Link Groups (SRLG).

In the physical network it is assumed that each physical link might be a bundle of fibers or cables connecting the same physical nodes. We must note that in this model, the physical network cannot distinguish between two fibers that connect the same pair of nodes but

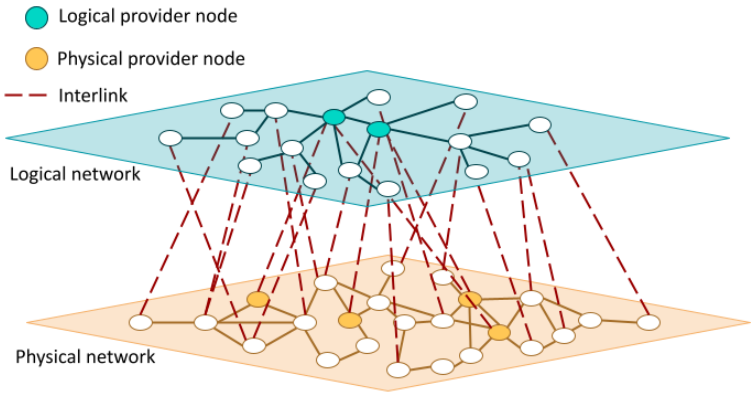


Figure 3.1: Interdependent model graphic example.

traverse different physical paths. However, different physical links are assumed to belong to different bundles.

In the following, we provide a detailed explanation of the consumer-provider behavior of our model, as well as the coupling conditions. In Figure 3.1 we can see a graphic example of the model proposed. The upper half of Figure 3.1 corresponds to the logical network, and the lower half corresponds to the physical network. Here, dotted lines represent interlinks between both networks. Darker colored nodes represent provider nodes within each network.

Consumer-provider behavior

Within each network we have provider nodes to represent ISPs, and consumer nodes that represent the users. A consumer node is considered to have Internet access if it has **a path** to a provider node within its own network. That is, there has to be a link sequence from the consumer node to the provider node, such that traffic from the consumer node can reach the provider node.

This consumer-provider behavior is based on the previous work of Parandehgheibi et al. [83]. In this work, it was used to model an interdependent network intended to represent a power grid coupled to its supporting Control and Communication Network. More recently, the work of Dong et al. [36] used an equivalent consumer-provider behavior to model the access to critical facilities in transportation networks after a disaster.

In our model, within each network there are one or more provider nodes to represent ISPs. This means that the physical network can represent the infrastructure of several ISPs combined. Specifically, there are $p_L \geq 1$ provider nodes in the logical network, where each

is intended to represent an autonomous system associated with an ISP.

For this work, provider nodes are assumed to be selected at random, however this can be modified to select these nodes according to specific parameters such as centrality measures or real world data. As for the providers in the physical network, physical nodes connected through an interlink with a logical provider node are considered to be provider nodes within the physical network. Since each provider node must have at least one physical counterpart, the physical network has a total $p_P \geq p_L$ physical provider nodes.

Coupling

As for the interdependencies, we want to represent the interactions between both networks. On one hand, each logical node has to be allocated on one or more physical nodes. If every physical node in which a logical node is allocated fails, then said logical node will not be able to function within the logical network. On the other hand, each physical node can have multiple logical nodes allocated within itself. However, if every logical node allocated within a physical node fails, then it will not be able to answer to other physical nodes, thus we consider it is no longer functional. Hence, a node u will remain functional if at least one of its interlinks is functional. Conversely, if all the interdependent nodes of a given node u fail, u will also fail. This condition is applied for both physical nodes, and logical nodes.

In this model we consider that each logical node u_L is interdependent with $N_I(u_L) \in \{1, \ldots, I_{max}\}$ nodes in the physical network. The I_{max} value represents the maximum number of interlinks that any logical node can have. To establish the interlinks between both networks, for each $u_L \in V_L$ we randomly select $N_I(u_L)$ physical nodes $(v_P^1, \ldots, v_P^{N_I(u_L)})$, and add an interlink (u_L, v_P^{i}) to I for each v_P^{i}, $\mathrm{i} \in (1, \ldots, N_I(u_L))$. For simplicity, in this work we randomly select each value $N_I(u_L)$ from the set $\{1, \ldots, I_{max}\}$ following a uniform distribution. However, we must note that the probability distribution used to select the values $N_I(u_L)$ can be tailored to be a better approximation of the the network being modeled. This can be achieved by considering logical node characteristics such as node importance, size, centrality measures, etc.

3.2.3 Cascading failures

Considering the functionality conditions of our physical-logical interdependent network model, we can summarize the cascading failure process as follows:

1. A fraction $(1 - p)$ of physical nodes is attacked. These nodes are considered to have failed.

2. Since physical nodes were lost in the previous step, a new set of physical consumer

nodes may lose all their paths to a provider node, and thus they fail.

3. The failure of physical nodes means their interlinks are no longer functional. Because of this some logical nodes may lose all their interlinks, and thus fail.

4. Since logical nodes were lost in the previous step, a new set of logical consumer nodes may lose all their paths to a provider, and thus fail.

5. The failure of logical nodes means their interlinks are no longer functional. Hence, a set of physical nodes may lose all their interlinks, and thus fail.

6. This process repeats from step 2) until no new nodes are lost.

3.3 Robustness measure

According to our robustness definition, we consider the Internet to be robust if it can keep users with Internet access in case of failure. Given our proposed model, we measure its robustness as 'the fraction of functional logical nodes after a failure'. To do this, we define the robustness measure G_L:

$$G_L = \frac{N_L^f}{N_L}$$

where N_L is initial number of functional logical nodes, and N_L^f is the number of functional logical nodes after the system has been damaged and the cascading failure has stopped. We must note that this measure was inspired by the R index presented by Schneider et al. which measures the fraction of nodes in the largest connected component [94].

Since a node is considered to be functional if (1) it has a path to a provider node, and (2) at least one of their original interlinks is still functional, if there are two or more logical provider nodes ($p_L > 1$), it is possible to have more than one connected component in the logical network (or physical network) with all its nodes still functional (see Figure 3.2). More specifically, it is possible to have up to p_L functional connected components on the logical network after an attack.

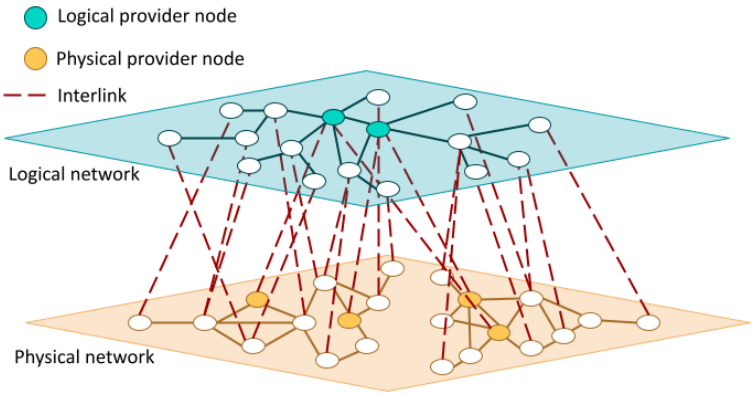


Figure 3.2: Example of a model with a **physical network split in two** that fully retains its functionality.

3.4 Experiments

In this section we describe the experiments performed to test the proposed model's robustness against physical failures using the proposed robustness measure. We test varying I_{max} values, physical network models, and space constraints to build the physical network.

3.4.1 Physical random attacks

To observe the effect of physical failures we use physical random attacks. These attacks randomly select a set of nodes to be removed. Here, a fraction p of the physical nodes survives the attack, and thus a fraction $(1-p)$ of physical nodes is selected at random to be removed. Given a fraction $(1-p)$ of physical nodes to be removed, a physical random attack will simultaneously remove $N_P(1-p)$ physical nodes from the initial undamaged physical-logical interdependent network.

The experiments presented here test the effect of randomly removing physical node sets of every non-trivial size possible. More specifically, we test 100 full physical random attacks iterations. Each one of these iterations tests the full range of possible fractions $(1-p) \in W$ that a random attack can remove, with $W = \{\frac{\mathrm{i}}{N_P} : \mathrm{i} \in \{1, \ldots, N_P - 1\}\}$. Thus, a total of $100 \times |W|$ random attacks are performed over each of the systems tested.

The results from these experiments show the average G_L value ($\langle G_L \rangle$) obtained by averaging all the 100 G_L values obtained for a given fraction $(1-p) \in W$ of nodes to be removed.

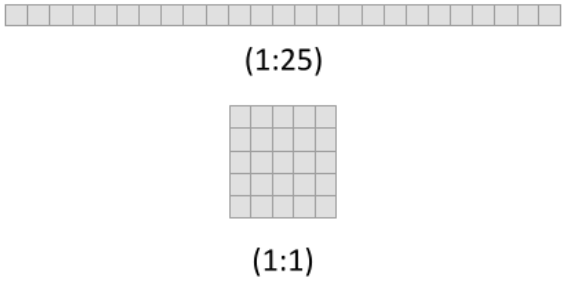


Figure 3.3: Representation of the physical spaces used for the experiments.

3.4.2 Spatial constraints

In our experiments we considered two spaces with the same total area and different width to length ratios: a square space with a (1:1) width to length ratio, and a long and narrow space with a width to length ratio of (1:25). The objective is to test whether the space shape in which we build the physical network has an effect over the robustness of the model or not.

The square space and the long and narrow space were selected as two extreme shapes that real countries have. Countries such as Spain, France, Sudan, and Colombia have a roughly square (1:1) width to length ratio. Whereas countries like Vietnam, Chile, Japan, and Norway have long and narrow shapes. Particularly, among the long and narrow countries Chile has the narrowest width to length ratio of (1:25). Figure 3.3 shows a representation of the spaces tested: both spaces have the same total area but different width to length ratios. We must note that the figure representing a space with a (1:25) width to length ratio has been placed horizontally for convenience.

3.4.3 Physical networks

In this section we show and explain the different physical network models used throughout this thesis. These models were used to generate the physical networks of the physical-logical interdependent networks used for the experiments.

First, we talk about our initial approach to generate physical networks: Relative Neighborhood Graph (RNG). Here, we explain the reasons for using physical networks based on RNGs. Then, we proceed to talk about other network models that were used to generate physical networks for our experiments. These models were selected after our initial approach, so we could compare the effect of having different physical networks.

First approach: Relative Neighborhood Graph (RNG)

Connections between nodes in the Internet backbone are usually placed alongside existing roads and highways to decrease the installation costs associated with adding new connections. Thus, we can expect the physical Internet topology and the roads/highway network topology to be similar. Urban roads networks (URN) have been studied and modeled as proximity graphs. Furthermore, URNs have been found to be planar fully connected graphs [23].

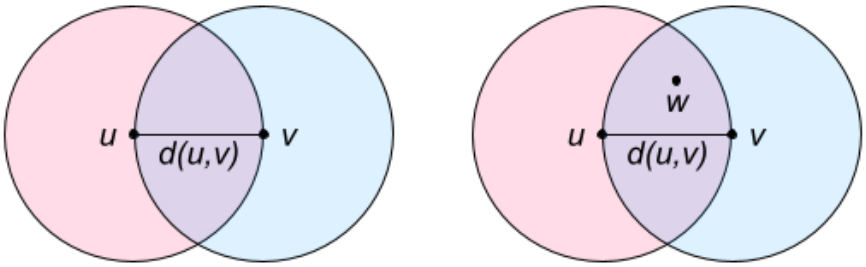
Among planar proximity graphs used to model roads networks, we find the Relative Neighborhood Graph (RNG), also referred to as RNG networks. RNG networks were first presented by Toussaint [106], following the definition of "relatively close neighbors" proposed by Lankford [63]. Relative neighborhood graphs are proximity graphs related to Minimum Spanning Trees (MST) and the Delaunay (Voronoi) Triangulation (DT). More specifically, relative neighborhood graphs are a superset of Minimum Spanning Trees, and a subset of the Delaunay Triangulation: $E_{MST} \subseteq E_{RNG} \subseteq E_{DT}$. Because of these characteristics RNG networks have been used in the area of urban transportation design [123, 33, 32], and the mobile networks and wireless communications area [58, 69].

In this work we use RNG networks as a first approximation of the physical network as it has been previously shown that RNG networks can be used to represent the evolution of urban roads [123, 32], and the railway network [33]. We must note that the usage of existing models such as RNG networks to represent the physical network is intended only as an approximation to test the interdependent network model presented.

- **Generating a RNG network:** Since relative neighborhood graphs are proximity graphs, to build an RNG network we must check each pair of nodes $u, v \in V_P$ and determine whether they meet the RNG proximity requirement or not. Consider a finite 2-dimensional space, a set of nodes V with $|V_P| = N_P$ allocated into the described space, and $\mathrm{d}(u, v)$ the euclidean distance between node u and v with $u, v \in V_P$. For RNG we have that two nodes u and v meet the proximity requirement, and thus can be connected, if there is no other node in the intersection area of the circles centered at u and v, each of radius $\mathrm{d}(u, v)$ (see Figure 3.4). This way two nodes will get to be connected if there is no other node closer to them in the area between them.

Other models for the physical network

To further understand the effect of the physical network topology over the robustness of the proposed model, we test other five models to generate the physical network: Yao Graphs [117], Geometric Preferential Attachment (GPA) [43], Gabriel Graphs (GG) [44], k-nearest neighbors (k-NN) [39], and Erdös-Rényi (ER) [48, 40].



(a) Link (u, v) is added. (b) Link (u, v) is not added.

Figure 3.4: (a) Shows a node configuration in which nodes u and v meet the proximity requirements, and thus can be connected. (b) Shows a node configuration in which nodes u and v do not meet the proximity requirements because of node w.

Yao Graphs

Yao Graphs [117] are spatially embedded networks, that is, nodes must be allocated into some space. These graphs are known to be geometric spanners [113]: weighted graphs that connect points in space such that any pair of points or nodes u and v are connected through a path whose weight is at most t times the spatial distance between u and v. Yao graphs have applications on wireless ad-hoc networks [69], and wireless sensor networks [113].

- **Generating Yao graphs:** Given a set of nodes V allocated into a space, and $k \geq 6$ an integer, we build a Yao graph by adding links using the following procedure. Using each node $u \in V$ as center, we divide the space into k equal areas using k rays originating at u. For each area, we select the node $v \neq u \in V$ that is the closest to u and add the link (u, v) to the Yao Graph. In order to obtain a single connected component while adding the least number of links, in this work we use $k = 6$. Please note that we are interested in keeping the number of links low whenever possible so the generated networks are comparable to RNG networks.

Geometric Preferential Attachment (GPA)

Networks generated using Geometric Preferential Attachment (GPA) [43] use the preferential attachment principles to add links [14], and incorporate a geometric component that ensures the presence of small separators [43]. We say that a graph has small separators if its subgraphs can be partitioned into two approximately equally sized parts by removing a relatively small number of vertices. Note that the subgraphs of a graph include the graph itself. Most nearest neighbor graphs in 3-dimension have small separators. Structures such as the network generated by the links of the web also present small separators [19]. We must

note that in GPA networks nodes might not be embedded into space, however the existence of a distance function between nodes is required. In the following, we will assume that nodes are embedded into some space.

- **Generating GPA networks:** Given a set of nodes V allocated into a space, to build a GPA network we follow an iterative algorithm. First, a random node $u \in V$ is selected. Within a specific radius r from node u the usual rules of preferential attachment are used [14]. That is, the node u will be connected to another node $v \in V$ within the radius r with a probability proportional to the degree of v. In the present work, we add five edges on each iteration.

k-nearest neighbors graphs (kNN)

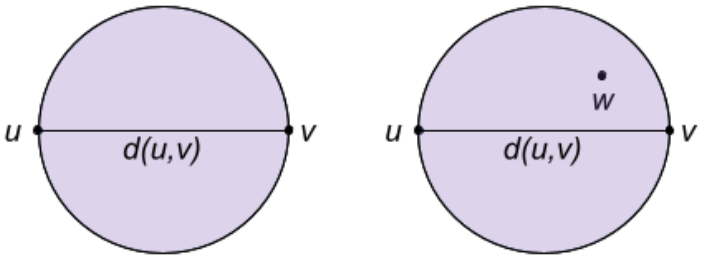
Given a set of points or nodes allocated into a metric space, Nearest Neighbor Graphs (NNG) [39] are graphs formed by connecting each node to its nearest neighbor. These graphs are usually described as directed graphs since the 'nearest neighbor' relation is not symmetric. However, NNG can also be created as undirected graphs. The generalization of NNG are the k-nearest neighbors graphs (kNN) [39] where each node is connected to its k nearest neighbors. Here, the usual NNG is equivalent to a 1NN.

- **Generating k-nearest neighbors graphs:** In this work we will use undirected links to generate our k-nearest neighbors graphs. Consider V a set of nodes allocated into space. To generate our kNN we connect each node $u \in V$ into the k nodes closest to it. In this work, in order to obtain a single connected component while adding the least number of links we use $k = 5$. Thus we obtain a 5-nearest neighbors graph (5NN). Using $k < 5$ may result in a network with multiple connected components, that is, a network that is not fully connected. Please note that we are interested in keeping the number of links low whenever possible so the generated networks are comparable to RNG networks.

Gabriel graphs (GG)

Gabriel Graphs (GG) [44] are spatially embedded networks known to be geometric spanners [113]: weighted graphs that connect points in space such that any pair of points or nodes u and v are connected through a path whose weight is at most t times the spatial distance between u and v. Particularly, Gabriel graphs are proximity graphs [74] related to Minimum Spanning Trees (MST), the Delaunay (Voronoi) Triangulation (DT), and the Relative Neighborhood Graph (RNG). Gabriel graphs are subset of the Delaunay Triangulation, and superset of the Relative Neighborhood Graph: $E_{MST} \subseteq E_{RNG} \subseteq E_{GG} \subseteq E_{DT}$ [113]. These graphs have been used on wireless networks routing [69, 58, 20], geographic variation [76], and urban networks [33].

- **Generating GG networks:** Consider a set of nodes V allocated into a space. Given two nodes u and v with $u, v \in V$, we add a link (u, v) between them if the circular area between both nodes does not contain any other nodes. The diameter of this area is the distance between u and v, with u and v are located on the circumference of this area (see Figure 3.5).



(a) Link (u, v) is added. (b) Link (u, v) is not added.

Figure 3.5: (a) Shows a node configuration in which nodes u and v meet the proximity requirements, and thus can be connected. (b) Shows a node configuration in which nodes u and v do not meet the proximity requirements because of node w.

Erdös-Rényi (ER) networks

Erdös-Rényi (ER) networks [48, 40] are randomly generated networks. In the literature Erdös-Rényi networks refer to two models for generating random networks, one proposed by Gilbert [48], and another proposed by Erdös and Rényi [40]. In Gilbert's model each link has a fixed probability of being present in the network and this probability is independent of the other links already present in the network. In Erdös and Rényi's model all graphs that have the same number of nodes and the same number of links are equally likely to be picked as the final randomly generated graph. These networks do not require a distance function, and do not have any spatial conditions.

In the present work we use this model as control for our experiments since this model does not use any spatial parameters to allocate its links.

- **Generating ER networks:** For our experiments we build ER networks following Gilbert's model. Consider a set of nodes V allocated into a space, with $|V| = n$. Given two nodes u and v with $u, v \in V$, with probability p we add a link (u, v) to our ER network. For each pair of nodes in V, we repeat this process. Here we set the probability $p = \frac{log(n)}{(n)}$ since this value is more likely to generate a single connected component [40].

3.4.4 Networks tested

Since we are testing physical-logical interdependent networks, to build each system we must generate a physical network P, a logical network L, and a set of interlinks I. In this section we explain how each of the interdependent networks tested was generated, and show the parameters used to generate them.

Interdependent networks

Let us begin with the physical network P. Consider model m one of the models described in section 3.4.3. To build the physical network, we start by randomly allocating N_P nodes into the space. Using these node locations, links are then placed according to the rules of model m. For each space shape, 10 sets of physical node locations are generated. Thus, for each space, and each physical model we generate 10 different physical networks. With this, we can characterize each physical network as follows: Given the space shape $s \in \{(1:1),(1:25)\}$, and model $m \in \{RNG, YAO, GPA, 5NN, GG, ER\}$, for each $j \in \{1, \ldots, 10\}$ we generate a physical network:

$$P_j(m, s) = (V_P, E_P^m(loc_j(V_P, s)))$$

Where V_P is the set of physical nodes with $|V_P| = N_P$, $loc_j(V_P, s)$ is the j-th set of physical nodes allocations over the space shape s, and $E_P^m(loc_j(V_P, s))$ is the set of links generated according to physical model m, given the set of physical nodes allocations $loc_j(V_P, s)$.

For simplicity, the logical network was modeled as a Scale-Free network with $\lambda = 2.5$ [42]. We tested a total of 10 instances of logic networks L_q, with $q \in \{1, \ldots, 10\}$. We must notice that this model assumes that the network links are non-directed, and thus it cannot fully capture the nature of the relationships between real ASes. Here, we model the logical network using Scale-Free networks as it can be used as a rough approximation of the topology of the logical Internet network.

For the interdependencies, we test $I_{max} \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. For each $I_{max} = u$, we generated a set $I(u)$ of interlinks according to the proposed physical-logical interdependent model. Thus, for each node v_L in the logical network, we randomly select up to u physical nodes and add an interlink between v_L and each of the selected physical nodes. In particular, if the logical node v_L is a provider node, we add exactly u interlinks between v_L and the physical network.

As for the provider nodes, on each logical network we randomly select p_L provider nodes. For each I_{max} value tested, we generated a different provider configuration. Thus, the provider node configuration is associated with u the I_{max} value used to generate the interlink set $I(u)$. Physical nodes connected through an interlink to a logical provider node

are considered to be provider nodes within the physical network. Thus, the physical network has a total of $u \cdot p_L$ provider nodes.

This way, given a space shape s, a model $m \in \{RNG, YAO, GPA, 5NN, GG, ER\}$, an interlink set $I(u)$, a logic network L_q with $q \in \{1, \ldots, 10\}$, and a set of physical nodes allocations $loc_j(V_P, s)$ with $j \in \{1, \ldots, 10\}$ we can characterize each physical-logical interdependent network by the tuple:

$$(P_j(m, s), L_q, I(u))$$

We must note that each network starts as a single connected component. Thus, we start with each logical node having a path to all other logical nodes, and each physical node having a path to all other physical nodes.

Network parameters

The narrowest space (1:25) is based on Chile's geography. To observe the effects that a wider space shape would have over the Internet robustness of a country with such restrictive conditions, we use for both spaces the number of physical nodes, logical nodes, and the number of logical providers that simulate the conditions of Chile. For each physical-logical system, we consider $p_L = 6$ to be the number of ISPs, $N_L = 300$ to be the number of logical nodes, and $N_P = 2000$ as the number of physical nodes. Please note that this data was obtained at the beginning of this work (2017), since then new AS have been added to the Chilean network, and others have stopped being used. As of October 05, 2021, the number of logical nodes in the Chilean network has increased to 375 [6].

3.5 Results

In this section we present and discuss the results obtained according to the experimental settings described in section 3.4. The results shown here were obtained by testing the robustness of a total of 12,000 different interdependent networks against physical random attacks. Given a physical-logical system, to present the results more succinctly we define its total G_L as:

$$TG_L = \sum_{\mathrm{i}=1}^{N_P - 1} \langle G_L(\frac{\mathrm{i}}{N_P}) \rangle$$

where $\langle G_L(\frac{\mathrm{i}}{N_P}) \rangle$ is the G_L value obtained on the experiments after removing a fraction $\frac{\mathrm{i}}{N_P} = (1 - p)$ of nodes from the physical network, averaged across all 100 iterations tested (see section 3.4.1).

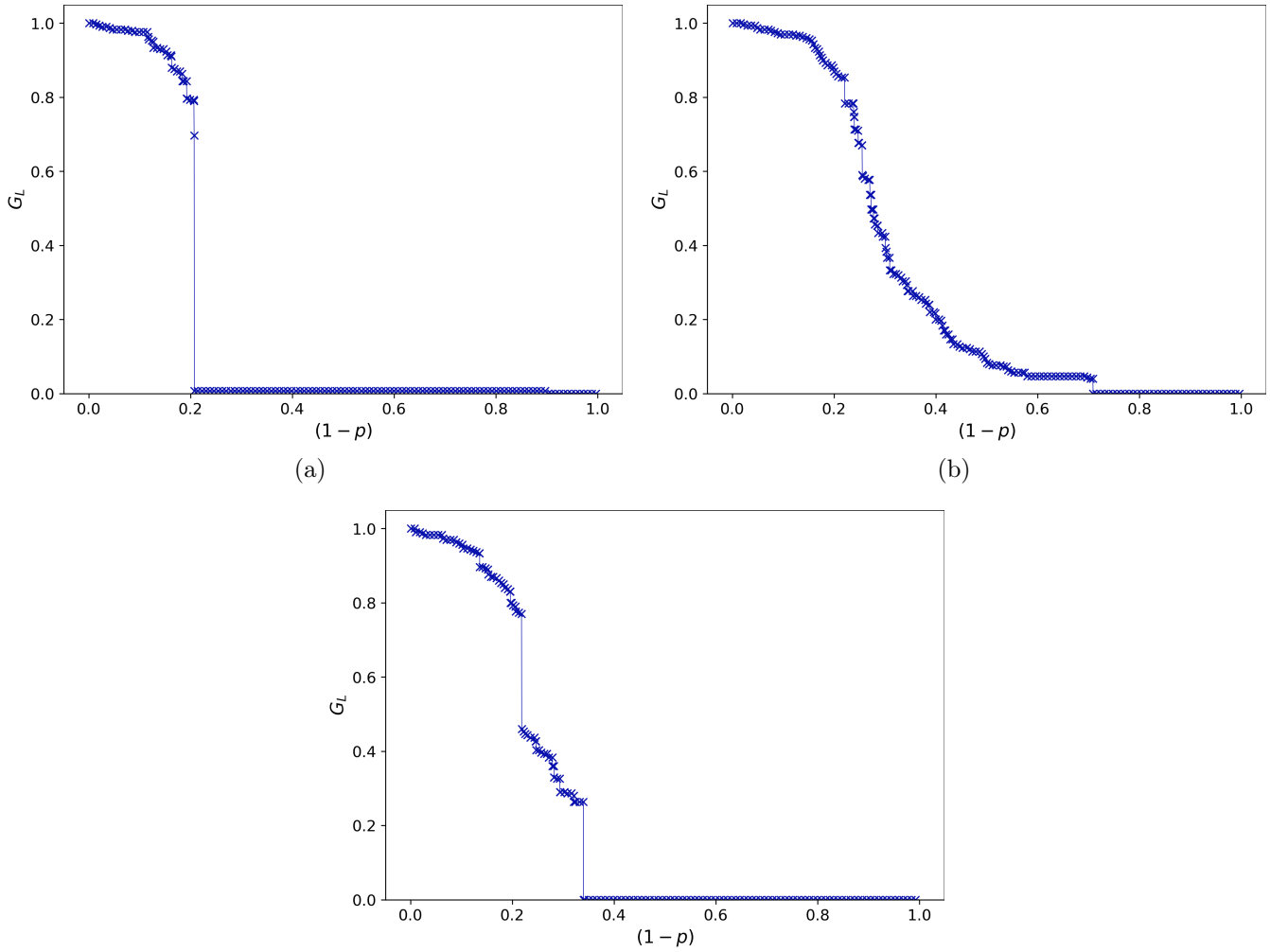
3.5.1 General robustness behavior

In Figures 3.7 and 3.8 we can see the average robustness behavior of systems built using logical network version $q = 1$. Figures for the remaining q values can be found in the appendix section A.1. Given a physical model m, in these figures we observe the average $\langle G_L \rangle$ across all 10 node location configurations j ($\overline{G}_L$). Here, we observe that our physical-logical interdependent network model, on average, presents a continuous decay against physical random attacks. This behavior is observed across all systems tested. These results suggest that physical-logical systems built as shown in 3.2 undergo a second order phase transition against physical random attacks when we consider the averaged results. However, given the small size of the networks being tested we cannot argue that these systems always undergo a second order phase transition.

Indeed, given a physical-logical interdependent network, if we observe each random physical node removal iteration, we observe that some iterations result in an abrupt collapse of the network, other iterations result in a smooth decay, whereas other iterations result in a mixed behavior (see figure 3.6).

Figure 3.9 shows the p_c values, and $G_L(p_c)$ values of systems built using logical network version $q = 1$ that undergo an abrupt collapse. Figures for the remaining q values can be found in the appendix section A.1. Here, we observe that the p_c values tend to decrease as the I_{max} value increases. Furthermore, we can see that physical-logical networks using $m =$ RNG have the highest p_c values, whereas physical-logical networks using $m =$ ER have the lowest p_c values.

Table 3.1 shows the fraction of iterations that undergo an abrupt collapse. Tables for the remaining q values can be found in the appendix section A.2. In these tables we observe that the fraction of iterations that undergo an abrupt collapse have a wide value range. Thus, although the average behavior shows a second order phase transition, we observe that in many of the iterations tested the physical-logical interdependent network undergoes a first order phase transition. Furthermore, in most cases, most of these iterations result in a first order phase transition.

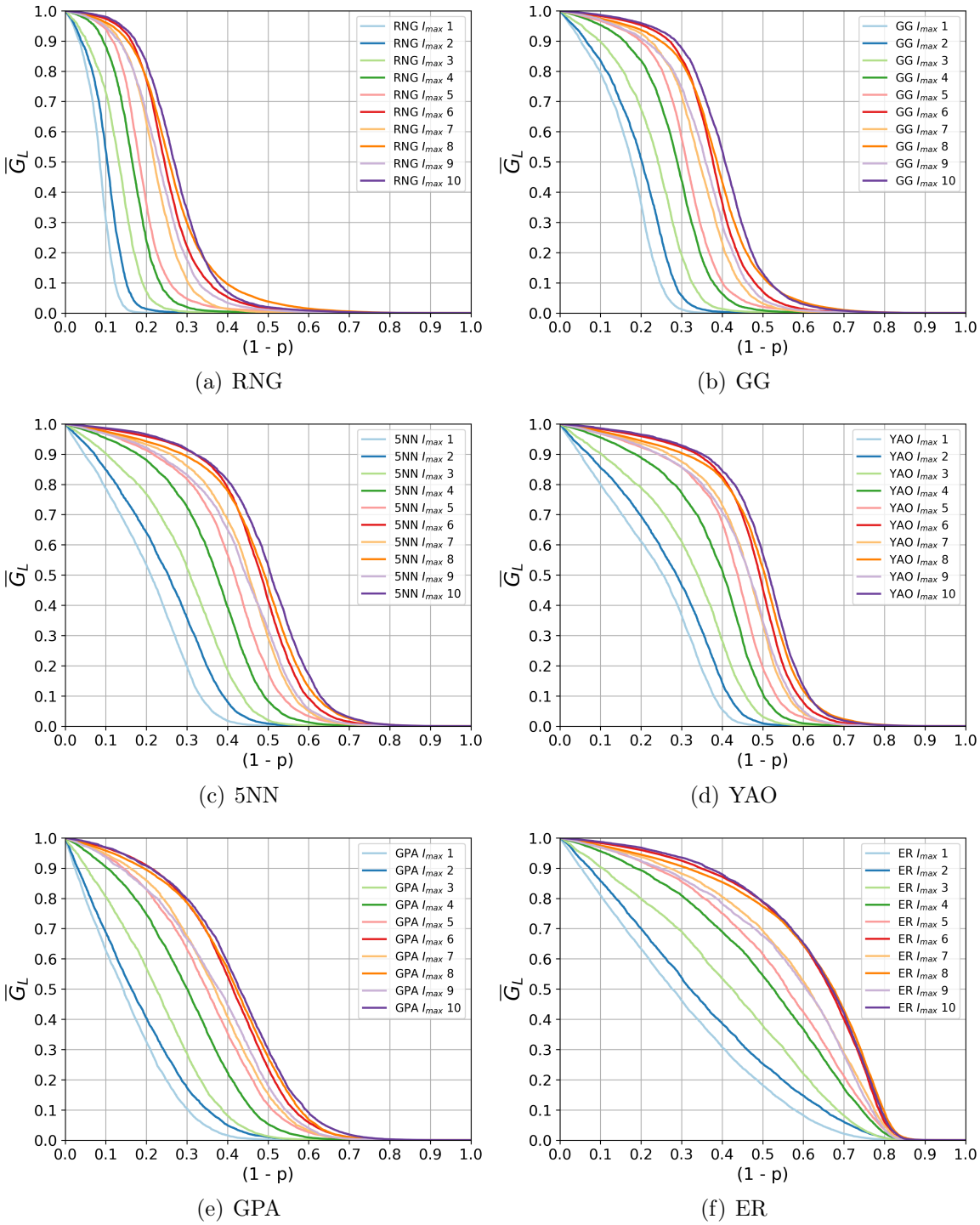


(a)

(b)

(c)

Figure 3.6: Decay of different iterations of the same physical-logical interdependent network. Here $m =$ RNG, $s =$ (1:25), $q = 1$, and $I_{max} = 6$.

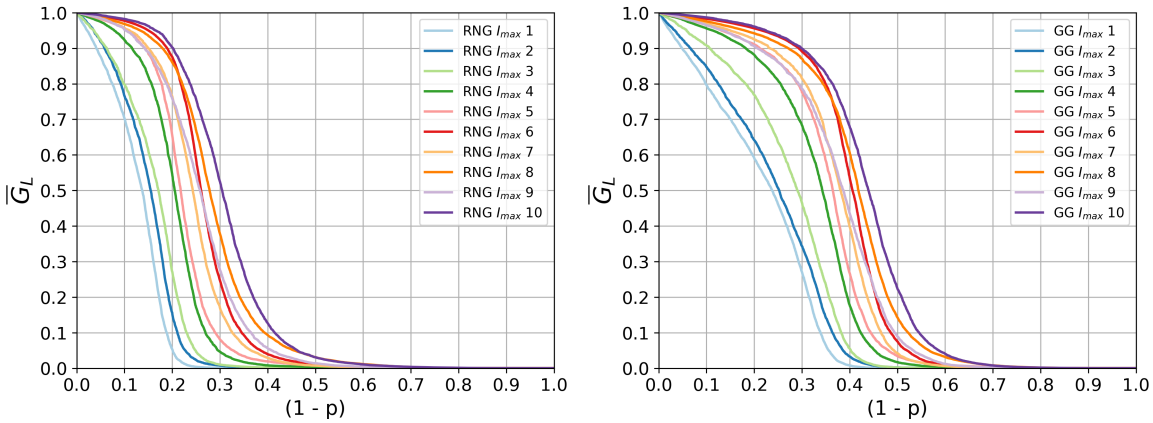


(a) RNG (b) GG

(c) 5NN (d) YAO

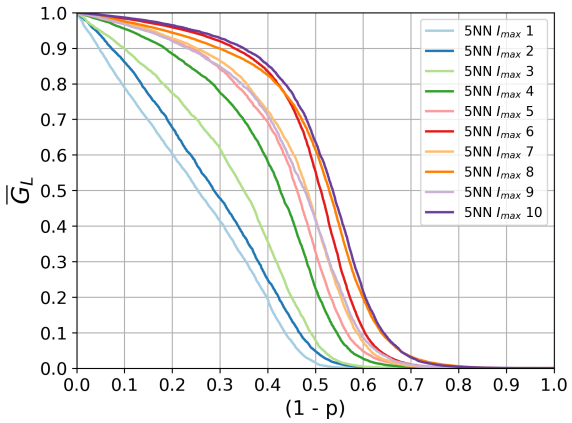
(e) GPA (f) ER

Figure 3.7: Average robustness by model for interdependent networks built over a (1:25) space, and logical network version $q = 1$.

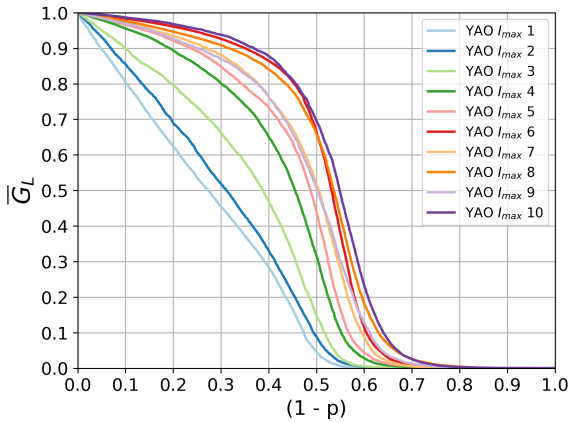


(a) RNG

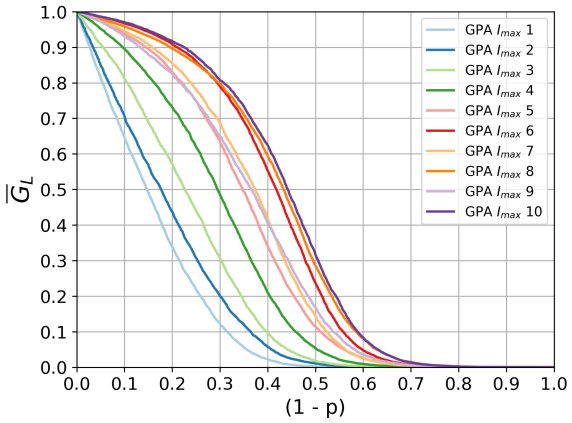
(b) GG



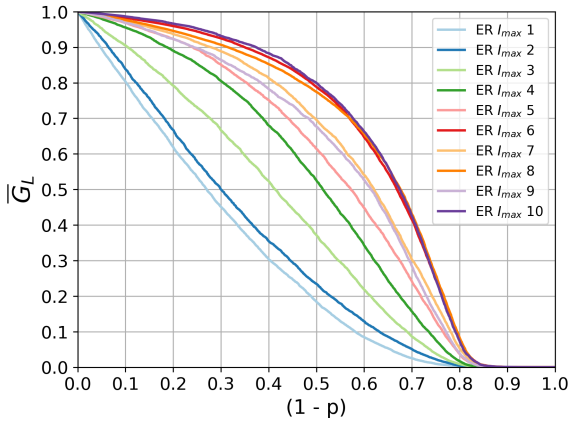
(c) 5NN



(d) YAO

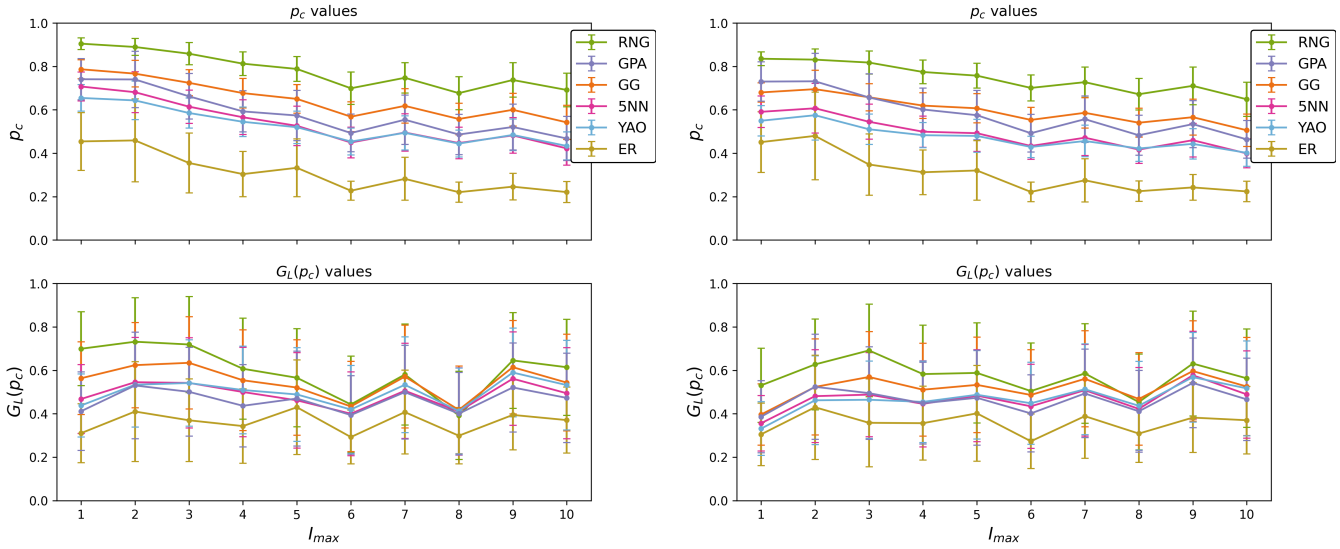


(e) GPA



(f) ER

Figure 3.8: Average robustness by model for interdependent networks built over a (1:1) space, and logical network version $q = 1$.



(a) (1:25) (b) (1:1)

Figure 3.9: Average values of p_c and $G_L(p_c)$ for each model m, space s, I_{max}, and logical network version $q = 1$. Bars represent the standard deviation.

s =(1:25)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.766	0.86	0.848	0.888	0.813	0.705	0.9	0.399	0.841	0.787
GG	0.652	0.765	0.708	0.81	0.844	0.72	0.884	0.486	0.817	0.719
5NN	0.514	0.744	0.606	0.768	0.837	0.699	0.842	0.537	0.679	0.595
YAO	0.556	0.695	0.552	0.749	0.82	0.711	0.867	0.552	0.746	0.676
GPA	0.592	0.73	0.545	0.686	0.809	0.652	0.847	0.696	0.669	0.54
ER	0.585	0.651	0.411	0.618	0.861	0.646	0.766	0.703	0.471	0.539
s =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.757	0.804	0.765	0.824	0.811	0.707	0.866	0.482	0.824	0.736
GG	0.654	0.708	0.662	0.76	0.801	0.783	0.883	0.536	0.784	0.669
5NN	0.641	0.674	0.5	0.7	0.838	0.752	0.839	0.554	0.67	0.621
YAO	0.598	0.662	0.537	0.701	0.853	0.757	0.833	0.56	0.659	0.648
GPA	0.646	0.772	0.56	0.704	0.816	0.725	0.837	0.663	0.599	0.576
ER	0.549	0.634	0.418	0.644	0.854	0.64	0.762	0.725	0.473	0.535

Table 3.1: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 1$.

3.5.2 Space shape effect

In Figure 3.10 we can observe the average TG_L values ($\overline{TG}_L$) obtained for each physical-logical interdependent network for $I_{max} = 3$ versus the logical network version q used to build the system. For this figure, we obtained each $\overline{TG}_L$ value by averaging the 100 TG_L values obtained for each of the 100 physical random attacks tested (see section 3.4.1) given a fixed m, $I_{max} = u$, s, and q. Figures for the remaining I_{max} values tested can be found in the appendix section A.3. A more detailed version of this data can be found in Table 3.2 where we can see the average $\overline{TG}_L$ and its standard deviation for $I_{max} = 3$. Here, the average $\overline{TG}_L$ is obtained by averaging $\overline{TG}_L$ values across all 10 node location configurations j. Tables for the remaining I_{max} values tested can be found in the appendix section A.4. In these tables, the averages were obtained across the 10 physical network instances for a given space s, and physical model m.

In Figure 3.10 we can see the results for interdependent networks with physical networks built in a (1:1) space, and the results for interdependent networks with physical networks built in a (1:25) space. Here we observe that interdependent networks with a physical network based on a physical model $m \in \{\text{RNG, GG, 5NN, YAO}\}$ built over a (1:1) space have a $\overline{TG}_L$ higher than that of interdependent networks with a physical network built on a (1:25) space. For interdependent networks that use physical networks based on GPA and ER models we observe that the space shape does not have a clear effect over the robustness of the interdependent network. We observe this behavior regardless of the I_{max} value (see appendix section A.3).

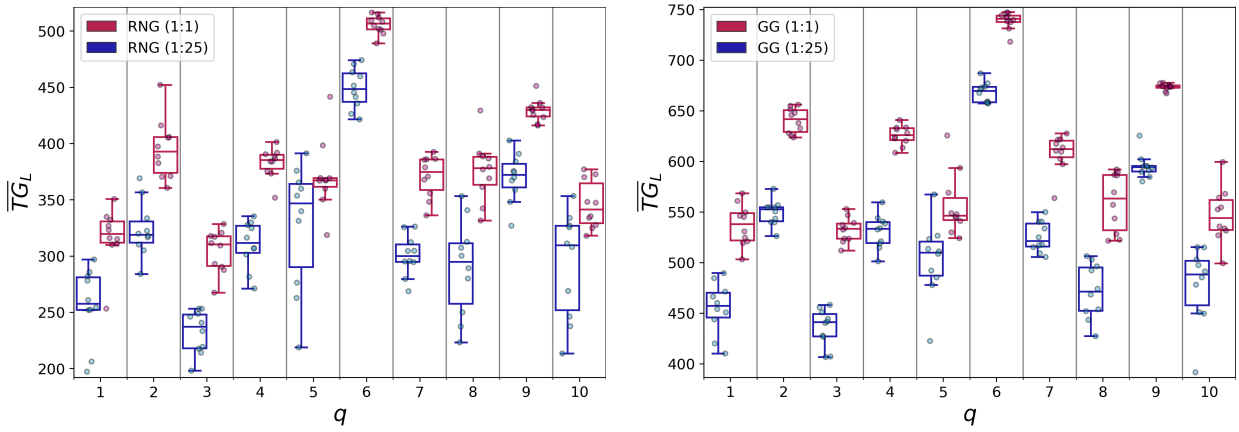
Our results show that the robustness of interdependent networks that use RNG, GG, 5NN, or YAO models to build their physical networks is affected by the space shape in which the physical network is built, with a (1:25) space resulting in more fragile systems than a (1:1) space. Whereas the robustness of systems that use GPA or ER based physical networks are not affected by the space s. This behavior can be explained by looking at whether or not the physical network topology is affected by the differences between both spaces. The structure of RNG, GG, 5NN, and YAO models depends on the node allocations into space $loc_j(V_P, s)$. As the location of each node is selected uniformly at random, changing the space shape from (1:1) to (1:25) will result in noticeable changes in the node allocation distribution, with nodes being much closer in one axis than the other for $s = (1{:}25)$. In the case of the GPA model and ER model, node allocation does not play such a crucial role. In GPA networks the role of node allocation is only relevant to decide whether a node will be included or not in the preferential attachment process associated with a certain node. The ER model completely ignores node allocation.

We also note that the difference between the robustness of interdependent networks that

use RNG, GG, 5NN, and YAO models built over a (1:1) space, versus interdependent networks using the same models built over a (1:25) space tends to decrease as the I_{max} increases. This suggests that we can decrease the fragility induced by the narrowness of the space by adding more interlinks between the logical and physical network.

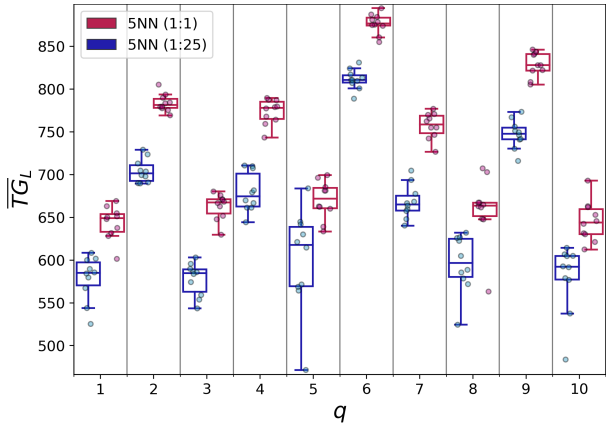
$I_{max} = 3$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	256.55 (31.17)	447.33 (32.6)	455.07 (24.21)	578.39 (25.02)	621.42 (13.73)	821.26 (18.12)
	(1:1)	317.2 (24.44)	457.31 (37.63)	536.91 (19.43)	643.34 (18.63)	694.08 (19.04)	812.3 (20.94)
2	(1:25)	323.51 (23.32)	594.27 (32.84)	549.32 (12.01)	703.99 (13.17)	740.46 (14.35)	995.28 (14.06)
	(1:1)	394.88 (25.46)	584.35 (28.25)	640.37 (11.79)	783.58 (9.74)	826.11 (12.95)	997.92 (12.19)
3	(1:25)	232.38 (18.13)	461.01 (34.74)	435.92 (17.54)	577.37 (18.43)	626.92 (9.15)	848.05 (13.66)
	(1:1)	304.29 (17.97)	467.13 (19.62)	532.26 (11.9)	662.3 (14.48)	709.53 (10.45)	845.78 (17.08)
4	(1:25)	310.1 (20.03)	567.9 (30.27)	530.5 (15.93)	679.03 (21.98)	727.06 (12.68)	982.54 (17.82)
	(1:1)	382.69 (12.81)	563.68 (21.71)	625.65 (9.37)	773.28 (13.95)	817.97 (8.83)	981.1 (13.28)
5	(1:25)	327.44 (53.26)	489.94 (36.75)	502.79 (35.86)	601.04 (56.5)	649.54 (23.39)	826.43 (23.74)
	(1:1)	370.81 (30.1)	489.67 (35.15)	556.94 (29.49)	669.93 (21.32)	710.49 (21.65)	834.47 (40.27)
6	(1:25)	448.87 (17.16)	688.81 (27.49)	668.26 (9.49)	811.13 (11.1)	845.07 (9.18)	1055.35 (16.14)
	(1:1)	505.45 (8.0)	689.71 (26.36)	738.85 (8.22)	876.37 (11.22)	904.87 (11.7)	1041.73 (16.06)
7	(1:25)	300.62 (17.31)	566.18 (26.87)	525.37 (14.14)	667.8 (18.62)	712.94 (11.03)	963.15 (7.8)
	(1:1)	370.71 (17.8)	566.47 (13.25)	608.52 (17.29)	756.89 (14.54)	796.28 (14.53)	954.98 (20.89)
8	(1:25)	289.33 (40.52)	492.39 (38.22)	471.68 (25.94)	595.9 (31.77)	638.6 (24.66)	813.46 (37.36)
	(1:1)	375.55 (25.92)	502.16 (37.57)	559.6 (27.46)	659.11 (37.25)	708.28 (23.79)	814.29 (25.94)
9	(1:25)	369.78 (20.53)	629.09 (22.01)	595.23 (11.62)	747.03 (15.85)	783.38 (12.01)	1038.47 (19.22)
	(1:1)	429.24 (9.58)	627.28 (31.85)	673.47 (3.17)	828.27 (13.7)	865.21 (8.83)	1046.99 (11.08)
10	(1:25)	292.5 (45.01)	460.77 (38.3)	477.74 (36.04)	579.01 (38.09)	632.16 (31.17)	789.27 (26.18)
	(1:1)	345.43 (20.24)	455.22 (45.2)	546.58 (26.05)	645.23 (22.38)	674.94 (33.51)	775.26 (27.44)

Table 3.2: Average $\overline{TG_L}$ results for $I_{max} = 3$, standard deviation in parenthesis. Variable q indicates the logical network version used.

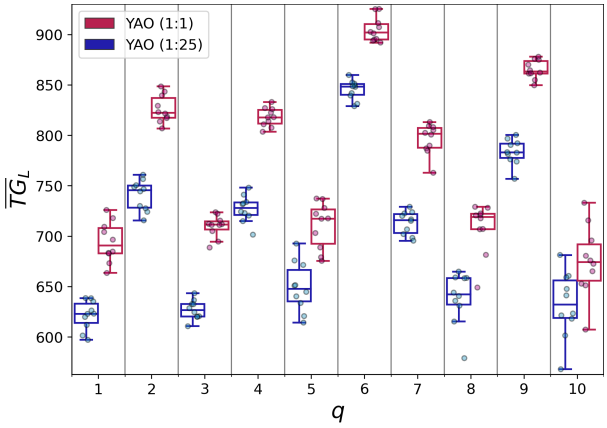


(a) RNG

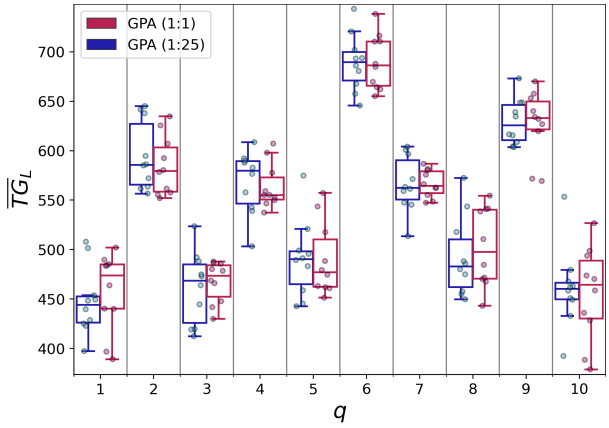
(b) GG



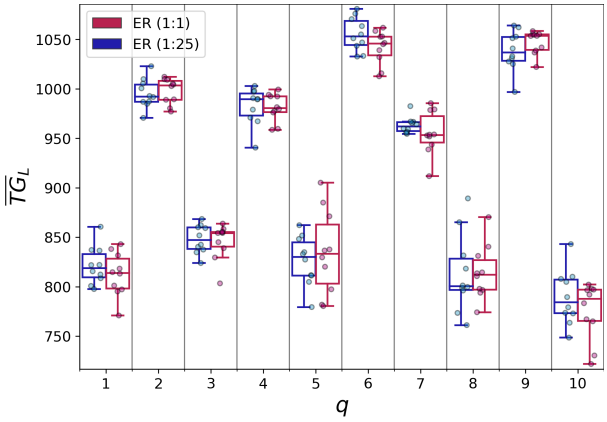
(c) 5NN



(d) YAO



(e) GPA



(f) ER

Figure 3.10: $\overline{TG_L}$ values obtained for each physical-logical interdependent network for $I_{max} = 3$ versus the logical network version q used to build the system.

3.5.3 Physical network model effect

Tables in the appendix section A.4 show the average $\overline{TG}_L$ and standard deviation of a given physical network model m, space s, and $I_{max} = u$. In Figure 3.11 we can see the results of the average $\overline{TG}_L$ for $I_{max} \in \{3, 7\}$ tested. Figures for all I_{max} tested can be found in the appendix section A.5. Our results show that on average we have the following relations.

$$\textbf{(1)}\ \overline{TG}_L(\text{RNG}) \leq \overline{TG}_L(\text{GG}) \leq \overline{TG}_L(\text{5NN}) \leq \overline{TG}_L(\text{YAO}) \leq \overline{TG}_L(\text{ER})$$

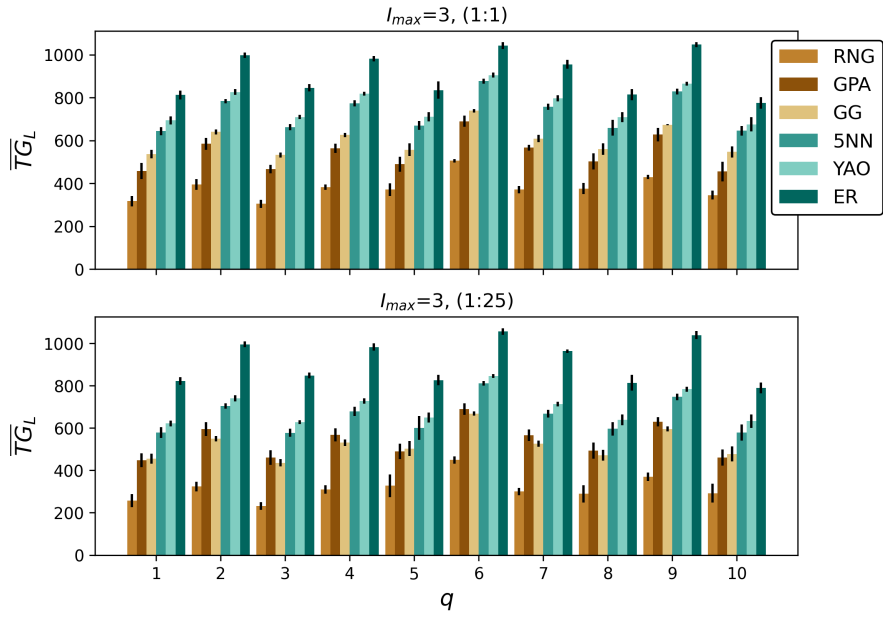
$$\textbf{(2)}\ \overline{TG}_L(\text{RNG}) \leq \overline{TG}_L(\text{GPA}) \leq \overline{TG}_L(\text{5NN})$$

This can be observed regardless of the space s, logical network version q, and I_{max} value u. We observe that the relation between $\overline{TG}_L(\text{GG})$ and $\overline{TG}_L(\text{GPA})$ is not clear as depending on the space shape s and I_{max} value u we can have that $\overline{TG}_L(\text{GPA}) \approx \overline{TG}_L(\text{GG})$, or $\overline{TG}_L(\text{GPA}) < \overline{TG}_L(\text{GG})$, or $\overline{TG}_L(\text{GPA}) > \overline{TG}_L(\text{GG})$.

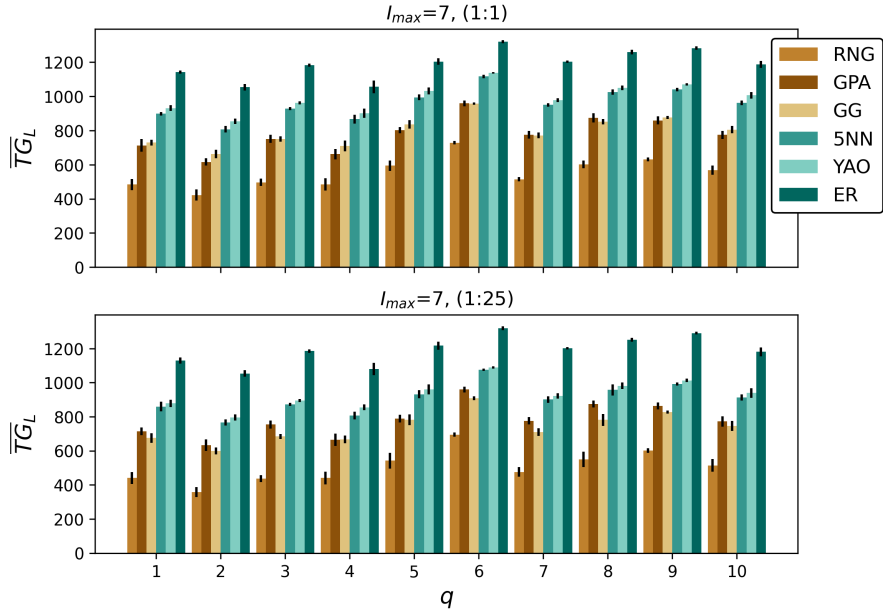
From Table 3.3 we observe that GPA networks have a number of links that is similar to the number of links of RNG networks. However, as we can see from figures in the appendix section A.5, interdependent networks built using RNG networks are on average much more fragile than systems that use GPA networks. Something similar is observed for interdependent networks that use 5NN and YAO networks, where the average number of links of YAO networks is slightly lower than the number of links of 5NN networks, but using a YAO physical network results in interdependent networks with higher $\overline{TG}_L$ values than that of interdependent networks using a 5NN physical network. This suggests that the robustness of these interdependent networks is not directly correlated to the number of physical links that the physical model has, and that the way in which the physical links are allocated might be more relevant.

m	(1:25)	(1:1)
RNG	2453.5 (11.4)	2518.6 (15.0)
GG	3743.2 (25.5)	3907.0 (32.8)
GPA	2599.7 (74.2)	2601.3 (58.1)
5NN	5881.8 (26.3)	6014.8 (61.8)
YAO	5560.7 (9.1)	5858.0 (4.7)
ER	7623.3 (60.7)	7540.8 (99.1)

Table 3.3: Average number of links of each physical network. Parenthesis shows standard deviation.



(a)



(b)

Figure 3.11: Comparison of the average $\overline{TG}_L$ for a given physical network model, for $I_{max} \in \{3, 7\}$. Black line on top shows the $\overline{TG}_L$ standard deviation.

3.5.4 I_{max} value effect

From the definition of our model we know that a node is functional if it has a path to a provider node and at least one of its original interlinks is still functional. The more interlinks a node has, the more robust the node is against failures caused by interlink loss. Thus, we would expect systems with more interlinks to be more robust. The number of interlinks of a system is associated with its I_{max} value and the distribution used to assign the number of interlinks of each logical node. Since, for the interdependent networks tested, the number of interlinks of each logical node was assigned uniformly at random, we have that a higher I_{max} results in a higher number of total interlinks.

We would expect the robustness of a system to monotonically increase with the I_{max} value. However, as we can see in Figure 3.12 there are cases where a higher I_{max} value results in a lower $\overline{TG}_L$. We define $U_{(q,m,s)}$ the set that contains these I_{max} values as follows.

$$U_{(q,m,s)} = \{\hat{u} \in \{1, \ldots, 10\} : \overline{TG}_L(q, m, s, \hat{u}) < \overline{TG}_L(q, m, s, \hat{u} - 1)\}\}$$

Where $\overline{TG}_L(q, m, s, \hat{u})$ is the $\overline{TG}_L$ value obtained in our experiments for an interdependent network built using logical network version q, physical model m, space shape s, and $I_{max} = \hat{u}$. In Table 3.4 we can see all the sets $U_{(q,m,s)}$.

We observe that, for a fixed logical network version q, in most cases the set $U_{(q,m,s)}$ does not depend of the space or physical model. Furthermore, the set $U_{(q,m,s)}$ changes for different logical network versions. An example of this can be seen in Figure 3.12, where for $q = 7$ having $I_{max} = 5$ results in a lower $\overline{TG}_L$ when compared to the $\overline{TG}_L$ values that result for $I_{max} \in \{3, 4\}$. Whereas for $q \in \{1, 3, 7\}$ an $I_{max} = 5$ does not result in a $\overline{TG}_L$ lower than the $\overline{TG}_L$ values obtained for $I_{max} < 5$. This behavior occurs across all logical network versions as we can see from the figures in the appendix section A.6, and Table 3.4. This suggests that there might be some interplay between the logical network version q and the interlink set $I(u)$ ($I_{max} = u$) that results in some interdependent networks having a lower $\overline{TG}_L$ than expected, which results in the emergence of set $U_{(q,m,s)}$. We further analyze this interplay in Chapter 4.

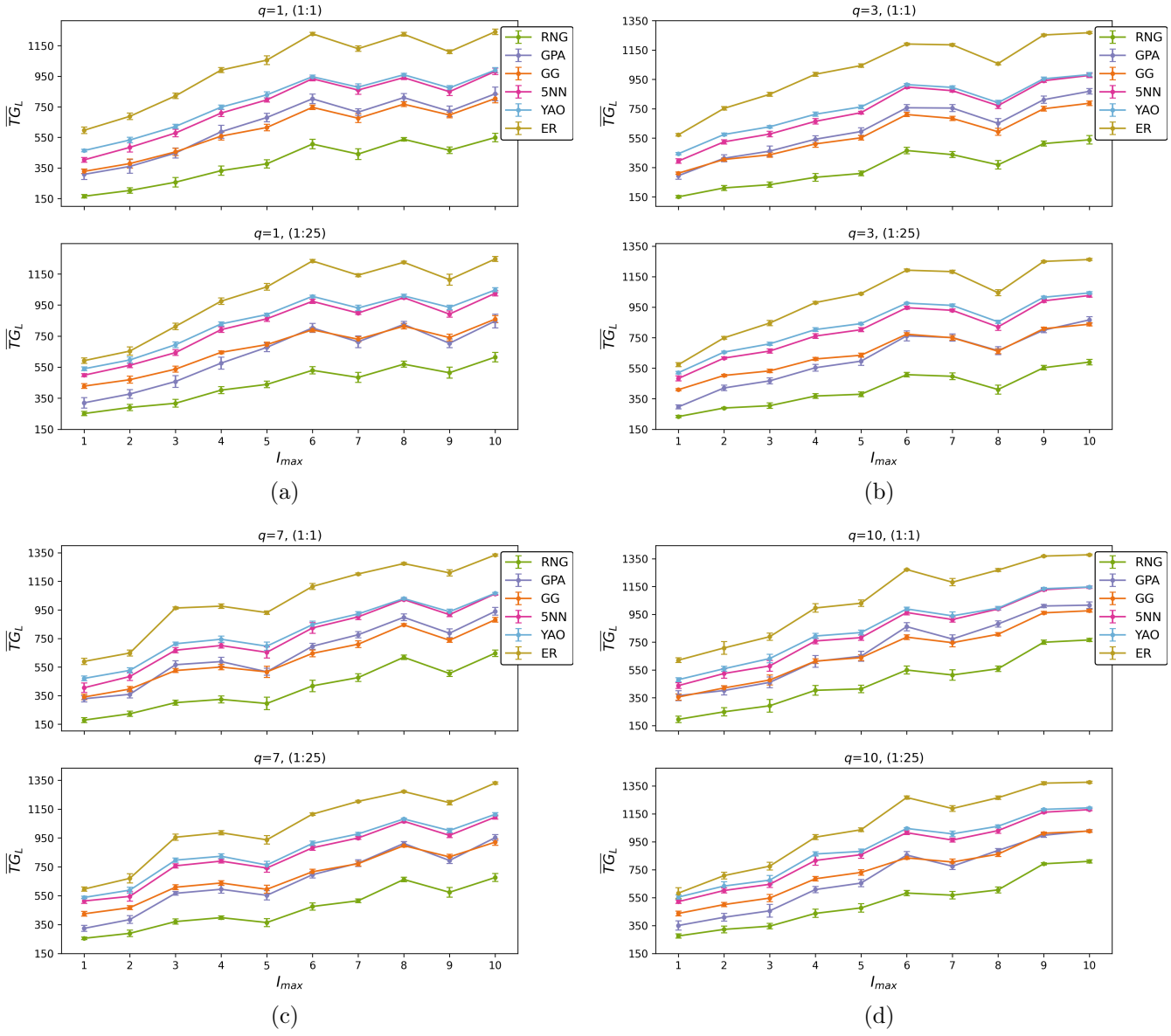


Figure 3.12: Average $\overline{TG}_L$ versus I_{max}, for logic network versions $q \in \{1, 3, 7, 10\}$.

q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	{7,9}	{7,9}	{7,9}	{7,9}	{7,9}	{7,9}
	(1:1)	{7,9}	{7,9}	{7,9}	{7,9}	{7,9}	{7,9}
2	(1:25)	{4,7}	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}
	(1:1)	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}
3	(1:25)	{7,8}	{7,8}	{7,8}	{7,8}	{7,8}	{7,8}
	(1:1)	{7,8}	{7,8}	{7,8}	{7,8}	{7,8}	{7,8}
4	(1:25)	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}
	(1:1)	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}	{4,7,9}
5	(1:25)	{7}	{7}	{7}	{7}	{7}	{7}
	(1:1)	{7}	{7}	{7}	{7}	{7}	{7}
6	(1:25)	{4,6,8,10}	{4,6,8,10}	{4,6,8}	{4,6,8}	{4,6,8}	{4,6,8}
	(1:1)	{4,6,8}	{4,6,8}	{4,6,8}	{4,6,8}	{4,6,8}	{4,6,8,10}
7	(1:25)	{5,9}	{5,9}	{5,9}	{5,9}	{5,9}	{5,9}
	(1:1)	{5,9}	{5,9}	{5,9}	{5,9}	{5,9}	{5,9}
8	(1:25)	{3,7}	{3,7}	{3,7}	{3,7}	{3,7}	{3,7}
	(1:1)	{3,7}	{3,7}	{3,7,9}	{3,7}	{3,7}	{3,7}
9	(1:25)	{4,8,10}	{4,8,10}	{4,8,10}	{4,8,10}	{4,8,10}	{4,8,10}
	(1:1)	{4,8,10}	{4,8,10}	{4,8,10}	{4,8,10}	{4,8,10}	{4,8,10}
10	(1:25)	{7}	{7}	{7}	{7}	{7}	{7}
	(1:1)	{7}	{7}	{7}	{7}	{7}	{7}

Table 3.4: Sets $U_{(q,m,s)}$ for each logical network version q, physical model m, and space shape s.

3.6 Summary

In this chapter we presented a definition of what we consider to be a *robust Internet network*. Using this definition we proposed a physical-logical interdependent network model inspired by the logical Internet network, the physical Internet network, and their interactions. We also proposed a robustness measure according to the presented robustness definition, and the proposed interdependent model.

Using the proposed physical-logical interdependent network model, and robustness measure, we performed experiments to measure the model robustness against physical failures. For the experiments we considered 6 different models to generate the physical network: Relative Neighborhood Graphs (RNG), Gabriel Graphs (GG), 5-Nearest Neighbors (5NN), Yao Graphs (YAO), Geometric Preferential Attachment (GPA), and Erdös-Rényi (ER). We also considered two space shapes as spatial constraints: a space with a (1:25) width to length ratio based on continental Chile's geography, and a square space with a (1:1) width to length ratio. For each physical model, and each space shape we generated 10 different physical networks according to 10 different node allocation configurations. For the interlinks we considered $I_{max} \in \{1, \ldots, 10\}$, which resulted in varying amounts of interlinks. For the logical network we generated 10 different logical networks. Thus, we tested a total of 12,000 different interdependent systems against physical random attacks.

The results in this chapter show that, on average, physical-logical interdependent networks present a continuous decay against physical random attacks. These results suggest that, on average, physical-logical interdependent networks undergo a second order phase transition against physical random attacks. However, upon further inspection we observe that there are attack iterations that result in an abrupt collapse of the network. This means that there is a mix of attacks that result in first order phase transitions, and attacks that do not. Furthermore, in most cases, most of these iterations result in a first order phase transition.

As for the space shape effect, we found that interdependent networks built using physical networks based on RNG, GG, 5NN, and YAO models over a (1:1) space are more robust than those built over a (1:25) space. For the case of interdependent networks built using physical networks based on GPA, and ER models the space shape effect is not clear. This behavior can be explained because RNG, GG, 5NN, and YAO models heavily on the node allocation configuration. Since the location of each node is selected uniformly at random, changing the space shape from (1:1) to (1:25) results in noticeable changes in the node allocation configuration, with nodes being much closer in one axis than the other for s = (1:25). For GPA, and ER models, node allocation does not play such a crucial role. In GPA networks the role of node allocation is only relevant to decide whether a node will be included or not in the preferential attachment process associated with a certain node, and ER networks

completely ignore node allocation.

Our results also show that the physical model used to generate the physical network does impact the robustness of the physical-logical interdependent system. We found that the most fragile systems use RNG model, whereas the most robust systems use ER model. Although RNG networks have on average the lowest number of links, and ER networks have on average the highest number of links, we observe that the number of physical links is not directly related with the system robustness. These results suggest that the way in which the physical links are allocated might be more relevant.

Given the characteristics of the proposed physical-logical interdependent network model we would expect interdependent networks with more interlinks to be more robust. More specifically we would expect the robustness of an interdependent network to monotonically increase with the I_{max} value. However, we found that this is not always the case. We found that, given a fixed logical network version q, it is possible to find one or more I_{max} values such that the robustness of interdependent networks built using a lower I_{max} results in a more robust interdependent network. Here, given logical network version q, physical model m, and space shape s we defined the set $U_{(q,m,s)}$ that contains I_{max} values $\hat{u}$ such that systems built using $I_{max} = \hat{u} - 1$ are more robust systems built using $I_{max} = \hat{u}$. We found that, in most cases, the values contained in $U_{(q,m,s)}$ do not depend on the space or physical model, but they do vary with the logical network version q. Suggesting that there might be some interplay between the logical network version and the interlink set which results in this behavior. We further analyze this interplay in Chapter 4.

Chapter 4

Interplay between the logical network and the interlinks

In the previous chapter we found that, contrary to the intuition, there are cases where a higher I_{max} does not result in a more robust interdependent network. To further understand this phenomenon we defined the set $U_{(q,m,s)}$. The set $U_{(q,m,s)}$ contains all the I_{max} values $\hat{u}$ such that the robustness of the interdependent network built using the interlink set $I(\hat{u})$ is lower than the robustness of the interdependent network built using the interlink set $I(\hat{u}-1)$, given logical network version q, physical model m, and space s. We found that for a fixed logical network version q, the set $U_{(q,m,s)}$ presents very few variations for different spaces and physical models. These results suggest that there might be some interplay between the logical network version q and the interlink set $I(u)$ ($I_{max} = u$) that strongly affects the emergence of the set $U_{(q,m,s)}$.

In this chapter we analyze the interplay between the logical network and the interlink set $I(u)$. Using the results from the analysis, we present and test a hypothesis to explain the emergence of the set $U_{(q,m,s)}$ as shown in section 3.5.4. We find that the set $U_{(q,m,s)}$ is strongly affected by a special type of logical node; we refer to these logical nodes as "bridge nodes".

4.1 Logical network analysis

In the previous chapter, we showed that given two I_{max} values u_1, u_2 with $u_1 < u_2$, we would expect that $\overline{TG_L}(q, m, s, u_1) \leq \overline{TG_L}(q, m, s, u_2)$. However, in section 3.5.4 we found that this is not always true, and that given the logical network version q, the physical model m,

and the space s, it is possible to find a set $U_{(q,m,s)}$ of I_{max} values as follows.

$$U_{(q,m,s)} = \{\hat{u} : \overline{TG_L}(q, m, s, \hat{u}) < \overline{TG_L}(q, m, s, \hat{u} - 1)\}\}$$

where $\overline{TG}_L(q, m, s, \hat{u})$ is the $\overline{TG}_L$ value obtained in our experiments for an interdependent network built using logical network version q, physical model m, space shape s, and $I_{max} = \hat{u}$.

For a fixed q, the set $U_{(q,m,s)}$ in most cases does not depend on the space shape s or physical model m. This suggests that there could be some weak point in the logical network that becomes particularly fragile to physical random attacks when paired with the interlink set $I(\hat{u})$ with $\hat{u} \in U_{(q,m,s)}$.

To test this, we started by searching for nodes that could act as weak points in the logical network. Here, we used the same physical-logical interdependent networks tested in Chapter 3.4. For each logical network q, and each provider configuration u, we removed a single logical node $v_L \in V_L$ and observed the number of logical nodes lost $(N_L - N_L^f)$ after the removal. In these tests we did not consider the interactions between the logical and the physical network, that is, we observed the effect of removing a single logical node over the isolated logical network. We repeated this process for each logical node v_L for each logical network, and each provider configuration u.

In Table 4.1 we can see the total percentage of logical nodes attacked that result in a given range of logical nodes lost $(N_L - N_L^f)$. These results were obtained across all logical network versions, and all provider node configurations. We observe that 84.5% of the nodes result in a $(N_L - N_L^f) = 1$. This means that most single node removals result in only losing the removed node itself. However, we also observe that there are nodes that result in a higher number of lost nodes, with some of them resulting in $(N_L - N_L^f) > 150$, that is, more than 50% of the logical nodes are lost after removing a single logical node. Since here we are not considering the interactions with the physical network, these nodes are lost because they lost access to all 6 provider nodes after the removal of a single logical node. Furthermore, Table 4.1 shows the percentage of provider nodes that result in a given range of logical nodes lost. Here, we can see that most nodes that result in $(N_L - N_L^f) > 1$ are not provider nodes. We will refer to nodes that result in $(N_L - N_L^f) > 1$ as *bridge nodes*.

- **Bridge node**: A bridge node is a node that acts as a bridge between areas of the network that contain one or more provider nodes, to areas that do not contain any provider node. If a bridge node is removed from the network the areas that do not contain any provider node lose all paths to a provider node, and thus become non-functional.

$(N_L - N_L^f)$	Total % of nodes	% of provider nodes
1	84.5	1.66
(1,3]	11.57	0.25
(3,5]	1.9	0.027
(5,15]	1.56	0.027
(15,30]	0.07	0.0
(30,60]	0.07	0.003
(60,90]	0.07	0.007
(90,120]	0.0	0.0
(120,150]	0.05	0.0
(150,180]	0.02	0.003
(180,210]	0.08	0.007
(210,240]	0.08	0.01
(240,270]	0.03	0.007
(270,300]	0.01	0.0

Table 4.1: Total percentage of logical nodes attacked or removed, that result in a given $(N_L - N_L^f)$. Third column shows the percentage of provider nodes that result in a given $(N_L - N_L^f)$. Results were obtained for all 10 logic network versions, and all 10 provider configurations.

In our model, we observe that logical bridge nodes in most cases are not provider nodes. However, in the actual logical Internet network the links between logical nodes are highly influenced by the business decisions of the administrative entities behind them. These administrative entities will do their best to ensure connections with nodes that can transit their traffic to the rest of the Internet, such as ISP nodes or "provider nodes". Thus, if there are bridge nodes in the actual logical Internet network, these are likely to be provider nodes.

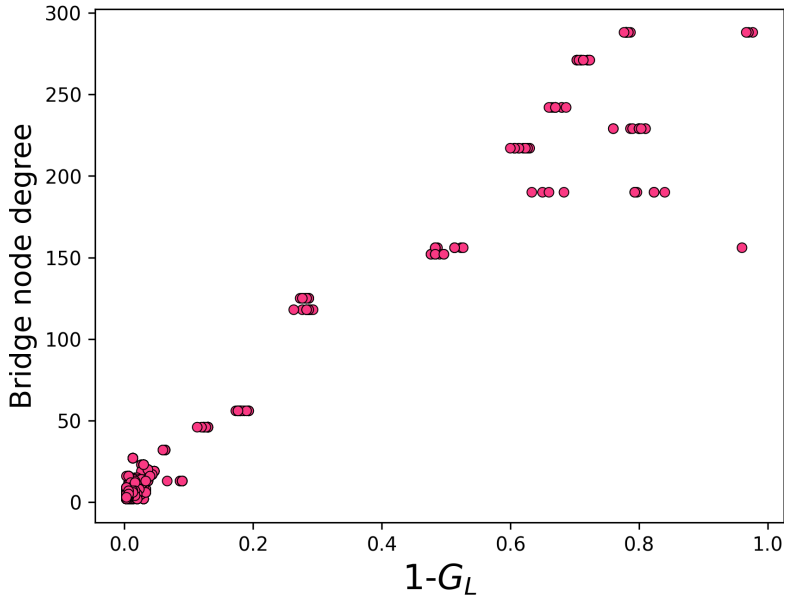
Note that all bridge nodes are cut vertex or cut nodes: a node that if removed results in an increment in the number of connected components. However, being a cut node is not sufficient to be a bridge node since, after removing a cut node, it is possible that each resulting connected component contains at least one provider node, and thus remain functional (see section 3.3, Figure 3.2).

Given that the logical networks tested are modeled after Scale-Free networks, we must wonder whether there is a relation between bridge nodes and "hubs" or high degree nodes [15]. Hubs in Scale-Free networks have been pointed out before as a source of fragility in interdependent networks [21]. In Figure 4.1(a), we can see that bridge nodes that result in a higher damage after being removed are indeed nodes of higher degree. However, from table 4.1 we can see that most bridge nodes damage less than 10% of the network, and as we can see in 4.1(a) these bridge nodes are not hubs. Thus, although bridge nodes are not the same as hubs, bridge nodes that result in higher damage are likely to be hubs within the logical network. In Figure 4.1(b) we can see the percentage of nodes from the nodes lost that belonged to a cluster with more than one node $NC_{>1}$. Here, $NC_{>1}$ is defined as $NC_{>1} = ((N_L - N_L^f) - NC_{=1})(N_L - N_L^f)^{-1}$ with $NC_{=1}$ the number of nodes lost after removing a bridge node that belonged to a cluster of size 1. In Figure 4.1(b) we can see that there are bridge nodes that only disconnect clusters of size 1 ($NC_{>1} = 0$), and bridge nodes that disconnect clusters containing more than one node. Approximately 19% of the bridge nodes found on the logical networks tested disconnect clusters of varying sizes after being removed. Furthermore, in figure 4.1(b) we observe that all bridge nodes whose removal result in the loss of at least 10% of the network also remove clusters of varying sizes.

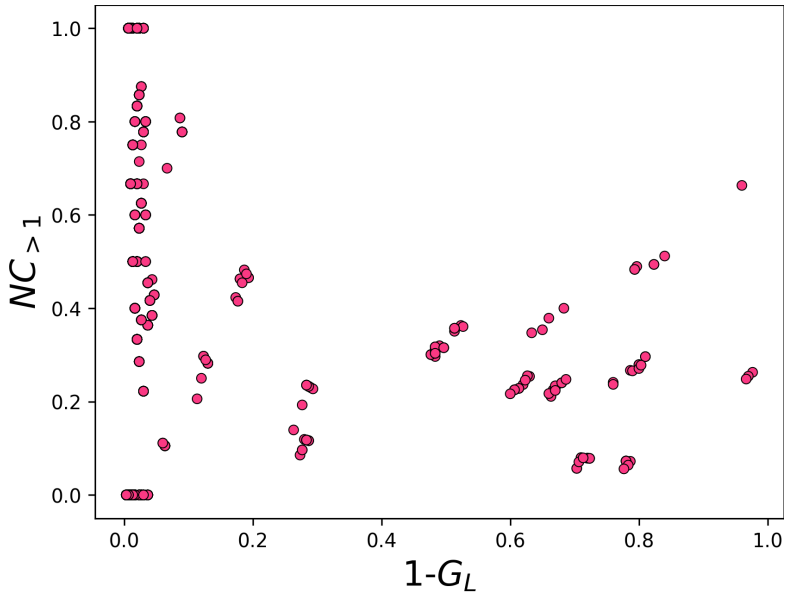
Using the concept of bridge nodes, we proceeded to observe if there was a relation between the $\overline{TG}_L$ and the damage caused by bridge nodes, given its number of interlinks. To do this, let us define the damage contribution $DC(v_L, q, u)$ of bridge node v_L given the interlink set $I(u)$, and the logical network version q as follows.

$$DC(v_L, q, u) = \frac{D(v_L, q, u)}{N_{I(u)}(v_L)}$$

where u is the I_{max} value, $D(v_L, q, u)$ corresponds to the damage $(1-G_L)$ caused by removing node v_L from the isolated logical network q given the provider configuration associated to



(a)



(b)

Figure 4.1: Each dot represents the effect of removing a single bridge node. (a) Degree of each bridge node versus the damage caused by its removal ($1 - G_L$). (b) Percentage of nodes from the nodes lost that belonged to a cluster of size at least two.

u, and $N_{I(u)}(v_L)$ is the number of interlinks that logical node v_L has for the given interlink set $I(u)$. Using the damage contribution of a single bridge node we define the total damage contributed by the bridge nodes $TDC(q, u)$.

$$TDC(q,u) = \sum_{v_L \in V_L^{(bn,q,u)}} DC(v_L, q, u)$$

where $V_L^{(bn,q,u)}$ contains all the bridge nodes of the logical network version q, and the provider configuration associated to $I_{max} = u$. Here, for a fixed q, the value $TD(v_L, q, u)$ will vary according to the interlink set $I(u)$. This happens because: (1) the set $V_L^{(bn,q,u)}$ may vary depending on the provider configuration associated to the interlink set $I(u)$, and (2) different interlink sets may assign a different number of interlinks to each bridge node in the set.

With this we measured the relation between the damage contributed by bridge nodes over a given logical network q and the interdependent network robustness. In Table 4.2 we can see the Pearson's correlation between TDC and $\overline{TG}_L$ for each model m, space s, and logic network version q. Here, we observe that there is an inverse relation between the total damage contributed by the logical bridge nodes and the interdependent network robustness. We also note that for a fixed q, and a fixed m, this correlation has minimal variation across different space shapes. This suggests the set $U_{(q,m,s)}$ emerges due to bridge nodes $v_L \in V_L^{(bn,q,\hat{u})}$ having a higher damage contribution for $\hat{u} \in U_{(q,m,s)}$. Therefore, set $U_{(q,m,s)}$ would be related to the number of interlinks that each $v_L \in V_L^{(bn,q,u)}$ has, and the damage $D(v_L, q, u)$ caused by its removal.

The results shown here suggest that we may be able to decrease the size of set $U_{(q,m,s)}$ by increasing the number of interlinks associated with bridge nodes. In the remainder of this chapter we will test this hypothesis.

q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	-0.955	-0.97	-0.985	-0.983	-0.985	-0.992
	(1:1)	-0.942	-0.976	-0.98	-0.987	-0.988	-0.991
2	(1:25)	-0.927	-0.952	-0.966	-0.962	-0.962	-0.972
	(1:1)	-0.934	-0.963	-0.967	-0.972	-0.974	-0.972
3	(1:25)	-0.931	-0.959	-0.964	-0.971	-0.979	-0.988
	(1:1)	-0.939	-0.969	-0.965	-0.981	-0.986	-0.988
4	(1:25)	-0.91	-0.945	-0.955	-0.957	-0.966	-0.983
	(1:1)	-0.918	-0.956	-0.951	-0.971	-0.976	-0.986
5	(1:25)	-0.94	-0.968	-0.975	-0.98	-0.982	-0.995
	(1:1)	-0.926	-0.968	-0.976	-0.984	-0.986	-0.995
6	(1:25)	-0.953	-0.964	-0.97	-0.967	-0.972	-0.968
	(1:1)	-0.947	-0.968	-0.975	-0.972	-0.973	-0.97
7	(1:25)	-0.845	-0.882	-0.916	-0.903	-0.914	-0.941
	(1:1)	-0.854	-0.899	-0.902	-0.928	-0.926	-0.935
8	(1:25)	-0.917	-0.941	-0.931	-0.946	-0.948	-0.961
	(1:1)	-0.922	-0.952	-0.93	-0.957	-0.956	-0.954
9	(1:25)	-0.909	-0.934	-0.939	-0.941	-0.945	-0.954
	(1:1)	-0.906	-0.944	-0.928	-0.953	-0.96	-0.962
10	(1:25)	-0.936	-0.964	-0.974	-0.977	-0.978	-0.99
	(1:1)	-0.924	-0.964	-0.974	-0.978	-0.984	-0.988

Table 4.2: Pearson's correlation between TDC and $\overline{TG}_L$ for each model m, space s, and logic network version q.

4.2 Experiments

In this section we will describe the experiment conditions to test if we can decrease the size of the set $U_{(q,m,s)}$ by adding interlinks to bridge nodes.

4.2.1 Test

In section 4.1 we showed that there is an inverse correlation between the total damage contributed by the logical bridge nodes and the robustness of the interdependent network, which suggests that the emergence of set $U_{(q,m,s)}$ is related to the number of interlinks that each $v_L \in V_L^{(bn,q,u)}$ has, and the damage $D(v_L, q, u)$ caused by its removal. Here, we want to test the relation between the emergence of the set $U_{(q,m,s)}$ and the number of interlinks that bridge nodes have.

To test this, we will add interlinks to bridge nodes such that for each interlink set $I(u)$, bridge nodes have the highest number of interlinks possible u. This way, bridge nodes will have more interlinks as the I_{max} value increases.

However, since around 15% of the logical nodes correspond to bridge nodes, adding the maximum amount of interlinks to each bridge node would have a noticeable impact in the interlink distribution. To avoid this, we will only add interlinks to bridge nodes that result in $(N_L - N_L^f) \geq 0.1 \times N_L$. That is, we will add interlinks only to bridge nodes that result in the loss of at least 10% of the logical network after being removed, which correspond to less than 0.5% of the logical nodes across all logical network versions, and provider configurations.

4.2.2 Physical-logical interdependent networks

For these experiments we will use the physical-logical interdependent networks tested in Chapter 3.4, with their physical networks built over a (1:25) space. Previously we observed that the set $U_{(q,m,s)}$ in most cases is not influenced by the space used to build the physical network (see section 3.5.4, Table 3.4). Furthermore, in section 4.1 we observed that correlation between the total damage contributed by the logical bridge nodes and the interdependent network robustness has minimal variations across different space shapes. Thus, we will not test interdependent networks with physical networks built over a (1:1) space.

4.2.3 Adding interlinks to bridge nodes

For these experiments, we will add interlinks to bridge nodes that result in the loss of at least 10% of the logical network after being removed. For the experiments we add interlinks as follows.

- **Interlink addition**: Given $I_{max} = u$, q the logical network version, we define the set of bridge nodes that result in the loss of at least 10% of the logical network after being removed $B_h^{(q,u)}$

$$B_h^{(q,u)} = \{v_L \in V_L^{(bn,q,u)} : D(v_L, q, u) \geq 0.1 \times N_L\}$$

  For each $v_L \in B_h^{(q,u)}$, we will add $(u - N_{I(u)}(v_L))$ interlinks at random. Here, u is the maximum number of interlinks that each logical node can have ($I_{max} = u$), and $N_{I(u)}(v_L)$ is the number of interlinks that the logical node v_L has for the given interlink set $I(u)$. The interlinks added must be different to those already present in $I(u)$. Notice that it is possible that $(u - N_{I(u)}(v_L)) = 0$. Particularly, we have that no extra interlinks are added to interdependent networks using the interlink set $I(1)$ as all logical nodes already have the maximum number of interlinks.

Cost of adding interlinks

In our model, adding interlinks between an existing physical node and a logical node can be interpreted as having an autonomous system allocate physical resources in a location that is considered to be a PoP. This means that it can be interpreted as an AS buying resources from a datacenter, renting space in an office building to set up part of its network, building a new structure within a neighborhood, or using resources that already belonged to the administrative entity in charge of the AS.

Each possible scenario has its own challenges that will add to the overall cost of adding an interlink. Thus, the cost of adding an interlink can greatly vary from case to case. Since there is not a reasonable way to estimate the cost from the perspective of the proposed physical-logical interdependent network model, we will not consider the costs associated with interlink addition.

4.3 Results

In this section we present and discuss the results obtained according to the experimental settings described in section 4.2. The results shown here were obtained by testing the robustness of a total of 6.000 different interdependent networks against physical random attacks. These interdependent networks were obtained by adding interlinks to physical-logical interdependent networks tested in Chapter 3.4, with their physical networks built over a (1:25) space.

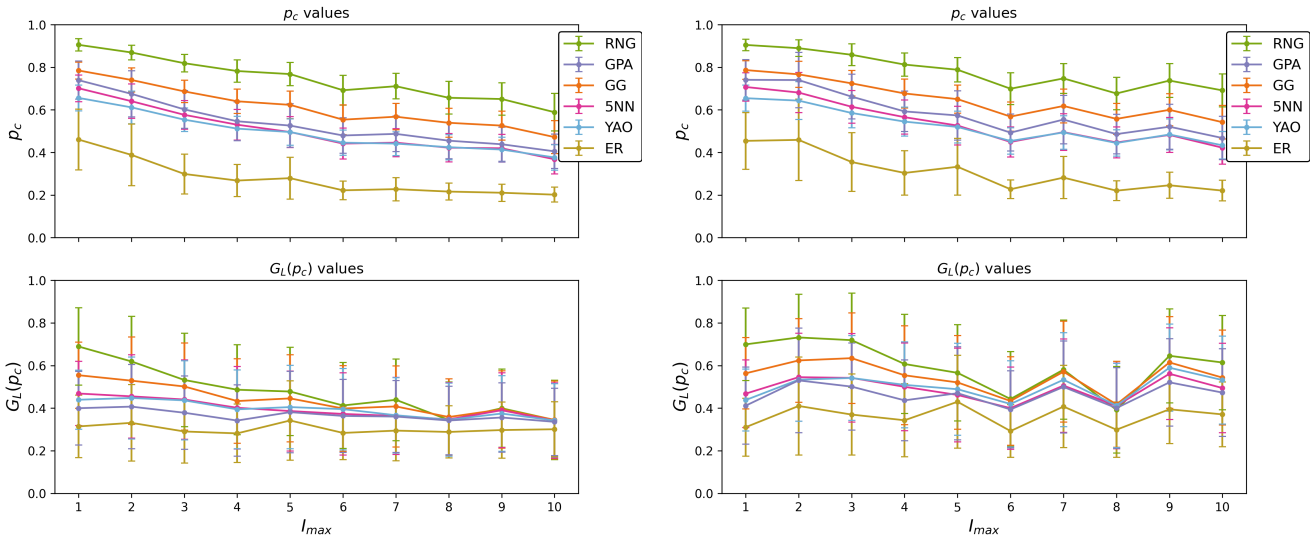
Figures 4.3, 4.4, and 4.5 shows the comparison of the average $\overline{TG}_L$ value of interdependent networks with and without extra interlinks added to bridge nodes in $B_h^{(q,u)}$. We observe that

after adding interlinks, we obtain a behavior that is much closer to a $\overline{TG}_L$ that monotonically increases with the I_{max} value (see section 3.5.4). Furthermore, in Table 4.3 we can see that after adding extra interlinks to bridge nodes in $B_h^{(q,u)}$ on interdependent networks with $q = 1$, the average robustness of each interdependent network either increases or is maintained. This happens for all $q \in \{1, \ldots, 10\}$ (see appendix section B.1).

Something similar is observed for attack iterations where the physical-logical network abruptly collapses. In Table 4.4 we can see the fraction of iterations that undergo an abrupt decay after extra interlinks have been added, for $q = 1$. The remaining tables can be found in the appendix section B.1. In Figure 4.2 we observe that, for systems with $q = 1$, after adding extra interlinks each p_c values either decreases or is maintained, and the G_L value at p_c also decreases. Furthermore, the p_c values show a behavior that is much closer to monotonically decreasing functions. This can be observed regardless of the logical network version q (see appendix section B.2).

$q = 1$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	164.83 (11.07)	327.53 (14.72)	307.93 (33.96)	402.73 (15.78)	463.75 (8.68)	596.58 (21.47)
	✓	164.86 (13.7)	325.43 (8.99)	308.07 (27.87)	409.96 (16.86)	464.31 (7.33)	592.63 (16.49)
2	×	202.29 (17.89)	378.51 (29.48)	359.78 (45.08)	484.42 (30.19)	532.64 (17.85)	687.58 (21.5)
	✓	235.81 (13.92)	438.24 (19.11)	453.74 (34.15)	566.87 (17.3)	611.95 (14.61)	810.06 (23.25)
3	×	256.55 (31.17)	455.07 (24.21)	447.33 (32.6)	578.39 (25.02)	621.42 (13.73)	821.26 (18.12)
	✓	315.61 (15.43)	542.27 (14.27)	575.83 (20.42)	693.24 (17.59)	735.49 (8.28)	984.9 (12.36)
4	×	332.13 (29.83)	558.14 (25.86)	586.43 (41.86)	708.9 (22.5)	747.63 (13.52)	990.42 (16.36)
	✓	367.16 (19.05)	604.43 (11.92)	667.08 (29.4)	766.94 (10.95)	802.57 (11.79)	1065.87 (12.7)
5	×	376.92 (26.95)	614.65 (21.6)	679.97 (27.39)	795.38 (14.25)	828.23 (20.28)	1055.31 (28.33)
	✓	397.32 (21.16)	643.85 (24.03)	729.05 (25.21)	834.42 (17.07)	851.58 (13.81)	1124.32 (11.11)
6	×	506.27 (30.75)	746.52 (14.35)	802.33 (31.0)	933.58 (13.19)	946.75 (10.11)	1227.81 (9.5)
	✓	509.79 (28.63)	759.14 (12.06)	819.77 (24.49)	943.82 (13.48)	957.37 (10.94)	1241.04 (6.96)
7	×	440.65 (35.32)	675.17 (28.79)	714.93 (22.19)	859.59 (28.51)	878.59 (21.23)	1130.48 (18.09)
	✓	484.48 (20.85)	729.65 (17.44)	790.6 (9.12)	916.67 (18.64)	940.15 (14.2)	1220.38 (6.77)
8	×	537.49 (11.93)	767.22 (14.86)	810.24 (25.83)	941.13 (13.49)	959.89 (9.11)	1224.65 (12.37)
	✓	548.37 (10.91)	778.8 (12.36)	838.54 (31.89)	965.58 (8.77)	973.07 (9.52)	1246.7 (7.16)
9	×	465.61 (21.66)	696.2 (18.54)	720.65 (34.82)	848.95 (26.03)	873.83 (14.53)	1110.41 (12.29)
	✓	559.66 (17.17)	798.11 (13.36)	877.2 (17.25)	975.6 (13.7)	997.05 (6.71)	1274.64 (6.73)
10	×	548.84 (27.08)	803.96 (27.17)	834.6 (45.24)	981.66 (21.56)	989.59 (16.85)	1240.85 (17.8)
	✓	665.24 (20.89)	891.26 (12.03)	951.28 (23.93)	1077.56 (14.58)	1081.07 (6.38)	1345.49 (7.05)

Table 4.3: Average $\overline{TG_L}$ of interdependent networks with $q = 1$, and $s = (1 : 25)$. Column $+I$ shows whether the interdependent networks has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.



(a) (1:25) with extra interlinks

(b) (1:25)

Figure 4.2: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 1$.

In Table 4.6 we can see the detail of sets $U_{(q,m,(1:25))}$ for interdependent networks with and without extra interlinks. Here, we observe that in most cases the size of set $U_{(q,m,(1:25))}$ decreases after adding interlinks to nodes in $B_h^{(q,u)}$. Even more, we can see that in some interdependent networks the set $U_{(q,m,(1:25))}$ becomes completely empty.

However, we must note that in some cases the size of the set $U_{(q,m,(1:25))}$ does not change after adding extra interlinks. What is even more interesting is that in these cases the contents of set $U_{(q,m,(1:25))}$ do change, meaning that there was indeed a change in the networks' behavior against physical random attacks after adding extra interlinks. We can see something similar on interdependent networks where the size of the set $U_{(q,m,(1:25))}$ decreases, but the new set contains elements that were not present in the original set.

This behavior might be caused by the combined effect of bridge nodes in $V_L^{(bn,q,u)} \setminus B_h^{(q,u)}$, that is, bridge nodes that result in losing less than 10% of the logical nodes. Although most of these nodes damage less than 1% of the logical nodes (see Table 4.1) they represent 15.1% of all the logical nodes. Another explanation may be that the effect of the physical network model becomes more noticeable once we add extra interlinks to bridge nodes in $B_h^{(q,u)}$. The cause could also be related to properties of the interlink set itself. In Table 4.5 we can see that some I_{max} values appear more often in the set $U_{(q,m,s)}$ than others. In particular, $I_{max} = 5$ appear at the same rate before and after adding extra interlinks.

$q = 1$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.762	0.685	0.669	0.757	0.725	0.703	0.745	0.321	0.737	0.463
GG	0.606	0.735	0.668	0.761	0.754	0.66	0.755	0.438	0.707	0.511
5NN	0.547	0.705	0.705	0.737	0.737	0.68	0.753	0.493	0.722	0.578
YAO	0.572	0.738	0.682	0.767	0.763	0.69	0.772	0.548	0.728	0.535
GPA	0.581	0.769	0.69	0.684	0.742	0.656	0.772	0.694	0.715	0.63
ER	0.582	0.769	0.686	0.749	0.837	0.688	0.854	0.807	0.823	0.781

Table 4.4: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks built using $q = 1$, after adding extra interlinks.

Our results suggest that adding more interlinks to bridge nodes in $B_h^{(q,u)}$ does decrease the number of elements found in the set $U_{(q,m,s)}$. Furthermore, adding interlinks to these nodes improves the average robustness of each of these networks. However, we also found that the number of interlinks that bridge nodes in $B_h^{(q,u)}$ have is not enough to fully avoid the emergence of set $U_{(q,m,s)}$. This suggests that some other characteristics such as the effect of bridge nodes in $V_L^{(bn,q,u)} \setminus B_h^{(q,u)}$, the effect of the physical network model, and properties of the interlink set itself may also influence the emergence of set $U_{(q,m,s)}$.

I_{max}	Combined (1:1) + (1:25)	(1:1)	(1:25)	(1:25) + extra interlinks
1	0.0%	0.0%	0.0%	0.0%
2	0.0%	0.0%	0.0%	0.0%
3	10.0%	10.0%	10.0%	0.0%
4	40.0%	40.0%	40.0%	3.33%
5	10.0%	10.0%	10.0%	10.0%
6	10.0%	10.0%	10.0%	0.0%
7	70.0%	70.0%	70.0%	45.0%
8	30.0%	30.0%	30.0%	21.67%
9	40.0%	41.67%	38.33%	8.33%
10	12.5%	11.67%	13.33%	0.0%

Table 4.5: Percentage of sets $U_{(q,m,s)}$ that contain a given I_{max} value u.

q	space	RNG	GG	GPA	5NN	YAO	ER
1	×	$\{7,9\}$	$\{7,9\}$	$\{7,9\}$	$\{7,9\}$	$\{7,9\}$	$\{7,9\}$
	✓	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$
2	×	$\{4,7\}$	$\{4,7,9\}$	$\{4,7,9\}$	$\{4,7,9\}$	$\{4,7,9\}$	$\{4,7,9\}$
	✓	$\{8\}$	$\{8\}$	$\{7\}$	$\{8\}$	$\{8\}$	$\{8\}$
3	×	$\{7,8\}$	$\{7,8\}$	$\{7,8\}$	$\{7,8\}$	$\{7,8\}$	$\{7,8\}$
	✓	$\{5,7\}$	$\{5,7\}$	$\{5,7\}$	$\{5,7\}$	$\{5,7\}$	$\{5\}$
4	×	$\{4,7,9\}$	$\{4,7,9\}$	$\{4,7,9\}$	$\{4,7,9\}$	$\{4,7,9\}$	$\{4,7,9\}$
	✓	ϕ	ϕ	$\{7\}$	$\{7\}$	ϕ	$\{7\}$
5	×	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$
	✓	$\{8\}$	ϕ	ϕ	ϕ	ϕ	ϕ
6	×	$\{4,6,8,10\}$	$\{4,6,8,10\}$	$\{4,6,8\}$	$\{4,6,8\}$	$\{4,6,8\}$	$\{4,6,8\}$
	✓	$\{4,8\}$	$\{4,8\}$	$\{8\}$	$\{8\}$	$\{8\}$	ϕ
7	×	$\{5,9\}$	$\{5,9\}$	$\{5,9\}$	$\{5,9\}$	$\{5,9\}$	$\{5,9\}$
	✓	$\{7,9\}$	$\{7,9\}$	$\{7,9\}$	$\{7,9\}$	$\{7,9\}$	$\{7\}$
8	×	$\{3,7\}$	$\{3,7\}$	$\{3,7\}$	$\{3,7\}$	$\{3,7\}$	$\{3,7\}$
	✓	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$
9	×	$\{4,8,10\}$	$\{4,8,10\}$	$\{4,8,10\}$	$\{4,8,10\}$	$\{4,8,10\}$	$\{4,8,10\}$
	✓	$\{8\}$	$\{8\}$	ϕ	ϕ	ϕ	ϕ
10	×	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$	$\{7\}$
	✓	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ

Table 4.6: Sets $U_{(q,m,(1:25))}$ for each logical network version q, physical model m, and space shape $s = (1{:}25)$. Column $+I$ shows whether the interdependent network has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

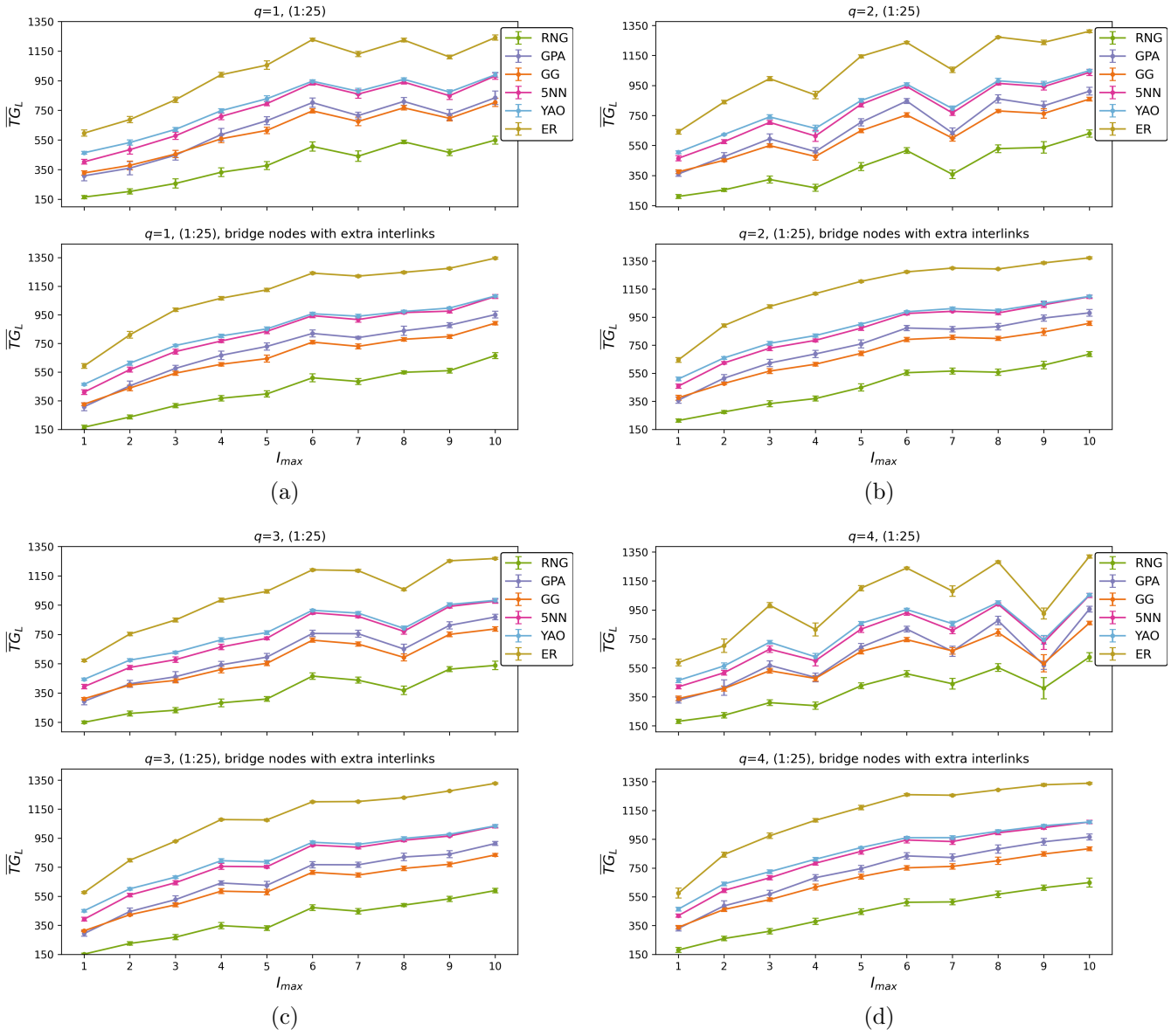


Figure 4.3: Average $\overline{TG}_L$ versus I_{max} with and without added interlinks for logic network versions $q \in \{1, 2, 3, 4\}$.

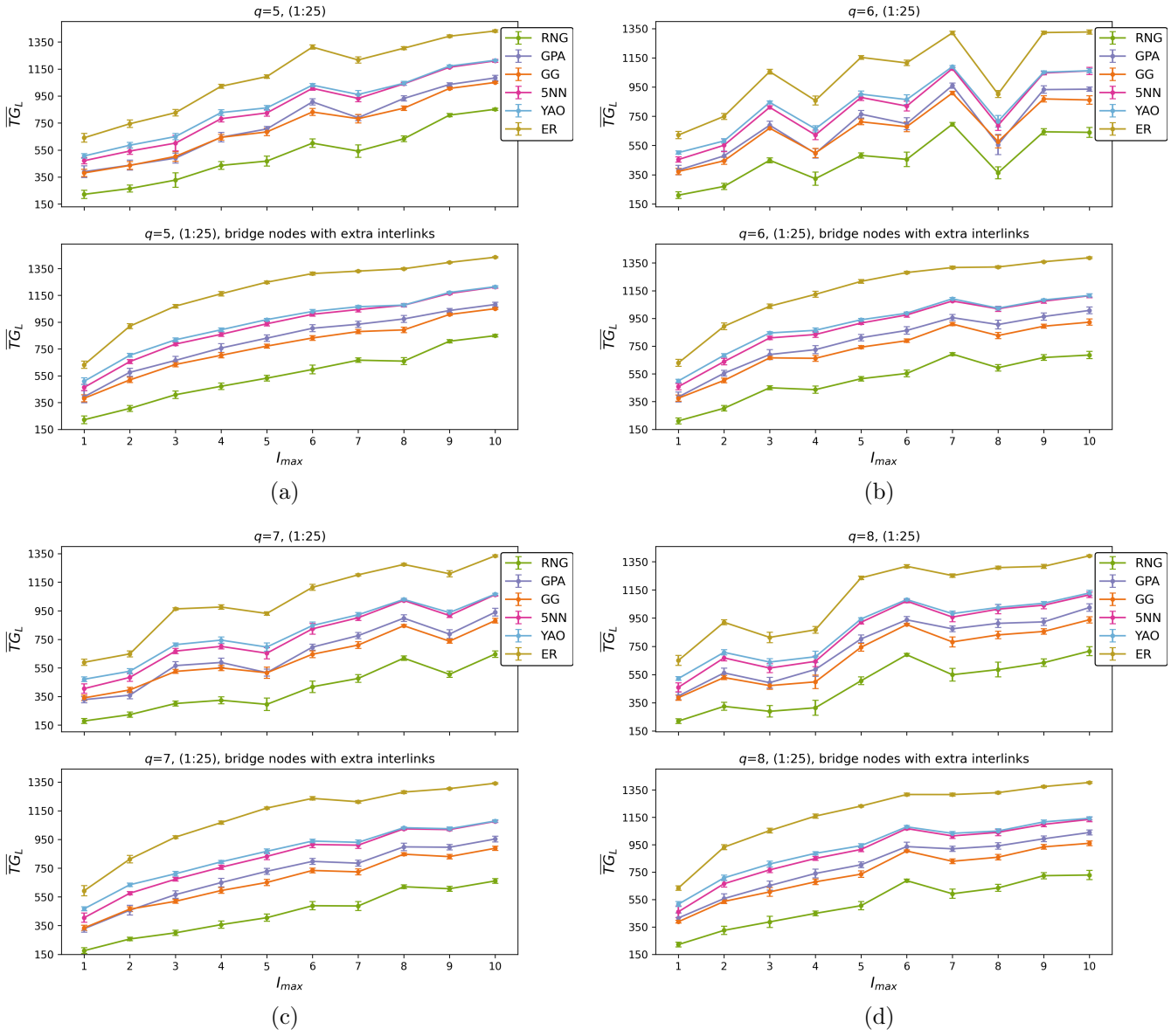
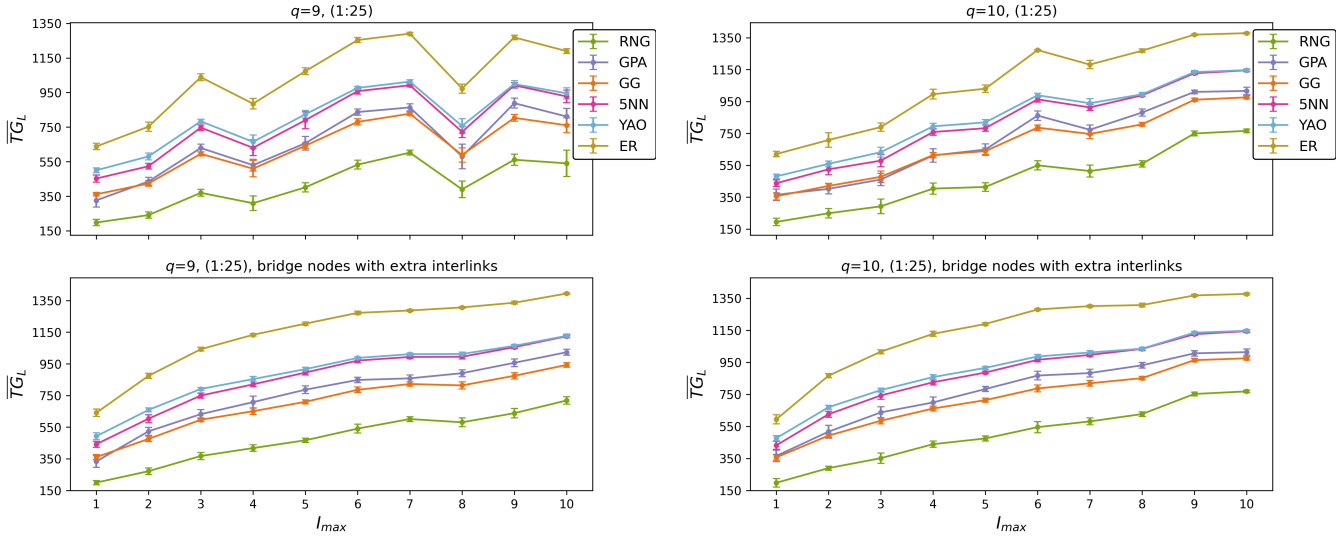


Figure 4.4: Average $\overline{TG}_L$ versus I_{max} with and without added interlinks for logic network versions $q \in \{5, 6, 7, 8\}$.



(a) (b)

Figure 4.5: Average $\overline{TG}_L$ versus I_{max} with and without added interlinks for logic network versions $q \in \{9, 10\}$.

4.4 Summary

In Chapter 3 we found that, contrary to the intuition, there are cases where a higher I_{max}, that is, a higher number of interlinks, does not result in a more robust interdependent network. To capture this behavior, given a logical network version q, physical model m, and space shape s, we defined the set $U_{(q,m,s)}$ that contains I_{max} values $\hat{u}$ such that interdependent networks built using $I_{max} = \hat{u} - 1$ are more robust than interdependent networks built using $I_{max} = \hat{u}$. The results from Chapter 3 showed that there might be some interplay between the logical network version and the interlink set that causes this behavior. To better understand these findings, in this chapter we analyzed this interplay.

First we analyzed each logical network tested in Chapter 3. Here, we found there are nodes in the logical network that result in the loss of more than 50% of the network after being removed from the isolated logical network. We found that these nodes result in such severe damage because they act as bridges between areas of the network that contain one or more provider nodes, to areas that do not contain any provider node. Thus, we refer to these types of nodes as *bridge nodes*. We found that approximately 15% of the logical nodes correspond to bridge nodes. However, most of these bridge nodes result in the loss of less than 10% of the network after being removed. Our analysis found that only 0.5% of logical nodes correspond to bridge nodes that result in the loss of more than 10% of the logical network. Furthermore, we found that bridge nodes that result in higher damage are likely to be hubs within the logical network, although not all bridge nodes are hub nodes.

Using the concept of bridge nodes, we studied the relation between the total damage contributed by logical bridge nodes and the interdependent network robustness. Here, the damage contributed by a bridge node was measured as the damage caused by a bridge node divided by the number of interlinks connected to said bridge node. Our results show that there is an inverse relation between the total damage contributed by logical bridge nodes and the interdependent network robustness, suggesting that we may be able to decrease the size of set $U_{(q,m,s)}$ by increasing the number of interlinks associated with bridge nodes.

To test this hypothesis we studied the robustness of physical-logical interdependent networks after adding interlinks to bridge nodes. Specifically, we added interlinks such that each bridge node has the highest number of interlinks possible $I_{max} = u$. Since approximately 15% of the logical nodes correspond to bridge nodes, adding the maximum amount of interlinks to each bridge node would have a noticeable impact in the interlink distribution. To avoid this, we decided to add interlinks only to bridge nodes that result in the loss of at least 10% of the logical network after being removed, which corresponds to less than 0.5% of the logical nodes across all logical network versions and provider configurations.

Our results show that, in most cases, adding interlinks to bridge nodes that result in the loss of at least 10% of the logical network does decrease the size of the set $U_{(q,m,s)}$. However, there are some cases where the size of $U_{(q,m,s)}$ does not change, but the contents of the set do change. We also found that in some cases the size of the set $U_{(q,m,s)}$ decreases, and/or changes. In terms of robustness, we found that adding interlinks to bridge nodes that result in the loss of at least 10% of the logical network improves the overall robustness. Even more, after adding extra interlinks, we obtain a behavior that is much closer to a robustness that monotonically increases with the I_{max} value. Our results show that adding more interlinks to bridge nodes that result in the loss of at least 10% of the logical network does decrease the number of elements found in the set $U_{(q,m,s)}$. Furthermore, adding interlinks to these nodes improves the average robustness of each of these interdependent networks. However, our results also suggest that some other characteristics such as the effect of bridge nodes that result in the loss of less than 10% of the logical network, the effect of the physical network model, and properties of the interlink set itself may also influence the emergence of set $U_{(q,m,s)}$.

Chapter 5

Effect of adding physical links

In this chapter we test the effect of adding links to the physical network over our physical-logical interdependent network model. We use four physical link addition strategies: Random, Distance, Local hubs, and Degree based addition.

We compare the effects of adding physical links over our interdependent model for different space shapes, and physical network models. To test the robustness we use physical random attacks.

5.1 Background

Within the area of communication networks, the addition of physical links has been used before to enhance the network's robustness and improve the recovery process after failure [105, 5, 78]. The addition of physical links increases the number of possible paths that can be used as a backup within the physical communication network. Furthermore, links can be added to the physical network with the specific goal of adding paths with high availability within the network [105, 5].

Similarly, within the area of complex networks, we can find studies regarding the effect of adding links within a single network of an interdependent system (connectivity links) over its robustness [55, 112, 59]. Here, the networks do not present a consumer-provider behavior, and the link addition is made using link addition strategies that use a variety of network properties and centrality measures such as degree, betweenness, algebraic connectivity, and inter degree-degree difference [55]. These works show that adding connectivity links using this type of link addition strategy does improve the robustness of interdependent networks.

Since our interdependent model is inspired by a communication network (the Internet), having more links within a network could increase the interdependent network's robustness by increasing the number of alternative paths from consumer nodes to provider nodes. Furthermore, it has been shown that adding connectivity links to interdependent networks does improve its robustness, even when it does not exhibit a consumer-provider behavior. In section 3.5.3 we observed that the number of links in the physical network is not directly related to the Internet's robustness, and that systems with similar numbers of physical links might show very different robustness behaviors. This suggests that the way in which physical links are allocated into space also plays a role in the robustness of our physical-logical model.

Our model currently does not handle SRLGs, thus in order to add a new physical link we must connect two nodes that were not previously connected. A new connection is interpreted as a single link even if multiple fibers or physical elements belonging to different SRLGs are added in the real world. As defined in section 3.2.2, different physical links are assumed to belong to different bundles. Thus, for the proposed model, adding a physical link ensures that the new physical connection does not share risks with previously existing elements.

To better understand the effect of having more physical links over the robustness of our physical-logical model against physical random attacks, we test the effect of adding links to the physical network. Furthermore, we want to add links using strategies that are simple enough to be used even when information of the physical network is incomplete or not accurate enough to use more complex strategies.

5.2 Physical link addition strategies

We want to measure the effect of adding links to the physical network using simple strategies, without modifying the logical network nor the interlinks. As mentioned in section 5.1, new links added cannot be already contained in the physical network being enhanced. Thus, for a given strategy, for each physical network $P_j(m, s)$, a different set of links must be generated. Here we developed and tested the following link addition strategies:

- **Random link addition:** For each graph (physical network) a set of physical links is selected at random from the set $E_P^c = E_P^{clique} \setminus E_P$, where E_P^{clique} is the set of physical links where each physical node is connected to all the other physical nodes, and E_P is the set of links of the original network P. For each physical network $P_j(m, s)$, a new random link set is generated.

- **Degree based addition:** Links are generated so as to connect low degree nodes with high degree nodes. The objective is to increase the possible paths that low degree nodes have to provider nodes. To do this, we add links between low degree nodes and

high degree nodes only if they were not previously connected. Here, for each low degree node, we add one link to a high degree node and then we mark high degree nodes as 'used' to avoid adding multiple links to the same high degree node. If all high degree nodes have been marked as 'used' and there are more links to be added, then all nodes are unmarked and the process starts again. We will add links to low degree nodes within the 97% of the lowest degree nodes in ascending order from low to high degree until N_{st} links have been added.

The link addition process is described by algorithm 1.

- **Distance based addition:** Similar to *Degree based link addition*, links are generated to increase the number of links of low degree nodes. However, here we pair low degree nodes to nodes that are physically close to them. If two nodes are at the same distance of a low degree node, we choose the one with the highest degree. Links are added only if they were not previously present in the network. The objective is to increase the possible paths that low degree nodes have to provider nodes while minimizing the length of new links. Once a link is added we mark the higher degree node as 'used' to avoid adding multiple links to the same high degree node. If all nodes are marked 'used' and there are more links to add, nodes are unmarked and the process starts again. We will add links to low degree nodes within the 97% of the lowest degree nodes in ascending order from low to high degree until N_{st} links have been added.

  The link addition process is described by algorithm 2.

- **Local hubs:** The link addition process for the Local hubs strategy is the same as the one described for Distance strategy. However, here we pair low degree nodes with nodes within the top 3% of highest degree nodes. Thus, for each low degree node v within the 97% of the lowest degree nodes, we add a link to the closest high degree node u, with u in the top 3% of highest degree nodes. Unlike Degree and Distance strategies, each high degree node can have multiple links to low degree nodes. The links added using this strategy result in several local hub nodes across the physical network.

  The link addition process is described by algorithm 3.

We must note that for both Distance based link addition strategy, and Degree based link addition strategy only 97% of the nodes with the lowest degree have new links added. Whereas for Local hubs strategy links are added between nodes within the 97% of the lowest degree nodes, and nodes within the top 3% of highest degree nodes. This decision was made due to the node degree distribution of RNG physical networks (see Figure 5.1), since RNG based systems lead to the most fragile systems among the systems tested (see Chapter 3).

We must also note that the links added by any strategy do not discriminate on whether the pair of nodes connected by the new links are consumer-consumer, provider-consumer, or provider-provider.

Algorithm 1: Degree based addition algorithm.

procedure DEGREE_LINKS($N_{st}, (V_P, E_P)$)
  $N \leftarrow |E_P|$
  $V_P^{high} \leftarrow V_P$ ▷ ordered by decreasing degree
  $U^{low} \leftarrow$ *97% lowest degree nodes in* V_P *ordered by increasing degree*
  $M \leftarrow \phi$ ▷ Marked nodes
  $E_{st} \leftarrow \phi$ ▷ Extra links set
  for $v \in U^{low}$ **do**
    for $w \in V_P^{high} \setminus M$ **do**
      if $(v, w) \notin E_P \cup E_{st}$ and $v \neq w$ **then**
        $E_{st} \leftarrow (v, w)$
        $M \leftarrow M \cup \{w\}$
        break
      end if
    end for
    if $|E_{st}| = N_{st}$ **then**
      return E_{st}
    end if
  end for
  $N_{st}^r \leftarrow N_{st} - |E_{st}|$
  $E_P^r \leftarrow E_P \cup E_{st}$
  $E_{st}^r \leftarrow$ degree_links$(N_{st}^r, (V_P, E_P^r))$
  return $E_{st} \cup E_{st}^r$
end procedure

Algorithm 2: Distance based addition algorithm.

```
1: procedure DISTANCE_LINKS(N_st, (V_P, E_P))
2:     N ← |E_P|
3:     V_P^high ← V_P                                   ▷ ordered by decreasing degree
4:     U^low ←  97% lowest degree nodes in V_P ordered by increasing degree
5:     M ← φ                                                          ▷ Marked nodes
6:     E_st ← φ                                                       ▷ Extra links set
7:     for v ∈ U^low do
8:         d ← ∞
9:         w ← φ
10:        for u ∈ V_P^high \ M do
11:            if (v, u) ∉ E_P and v ≠ u then
12:                if distance(v, u) < d then
13:                    d ← distance(v, u)
14:                    w ← u
15:                end if
16:            end if
17:        end for
18:        E_st ← (v, w)
19:        M ← M ∪ {w}
20:        if |E_st| = N_st then
21:            return E_st
22:        end if
23:    end for
24:    N_st^r ← N_st − |E_st|
25:    E_P^r ← E_P ∪ E_st
26:    E_st^r ← distance_links(N_st^r, (V_P, E_P^r))
27:    return E_st ∪ E_st^r
28: end procedure
```

Algorithm 3: Local hubs addition algorithm.

```
1: procedure HUBS_LINKS(N_st, (V_P, E_P))
2:     N ← |E_P|
3:     U^high ← 3% highest degree nodes in V_P ordered by increasing degree
4:     U^low ← 97% lowest degree nodes in V_P ordered by increasing degree
5:     E_st ← φ                                                    ▷ Extra links set
6:     for v ∈ U^low do
7:         d ← ∞
8:         w ← φ
9:         for u ∈ U^high do
10:            if (v, u) ∉ E_P and v ≠ u then
11:                if distance(v, u) < d then
12:                    d ← distance(v, u)
13:                    w ← u
14:                end if
15:            end if
16:        end for
17:        E_st ← (v, w)
18:        if |E_st| = N_st then
19:            return E_st
20:        end if
21:    end for
22:    N^r_st ← N_st − |E_st|
23:    E^r_P ← E_P ∪ E_st
24:    E^r_st ← distance_links(N^r_st, (V_P, E^r_P))
25:    return E_st ∪ E^r_st
26: end procedure
```

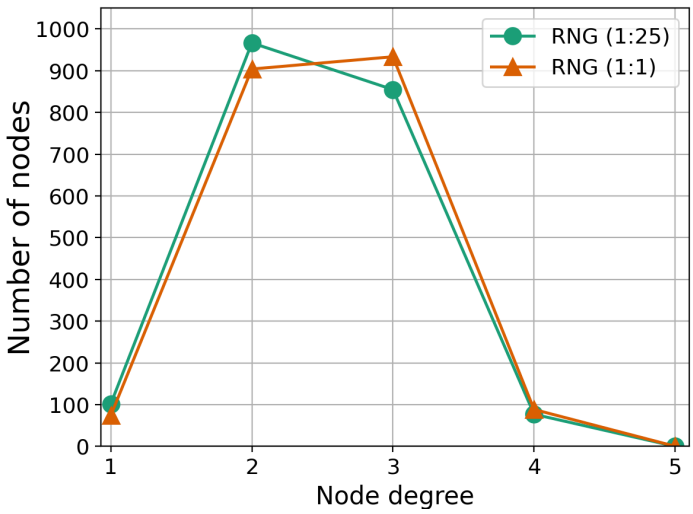


Figure 5.1: Average degree distribution of RNG physical networks across all 10 physical network versions j.

5.3 Experiments

In this chapter we test the robustness of the physical-logical interdependent networks against physical random attacks as described in section 3.4.1. The conditions over the physical space, and interlinks between the physical and logical network are the same in section 3.4.

In the remainder of this section we describe the interdependent networks tested, and how we measured the cost of adding physical links.

5.3.1 Networks tested

For these experiments we will add interlinks to a subset of the systems tested in Chapter 3.4 in order to present a more manageable amount of information. Here, we will only use logical network version $q = 1$, and $I_{max} = u$ with $u \in \{3, 5, 7, 10\}$. We have chosen $q = 1$ because, as we can see in Table 5.1, the bridge nodes that appear in this network result in moderate damage when compared to other logical network versions. The I_{max} values have been selected such that if $u_1 < u_2$ then $\overline{TG}_L(q, m, s, u_1) < \overline{TG}_L(q, m, s, u_2)$ for $q = 1$.

Interdependent networks

We build our interdependent networks starting from the networks tested in section 3.4.4. We then add physical links to each system according to section 5.2. Thus, we initially have physical-logical interdependent network described by the tuple:

$$(P_j(m, s), L_1, I(u))$$

where $P_j(m, s)$ the physical network, L_1 the logical network, and $I(k)$ is the interlink set. Here $j \in \{1, \ldots, 10\}$, $u \in \{3, 5, 7, 10\}$, s the space shape in which we build the physical network, and $m \in \{RNG, YAO, GPA, 5NN, GG, ER\}$ the physical network model.

Then, for each strategy st described in section 5.2, and each physical network $P_j(m, s)$ we generate a set of physical links

$$E^{st}(P_j(m, s)) = E^{st}_{(j,m,s)}$$

with $E^{st}_{(j,m,s)} \cap P_j(m, s) = \phi$. After adding these links we obtain the following physical network:

$$P^{st}_j(m, s) = (V_P, E^m_P(loc_j(V_P, s)) \cup E^{st}_{(j,m,s)})$$

Thus, the interdependent network after physical link addition is described by the tuple:

$$(P^{st}_j(m, s), L_1, I(k))$$

q	G_L range
1	(0.50, 0.997)
2	(0.71, 0.997)
3	(0.81, 0.997)
4	(0.16, 0.997)
5	(0.02, 0.997)
6	(0.31, 0.997)
7	(0.04, 0.997)
8	(0.28, 0.997)
9	(0.37, 0.997)
10	(0.19, 0.997)

Table 5.1: Bridge nodes G_L values ranges for each logical network version q. The G_L ranges were obtained considering $I_{max} \in \{1, \ldots, 10\}$.

with L_1 the logical network and $I(u)$ the interlink set given $I_{max} = u$.

In this chapter we test all the interdependent networks with the form $(P_j^{st}(m, s), L_1, I(u))$ derived from each strategy st described in section 5.2.

Network parameters

The parameters for each base interdependent network $(P_j(m, s), L_1, I(u))$ are the same as those described in Chapter 3. Here, we considered for each physical-logical network $p_L = 6$ the number of provider nodes, $N_L = 300$ the number of logical nodes, and $N_P = 2000$ the number of physical nodes. To generate each final network $(P_j^{st}(m, s), L_1, I(k))$ we add the same number of links $|E^{st}_{(j,m,s)}| \approx \frac{E_{RNG}}{4}$ for every strategy st.

5.3.2 Costs

For each link addition strategy, we add the same amount of links, however these links connect different nodes at different distances from one another. Higher distances usually mean higher link costs.

Given $u, v \in \mathrm{V}_P$ physical nodes, we calculate the average cost of each system, and each addition strategy assuming that the cost of adding a link is equivalent to the euclidean distance $\mathrm{d}(u, v)$ between the nodes connected by that link. We also assume that the total cost of adding n links is the sum of their costs.

We define the cost of a physical network built over a space s, based on physical model m,

using the j-th node allocation configuration $loc_j(V_P, s)$ as follows.

$$Cost^{(j,s)}(m) = \sum_{(u,v)\in E_P^m(loc_j(V_P,s))} \mathrm{d}(u,v)$$

The average cost of physical networks built over a space s, based on physical model m is denoted by $\overline{Cost}^s(m)$. We obtain $\overline{Cost}^s(m)$ by averaging $Cost^{(j,s)}(m)$ across all j values.

Similarly, we define the cost of adding extra physical links according to a strategy st to a physical network built over a space s, based on physical model m, using the j-th node allocation configuration $loc_j(V_P, s)$ as follows.

$$Cost^{(j,m,s)}(st) = \sum_{(u,v)\in E^{st}_{(j,m,s)}} \mathrm{d}(u,v)$$

The average cost of adding links using strategy st over physical networks built over a space s, based on physical model m is denoted by $\overline{Cost}^{(m,s)}(st)$. We obtain $\overline{Cost}^{(m,s)}(st)$ by averaging $Cost^{(j,s)}(m)$ across all j values.

5.3.3 Cost efficiency

Along with the costs we also calculate the cost efficiency of each strategy in terms of improving the robustness. To measure how cost efficient is each physical link addition strategy, we define $\Delta\overline{TG}_L(j, m, s, u, st)$ as the average total G_L improvement induced by strategy st over an interdependent network built using a physical model m over a space s, using the j-th node allocation configuration, and interlink set $I(u)$.

$$\Delta\overline{TG}_L(j, m, s, u, st) = \overline{TG}_L(j, m, s, u, st) - \overline{TG}_L(j, m, s, u)$$

Here, $\overline{TG}_L(j, m, s, u, st)$ is the average TG_L obtained after adding links to the physical network using strategy st, and $\overline{TG}_L(j, m, s, u)$ is the average TG_L obtained on the original interdependent network, that is, before adding extra links to the physical network. Note that since for all experiments we have $q = 1$ we have $\overline{TG}_L(j, m, s, u, st) = \overline{TG}_L(1, j, m, s, u, st)$, and $\overline{TG}_L(j, m, s, u) = \overline{TG}_L(1, j, m, s, u)$.

Given $\overline{Cost}^{(m,s)}(st)$ the average cost of adding physical links using strategy st over a physical model m, and space s. We define $Cost_E(st)$ to measure how cost efficient is a strategy as follows

$$Cost_E^{(m,s)}(st) = \frac{\langle\Delta\overline{TG}_L(m, s, u, st)\rangle}{\overline{Cost}^{(m,s)}(st)}$$

where $\langle\Delta\overline{TG}_L(m, s, u, st)\rangle$ is obtained by averaging $\overline{TG}_L(j, m, s, u)$ across all 10 node allocation configurations j.

5.4 Results

In this section we present and discuss the results obtained according to the experimental settings described in section 5.3.

5.4.1 General robustness behavior

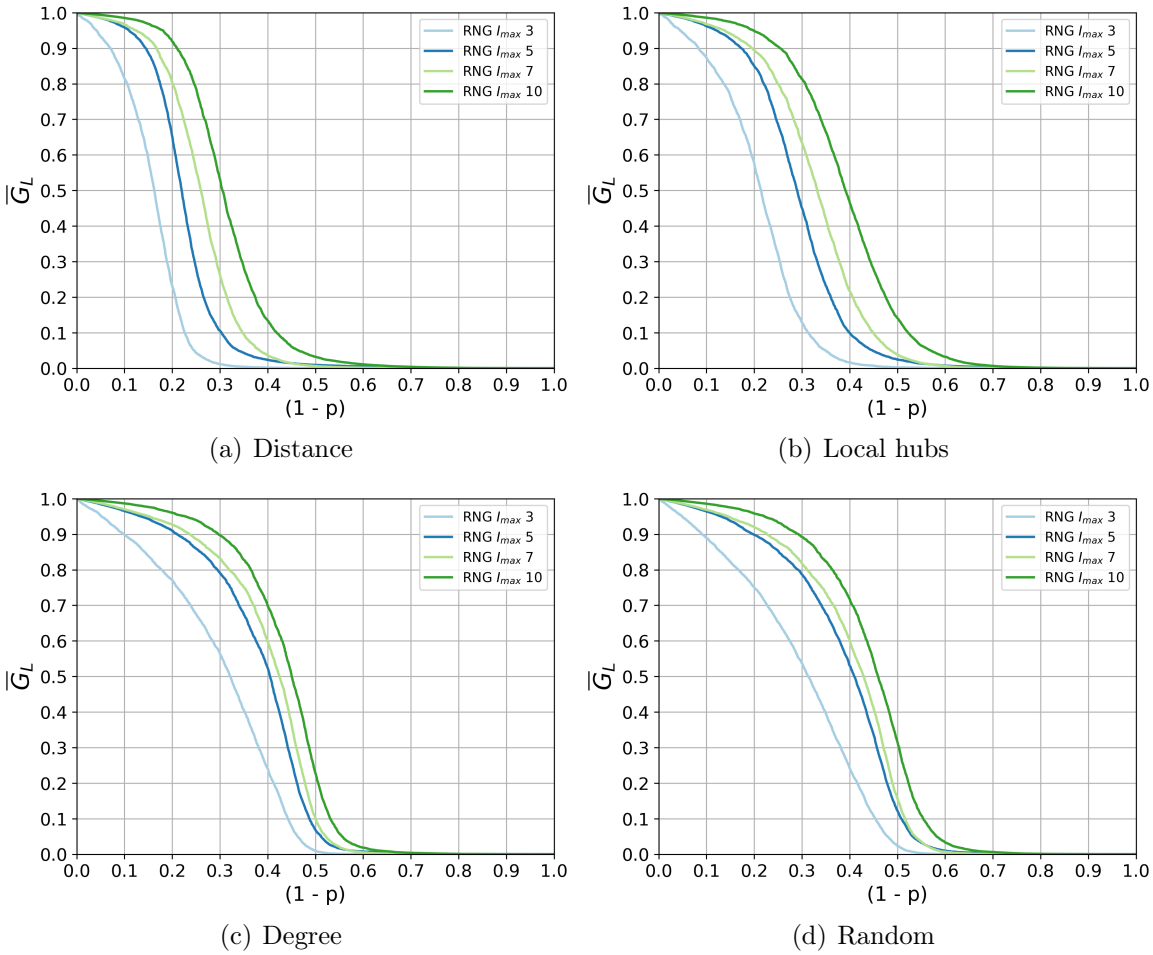
In Figure 5.2 we can see the average robustness behavior of systems built using physical model m = RNG over a (1:25) space after extra physical links have been added. Figures for each model and each strategy can be found in the appendix section C.1. Given a physical model m, in these figures we observe the average G_L ($\overline{G}_L$) across all 10 node location configurations j. In Figure 5.2 we can see that, on average, physical-logical interdependent networks built using physical model m = RNG present a continuous decay against physical random attacks, regardless of the link addition strategy used. Furthermore, this behavior is observed across all the systems tested. These results suggest that, on average, after adding extra links to the physical network, physical-logical systems undergo a second order phase transition against physical random attacks.

However, as we have shown in previous chapters, this does not mean that each attack iteration undergoes a second order phase transition. Indeed, in Table 5.2 we can see the fraction of iterations that undergo an abrupt decay for systems built using a (1:25) space after extra physical links have been added. Tables for each model and each strategy can be found in the appendix section C.2. In Figure 5.3, we can see the p_c and $G_L(p_c)$ values obtained for systems built using a (1:25) space after extra physical links have been added. Figures for each model, and each strategy can be found in the appendix section C.1. These results suggest that the interdependent network tested are likely to undergo a first order phase transition, even after adding extra physical links.

5.4.2 Effect of adding physical links

Let us start by observing the effect of adding links to the physical network over the interdependent networks' robustness against physical random attacks. In Figures 5.4 and 5.5 we observe the $\overline{TG}_L$ comparison of interdependent networks with $I_{max} = 5$. See appendix section C.3 to see the figures for $I_{max} \in \{3, 5, 7, 10\}$. Figure 5.4 shows the results for s =(1:25), and Figure 5.5 shows the results for s =(1:1). In these Figures we can see that adding extra links to the physical network results in a $\overline{TG}_L$ improvement for almost every physical model tested regardless of the physical space s. The only exception to this are interdependent networks built using physical networks based on ER networks.

Figures 5.6 and 5.7 show the average $\overline{TG}_L$ of all systems tested. Here, we can observe



(a) Distance

(b) Local hubs

(c) Degree

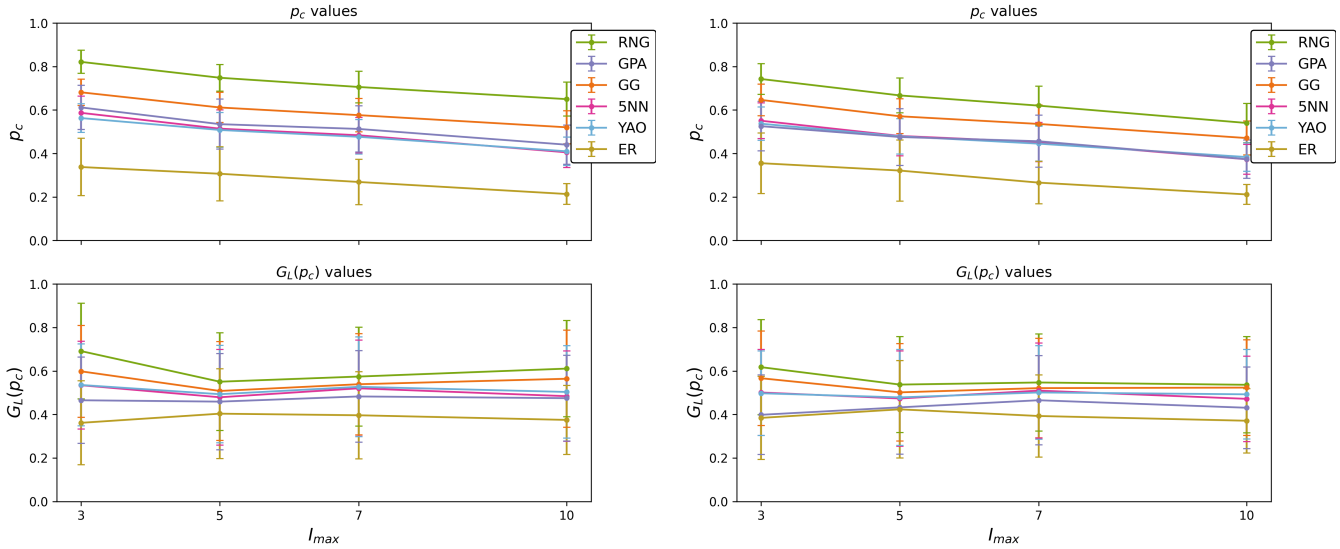
(d) Random

Figure 5.2: Average robustness for interdependent networks built using RNG physical model over a (1:25) space, and logical network version $q = 1$ after adding extra physical links.

that Random and Degree strategies result in the highest average $\overline{TG}_L$, followed by Local hubs strategy in second place, and Distance strategy in third place. Since we have added the same number of physical links for each link addition strategy, this shows that the way in which we add the physical links plays an important role. In Figures 5.6 and 5.7 we also observe that some interdependent networks improve much more than others for the same link addition strategy. More specifically, the more robust the original system is, the lower the increment of its $\overline{TG}_L$ values.

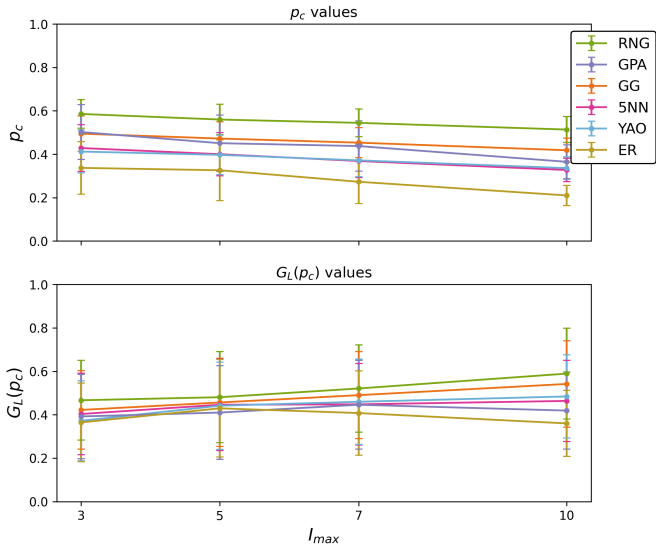
st = Distance				
m/I_{max}	3	5	7	10
RNG	0.803	0.826	0.897	0.773
GG	0.662	0.855	0.861	0.723
5NN	0.608	0.818	0.844	0.609
YAO	0.555	0.822	0.819	0.671
GPA	0.517	0.802	0.818	0.567
ER	0.402	0.859	0.75	0.552
st = Local hubs				
m/I_{max}	3	5	7	10
RNG	0.714	0.825	0.882	0.678
GG	0.616	0.831	0.867	0.642
5NN	0.532	0.834	0.835	0.594
YAO	0.537	0.811	0.834	0.618
GPA	0.512	0.838	0.8	0.514
ER	0.433	0.866	0.76	0.536
st = Degree				
m/I_{max}	3	5	7	10
RNG	0.573	0.857	0.861	0.771
GG	0.501	0.843	0.852	0.683
5NN	0.492	0.857	0.795	0.606
YAO	0.453	0.856	0.823	0.67
GPA	0.513	0.878	0.803	0.566
ER	0.413	0.87	0.762	0.577
st = Random				
m/I_{max}	3	5	7	10
RNG	0.537	0.881	0.882	0.753
GG	0.494	0.841	0.835	0.676
5NN	0.429	0.848	0.819	0.65
YAO	0.446	0.856	0.811	0.624
GPA	0.458	0.853	0.81	0.547
ER	0.418	0.84	0.766	0.529

Table 5.2: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks built using $s = (1{:}25)$, after adding extra physical links.

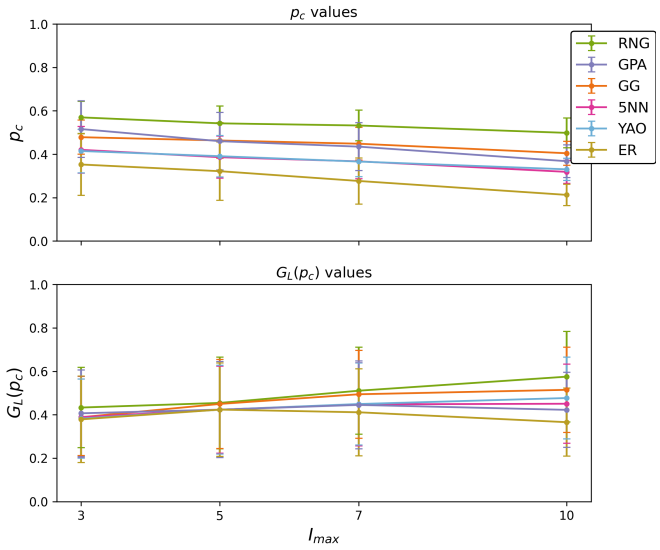


(a) Distance

(b) Local hubs



(c) Degree



(d) Random

Figure 5.3: Average values of p_c and $G_L(p_c)$ for each physical-logical interdependent network built using $s = (1{:}25)$, after adding extra physical links. Bars represent the standard deviation.

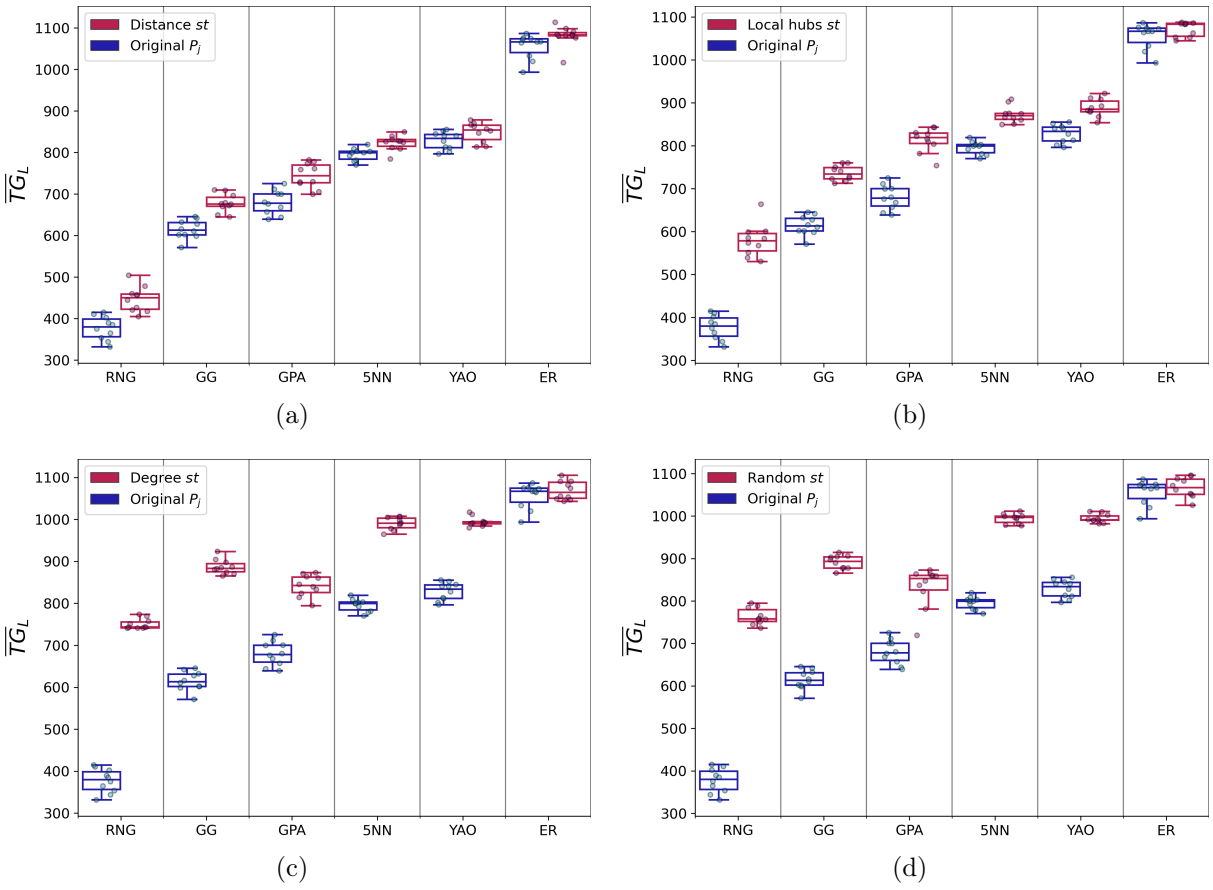


Figure 5.4: $\overline{TG_L}$ comparison of interdependent networks with and without extra physical links for s =(1:25), and $I_{max} = 5$.

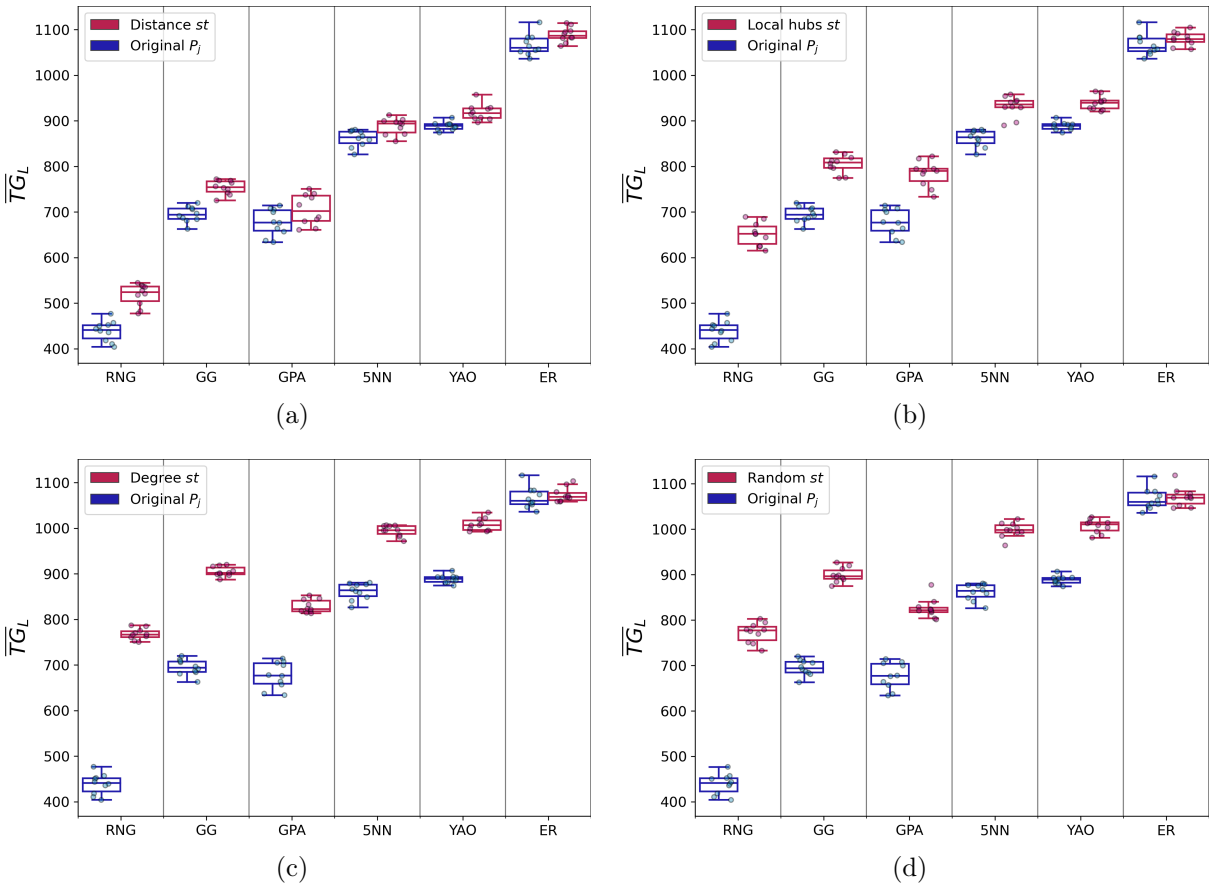


Figure 5.5: $\overline{TG_L}$ comparison of interdependent networks with and without extra physical links for s =(1:1), and $I_{max} = 5$.

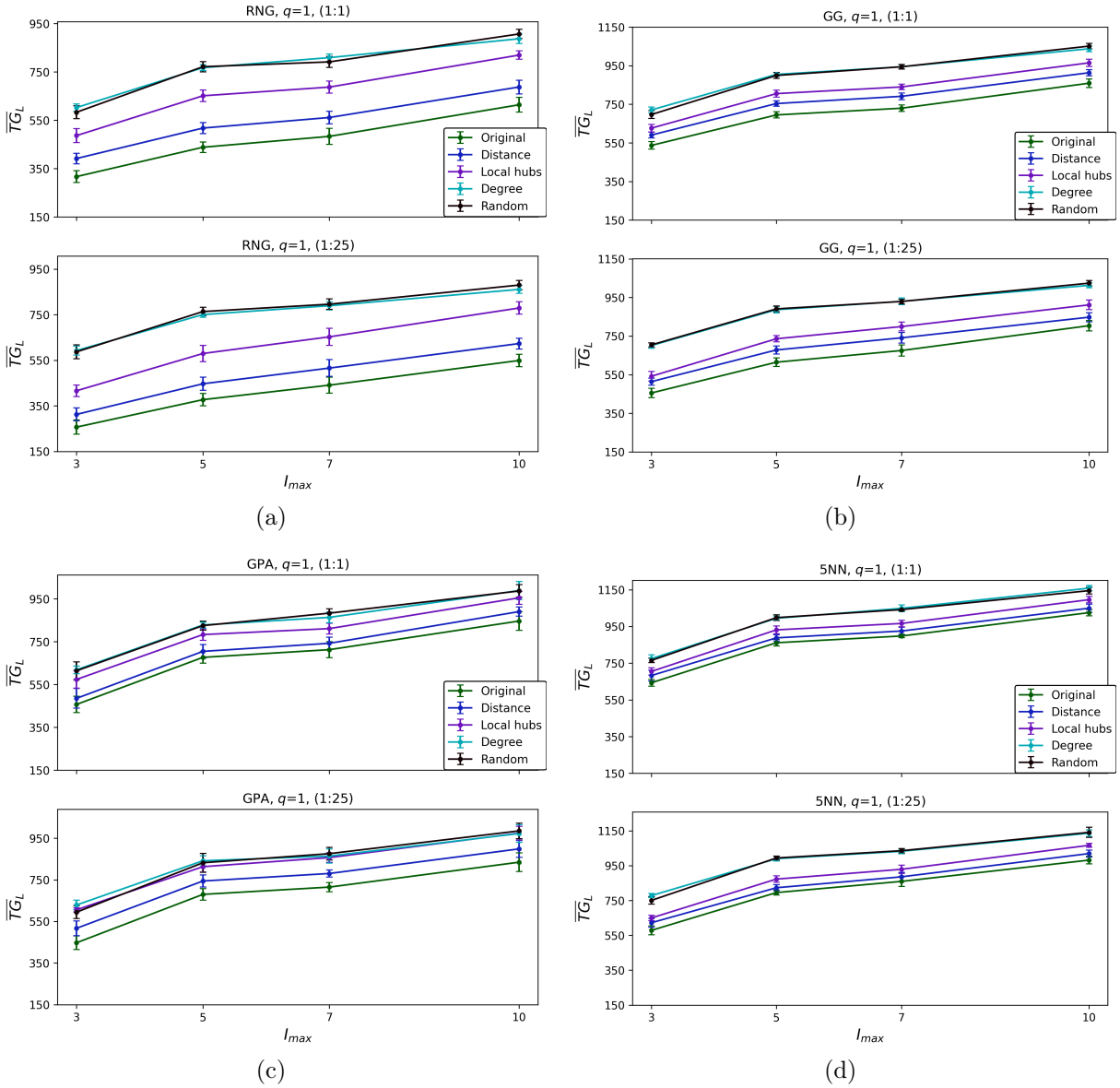
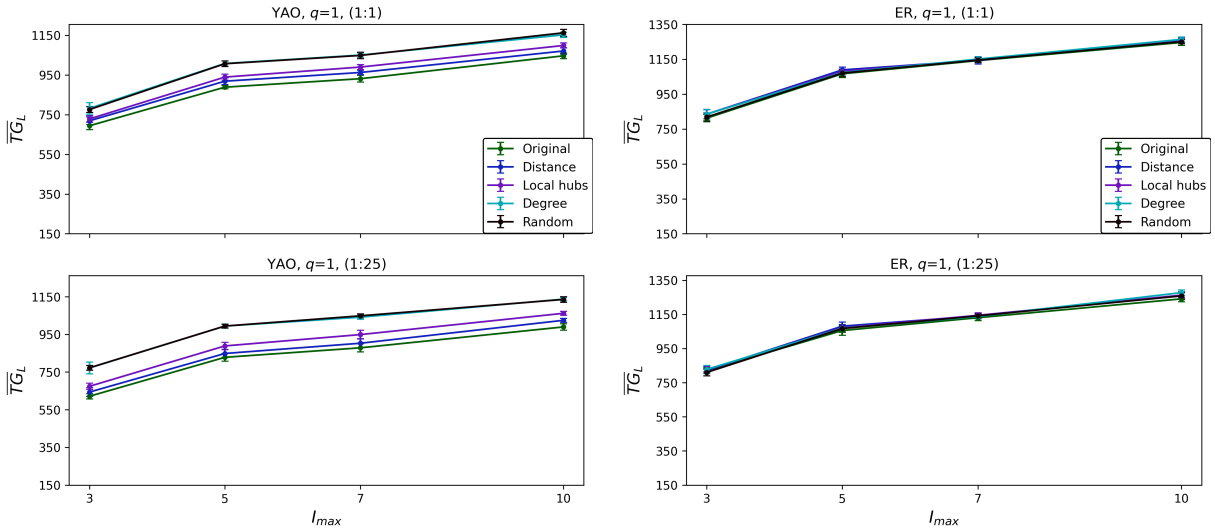


Figure 5.6: Average $\overline{TG_L}$ comparison of interdependent networks with and without extra physical links for $m \in \{\text{RNG}, \text{GG}, \text{GPA}, \text{5NN}\}$.



(a) (b)

Figure 5.7: Average $\overline{TG}_L$ comparison of interdependent networks with and without extra physical links for $m \in \{\text{YAO}, \text{ER}\}$.

5.4.3 Relation between robustness and link length

Our results so far show that random link addition is one of the best physical link addition strategies in terms of improving the robustness of physical-logical interdependent networks. These results may seem counterintuitive, since random link addition does not require any information about the physical network structure other than which links are already present in the physical network, and thus, are not eligible to be added. We observe that, by the definition of the addition strategies tested, Degree and Random strategies do not limit the length of the links added. In contrast, Local hubs and Distance strategies do impose limits in the length of the links added. This suggests that there might be a relation between the length of the added links and the robustness improvement that a particular strategy induces. To test this we define ρ as the length of the longest link added by a strategy as follows.

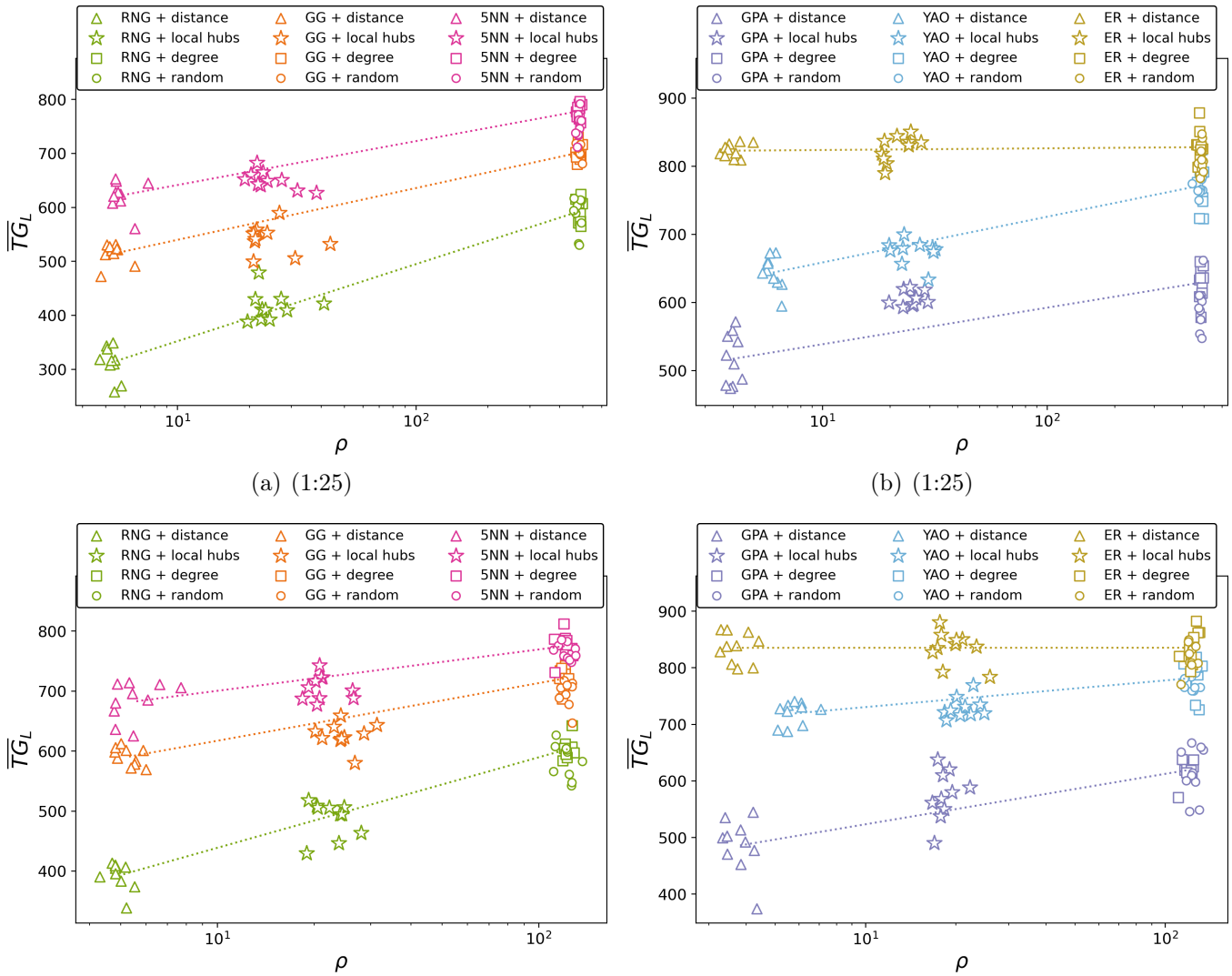
$$\rho(st)_{(j,m,s)} = \max_{(u,v)\in E^{st}_{(j,m,s)}} \mathrm{d}(u,v)$$

Where st is the strategy, $E^{st}_{(j,m,s)}$ is the set of physical links added by strategy st over a physical network built using model m, space s, and physical node locations $loc_j(V_P, s)$. And $\mathrm{d}(u,v)$ is the length of the link (u,v).

s = (1:25)						
Strategy	RNG	GG	5NN	GPA	YAO	ER
Distance	5.29 (0.28)	5.41 (0.48)	5.87 (0.66)	3.99 (0.2)	6.01 (0.39)	4.02 (0.4)
Local hubs	25.3 (5.9)	25.22 (6.96)	24.96 (5.66)	25.09 (2.66)	25.92 (4.52)	21.67 (3.11)
Degree	485.5 (8.23)	481.58 (9.28)	482.28 (7.24)	484.96 (6.73)	486.09 (9.48)	478.03 (8.07)
Random	478.15 (12.45)	485.52 (7.57)	481.52 (6.85)	483.6 (6.35)	479.45 (14.1)	487.75 (7.28)
s = (1:1)						
Distance	4.93 (0.32)	5.32 (0.41)	5.61 (0.91)	3.82 (0.36)	5.82 (0.56)	3.72 (0.37)
Local hubs	22.7 (2.75)	24.91 (3.16)	21.53 (2.61)	18.43 (1.53)	21.31 (2.16)	19.86 (2.82)
Degree	123.08 (3.17)	120.07 (2.6)	120.41 (5.0)	118.78 (4.27)	124.49 (5.56)	122.4 (5.48)
Random	122.03 (7.43)	122.69 (3.85)	122.24 (5.92)	124.24 (6.14)	123.52 (4.61)	121.63 (4.05)

Table 5.3: Average ρ for each model and space. Each value was obtained by averaging across the 10 systems associated to each pair model-space.

Table 5.3 shows the average ρ for each model and space. We observe that the strategies that result in higher average ρ values are also the ones that improve the robustness the most. Indeed, in Figure 5.8 we observe that there is a relation between the average total robustness $\overline{TG}_L$ and ρ for systems built using $I_{max} = 3$. Figures for $I_{max} \in \{3, 5, 7, 10\}$ can be found in the appendix section C.4. Here we observe that the relation between the average total robustness $\overline{TG}_L$ and ρ is also present for interdependent networks with $I_{max} \in \{3, 5, 7, 10\}$.



(a) (1:25)

(b) (1:25)

(c) (1:1)

(d) (1:1)

Figure 5.8: Length of the longest link added by each strategy over each interdependent network tested ρ versus the $\overline{TG}_L$ for interdependent networks built using $I_{max} = 3$. ρ axis is shown using logarithmic scale.

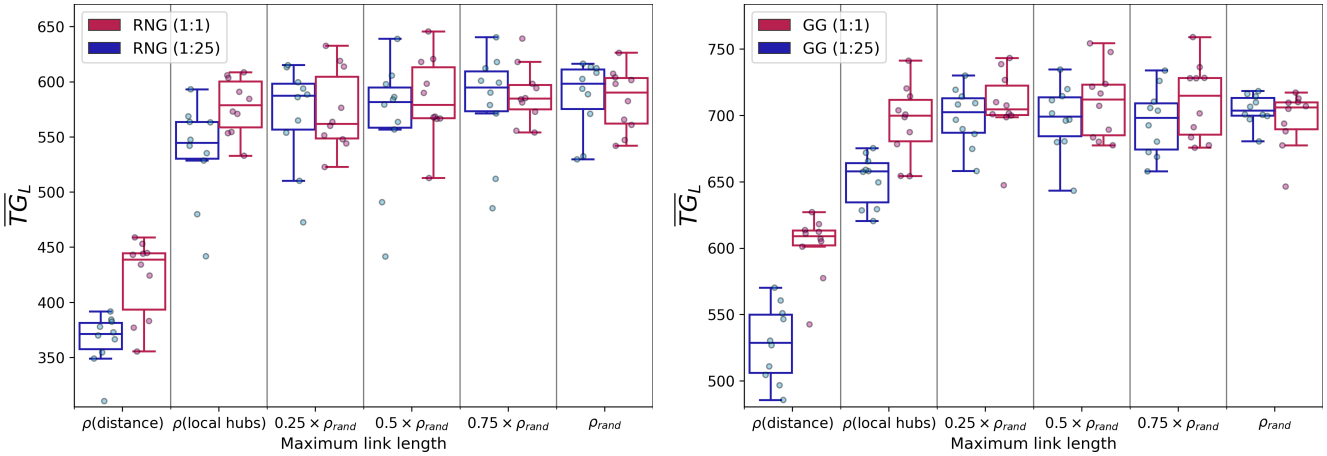
To further study this relation we test the effect of adding physical links at random with the condition that the links added cannot surpass a specific length. We refer to links added in this way as random addition with maximum link length. Here, for a given maximum link length we add the same number of physical links as the original strategies tested E_{add}. Let us define $\rho_{rand} = \rho(\text{Random})_{(j,m,s)}$, and $\rho(st)_{(j,m,s)} = \rho(st)$. We test the effect of setting the

maximum link length to ρ(Distance), to ρ(Local hubs), and varying fractions of ρ_{rand}. In Table 5.4 we can see the maximum link lengths tested, and the average ρ obtained for each case.

$s = (1{:}25)$						
Max. link length	RNG	GG	5NN	GPA	YAO	ER
ρ(Distance)	5.29 (0.28)	5.41 (0.48)	5.87 (0.66)	3.98 (0.2)	6.01 (0.39)	4.02 (0.4)
ρ(Local hubs)	25.27 (5.9)	25.19 (6.97)	24.9 (5.65)	25.05 (2.65)	25.86 (4.49)	21.66 (3.11)
$0.25 \times \rho_{rand}$	119.37 (3.1)	121.28 (1.84)	120.24 (1.7)	120.59 (1.59)	119.67 (3.54)	121.72 (1.84)
$0.5 \times \rho_{rand}$	238.56 (6.17)	242.3 (3.73)	239.95 (3.44)	241.4 (3.17)	239.49 (7.04)	243.24 (3.59)
$0.75 \times \rho_{rand}$	356.53 (9.76)	362.96 (5.84)	360.37 (4.99)	361.14 (4.58)	358.84 (10.58)	365.08 (5.67)
$s = (1{:}1)$						
ρ(Distance)	4.93 (0.32)	5.32 (0.41)	5.6 (0.91)	3.81 (0.36)	5.81 (0.56)	3.72 (0.37)
ρ(Local hubs)	22.69 (2.75)	24.88 (3.13)	21.51 (2.6)	18.42 (1.54)	21.29 (2.17)	19.84 (2.83)
$0.25 \times \rho_{rand}$	30.48 (1.85)	30.64 (0.96)	30.51 (1.45)	31.04 (1.54)	30.86 (1.16)	30.39 (1.02)
$0.5 \times \rho_{rand}$	60.96 (3.7)	61.29 (1.92)	61.02 (2.95)	62.03 (3.05)	61.68 (2.36)	60.75 (2.02)
$0.75 \times \rho_{rand}$	91.24 (5.5)	91.78 (2.85)	91.5 (4.45)	92.77 (4.48)	92.34 (3.33)	91.05 (3.05)

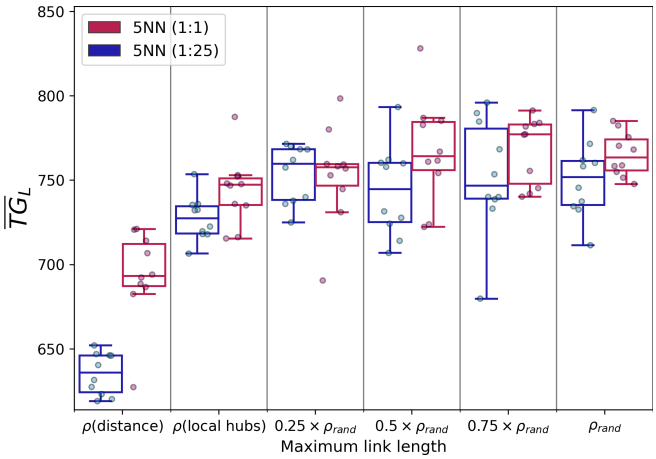
Table 5.4: Average ρ values obtained for random addition with maximum link length. Each value was obtained by averaging across the 10 interdependent interdependent networks associated to each pair model-space.

In Figures 5.9 and 5.10 we can see the $\overline{TG}_L$ after randomly adding physical links with different maximum link lengths. Figures for $I_{max} \in \{3, 5, 7, 10\}$ can be found in appendix section C.5. In Figures 5.9 and 5.10 we observe that the robustness decreases as the maximum link length decreases. Furthermore, for interdependent networks built using $m \in \{\text{RNG}, \text{GG}, \text{5NN}, \text{YAO}\}$ and $I_{max} = 3$ we can see that there is a rapid increment in the robustness for maximum link lengths $0.25 \times \rho_{rand}$ and below. The robustness increment becomes slower for maximum link lengths $0.5 \times \rho_{rand}$ and above, with some cases resulting in a similar robustness for link lengths $0.75 \times \rho_{rand}$ and ρ_{rand}. For the case of interdependent networks built using $m = \text{GPA}$ and $I_{max} = 3$ we observe that the increment in the robustness for maximum link lengths $0.25 \times \rho_{rand}$ and below is slower compared to systems with $m \in \{\text{RNG}, \text{GG}, \text{5NN}, \text{YAO}\}$. In the case of $m = \text{ER}$ and $I_{max} = 3$ we can see that the link length does not impact the robustness. From appendix section C.5 we observe that this behavior occurs regardless of the I_{max} value used to build the interdependent networks. These results suggest that Random strategy results in such a great robustness improvement because the picked link set likely contains longer links.

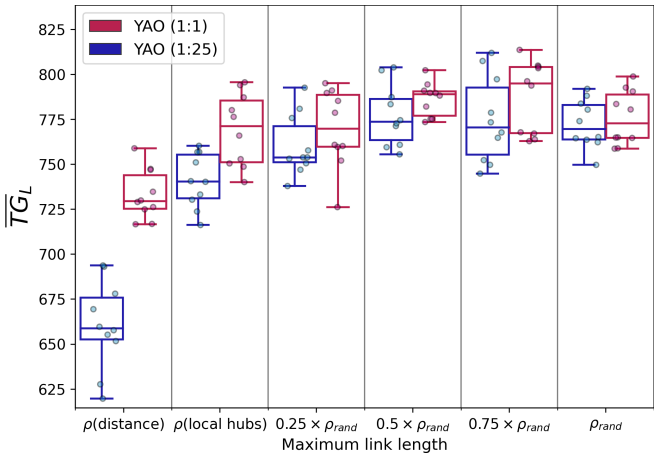


(a) RNG

(b) GG

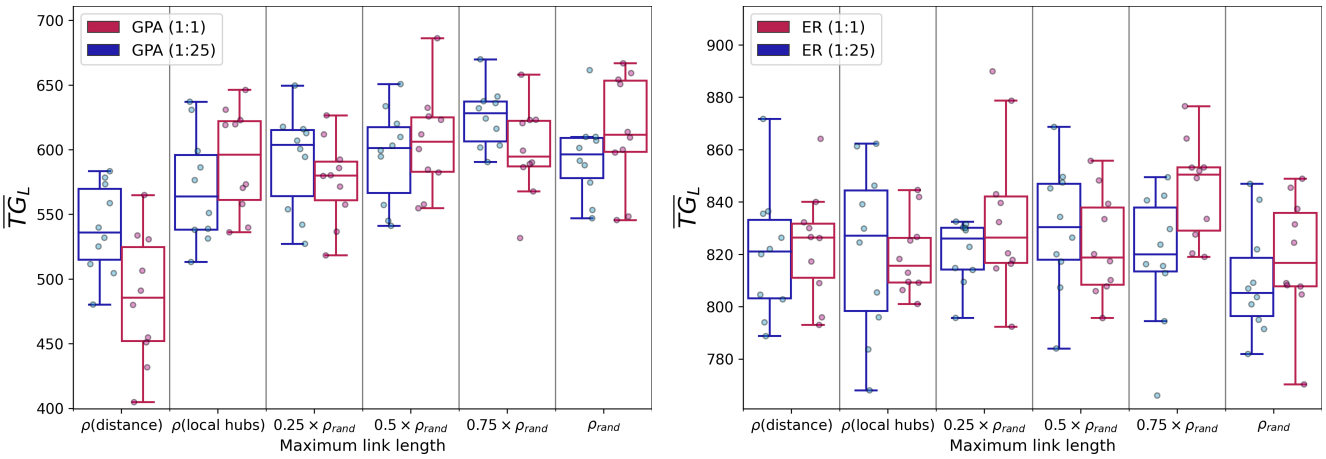


(c) 5NN



(d) YAO

Figure 5.9: $\overline{TG}_L$ values after randomly adding physical links with different maximum link lengths ($I_{max} = 3$). Each point shows the $\overline{TG}_L$ of a single physical network $P_j^{st}(m, s)$.



(a) GPA (b) ER

Figure 5.10: $\overline{TG}_L$ values after randomly adding physical links with different maximum link lengths ($I_{max} = 3$). Each point shows the $\overline{TG}_L$ of a single physical network $P_j^{st}(m, s)$.

5.4.4 Cost of adding physical links

In Table 5.5 we can see the average cost of each link addition strategy *st* for each space s and model m. Here, we observe that the most expensive strategies are also the strategies that result in a higher increment of $\overline{TG}_L$ as shown in section 5.4.2. That is, Random and Degree strategies are the most expensive strategies, followed by Local hubs in second place, and Distance in third place. This can be further observed in Figure 5.11 which shows the robustness gain $\Delta\overline{TG}_L$ versus the cost of adding extra physical links for interdependent networks with $I_{max} = 3$. Figures for $I_{max} \in \{3, 5, 7, 10\}$ can be found in the appendix section C.7. Table 5.6 shows the average cost of each type of physical network. We observe that, similar to the link addition strategy costs, physical models that result in more robust interdependent networks are also more expensive (see section 3.5.3).

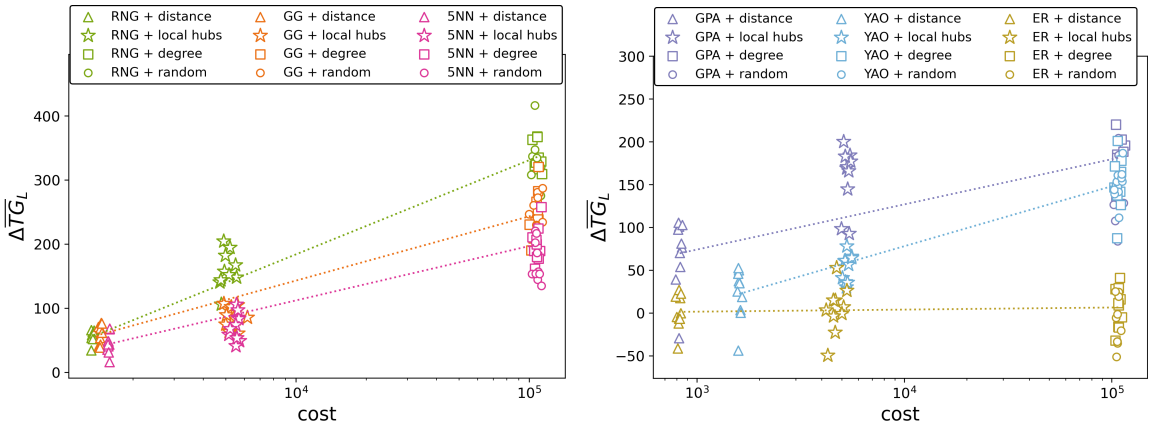
In Tables 5.5 and 5.6 the cost is calculated according to section 5.3.2. That is, the cost is given by the sum of the length of all physical links added using a given model or strategy. Thus, these costs suggest that there is an association between the length of the links used in a given physical network, and its robustness against physical random attacks.

So far we have seen that more expensive link addition strategies result in higher $\overline{TG}_L$ values. Thus, we would like to know which strategy is the most cost efficient in terms of improving the robustness. In Table 5.7 we can see the cost efficiency of each link addition strategy for $I_{max} = 5$. The results for $I_{max} \in \{3, 5, 7, 10\}$ can be found in the appendix section C.6. Note that cost efficiency values in these Tables have been amplified by a factor of 10^3 to improve its readability. In these Tables we can see that lower cost strategies are much more efficient than higher cost strategies, with Distance strategy being the most cost efficient, followed by Local hubs in second place, and Random and Degree in third place. This suggests that it might be better in terms of cost to add more physical links using Distance addition strategy, than to add fewer physical links using other strategies.

5.4.5 Adding more physical links using Distance strategy

Let us test the effect of adding more physical links using Distance strategy. To do this, we added to each interdependent network tested in this chapter approximately $\frac{E_{RNG}}{2}$ physical links using Distance strategy. We will refer to this addition as Distance+. Figures 5.12 and 5.13 shows the effect of the initial link addition according to each strategy plus the effect of adding approximately twice as many links using Distance strategy (Distance+).

We can see that, for most physical models, Distance+ results in an average $\overline{TG}_L$ that is similar to the robustness obtained using Local hubs. Furthermore, as we can see in Table 5.9, Distance+ costs less than Local hubs strategy. In Table 5.8 we can see the cost efficiency obtained for Distance+. We observe that Distance+ is more cost efficient than Local hubs,



(a) $s = (1 : 25)$ (b) $s = (1 : 25)$

(c) $s = (1 : 1)$ (d) $s = (1 : 1)$

Figure 5.11: Robustness gain $\Delta\overline{TG}_L$ versus the cost of adding extra physical links for interdependent networks with $I_{max} = 3$.

(1:25)				
m/st	Distance	Local hubs	Degree	Random
RNG	1,345.94 (16.04)	5,053.18 (285.33)	108,260.99 (2,901.07)	108,007.94 (3,394.89)
GG	1,450.28 (15.54)	5,348.77 (374.71)	106,637.27 (3,164.92)	108,196.79 (3,918.48)
GPA	826.92 (17.22)	5,303.49 (161.1)	109,073.1 (3,729.8)	108,132.88 (3,434.76)
5NN	1,574.63 (11.57)	5,525.47 (180.68)	107,967.13 (27,74.5)	108,008.62 (2,627.47)
YAO	1,602.83 (23.68)	5,303.41 (166.48)	107,249.68 (2,881.09)	108,428.97 (3,555.51)
ER	820.1 (14.73)	4,701.63 (326.96)	107,844.99 (2,248.73)	106,857.63 (1,814.87)
(1:1)				
RNG	1,295.18 (16.96)	4,830.97 (87.96)	33,474.73 (443.23)	33,555.28 (678.25)
GG	1,379.3 (20.17)	5,230.64 (409.03)	34,003.93 (656.48)	33,542.83 (552.82)
GPA	805.06 (18.56)	5,795.72 (100.93)	33,998.42 (749.23)	33,339.42 (1,327.97)
5NN	1,530.73 (16.75)	5,260.35 (148.66)	33,613.86 (619.23)	33,659.34 (641.82)
YAO	1,521.17 (18.95)	5,051.47 (174.42)	34,129.78 (703.31)	33,352.85 (845.19)
ER	794.78 (10.48)	4,325.52 (150.99)	33,323.48 (622.11)	33,328.96 (820.4)

Table 5.5: Average cost of adding links to the physical network for each link addition strategy. Standard deviation is shown in parenthesis.

s	model	RNG	GG	GPA	5NN	YAO	ER
(1:25)	mean	4,386.83	8,276.02	47,189.99	16,881.52	15,108.9	1,277,914.9
	std	42.4	77.74	1,739.73	178.34	47.74	17,765.85
(1:1)	mean	4,504.97	8,691.3	14,752.24	17,076.08	16,310.33	393,755.05
	std	63.15	100.03	379.29	280.59	117.53	6,884.71

Table 5.6: Average cost of each physical network given a model m, and a space s.

$I_{max} = 5$				
(1:25)				
m/st	Distance	Local hubs	Degree	Random
RNG	51.16	39.91	3.44	3.57
GG	41.01	21.97	2.51	2.52
GPA	82.34	25.83	1.52	1.44
5NN	17.5	13.97	1.8	1.84
YAO	15.39	12.2	1.59	1.57
ER	24.39	2.4	0.07	0.06
(1:1)				
RNG	58.34	43.28	9.72	9.82
GG	42.02	20.93	6.14	6.07
GPA	39.48	19.02	4.56	4.56
5NN	19.19	13.87	4.05	4.15
YAO	17.4	9.32	3.39	3.43
ER	26.51	2.81	0.16	0.08

Table 5.7: Cost efficiency $Cost_E^{(m,s)}$ of each link addition strategy, for interdependent networks built using $I_{max} = 5$. Cost efficiency values have been amplified by a factor of 10^3 to improve its readability.

s	I_{max}	RNG	GG	GPA	5NN	YAO	ER
	3	44.27	30.42	73.81	19.25	14.26	13.7
(1:25)	5	56.65	36.24	64.2	17.93	15.74	10.32
	7	56.59	34.61	63.42	18.81	16.51	13.9
	10	56.73	34.4	58.15	16.94	16.11	12.84
	3	47.93	27.58	34.46	13.75	13.1	4.5
(1:1)	5	56.17	32.91	36.44	17.32	17.29	11.88
	7	56.49	35.63	39.66	17.7	14.86	10.83
	10	53.81	31.02	40.07	16.11	15.63	12.65

Table 5.8: Cost efficiency $Cost_E^{(m,s)}$ of Distance+. Cost efficiency values have been amplified by a factor of 10^3 to improve its readability.

but not as cost efficient as Distance. These results suggest that indeed adding more links using Distance is more cost efficient than to add less physical links using other strategies. However, it also suggests that the $\overline{TG}_L$ increments become smaller as we add more physical links.

Another way to test the effect of adding more physical links is to fix the budget instead of the number of physical links. Since RNG physical networks are both the most fragile and the least expensive among the built physical networks, we test the effect of adding physical links using Distance strategy given the following budget B^s.

$$B^s = \overline{Cost}^s(GG) - \overline{Cost}^s(RNG)$$

Here, $\overline{Cost}^s$ is the average cost of physical networks built using a given model on a space s. Note that the budget B^s is given by the difference between the cost of RNG networks, and the cost of GG networks since GG networks result in systems that are more robust than RNG systems, but not as robust as systems built using other physical models. Here, we have $B^{(1:25)} \approx 3,889$, and $B^{(1:1)} \approx 4,186$. We will refer to the physical links added using Distance strategy and budget B^s as Distance(B^s).

Table 5.10 we show the average $\overline{TG}_L$ results obtained after adding physical links to RNG physical networks using Distance(B^s) strategy compared to the robustness of GG systems, and the robustness of RNG + Local hubs interdependent networks. We have included RNG + Local hubs interdependent networks to this comparison because these systems have a total cost similar to GG interdependent networks, and thus to RNG + Distance(B^s). In Table 5.10 we can see that the robustness $\overline{TG}_L$ of RNG interdependent networks, after adding links to the physical network using Distance(B^s), is still lower than the average robustness of GG interdependent networks, despite having similar costs. This suggests that in order for RNG interdependent networks to be as robust as GG interdependent networks it might be

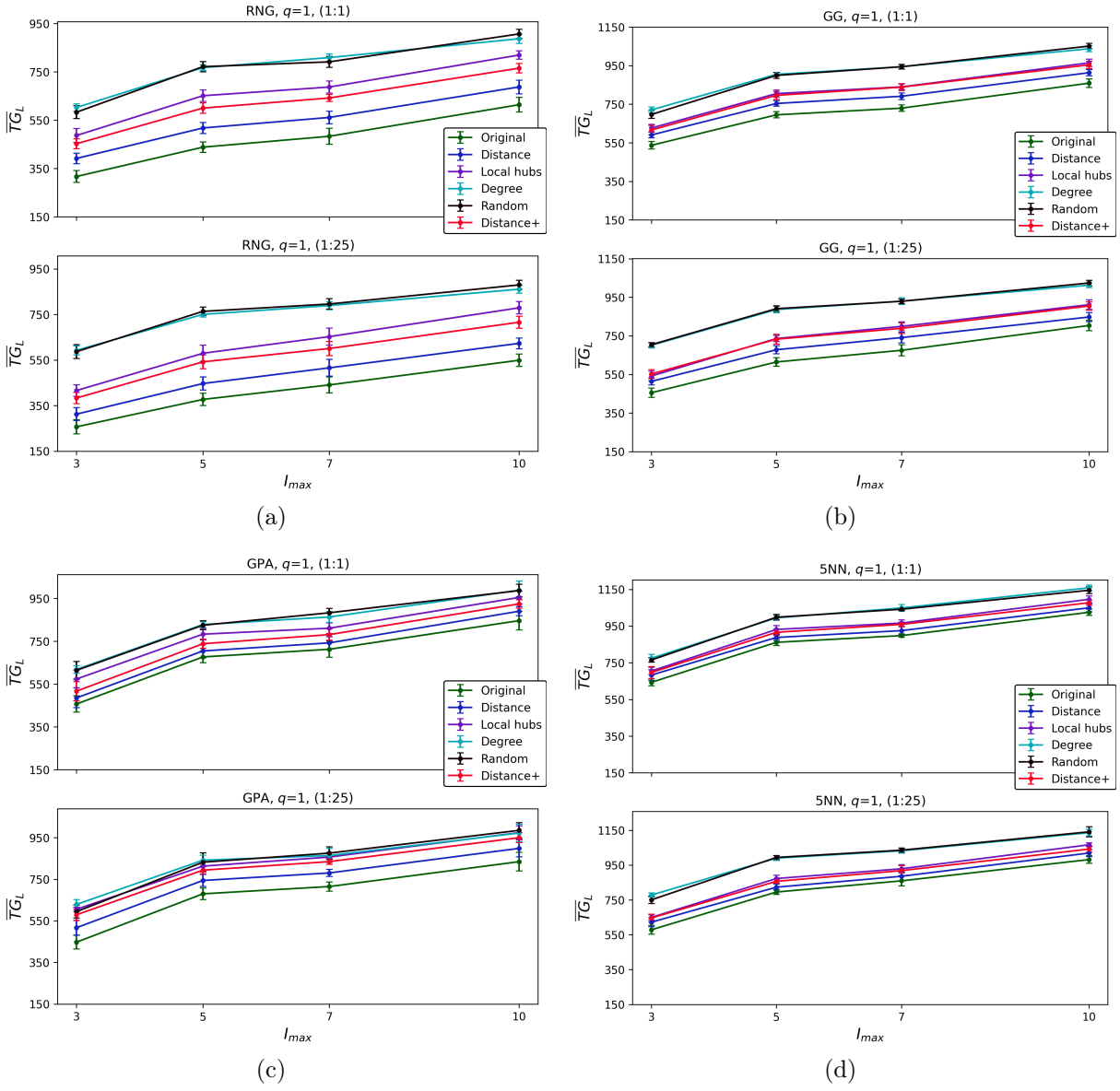
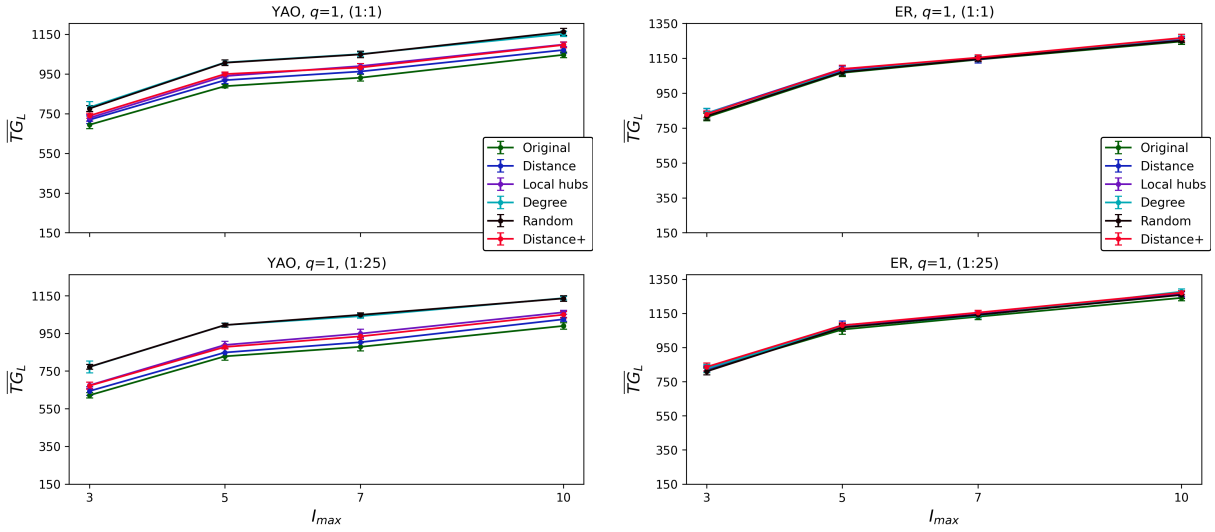


Figure 5.12: Average $\overline{TG_L}$ comparison of systems with and without extra physical links (including strategy Distance+) for $m \in \{\text{RNG}, \text{GG}, \text{GPA}, \text{5NN}\}$.



(a) (b)

Figure 5.13: Average $\overline{TG_L}$ comparison of interdependent networks with and without extra physical links (including strategy Distance+) for $m \in \{\text{YAO}, \text{ER}\}$.

(1:25)					
m	Distance	Distance+	Local hubs	Degree	Random
RNG	1,345.94 (16.04)	2,897.24 (16.85)	5,053.18 (285.33)	108,260.99 (2,901.07)	108,007.94 (3,394.89)
GG	1,450.28 (15.54)	3,148.79 (27.84)	5,348.77 (374.71)	106,637.27 (3,164.92)	108,196.79 (3,918.48)
GPA	826.92 (17.22)	1,832.63 (19.41)	5,303.49 (161.1)	109,073.1 (3,729.8)	108,132.88 (3,434.76)
5NN	1,574.63 (11.57)	3,408.5 (19.73)	5,525.47 (180.68)	107,967.13 (27,74.5)	108,008.62 (2,627.47)
YAO	1,602.83 (23.68)	3,429.99 (29.91)	5,303.41 (166.48)	107,249.68 (2,881.09)	108,428.97 (3,555.51)
ER	820.1 (14.73)	1,805.55 (21.77)	4,701.63 (326.96)	107,844.99 (2,248.73)	106,857.63 (1,814.87)
(1:1)					
RNG	1,295.18 (16.96)	2,810.95 (28.86)	4,830.97 (87.96)	33,474.73 (443.23)	33,555.28 (678.25)
GG	1,379.3 (20.17)	3,043.44 (26.67)	5,230.64 (409.03)	34,003.93 (656.48)	33,542.83 (552.82)
GPA	805.06 (18.56)	1,798.96 (25.26)	5,795.72 (100.93)	33,998.42 (749.23)	33,339.42 (1,327.97)
5NN	1,530.73 (16.75)	3,321.78 (24.43)	5,260.35 (148.66)	33,613.86 (619.23)	33,659.34 (641.82)
YAO	1,521.17 (18.95)	3,313.66 (28.81)	5,051.47 (174.42)	34,129.78 (703.31)	33,352.85 (845.19)
ER	794.78 (10.48)	1,761.92 (23.2)	4,325.52 (150.99)	33,323.48 (622.11)	33,328.96 (820.4)

Table 5.9: Average cost of adding links to the physical network. Distance, Local hubs, Degree, and Random strategies add approximately $\frac{E_{RNG}}{4}$ physical links each. Distance+ adds approximately $\frac{E_{RNG}}{2}$ physical links using Distance strategy.

s	I_{max}	RNG + Distance(B^s)	RNG + Local hubs	GG
	3	424.61 (13.69)	415.95 (18.88)	456.51 (22.57)
(1:25)	5	581.58 (22.44)	583.51 (30.16)	618.66 (24.22)
	7	648.48 (32.56)	656.05 (33.99)	680.21 (26.79)
	10	776.3 (25.29)	778.11 (20.04)	796.76 (20.82)
	3	507.53 (15.17)	488.72 (15.09)	532.53 (16.14)
(1:1)	5	665.79 (21.87)	650.8 (20.52)	695.82 (13.59)
	7	706.99 (15.64)	697.98 (19.42)	730.11 (18.36)
	10	835.55 (22.89)	817.92 (22.67)	859.71 (20.03)

Table 5.10: Average $\overline{TG}_L$ comparison of RNG + Distance(B^s) systems, GG systems, and RNG + Local hubs systems.

necessary to increase the budget, and highlights the importance of the way in which physical links are added.

In Table 5.10 we also observe that $\overline{TG}_L$ of RNG + Distance(B^s) systems is similar to the average robustness of RNG + Local hubs systems. From Table 5.5 we can see that the cost of adding physical links to RNG networks using the Local hubs strategy is higher than the budget B^s regardless of the space s. Thus, for RNG systems, we can obtain a similar robustness improvement to the one obtained with Local hubs by adding more physical links using Distance strategy. Furthermore, adding more physical links using Distance strategy is less expensive than adding less physical links using Local hubs.

5.5 Summary

In this chapter we tested the effect of adding links to the physical network over the robustness of physical-logical interdependent networks against physical random attacks. Here, we studied the effect of four physical link addition strategies: Random, Distance, Local hubs, and Degree based addition. We studied the robustness improvement obtained after adding physical links according to each strategy, and analyzed the cost efficiency of each strategy in terms of the robustness improvement.

For the experiments we used a subset of the interdependent networks tested in Chapter 3 as base systems. We then added extra physical links to each base system according to each link addition strategy. For each base interdependent network, and for each addition strategy, we added the same number of physical links. For the base systems, we considered the same physical networks and space shapes from Chapter 3. That is, we have $m \in \{RNG, GG, 5NN, YAO, GPA, ER\}$, $s \in \{(1:25), (1:1)\}$, plus the 10 different node allocation configurations as described in Chapter 3. For the logical network we only use logical

network version $q = 1$, and for the interlinks we considered $I_{max} = u$ with $u \in \{3, 5, 7, 10\}$. We chose $q = 1$ because the bridge nodes that appear in this network result in moderate damage compared to other logical network versions. The I_{max} values were selected such that the physical-logical interdependent networks' robustness monotonically increases with the I_{max} value. In this chapter we tested a total of 1,920 new interdependent networks against physical random attacks.

Our results show that Random and Degree strategies result in the highest robustness improvement, followed by Local hubs strategy in second place, and Distance strategy in third place. Since, we added the same number of physical links for each link addition strategy, these results suggest that the way in which we add the physical links plays an important role. We also found that the more robust the base system is, the lower the improvement of its robustness.

Here, we note that the results show that random addition strategy is one of the best strategies in terms of improving the robustness against random attacks despite this strategy's simplicity. We found that this can be explained by the length of the links added by random strategy. Specifically, we found that these results are related to the maximum link length of the added physical links. Indeed, if we condition random strategy to only consider links below a specific length, we observe that the robustness obtained decreases as the maximum link length decreases. The physical models tested in our experiments use relatively short links as they use proximity criteria to add the links. Thus, the set of available physical links to add using a strategy contains a high number of long links. These results suggest that Random strategy results in such a great robustness improvement because the picked link set likely contains longer links.

As for the costs, we observe that the most expensive strategies are also the strategies that result in a higher robustness improvement. That is, Random and Degree strategies are the most expensive strategies, followed by Local hubs in second place, and Distance in third place. Interestingly, in terms of cost efficiency we observe that lower cost strategies are much more efficient than higher cost strategies, with Distance strategy being the most cost efficient, followed by Local hubs in second place, and Random and Degree in third place. This suggests that it might be better in terms of cost to add more physical links using Distance addition strategy, than to add fewer physical links using other strategies.

To test whether adding more physical links using distance strategy than to add fewer physical links using other strategies we studied the effect of adding more physical links using Distance strategy in two ways: (1) by adding twice as much physical links as the original strategies using Distance strategy, and (2) by adding more physical links according to an increased "budget". We refer to the first way of adding more links using distance strategy

as Distance+, and to the second one as Distance(B^s) with B^s the available budget to add more physical links for an interdependent network built over a space s.

The results obtained by adding physical links according to Distance+ show that, for most physical models, Distance+ has a lower cost than Local hubs, and results in a similar robustness improvement. Thus, Distance+ is more cost efficient than Local hubs. However, we also observe that Distance+ is not as cost efficient as Distance. Our results suggest that adding more links using Distance strategy is more cost efficient than adding less physical links using other strategies. However, it also suggests that robustness increments become smaller as we add more physical links.

To test Distance(B^s) strategy we set as a budget the difference between the cost of interdependent networks built using GG physical networks, and the cost of RNG physical networks. With this budget we tested the effect of adding physical links according to Distance(B^s) strategy over interdependent networks built using RNG physical networks. Our findings show that, similar to the case of Distance+, interdependent networks built using RNG physical networks and Distance(B^s) result in robustness improvement similar to that of interdependent networks built using RNG physical networks and Local hubs strategy. Our results also show that the robustness of RNG systems after adding links to the physical network using Distance(B^s) is still lower than the average robustness of GG interdependent networks, despite having similar costs. These results suggest that in order for RNG interdependent networks to be as robust as GG systems it might be necessary to increase the budget, and highlight the importance of the way in which physical links are added.

Chapter 6

Robustness against localized attacks

In previous chapters we tested the robustness of our physical-logical model against physical random attacks. Using these types of attacks we tested the effect of the space shape, the number of interlinks, the physical network model, and physical link addition over the interdependent network's robustness. However, physical random attacks are not the best representation for physical damage caused by physical events such as earthquakes, floods, tsunamis, etc. A better representation of these types of adverse events are 'localized attacks'.

In this chapter we test the effect of localized attacks over the robustness of physical-logical interdependent networks as modeled in Chapter 3. We use the physical link addition strategies presented in Chapter 5 to test the effect of localized attacks over the robustness of interdependent networks with and without extra physical links added, and compare it to the effect of physical random attacks.

6.1 Background

One way to test the robustness of a physically embedded network is by using localized attacks. Given a network allocated into a 2-dimensional space S, localized attacks damage all the nodes and/or links contained within a circular area of radius r and centered in $(x, y) \in S$ [101, 17].

Localized attacks are often used to model natural disasters or intentional attacks. Indeed, physical adverse events such as earthquakes, floods, tornadoes, as well as physical attacks cause damage within a contiguous area in the physical world. Protecting fiber infrastructures associated with communication networks from these types of events first motivated the study

of attacks that affect a specific area [79]. The work of Neumayer et al. studied the effects of damaging all network components that intersect a line in space, and attacks that damage all network components within a disk or circular area. The objective was to model the damage caused by tornadoes (line), and the damage caused by other events such as earthquakes (disk). Definitions for Localized attacks would later emerge from the works of Berezin et al. [17], and Shao et al. [101].

It has been shown that localized attacks cause substantially more damage than an equivalent random attack in interdependent lattices when measuring the damage using percolation methods [17], making these attacks especially interesting to test over interdependent networks that contain physically embedded networks.

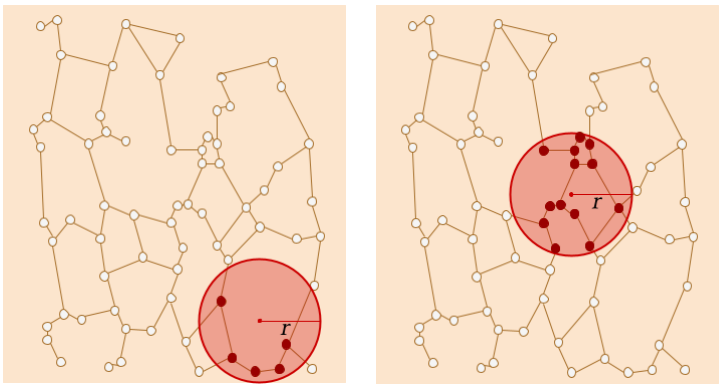
6.2 Experiments

In this chapter we test the robustness of physical-logical interdependent networks under localized attacks. To do this we use the same interdependent networks used for the experiments of Chapter 5. Here we describe localized attacks, how we tested them, and how we compared localized attacks versus physical random attacks.

6.2.1 Localized attacks

Localized Attacks (LA) remove all physical nodes within a circular area of radius r in the physical network. For each LA, all the physical nodes within the LA radius are simultaneously removed from the initial undamaged physical-logical interdependent network. Once the cascading failure has stopped we measure the G_L value associated with that LA. We must note that two LA with the same radius but different centers may contain different fractions $(1-p)$ of physical nodes within their attack areas (see Figure 6.1).

For each space shape $s \in \{(1{:}1),(1{:}25)\}$, a set $C(s)$ of 100 LA centers were generated to be used for testing. Centers in $C(s)$ were spread uniformly to cover the space s. For each center, five r values were tested, with $r = aw_{ln}, a \in \{0.2, 0.4, 0.6, 0.8, 1\}$, and w_{ln} the width of the (1:25) space. We must note that the set of centers $C(s)$ is not necessarily a subset of the node allocation set $loc_j(V_P, s)$. Given a space shape s, the same set of centers was used for all interdependent networks and all LA radii tested. Here, each LA can be described by the tuple (c, r) with $c \in C(s)$ the attack center, and r the attack radius. The results for these experiments show the G_L value obtained for each LA (c, r).



(a) 5 nodes affected by LA (b) 13 nodes affected by LA

Figure 6.1: Example of two localized attacks with the same radius r and different centers that affect different fractions of nodes $(1 - p)$.

Localized attacks versus physical random attacks

Consider physical-logical interdependent network (P, L, I), LA radius r, and $C(s)$ the set of LA centers for space s. To compare the effects of localized attacks over the robustness of (P, L, I) versus the effects of physical random attacks over the same interdependent network, we measure the difference between the average system robustness $\overline{G}_L$ obtained for localized attacks and the $\overline{G}_L$ obtained for physical random attacks. Let $(1 - p_{LA(r)})$ be the average fraction of physical nodes affected by localized attacks of radius r. We define the difference between the damage caused by localized attacks of radius r, and physical random attacks that remove a similar amount of physical nodes $\Delta\overline{G}_L(r)$ as

$$\Delta\overline{G}_L(r) = \overline{G}_L(\mathrm{LA(r)}) - \overline{G}_L(\mathrm{RA}(1 - p_{LA(r)}))$$

where $\overline{G}_L(\mathrm{LA}(r))$ is the average G_L value obtained across all 100 the localized attacks (c, r) tested over interdependent network (P, L, I), and $\overline{G}_L(\mathrm{RA}(1 - p_{LA(r)}))$ is the average G_L obtained after damaging the interdependent network using physical random attacks that remove a fraction $(1 - p_{LA(r)})$ of physical nodes.

With this, a $\Delta\overline{G}_L$ close to 0 means that on average the damage caused by localized attacks is similar to the damage caused by comparable physical random attacks.

6.2.2 Networks tested

In this chapter we use the interdependent networks previously used in Chapter 5. Here, we test physical-logical interdependent networks before adding extra physical links.

$$(P_j(m, s), L_1, I(u))$$

And after adding links using a strategy st, with st a physical link addition strategy defined in section 5.2.

$$(P_j^{st}(m,s), L_1, I(u))$$

Here $P_j(m,s)$ is the physical network generated using model m over the space s, and the j-th physical node allocation configuration $loc_j(V_P, s)$, $P_j^{st}(m,s)$ is the physical network obtained after adding extra physical links to network $P_j(m,s)$ according to strategy st, L_1 is the logical network ($q = 1$), and $I(u)$ is the set of interlinks generated given $I_{max} = u$. In this chapter we use the same physical-logical interdependent networks tested in Chapter 5, thus we consider $u \in \{3,5,7,10\}$, $j \in \{1,\ldots,10\}$, $s \in \{(1{:}25),(1{:}1)\}$, and $m \in \{RNG, YAO, GPA, 5NN, GG, ER\}$.

The parameters for each base interdependent network $(P_j(m,s), L_1, I(u))$ are the same as those described in Chapter 3. Thus, for each physical-logical interdependent network, we have $p_L = 6$ the number of provider nodes, $N_L = 300$ the number of logical nodes, and $N_P = 2000$ the number of physical nodes. To generate each network $(P_j^{st}(m,s), L_1, I(u))$ we add the same number of links $|E^{st}_{(j,m,s)}| \approx \frac{E_{RNG}}{4}$ for each strategy st as defined in Chapter 5.

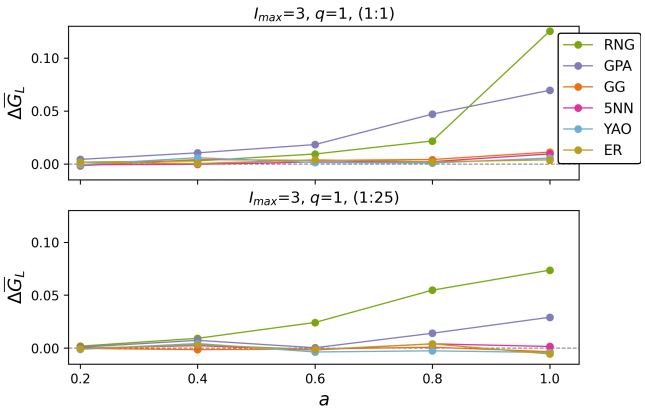
6.3 Results

In this section we will show the results of testing the robustness of each physical-logical interdependent network described in section 6.2 against LA. Here, we will show the results with and without extra physical links added using the strategies presented in Chapter 5.

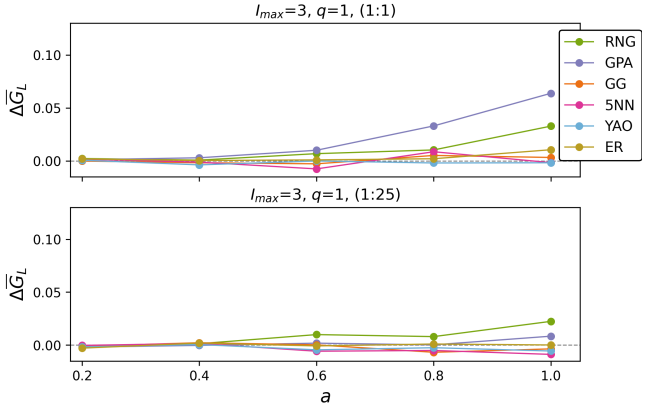
6.3.1 Comparison: LA versus RA

First, let us compare the robustness of the interdependent networks against localized attacks (LA), and against physical random attacks (RA). In Figure 6.2 for each LA radius r, we can see the comparison of the difference between the average interdependent network robustness $\overline{G}_L$ obtained for each type of attack for systems with $I_{max} = 3$. We can observe that, before adding links to the physical network, the average damage that LA and RA make are relatively similar for most interdependent networks. Here we can see that interdependent networks using $m \in \{\text{RNG, GPA}\}$ result in higher $\Delta\overline{G}_L$ values, meaning that these systems are more fragile against localized attacks than physical random attacks.

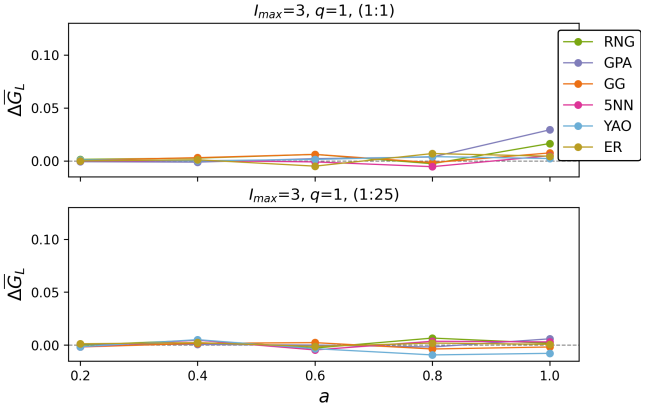
Results for $I_{max} \in \{3,5,7,10\}$ show that having a higher I_{max} value results in a decrease of $\Delta\overline{G}_L$ (see appendix D.1). In Figure 6.2 we observe that, for $I_{max} = 3$, after adding physical links to the physical network the $\Delta\overline{G}_L$ decreases, suggesting that adding more physical links increases the interdependent networks' robustness against localized attacks. The same is observed on interdependent networks with $I_{max} \in \{5,7,10\}$ (see appendix D.1).



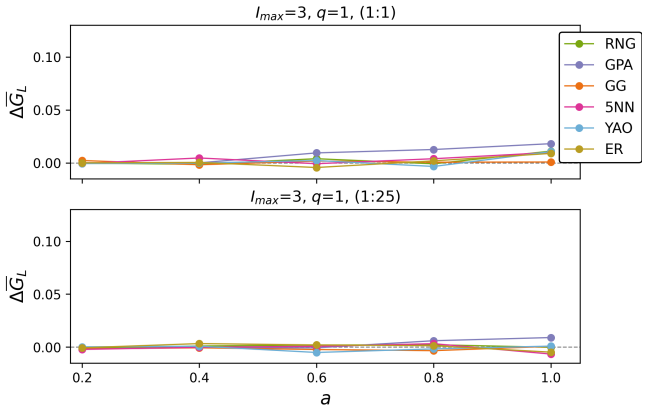
(a) No links added



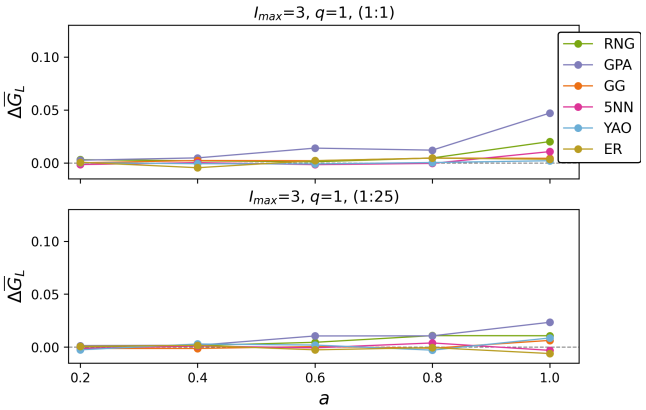
(b) Distance links added



(c) Local hubs links added



(d) Degree links added



(e) Random links added

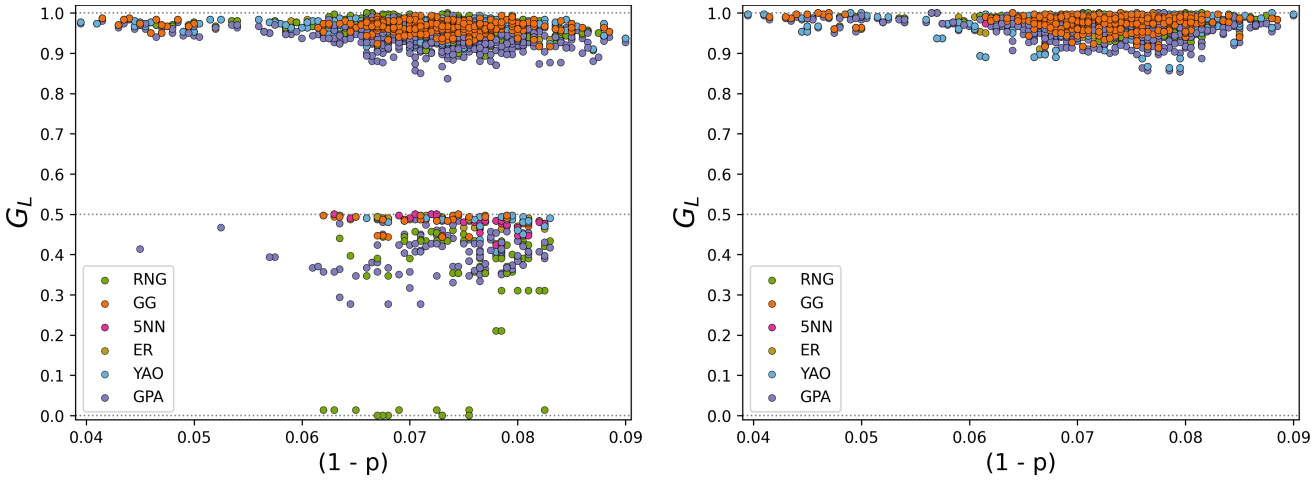
Figure 6.2: $\overline{G}_L$ value difference between LA and RA for $I_{max} = 3$. Here, $\Delta\overline{G}_L = \overline{G}_L(\text{LA}) - \overline{G}_L(\text{RA})$, and LA radius $r = aw_{ln}, a \in \{0.2, 0.4, 0.6, 0.8, 1\}$, with w_{ln} the width of the (1:25) space.

6.3.2 High damage localized attacks

Although the average G_L values of LA are somewhat similar to that of RA, we found that some LA can damage more than half of the logical network, and even result in its total destruction. In Figures 6.3 and 6.4 we can see the effect of localized attacks with $a = 1$. For each LA we can see the G_L value, versus the fraction of physical nodes $(1 - p)$ contained within the LA area. We observe that some localized attacks result in $G_L \leq 0.5$. Furthermore, some of these LA result in $G_L = 0$. These attacks do not appear as a continuum, but rather as a distinct group that always damages at least half of the logical network. We will refer to LA that result in a $G_L \leq 0.5$ as High Damage Localized Attacks (HDLA).

We must note that HDLA are only observed in interdependent networks with $I_{max} = 3$. Interdependent networks with higher I_{max} values do not present HDLA. This suggests that HDLA are related to the number of interlinks in the physical-logical interdependent network. Furthermore, the gap between the G_L values of HDLA and non-HDLA suggests that HDLA might be caused by the removal of bridge nodes during the cascading failure process. Indeed, for $q = 1$ and $I_{max} = 3$ we have that the set of bridge nodes that result in the loss of at least 10% of the logical network after being removed $B_h^{(q,u)}$ contains only one node u_L^b, and removing node u_L^b from the isolated logical network results in a $G_L = 0.517$. Thus, HDLA could be related to the removal of node u_L^b during the cascading failure process.

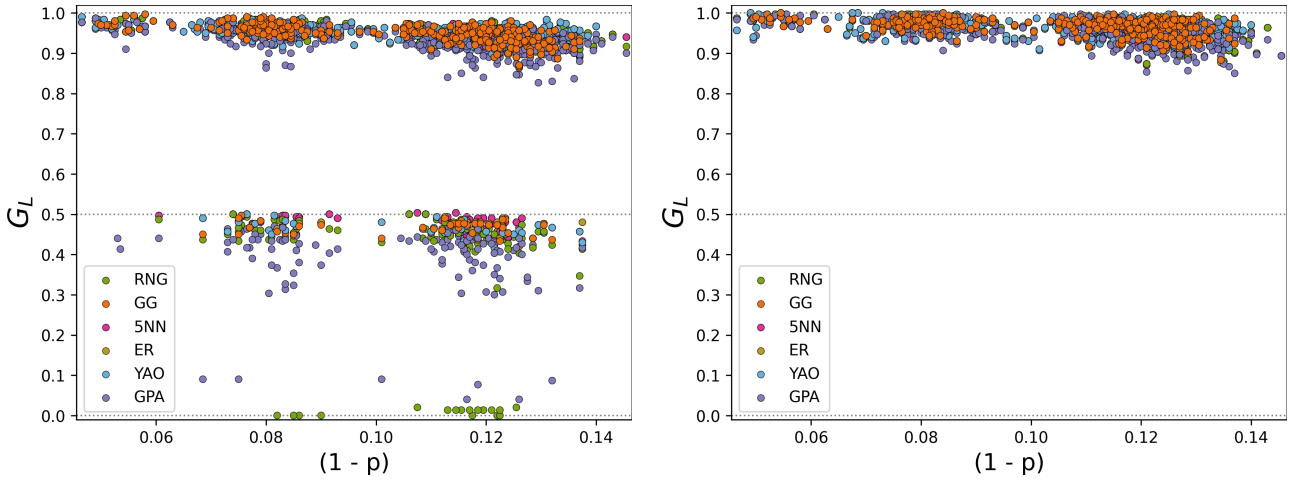
In Figures 6.5 and 6.6 red dots correspond to LA that remove node u_L^b during the cascading failure process (denoted as CF), and black dots show LA that do not remove u_L^b. We observe that indeed HDLA remove node u_L^b during the cascading failure process, while non-HDLA do not remove said node. In Figures 6.7 and 6.8 we can see that this behavior is also observed after adding links to the physical network on interdependent networks with $I_{max} = 3$. In the appendix section D.2 we can see this holds true for all I_{max} value tested.



(a) $I_{max} = 3$ (b) $I_{max} = 5$

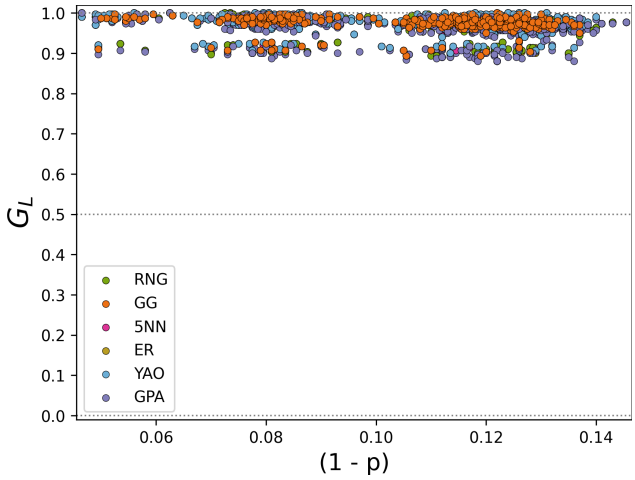
(c) $I_{max} = 7$ (d) $I_{max} = 10$

Figure 6.3: Each localized attack G_L versus the fraction of nodes contained within the attack radius $(1-p)$ for interdependent networks built using $s = (1{:}25)$ without extra physical links $(r = 1 \cdot w_{ln})$.

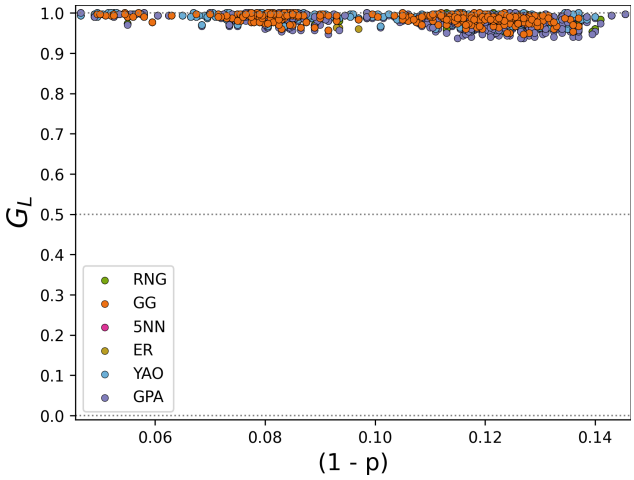


(a) $I_{max} = 3$

(b) $I_{max} = 5$

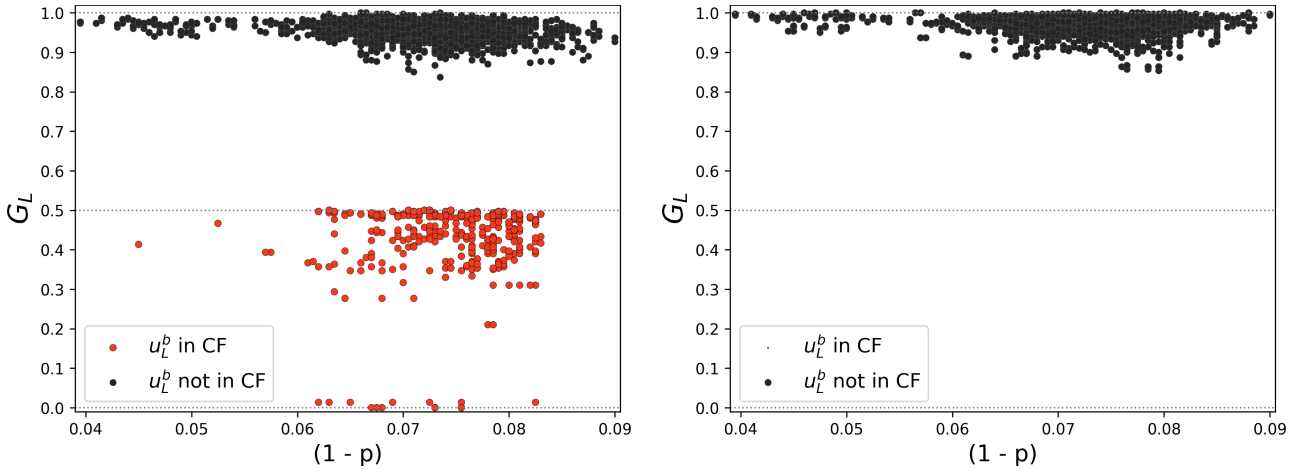


(c) $I_{max} = 7$



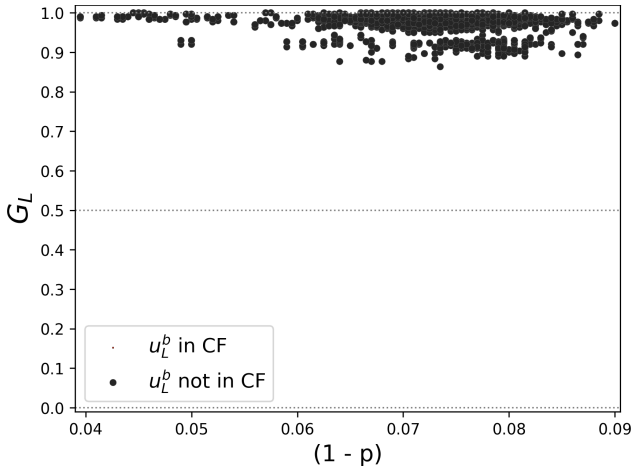
(d) $I_{max} = 10$

Figure 6.4: Each localized attack G_L versus the fraction of nodes contained within the attack radius $(1 - p)$ for interdependent networks built using $s = (1{:}1)$ without extra physical links $(r = 1 \cdot w_{ln})$.

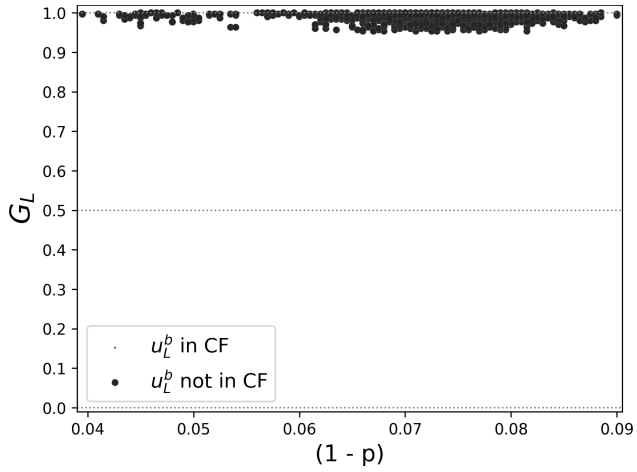


(a) $I_{max} = 3$

(b) $I_{max} = 5$

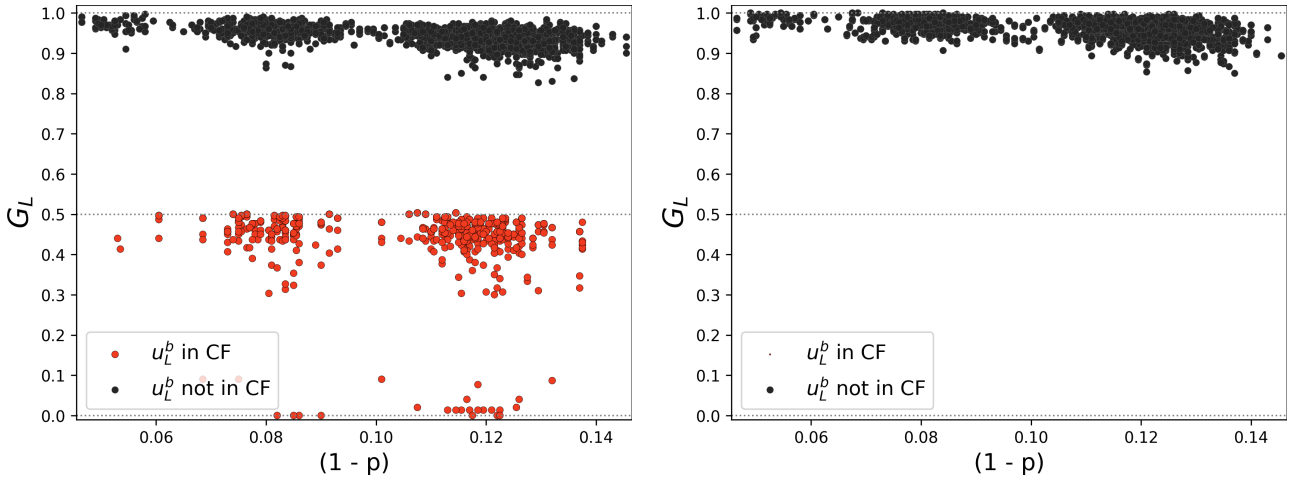


(c) $I_{max} = 7$



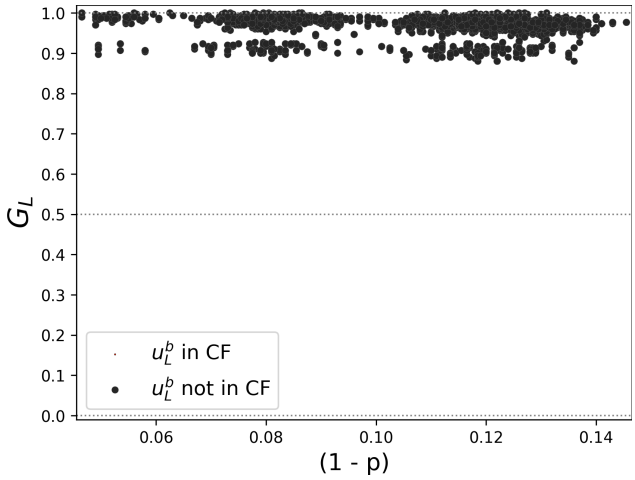
(d) $I_{max} = 10$

Figure 6.5: Each localized attack G_L value versus $(1 - p)$ for interdependent networks built using $s = (1{:}25)$ without extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

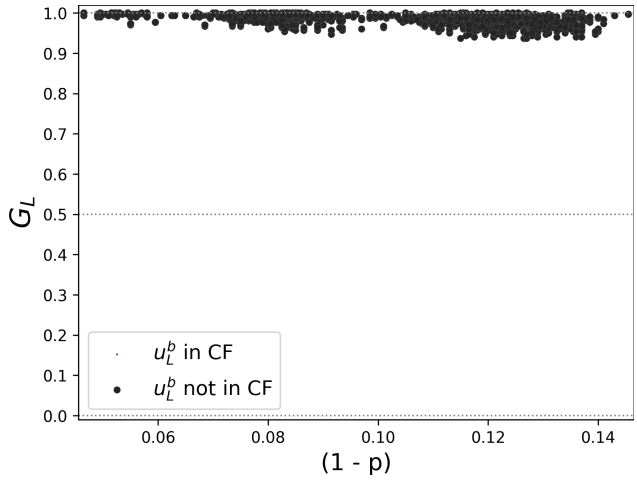


(a) $I_{max} = 3$

(b) $I_{max} = 5$

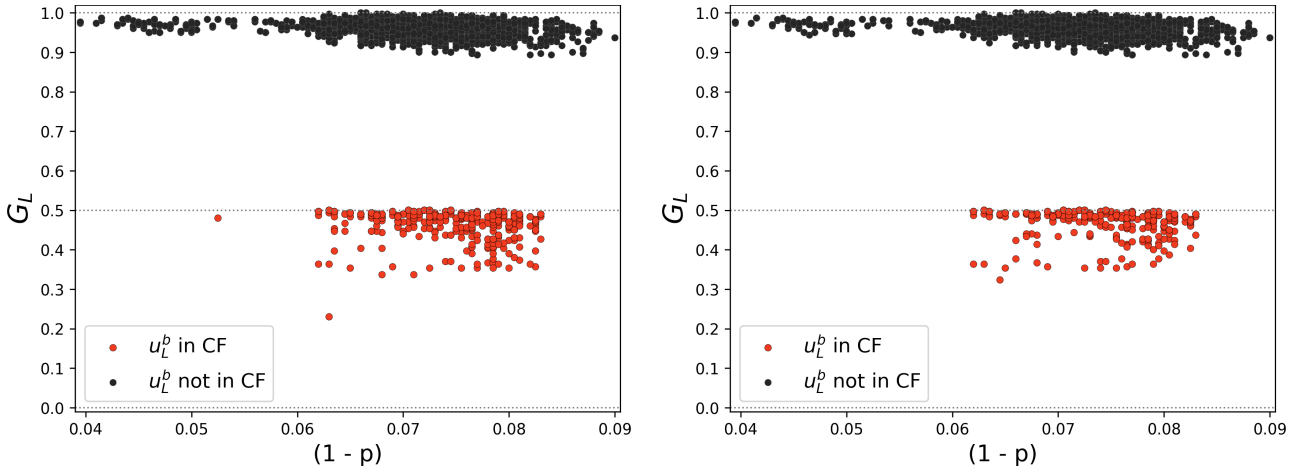


(c) $I_{max} = 7$



(d) $I_{max} = 10$

Figure 6.6: Each localized attack G_L value versus $(1 - p)$ for interdependent networks built using $s = (1{:}1)$ without extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.



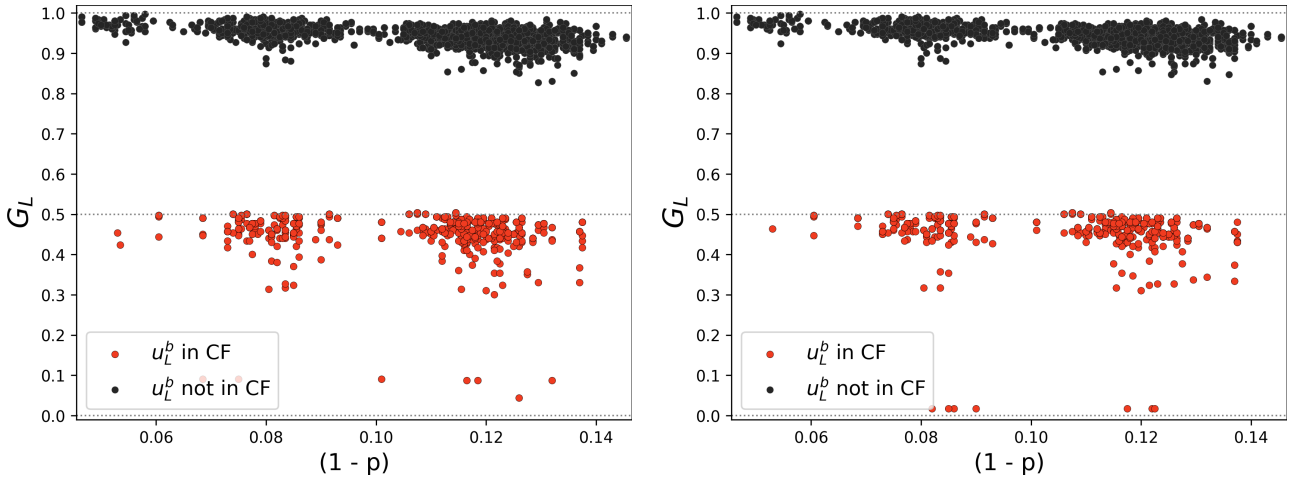
(a) Distance

(b) Local hubs

(c) Degree

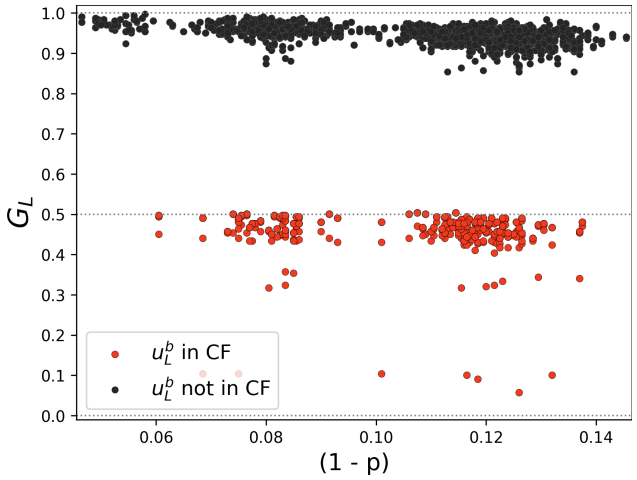
(d) Random

Figure 6.7: Each localized attack G_L value versus $(1-p)$ for interdependent networks built using $s = (1{:}25)$ and $I_{max} = 3$ after adding extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

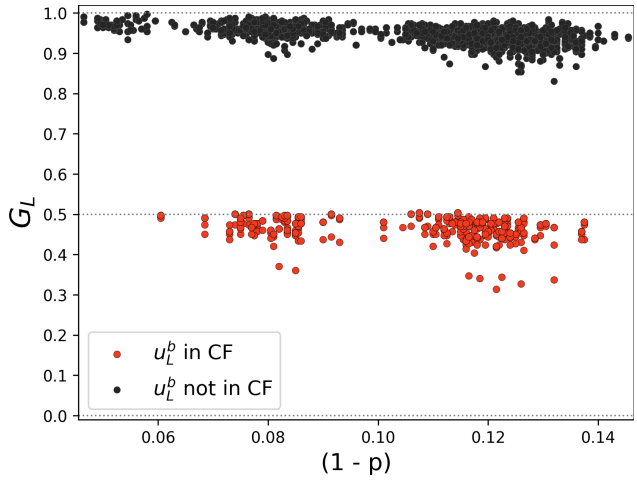


(a) Distance

(b) Local hubs



(c) Degree



(d) Random

Figure 6.8: Each localized attack G_L value versus $(1-p)$ for interdependent networks built using s = (1:1) and $I_{max} = 3$ after adding extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

6.3.3 Physical link addition and localized attacks

In Table 6.1 we can see the total number of localized attacks that result in HDLA, and the G_L ranges of HDLA and non-HDLA for interdependent networks with $I_{max} = 3$, and localized attacks with $a = 1$. Results for other I_{max} tested can be found in appendix section D.3. Here, we can see these results before and after adding links to the physical network. In Table 6.1 we can see that the addition of physical links decreases the number of HDLA, and increases their G_L values compared to physical-logical interdependent networks without physical links added. In Tables 6.2, 6.3, 6.4, and 6.5 we can see that the same behavior is observed for interdependent networks with $I_{max} = 3$, and localized attacks with $a \in \{0.2, 0.4, 0.6, 0.8\}$. Furthermore, we observe that even localized attacks with $a = 0.2$ can result in HDLA over interdependent networks built using $I_{max} = 3$.

In appendix section D.3 we observe that for $I_{max} > 3$ the G_L range of the localized attacks with $a = 1$ tends to contain higher G_L values or remain unchanged after adding extra physical links. We also observe that, as seen in section 6.3.2, localized attacks with $a = 1$ over interdependent networks with $I_{max} > 3$ do not result in HDLA. Note that localized attacks with $a < 1$ remove a subset of the physical nodes removed by LA with $a = 1$. Thus, if LA with $a = 1$ do not result in HDLA for a given interdependent network, then LA with $a < 1$ will not result in HDLA over said system.

Our results show that adding links to the physical network does improve the system's robustness. However, our results also show that, for systems with $I_{max} = 3$, adding physical links cannot fully protect the interdependent networks against HDLA.

$I_{max} = 3, a = 1$										
s	st	Number of HDLA							G_L range (HDLA)	G_L range (Non-HDLA)
		Total	RNG	GG	GPA	5NN	YAO	ER		
(1:25)	Original	480	74	73	114	73	73	73	$(0.0, 0.5)$	$(0.837, 1.0)$
	Distance	458	74	73	92	73	73	73	$(0.23, 0.5)$	$(0.893, 1.0)$
	Local hubs	447	74	73	81	73	73	73	$(0.323, 0.5)$	$(0.893, 1.0)$
	Degree	442	73	73	77	73	73	73	$(0.353, 0.5)$	$(0.897, 1.0)$
	Random	458	74	73	92	73	73	73	$(0.353, 0.5)$	$(0.873, 1.0)$
(1:1)	Original	619	100	99	122	100	99	99	$(0.0, 0.5)$	$(0.827, 0.997)$
	Distance	618	100	99	121	100	99	99	$(0.043, 0.5)$	$(0.827, 0.997)$
	Local hubs	607	99	99	112	99	99	99	$(0.017, 0.5)$	$(0.83, 0.997)$
	Degree	594	99	99	99	99	99	99	$(0.057, 0.5)$	$(0.853, 0.997)$
	Random	596	99	99	101	99	99	99	$(0.313, 0.5)$	$(0.83, 0.997)$

Table 6.1: G_L ranges of HDLA, and LA minus HDLA (Non-HDLA) of interdependent network with and without physical links added for $I_{max} = 3$, and $a = 1$.

$I_{max} = 3, a = 0.2$										
s	st	Number of HDLA							G_L range (HDLA)	G_L range (Non-HDLA)
		Total	RNG	GG	GPA	5NN	YAO	ER		
(1:25)	Original	48	8	8	10	8	7	7	$(0.0, 0.5)$	$(0.963, 1.0)$
	Distance	46	8	8	8	8	7	7	$(0.367, 0.5)$	$(0.973, 1.0)$
	Local hubs	43	7	7	7	8	7	7	$(0.367, 0.5)$	$(0.97, 1.0)$
	Degree	42	7	7	7	7	7	7	$(0.367, 0.5)$	$(0.97, 1.0)$
	Random	43	7	7	8	7	7	7	$(0.37, 0.5)$	$(0.963, 1.0)$
(1:1)	Original	25	4	4	5	4	4	4	$(0.0, 0.5)$	$(0.96, 1.0)$
	Distance	25	4	4	5	4	4	4	$(0.417, 0.5)$	$(0.967, 1.0)$
	Local hubs	24	4	4	4	4	4	4	$(0.017, 0.5)$	$(0.967, 1.0)$
	Degree	24	4	4	4	4	4	4	$(0.457, 0.5)$	$(0.967, 1.0)$
	Random	24	4	4	4	4	4	4	$(0.45, 0.5)$	$(0.967, 1.0)$

Table 6.2: G_L ranges of HDLA, and LA minus HDLA (Non-HDLA) of interdependent networks with and without physical links added for $I_{max} = 3$, and $a = 0.2$.

$I_{max} = 3, a = 0.4$										
s	st	Number of HDLA							G_L range (HDLA)	G_L range (Non-HDLA)
		Total	RNG	GG	GPA	5NN	YAO	ER		
(1:25)	Original	107	16	15	31	15	15	15	$(0.0, 0.5)$	$(0.927, 1.0)$
	Distance	100	16	15	24	15	15	15	$(0.367, 0.5)$	$(0.947, 1.0)$
	Local hubs	92	15	15	17	15	15	15	$(0.367, 0.5)$	$(0.95, 1.0)$
	Degree	92	15	15	17	15	15	15	$(0.367, 0.5)$	$(0.95, 1.0)$
	Random	100	15	15	25	15	15	15	$(0.367, 0.5)$	$(0.953, 1.0)$
(1:1)	Original	123	19	19	28	19	19	19	$(0.0, 0.5)$	$(0.927, 1.0)$
	Distance	120	19	19	25	19	19	19	$(0.403, 0.5)$	$(0.933, 1.0)$
	Local hubs	115	19	19	20	19	19	19	$(0.017, 0.5)$	$(0.933, 1.0)$
	Degree	114	19	19	19	19	19	19	$(0.443, 0.5)$	$(0.94, 1.0)$
	Random	115	19	19	20	19	19	19	$(0.443, 0.5)$	$(0.953, 1.0)$

Table 6.3: G_L ranges of HDLA, and LA minus HDLA (Non-HDLA) of interdependent networks with and without physical links added for $I_{max} = 3$, and $a = 0.4$.

$I_{max} = 3, a = 0.6$										
s	st	Number of HDLA							G_L range (HDLA)	G_L range (Non-HDLA)
		Total	RNG	GG	GPA	5NN	YAO	ER		
(1:25)	Original	230	36	34	57	35	34	34	$(0.0, 0.5)$	$(0.903, 1.0)$
	Distance	217	34	34	46	35	34	34	$(0.357, 0.5)$	$(0.917, 1.0)$
	Local hubs	208	35	34	37	34	34	34	$(0.357, 0.5)$	$(0.917, 1.0)$
	Degree	207	34	34	37	34	34	34	$(0.357, 0.5)$	$(0.937, 1.0)$
	Random	213	34	34	43	34	34	34	$(0.36, 0.5)$	$(0.937, 1.0)$
(1:1)	Original	252	40	40	51	41	40	40	$(0.0, 0.5)$	$(0.893, 1.0)$
	Distance	252	40	40	51	41	40	40	$(0.09, 0.5)$	$(0.907, 1.0)$
	Local hubs	245	40	40	45	40	40	40	$(0.017, 0.5)$	$(0.903, 1.0)$
	Degree	240	40	40	40	40	40	40	$(0.103, 0.5)$	$(0.903, 1.0)$
	Random	242	40	40	42	40	40	40	$(0.35, 0.5)$	$(0.917, 1.0)$

Table 6.4: G_L ranges of HDLA, and LA minus HDLA (Non-HDLA) of interdependent networks with and without physical links added for $I_{max} = 3$, and $a = 0.6$.

$I_{max} = 3, a = 0.8$										
s	st	Number of HDLA							G_L range (HDLA)	G_L range (Non-HDLA)
		Total	RNG	GG	GPA	5NN	YAO	ER		
(1:25)	Original	366	55	54	95	54	54	54	$(0.0, 0.5)$	$(0.88, 1.0)$
	Distance	347	55	54	76	54	54	54	$(0.353, 0.5)$	$(0.9, 1.0)$
	Local hubs	336	55	54	65	54	54	54	$(0.353, 0.5)$	$(0.9, 1.0)$
	Degree	328	54	54	58	54	54	54	$(0.353, 0.5)$	$(0.907, 1.0)$
	Random	344	55	54	73	54	54	54	$(0.353, 0.5)$	$(0.917, 1.0)$
(1:1)	Original	453	73	72	92	72	72	72	$(0.0, 0.5)$	$(0.857, 1.0)$
	Distance	448	72	72	88	72	72	72	$(0.09, 0.5)$	$(0.86, 1.0)$
	Local hubs	441	73	72	80	72	72	72	$(0.017, 0.5)$	$(0.86, 1.0)$
	Degree	432	72	72	72	72	72	72	$(0.103, 0.5)$	$(0.873, 1.0)$
	Random	434	72	72	74	72	72	72	$(0.343, 0.5)$	$(0.88, 1.0)$

Table 6.5: G_L ranges of HDLA, and LA minus HDLA (Non-HDLA) of interdependent networks with and without physical links added for $I_{max} = 3$, and $a = 0.8$.

6.4 Summary

In this chapter we tested the effect of localized attacks over the robustness of physical-logical interdependent networks as modeled in Chapter 3. Here, we used the physical link addition strategies presented in Chapter 5 to test the effect of localized attacks over the robustness of interdependent networks, and compare it to the effect of physical random attacks.

For the experiments we tested the effect of using localized attacks over the robustness of interdependent networks with and without extra physical link added. Extra physical links were added to base interdependent networks according to the link addition strategies described in Chapter 5: Random, Distance, Local hubs, and Degree based addition. Here we use the same base interdependent networks tested in Chapter 5. Thus, for the base systems we consider space shape $s \in \{(1{:}1),(1{:}25)\}$, logical network version $q = 1$, $I_{max} \in \{3, 5, 7, 10\}$, model $m \in \{RNG, GG, 5NN, YAO, GPA, ER\}$, and the 10 different node allocation configurations described in Chapter 3.

In order to test localized attacks, we generated an attack set as follows. For each space shape $s \in \{(1{:}1),(1{:}25)\}$, we generated a set $C(s)$ of 100 localized attack centers. Centers in $C(s)$ were spread uniformly to cover the space s. For each center, five radii values r were tested with $r = aw_{ln}, a \in \{0.2, 0.4, 0.6, 0.8, 1\}$, and w_{ln} the width of the (1:25) space. Then, each localized attack was performed over each physical-logical interdependent network.

Our results show that, for interdependent networks without extra physical links added, the average damage caused by a localized attack is relatively similar to the damage caused by comparable physical random attacks. We also found that for $I_{max} = 3$, interdependent networks using $m \in \{\text{RNG,GPA}\}$ are on average more fragile against localized attacks than against physical random attacks. However, this difference decreases as the I_{max} value increases. A similar effect is observed after adding extra physical links. This suggests that adding more physical links increases the systems' robustness against localized attacks.

For base systems with $I_{max} = 3$ we found that some localized attacks can damage more than 50% of the logical network, and even result in its total destruction. We refer to localized attacks that result in the loss of more than half of the logical network as High Damage Localized Attacks (HDLA). We found that HDLA occur because during their cascading failure they remove the logical bridge node u_L^b. Removing node u_L^b from the isolated logical network is enough to lose more than 45% of the logical nodes. We found that adding extra physical links increases the robustness against localized attacks, and decreases the number of HDLA (but does not fully prevent them). This suggests that adding physical links does improve the interdependent networks' robustness, but in order to avoid HDLA other measures must be implemented.

Chapter 7

Localized attacks with probabilistic failure: Seismic attacks case

In this chapter we present a novel type of attack: Localized Attacks with Probabilistic Failures (LAPF). We start by explaining the motivation for these attacks, and then we present the definition of LAPF.

We show an application of LAPF by using them to define "seismic attacks" or attacks that simulate the effect of seismic events over the physical network. Finally, we test the effect of seismic attacks over the robustness of physical-logical interdependent networks as modeled in Chapter 3, and compare it to the effect of localized attacks.

7.1 Motivation

So far we have aimed to test the effect of physical adverse events over the robustness of the proposed physical-logical interdependent network in an attempt to represent the effect that natural disasters such as earthquakes, floods, tsunamis, etc. would have over its robustness. In Chapters 3 and 5 we tested the effect of physical random attacks, and in Chapter 6 we tested the effect of localized attacks. From the attacks tested, localized attacks are the best approximation to natural disasters. Indeed, natural disasters cause damages within a geographic area, similar to how localized attacks affect a circular area of the physical space. However, while localized attacks cause everything within its attack area to fail, natural disasters can cause different levels of damage for different infrastructures located in the same area. This damage may induce failure on some infrastructure, and leave others fully functional. Here, the damage perceived by an infrastructure depends on the characteristics

of the event, local geographical conditions, infrastructure characteristics, etc.

Let us look at some examples. In the case of tsunamis, the damage level perceived by an infrastructure will depend on variables such as the distance to the shore, the elevation at which the infrastructure was built, the tsunami characteristics, etc. Another example is earthquakes. In the case of earthquakes, the damage level perceived by an infrastructure will depend on the distance to the epicenter, the soil in which the infrastructure was built, the earthquake magnitude, and the type of earthquake, among others. Because of this, two infrastructures that are geographically close to each other can experience different damage levels despite being affected by the same event. Assimaki et al. [7] observed that, after the 2010 earthquake in Chile, two adjacent multi-story buildings located in downtown Concepción suffered vastly different damage levels due to the soil conditions assumed when designing each building. Here, one of the buildings collapsed, whereas the other building only suffered minor damages. The distance between these buildings was approximately 20 meters. Differences as the ones observed by Assimaki et al. are not captured by localized attacks. To capture these differences we need to consider the specific characteristics that contribute to the damage caused by a natural disaster. Furthermore, since the damage caused by an earthquake cannot be modeled in the same way as the damage caused by a tsunami, flood, or tornado, we need to consider the characteristics specific to the type of natural disaster that we wish to represent.

To have a more accurate representation of the damage caused by natural disasters over physical networks we propose to use localized attacks such that the elements of the network affected by the attack have a "probability of failure" or probabilistic failures. Here, we propose to describe the probability of failure using probability distributions. Given a type of natural disaster, the failure probability distribution can be tailored to consider the specific characteristics that contribute to the damage caused by it. We refer to these localized attacks as: **Localized Attack with Probabilistic Failures (LAPF)**.

We must note that a similar probabilistic approach was used by Dong et al. [36] to simulate the damage caused by an earthquake over a transportation network. Here, each link has a failure probability, which was obtained using publicly available data. We can capture the probabilistic failures presented by Dong et al. using LAPF.

7.2 Definition

7.2.1 Localized Attack with Probabilistic Failures (LAPF)

Consider a physical network $P(V_P, E_P)$. We define a localized attack with probabilistic failures or (LAPF) as an attack that affects a circular area of radius $r \in [0, \infty)$, where each

node $u \in V_P$ contained within the attack area has a failure probability given by the failure probability distribution F. In Figure 7.1 we can see a visualization of a LAPF. Here we observe that different areas within the attack area have different failure probabilities. We must note that LAPFs can be tailored to affect areas of any shape by using an appropriate failure probability distribution F.

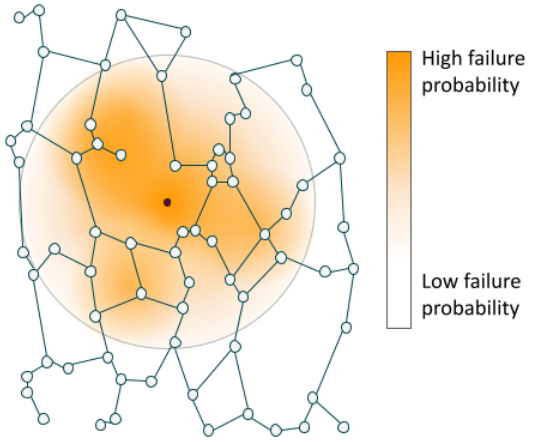


Figure 7.1: Graphic example of the failure probability distribution associated to a specific LAPF.

7.2.2 Failure probability

The failure probability distribution F is defined as a function $F : X \longrightarrow [0, 1]$, where X is the set of network elements that can be affected by the attack. In order to capture the local conditions that affect the failure probability of an element we define the function $g : X \longrightarrow \Gamma$ where Γ contains n-tuples that describe the necessary data to determine the failure probability of a node, and the function $\Phi : \Gamma \longrightarrow [0, 1]$ that determines the failure probability that an event induces given the local condition described by $\gamma \in \Gamma$. Using functions g and Φ we can define F as the function composition of Φ and g ($F = \Phi \circ g$).

7.3 Application: Seismic attacks

Given an infrastructure located at a geographic point x, the damage caused by an earthquake or seismic event over said infrastructure will depend on variables such as the event magnitude, the distance from the x to the epicenter, the depth of the event, the soil type at x, etc. Some of these variables are characteristics of the seismic event itself, such as the event magnitude and depth. Other variables are related to local characteristics of the geographic point, such

as the soil type, and the distance to the epicenter of the event. Variations in the local properties of a point can lead to infrastructures located in different points to experience vastly different levels of damage. When we translate this behavior to a physical network, such as the physical Internet network, this means that not all the nodes affected by the same seismic event will be affected in the same way. Furthermore, two nodes located at similar distances of the same seismic event epicenter might experience different damage levels. The higher the damage level experienced by a node, the more likely is the node to fail.

To capture this behavior we model seismic events using localized attacks with probabilistic failures (LAPF). As defined in section 7.2 in order to test LAPF we must define a failure probability distribution F. Here, we estimate the damage perceived by a node after a seismic event using the Ground Acceleration at the node's location. Then, we use this data to define the failure probability distribution used by the LAPF.

7.3.1 Ground Motion Prediction Equations

The ground acceleration describes the acceleration perceived in a given location during an earthquake and it can be measured using instruments. This acceleration can be used to estimate how strong the shaking produced by an earthquake in a specific location. Given a single seismic event, the acceleration of two different locations during the event can differ.

In the literature we can find different Ground Motion Prediction Equations equations (GMPE) to estimate or predict the acceleration perceived in a given point in space given the local conditions [30, 77, 108, 54]. In this work we aim to represent the conditions of Chile, to do this we use the equations presented by Idini et al. [54] which were developed for the specific case of the Chilean subduction zone.

The equations presented by Idini et al. consider the contribution of the seismic source F_F, the path contribution F_D, and the local site effects F_S as follows.

$$log_{10}Y = F_F(M_w, H, F_{\text{eve}}) + F_D(R, M_w, F_{\text{eve}}) + F_S(V_{s30}, s_{T^*})$$

In this formula, Y is the ground acceleration, M_w is the moment magnitude of the event, F_{eve} is a variable representing whether the event is an interface event ($F_{\text{eve}} = 0$) or an intraslab event ($F_{\text{eve}} = 1$), H is the hypocentral depth, R is the hypocentral distance, V_{s30} is the average shear wave velocity down to 30 meters depth, and s_{T^*} is the site effect coefficient given by the local soil.

In the work of Idini et al. we find that the GMPE proposed can be used to calculate the ground acceleration for several different time periods, including the Peak Ground Acceleration (PGA). In a given location, the PGA is the highest acceleration registered during a seismic event.

7.3.2 Failure probability for seismic attacks

In this application we want to observe the effect of seismic events over the physical-logical interdependent network. In particular we are interested in the effect of seismic events over the physical nodes. To estimate the failure probability of a physical node after a seismic event we want to use the ground acceleration experienced by the node. To obtain this acceleration we use the GMPE provided by Idini et al. [54].

Following the definition given in section 7.2, we have that $X = V_P$ the set of physical nodes, and the set Γ must contain all the necessary data to calculate the ground acceleration. This means that $\gamma \in \Gamma$ is a 6-tuple that contains the moment magnitude of the event M_w, the depth of the event H, the type of event F_{eve}, the hypocentral distance from the node to the event R, the average shear wave velocity down to 30 meters depth V_{s30} at the node's location, and the site effect coefficient of the soil in which the node is located s_{T^*}.

Given a physical node $v \in V_P$, and a seismic event ev centered in (x_{ev}, y_{ev}), with depth H, type F_{eve}, and moment magnitude M_w, we have that the failure probability of node v during a seismic event ev is given by $F_{ev}(v) = \Phi(g_{ev}(v))$ where $g_{ev} : V_P \longrightarrow \Gamma$ is the function that returns the 6-tuple that contains all the necessary data to calculate the ground acceleration perceived by a node given the characteristics of the seismic event ev. Given $\gamma \in \Gamma$, we define the function $\Phi(\gamma) = \Phi_2(\Phi_1(\gamma))$ where Φ_1 corresponds to the equation provided by Idini et al. [54], that is, the equation that returns the ground acceleration associated to the conditions described by γ, and function Φ_2 gives us the failure probability given a ground acceleration value. Here, we define Φ_2 as follows.

$$\Phi_2(a) = \begin{cases} 0 & \text{if } a \leq c_1 \\ \phi(a) & \text{if } c_1 \leq a \leq c_2 \\ 1 & \text{if } a \geq c_2 \end{cases}$$

In this formula we have that $a = \Phi_1(\gamma)$, c_1 is the limit below which we assume that node failure will not occur, and c_2 is the limit above which we assume failure will always occur. Limits c_1 and c_2 have been selected based on the Japan Meteorological Agency (JMA) Seismic Intensity Scale [57]. The JMA Seismic Intensity Scale describes 10 intensity levels, with its lowest intensity level being 0 and its highest intensity level being 7. Each intensity level is associated to a seismic intensity defined by the JMA,

$$I_{JMA} = 2log(a) + 0.94$$

where a is the ground acceleration measured in gal ($1gal = 0.01m/s^2$) at time period $\tau = 0.3s$ [57]. Since the I_{JMA} is calculated using $\tau = 0.3s$, we set Φ_1 using the coefficients associated to a time period of $0.3s$ as described in [54]. We must note that the GMPE used here give

acceleration measured as fractions of g with $g = 9.81m/s^2$, thus we have set Φ_1 to convert the results of the GMPE to m/s^2. Using the JMA Seismic Intensity Scale as guideline we chose c_1 as the lowest ground acceleration for intensity 3 of the seismic scale ($c_1 = 0.06m/s^2$), and c_2 as the ground acceleration above which the seismic event is considered to have an intensity of 7 ($c_2 = 6m/s^2$). For simplicity in this application we define ϕ as a linear function with $\phi(c_1) = 0$ and $\phi(c_2) = 1$, however we must note that Φ_2 and ϕ can be tailored to follow any function that gives a probability as its output.

7.4 Experiments

In this chapter we test the robustness of physical-logical interdependent networks against seismic attacks. In particular, here we test the effect of seismic events using data from Chile's geography and seismic activity. Thus, we only test interdependent networks built over a (1:25) physical space. In this section we describe the seismic attacks tested, the seismic data used to run these tests, and the set of networks tested.

7.4.1 Seismic data

To test the effect of seismic attacks as described in section 7.3 we need information regarding the average shear wave velocity down to 30 meters depth V_{s30} and soil type s_{T^*} at the node's location, the distance between the seismic event and the node R, plus data regarding the seismic event itself: the event's depth H, moment magnitude M_w, and type F_{eve}.

For the data regarding the seismic event conditions we use the data set provided in the work of Idini et al. [54] which describes, among other things, the moment magnitude M_w, depth H, and type F_{eve} of several seismic events registered in Chile. The average shear wave velocity down to 30 meters depth V_{s30} at each node location was approximated from the image provided on Rauld et al. work [89]. We must note that the raw data used by Rauld et al. to generate this map is currently not available for public use, and efforts to gain access to this data were unsuccessful. Finally, since not enough data regarding the soil types as described in [54] is available, the soil type for the entire physical space has been approximated to s_{II} soil. This soil was selected because soil s_{II} has been found to be present in similar proportions in both soil (55%) and rock (45%) [66].

7.4.2 Seismic attacks

To test seismic attacks we use the definition provided in section 7.3. Here, the coefficients used in equation Φ_1 correspond to the coefficients described in [54] for $\tau = 0.3s$. We must note that since seismic attacks are LAPF they do not necessarily have a maximum radius

r. However, for the experiments we set a maximum radius $r_{ev} = 400km$ beyond which no physical nodes can be affected by the seismic attack.

Given the physical space s we define $C(s)$ as the set of attack centers tested. The set $C(s)$ contains a total of 100 centers uniformly spread over the space s. Each seismic event is simulated over each center $c \in C(s)$. Here, we test a total of 103 different seismic events using the seismic data described in section 7.4.1. Thus, a total of 10300 seismic attacks are tested over each physical-logical interdependent network considered for the experiments.

7.4.3 Networks tested

In this chapter we use interdependent networks previously used in Chapter 5. In this chapter we aim to simulate the effect of seismic events over the Chilean country, thus we only use interdependent networks built over space $s = (1{:}25)$. Here, we test physical-logical interdependent networks before adding extra physical links.

$$(P_j(m, s), L_1, I(u))$$

And after adding links using a strategy st, with st a physical link addition strategy defined in section 5.2.

$$(P_j^{st}(m, s), L_1, I(u))$$

Here $P_j(m, s)$ is the physical network generated using model m over the space s, and the j-th physical node allocation configuration $loc_j(V_P, s)$, $P_j^{st}(m, s)$ is the physical network obtained after adding extra physical links to network $P_j(m, s)$ according to strategy st, L_1 is the logical network ($q = 1$), and $I(u)$ is the set of interlinks generated given $I_{max} = u$. In this chapter we use the same interdependent networks tested in Chapter 5, thus we consider $u \in \{3, 5, 7, 10\}$, $j \in \{1, \ldots, 10\}$, $s \in \{(1{:}25), (1{:}1)\}$, and $m \in \{RNG, YAO, GPA, 5NN, GG, ER\}$.

The parameters for each base interdependent network $(P_j(m, s), L_1, I(u))$ are the same as those described in Chapter 3. Thus, for each physical-logical interdependent network, we have $p_L = 6$ the number of provider nodes, $N_L = 300$ the number of logical nodes, and $N_P = 2000$ the number of physical nodes. To generate each network $(P_j^{st}(m, s), L_1, I(u))$ we add the same number of links $|E^{st}_{(j,m,s)}| \approx \frac{E_{RNG}}{4}$ for each strategy st as defined in Chapter 5.

7.5 Results

In this section we will show the results of testing the robustness of each physical-logical interdependent network described in section 7.4 against seismic attacks. Here, we will show the results with and without extra physical links added using the strategies presented in Chapter 5.

7.5.1 Seismic attacks

In Figure 7.3 we can see the effect of each seismic attack tested over each of the physical-logical interdependent networks before adding extra physical links. Here we can see that, similar to localized attacks, seismic attacks can cause High Damage Seismic Attacks (HDSA), that is, seismic attacks that result in $G_L \leq 0.5$. In Figure 7.3 we can see that HDSA occur on interdependent networks with $I_{max} = 3$ and $I_{max} = 10$. As we can see in Figure 7.4, each of these HDSA remove the logical bridge node u_L^b described in section 6.3.2. This suggests that, for seismic attacks, HDSA are caused by the removal of the logical node u_L^b during the cascading failure process.

Figure 7.5 shows the effect of each seismic attack tested over each of the physical-logical interdependent networks before adding extra physical links, and the moment magnitude M_w of the event associated with each seismic attack. Here we observe that for $I_{max} = 3$ the magnitude of the event is not correlated with the occurrence of HDSA. However, we observe that for $I_{max} = 10$ HDSA only occur with higher M_w events. This can be further observed in Table 7.1, here we can see the detailed information regarding the number of HDSA, the percentage that these HDSA represent from the total, the M_w range associated to HDSA, and the range of G_L values associated to HDSA and non-HDSA. In Table 7.1 we can see that HDSA represent a very small percentage of the total number of seismic attacks tested. For $I_{max} = 3$, all the HDSA combined represent less than 3% of all the seismic attacks tested. For $I_{max} = 10$ this percentage drops to less than 0.0023%.

In Chapter 6 we observed that interdependent networks built using an I_{max} value $u > 3$ ($u \in \{5, 7, 10\}$) do not suffer High Damage Localize Attacks (HDLA). Here, we observe that most HDSA occur on interdependent networks built using $I_{max} = 3$. However, unlike against localized attacks, here we observe that some HDSA occur on systems built using $I_{max} = 10$. We found that all HDSA occur on interdependent networks built using the same physical nodes locations version $j = 10$ to generate the physical network $P_{10}(m, s) = (V_P, E_P^m(loc_{10}(V_P, s))$. The combination of $loc_{10}(V_P, s)$ with the interlink set $I(10)$ results in a physical network that contains all the physical counterparts of node u_L^b within an area that can be damaged by higher intensity seismic attacks. In Figure 7.2 we can see the effect of an HDSA over an interdependent network built using $j = 10$, $m =$ RNG, and $I_{max} = 10$. Here we can see all 3 physical counterparts of node u_L^b. We observe that although only one u_L^b counterpart is removed during the first step of the cascading failure process (see section 3.2.3), the other two u_L^b counterparts become unable to reach any provider node once the nodes damaged during the first step cascading failure process are removed.

$I_{max} = 3$				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	3360	(5.5, 8.8)	(0.0, 0.487)	(0.82, 1.0)
GG	1963	(5.5, 8.8)	(0.027, 0.503)	(0.84, 1.0)
GPA	3889	(5.5, 8.8)	(0.01, 0.493)	(0.767, 1.0)
5NN	1659	(5.5, 8.8)	(0.027, 0.503)	(0.86, 1.0)
YAO	1607	(5.5, 8.8)	(0.027, 0.503)	(0.853, 1.0)
ER	1652	(5.5, 8.8)	(0.027, 0.503)	(0.847, 1.0)
$I_{max} = 5$				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.823, 1.0)
GG	0	-	-	(0.827, 1.0)
GPA	0	-	-	(0.833, 1.0)
5NN	0	-	-	(0.85, 1.0)
YAO	0	-	-	(0.84, 1.0)
ER	0	-	-	(0.893, 1.0)
$I_{max} = 7$				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.867, 1.0)
GG	0	-	-	(0.867, 1.0)
GPA	0	-	-	(0.833, 1.0)
5NN	0	-	-	(0.873, 1.0)
YAO	0	-	-	(0.873, 1.0)
ER	0	-	-	(0.88, 1.0)
$I_{max} = 10$				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	6	(7.8, 8.8)	(0.46, 0.467)	(0.943, 1.0)
GG	3	(7.8, 8.3)	(0.48, 0.48)	(0.95, 1.0)
GPA	0	-	-	(0.92, 1.0)
5NN	1	(8.8, 8.8)	(0.483, 0.483)	(0.95, 1.0)
YAO	1	(7.8, 7.8)	(0.49, 0.49)	(0.95, 1.0)
ER	3	(7.8, 7.8)	(0.49, 0.49)	(0.95, 1.0)

Table 7.1: Summary of seismic attacks performed over interdependent networks with no extra physical links added.

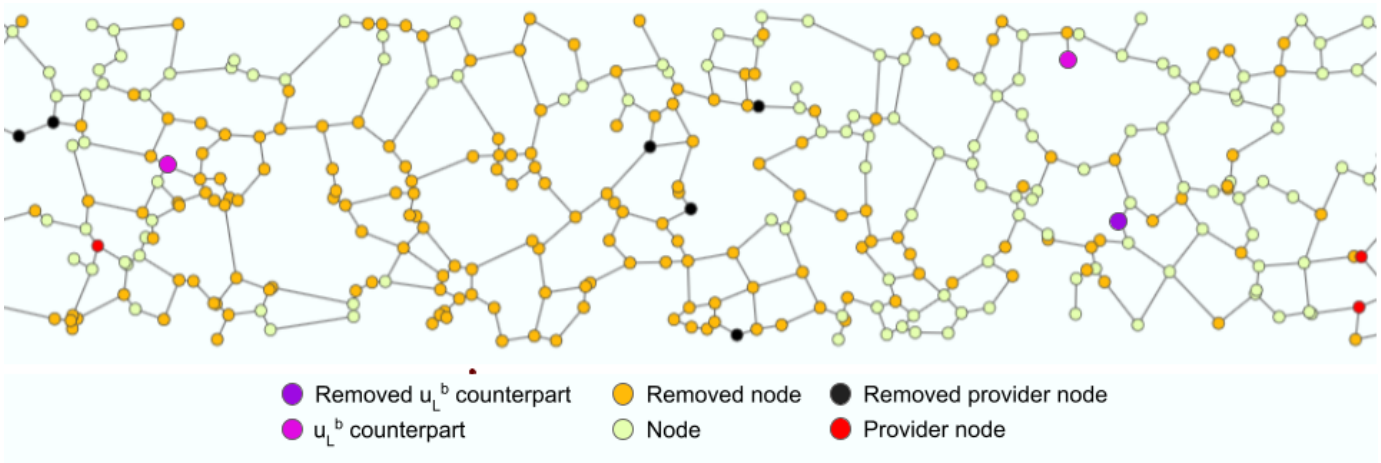
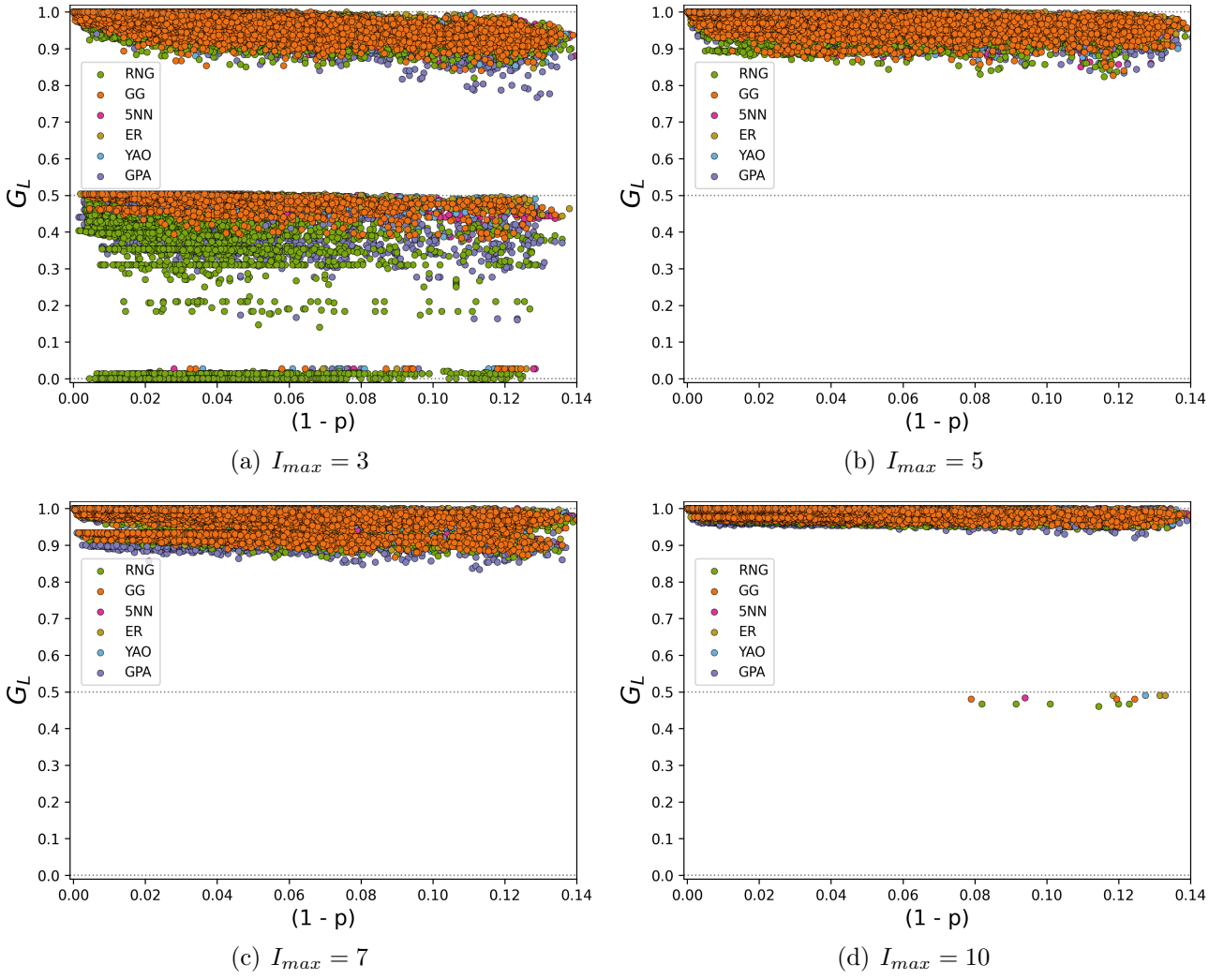


Figure 7.2: Effect of an HDSA over node u_L^b physical counterparts for an interdependent network built using $j = 10$, $m =$ RNG, and $I_{max} = 10$. Image shows the fraction of the physical network that contains all node u_L^b counterparts. Nodes marked as 'removed' correspond to nodes removed during step 1) of the cascading failure process (see section 3.2.3). Nodes not removed during step 1) of the cascading failure process can be removed in subsequent steps.



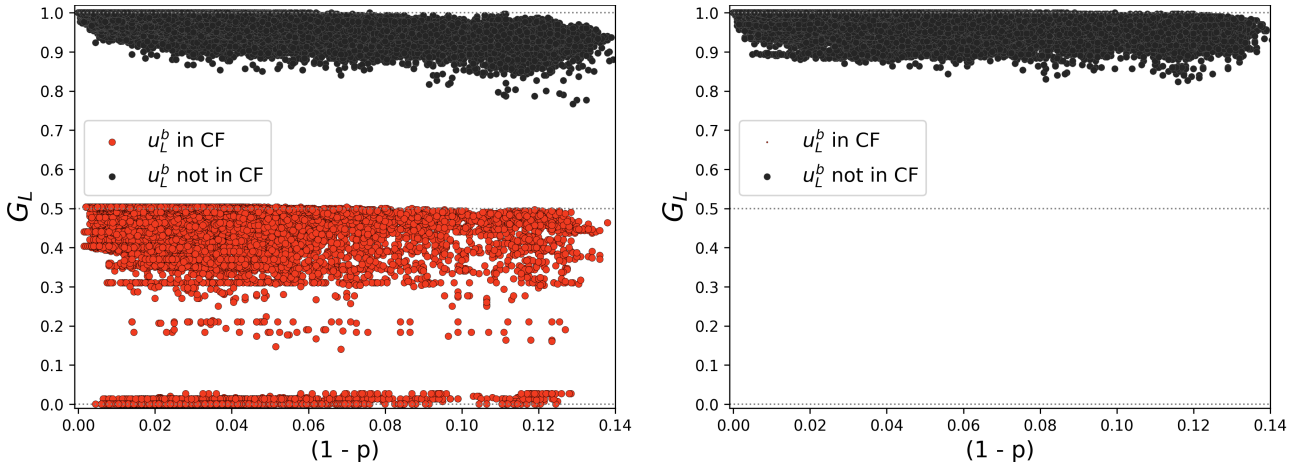
(a) $I_{max} = 3$

(b) $I_{max} = 5$

(c) $I_{max} = 7$

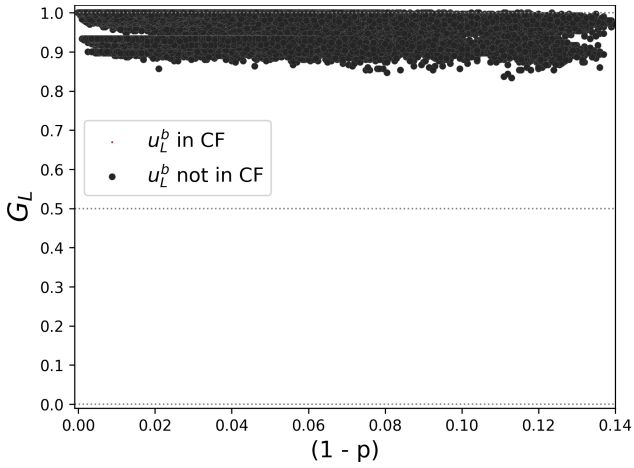
(d) $I_{max} = 10$

Figure 7.3: G_L values obtained after each seismic attack tested. Each color represents a different physical model m.

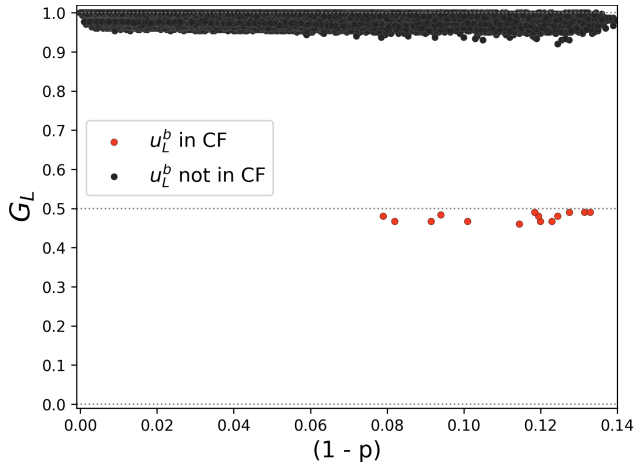


(a) $I_{max} = 3$

(b) $I_{max} = 5$

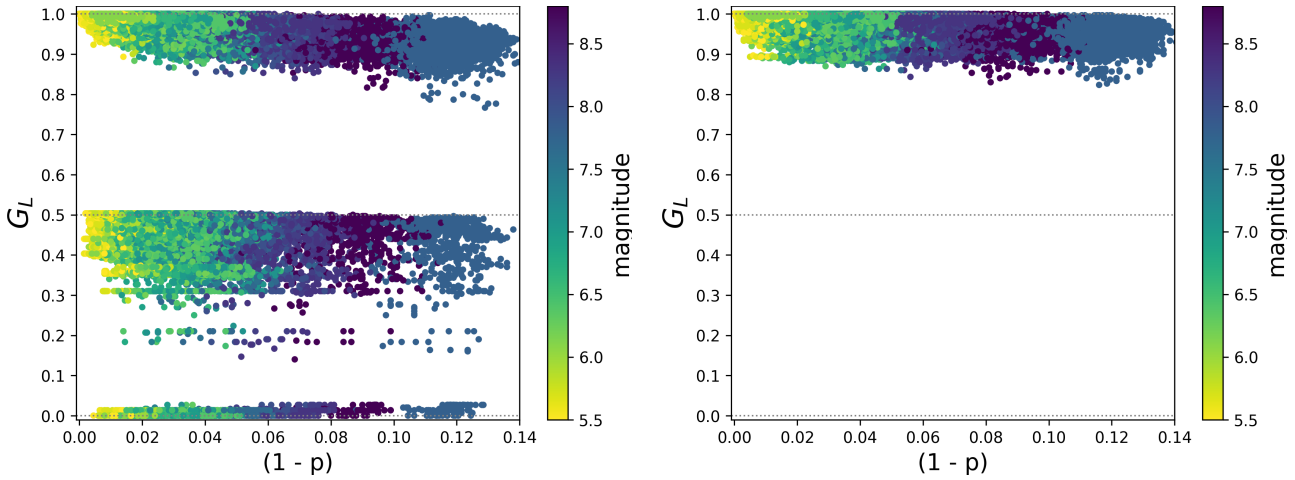


(c) $I_{max} = 7$



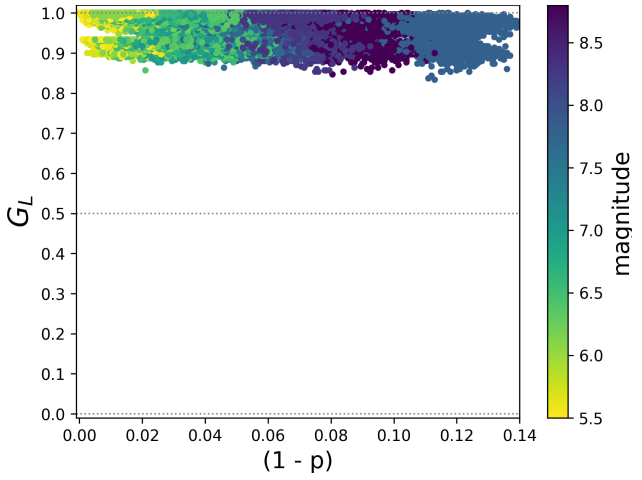
(d) $I_{max} = 10$

Figure 7.4: Each seismic attack G_L value versus $(1-p)$ for interdependent networks without extra physical links. Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

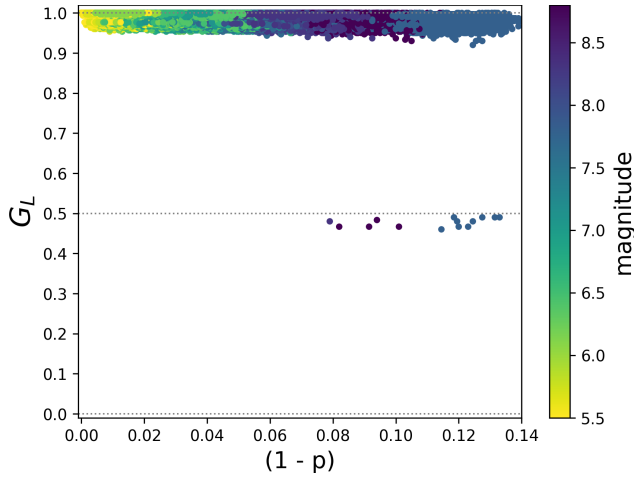


(a) $I_{max} = 3$

(b) $I_{max} = 5$



(c) $I_{max} = 7$



(d) $I_{max} = 10$

Figure 7.5: Each seismic attack G_L value versus $(1-p)$ for interdependent networks without extra physical links. Colors show the moment magnitude M_w associated to each seismic attack.

7.5.2 Comparison: Seismic Attacks vs Localized Attacks

Unlike localized attacks, the damage made by a seismic attack is not deterministic. Thus, if we perform a seismic attack with the same initial conditions twice we may observe that each seismic attack damages a different fraction $(1-p)$ of physical nodes. In contrast, for the case of localized attacks, performing an attack with the same initial conditions twice will always result in the same fraction $(1-p)$ of physical nodes being damaged. In order to compare the effect of seismic attacks versus localized attack we must first establish a way to compare the damages caused by each type of attack that allow us to account for their differences.

In Chapter 6 we tested 5 different localized attack radii r, and 100 attack centers $c \in C(s)$, with s the space shape. In the current chapter, for each pair (j, c) with j the physical network version, and $c \in C(s)$ the attack center a total of 103 seismic attacks were tested. To compare these seismic attacks with localized attacks we classify them into three categories: (1) seismic attacks that make more damage to the network than a localized attack that removes a similar number of nodes, (2) seismic attacks that make less damage to the network than a localized attack that removes a similar number of nodes, and (3) seismic attacks that make a similar damage compared to a localized attack that removes a similar number of nodes.

Given a center c, space shape s, physical model m, node allocation configuration version j, and radius r_{i}, a localized attack will always damage the same fraction of nodes $f(r_{\mathrm{i}}, m, j, c, s)$ and will result in a G_L value $G_L = G_L^{LA}(r_{\mathrm{i}}, m, j, c, s)$. Consider $\hat{s} = (1{:}25)$, we define the set $\mathcal{B}^{\hat{s}}(m, j, c)$:

$$\mathcal{B}^{\hat{s}}(m, j, c) = \{(f(r_{\mathrm{i}}, m, j, c, s), G_L^{LA}(r_{\mathrm{i}}, m, j, c, \hat{s}))\} \cup \{(0, 1), (1, 0)\}$$

This set contains tuples of the form (f, G_L) where $f = (1-p)$ represents the fraction of nodes removed by a localized attack, and G_L corresponds to the G_L obtained after the attack. More specifically, the set $\mathcal{B}^{\hat{s}}(m, j, c)$ contains tuple $(0, 1)$ representing an attack that damages a fraction $f = 0$ and thus results in a $G_L = 1$, tuple $(1, 0)$ representing an attack that removes all the nodes $(f = 1)$ and thus results in a $G_L = 0$, and a tuple containing the fraction of nodes removed $f(r_{\mathrm{i}}, m, j, c, \hat{s})$, and the $G_L(r_{\mathrm{i}}, m, j, c, \hat{s})$ obtained for each of the localized attacks tested in Chapter 6 over the interdependent network built using physical model m version j, and space shape $\hat{s} = (1{:}25)$ at center c.

With this we can classify each seismic attack as follows. Given a seismic event ev we represent the effect that a seismic attack has over a system built using physical model m version j, and space shape $\hat{s} = (1{:}25)$ at center c as

$$(f(\mathrm{e}v, m, j, c, \hat{s}), G_L^{SA}(\mathrm{e}v, m, j, c, \hat{s}))$$

where $f(ev, m, j, c, \hat{s})$ is the fraction of nodes removed by the seismic attack, and $G_L^{SA}(ev, m, j, c, \hat{s})$ is the G_L value obtained after the seismic attack. We can find 2 tuples (f^a, G_L^a) and (f^b, G_L^b) in $\mathcal{B}^{\hat{s}}(m, j, c)$ such that the following is true.

$$f^a \leq f(ev, m, j, c, \hat{s}) < f^b$$

Using this we can classify the seismic attack into one of these 3 categories:

- **Damage SA > Damage LA**: If $f^a \leq f(ev, m, j, c, \hat{s}) < f^b$ and $G_L^{SA}(ev, m, j, c, \hat{s}) \leq G_L^b$. That is, the seismic attack removes a fraction of nodes within the range $[f^a, f^b)$ and results in more damage than the localized attack that removes the most number of nodes (f^b, G_L^b).

- **Damage SA ∼ Damage LA**: If $f^a \leq f(ev, m, j, c, \hat{s}) < f^b$ and $G_L^b \leq G_L^{SA}(ev, m, j, c, \hat{s}) < G_L^a$. That is, the seismic attack results in a damage level similar to that of localized attacks (f^a, G_L^a) and (f^b, G_L^b).

- **Damage SA < Damage LA**: If $f^a \leq f(ev, m, j, c, \hat{s}) < f^b$ and $G_L^{SA}(ev, m, j, c, \hat{s}) \leq G_L^b$. That is, the seismic attack removes a fraction of nodes within the range $[f^a, f^b)$ and results in less damage than the localized attack that removes the least number of nodes (f^a, G_L^a).

Table 7.2 shows the percentage of seismic attacks contained within each category for each model, and each I_{max} tested for interdependent networks with no extra physical links added. Here we can see that, regardless of the model or I_{max} value, most seismic attacks result in a damage level comparable to that of localized attacks. In Table 7.2 we also observe that in all cases the percentage of seismic attacks in the category **Damage SA > Damage LA** is at least twice as much as the percentage of seismic attacks in the category **Damage SA < Damage LA**. Furthermore, given a fixed I_{max}, we observe that less than 13% of the seismic attacks result in less damage than localized attacks. These results show that seismic attacks are much more likely to cause a similar or higher level of damage when compared to localized attacks, than to cause a lower damage level.

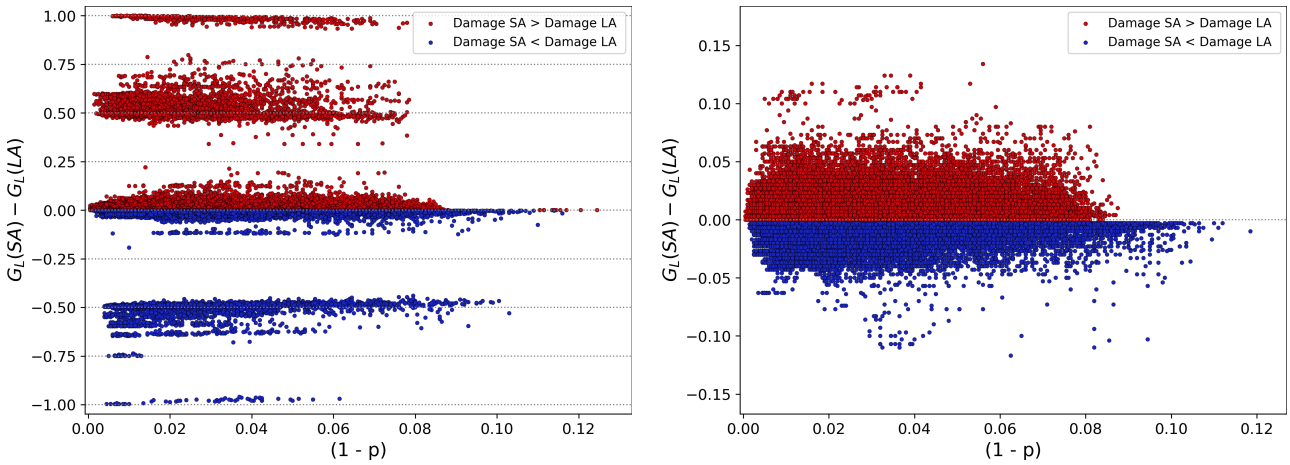
In Figure 7.6 we can see the difference between the G_L value of seismic attack and the G_L value of comparable localized attacks. To observe the damage difference between localized attacks and seismic attacks we define $G_L(LA) - G_L(SA)$ as follows. Given $\hat{a}$ a seismic attack represented by $(f(\hat{a}), G_L(\hat{a}))$ with $f(\hat{a}) = f(ev, m, j, c, \hat{s})$ and $G_L(\hat{a}) = G_L^{SA}(ev, m, j, c, \hat{s})$, and $(f^a, G_L^a), (f^b, G_L^b) \in \mathcal{B}^{\hat{s}}(m, j, c)$ such that $f^a \leq f(\hat{a}) < f^b$. We define the value $G_L(LA) - G_L(SA)$ for seismic attack $\hat{a}$ as:

$$(G_L(LA) - G_L(SA))(\hat{a}) = \begin{cases} G_L^b - G_L(\hat{a}) & \text{if } \hat{a} \text{ in } \textbf{Damage SA} > \textbf{Damage LA} \\ G_L^a - G_L(\hat{a}) & \text{if } \hat{a} \text{ in } \textbf{Damage SA} < \textbf{Damage LA} \end{cases}$$

$I_{max} = 3$							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA $>$ Damage LA	52.3%	37.6%	33.9%	34.2%	33.3%	32.4%	37.3%
Damage SA $\sim$ Damage LA	41.7%	51.4%	50.2%	52.7%	53.2%	52.7%	50.3%
Damage SA $<$ Damage LA	6.0%	11.0%	16.0%	13.1%	13.5%	14.9%	12.4%
$I_{max} = 5$							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA $>$ Damage LA	41.5%	29.6%	29.6%	26.6%	25.9%	25.3%	29.7%
Damage SA $\sim$ Damage LA	52.3%	59.7%	54.8%	60.8%	61.0%	60.4%	58.2%
Damage SA $<$ Damage LA	6.2%	10.7%	15.6%	12.7%	13.1%	14.3%	12.1%
$I_{max} = 7$							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA $>$ Damage LA	38.0%	28.2%	28.9%	26.2%	25.4%	24.8%	28.6%
Damage SA $\sim$ Damage LA	56.8%	63.1%	57.2%	63.5%	64.1%	63.7%	61.4%
Damage SA $<$ Damage LA	5.3%	8.8%	13.9%	10.3%	10.6%	11.5%	10.1%
$I_{max} = 10$							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA $>$ Damage LA	30.5%	22.5%	26.0%	20.5%	19.9%	19.7%	23.2%
Damage SA $\sim$ Damage LA	65.5%	70.8%	63.4%	71.5%	71.9%	71.3%	69.0%
Damage SA $<$ Damage LA	4.0%	6.8%	10.6%	7.9%	8.3%	9.1%	7.8%

Table 7.2: Comparison between localized attacks and seismic attacks for interdependent networks with no extra physical links added.

With this we can observe how much more (or less) severe a seismic attack is compared to localized attacks. In Figure 7.6 we can see the $G_L(LA) - G_L(SA)$ values obtained for each seismic attack classified within the **Damage SA $>$ Damage LA** category or within the **Damage SA $<$ Damage LA** category. From Table 7.2 we know that there are more dots within the **Damage SA $>$ Damage LA** category than the **Damage SA $<$ Damage LA** category. In Figure 7.6 we observe that for $I_{max} = 3$ the range of $G_L(LA) - G_L(SA)$ values is similar for both seismic attack categories, despite there being more dots in the **Damage SA $>$ Damage LA** category. Furthermore we observe that some seismic attacks result in $G_L(LA) - G_L(SA) = 1$ or $G_L(LA) - G_L(SA) = -1$, that is, there are seismic attacks that completely destroy the logical network by removing a fraction of physical nodes comparable to localized attacks that result in no damage to the logical network, and vice versa. For $I_{max} \in \{5, 7\}$ each $G_L(LA) - G_L(SA)$ value can be found within the range $(-0.15, 0.15)$. Finally, for $I_{max} = 10$ we observe that for most seismic attacks the difference $G_L(LA) - G_L(SA)$ falls within the range $(-0.05, 0.05)$. However, we also observe that some $G_L(LA) - G_L(SA)$ are greater than 0.5. These points correspond to the HDSA observed in section 7.5.1.



(a) $I_{max} = 3$ (b) $I_{max} = 5$

(c) $I_{max} = 7$ (d) $I_{max} = 10$

Figure 7.6: $G_L(LA) - G_L(SA)$ values obtained for each seismic attack classified within the **Damage SA > Damage LA** category or within the **Damage SA < Damage LA** category. Interdependent networks have no extra physical links added.

7.5.3 Link addition effect against seismic attacks

Figure 7.7 shows the effect of each seismic attack tested over each of the physical-logical interdependent networks after adding extra physical links for systems built using $I_{max} = 3$. Here we observe that after adding extra links to the physical networks the range of G_L values of non-HDSA becomes narrower and contains higher G_L values compared to the range of G_L values obtained for interdependent networks with no extra links added. This can be observed in more detail in Table 7.3. Tables for $I_{max} \in \{3, 5, 7, 10\}$ can be found in the appendix section E.3. Although no physical link addition strategy is able to fully avoid catastrophic HDSA or HDSA that result in a $G_L \approx 0$, we observe that range of G_L values for HDSA that result in a $G_L > 0.1$ becomes narrower and contains higher G_L values after adding extra physical links. In Figure 7.8 we can see that, after adding extra physical links, HDSA remove the logical bridge node u_L^b during the cascading failure process, whereas non-HDSA do not.

In the appendix section E.1 we can see Figures showing the effect of each seismic attack tested over each of the physical-logical interdependent networks after adding extra physical links for systems built using $I_{max} \in \{5, 7, 10\}$. In these Figures we observe that in most cases after adding extra links to the physical networks the range of G_L values of non-HDSA becomes narrower and contains higher G_L values compared to the range of G_L values obtained for interdependent networks with no extra links added. Tables in the appendix section E.3 show the detailed summary of HDSA for systems with $I_{max} \in \{5, 7, 10\}$. However, for interdependent networks built using $I_{max} = 5$ we observe that after adding physical links using Degree strategy one seismic attack results in an HDSA, whereas the original interdependent network did not have any HDSA. As this is not a trend but rather an isolated case, it can be explained due to the probabilistic nature of seismic attacks which can result in two seismic attacks with the same initial condition having different outcomes. In the appendix section E.1 we can also see that, after adding extra physical links, HDSA remove the logical bridge node u_L^b during the cascading failure process, whereas non-HDSA do not.

As for the relation between the magnitude associated to the seismic attack and its G_L value, in Figure 7.9 we can see that after adding extra links to the physical network the moment magnitude M_w of the seismic attack is not correlated to the occurrence of HDSA for interdependent networks using $I_{max} = 3$. However we observe that after adding physical links catastrophic HDSA only occur for seismic events with a $M_w = 6.5$ or higher. In appendix sections E.1 and E.3 we can see that for interdependent networks using $I_{max} = 10$ HDSA still only occur with higher M_w events. However adding physical links does not necessarily result in HDSA being caused by seismic events with a higher M_w when compared to the interdependent network without extra physical links added.

In Table 7.3 we can see the comparison of the results obtained for interdependent networks

with and without added physical links, for systems built using $I_{max} = 3$. Tables for $I_{max} \in \{5, 7, 10\}$ can be found in the appendix section E.3. Here we can see the detailed information regarding the number of HDSA, the M_w range associated with HDSA, and the range of G_L values associated with HDSA and non-HDSA. In Table 7.3 we observe that, with the exception of models based on 5NN, adding physical links using any strategy results in a lower number of HDSA compared to interdependent networks without extra physical links. For the case of interdependent networks built using $I_{max} = 10$, in Table E.4 we observe a reduction in the total number of HDSA after adding physical links. However, given a fixed model m, we may not observe a consistent decrease in the number of HDSA after adding physical links to a physical network. As the number of total HDSA in interdependent networks with $I_{max} = 10$ before adding extra physical links represents less than 0.0023% of all the seismic attacks tested, these variations are likely caused by the probabilistic nature of seismic attacks rather than the addition of physical links. From Table 7.3 we can see that Degree strategy results in the greatest HDSA reduction, and G_L range improvement for non-HDSA, followed by Random strategy in second place, Local hubs in third place, and Distance strategy in fourth place. The same is true for interdependent networks built using other I_{max} values as seen in the appendix section E.3. These results suggest that adding extra links to the physical network does improve the robustness of physical-logical interdependent networks against seismic attacks.

Now let us compare the effect of adding physical links against seismic attacks versus the effect of adding physical links against localized attacks. In Table 7.4 we can see the percentage of seismic attacks contained within each category defined in section 7.5.2, for $I_{max} = 3$, and systems with and without extra physical links added. Figures for $I_{max} \in \{5, 7, 10\}$ can be found in appendix section E.2. For $I_{max} = 3$, we observe that adding physical links always results in a reduction in the percentage of seismic attacks within the **Damage SA** $>$ **Damage LA** category, and an increment in the number of seismic attacks in the categories **Damage SA** $\sim$ **Damage LA**, and **Damage SA** $<$ **Damage LA**. From Table 7.4 we can see that Degree strategy reduces the percentage attacks in the **Damage SA** $>$ **Damage LA** category the most, followed by Random strategy in second place, Local hubs in third place, and Distance in fourth place. Furthermore, Degree strategy increases the percentage of seismic attacks contained in the **Damage SA** $<$ **Damage LA** category the most, followed by Random strategy, Local hubs, and Distance. From Tables in appendix section E.4 we can see the same behavior is observed for interdependent networks with $I_{max} \in \{5, 7, 10\}$. This suggests that adding physical links can effectively decrease the severity of seismic attacks. However we must note that even after adding links to the physical network 30% of the seismic attacks tested result in a higher damage compared to localized attacks.

Figure 7.10 shows the $G_L(LA) - G_L(SA)$ values obtained for each seismic attack classified within the **Damage SA** $>$ **Damage LA** category or within the **Damage SA** $<$ **Damage**

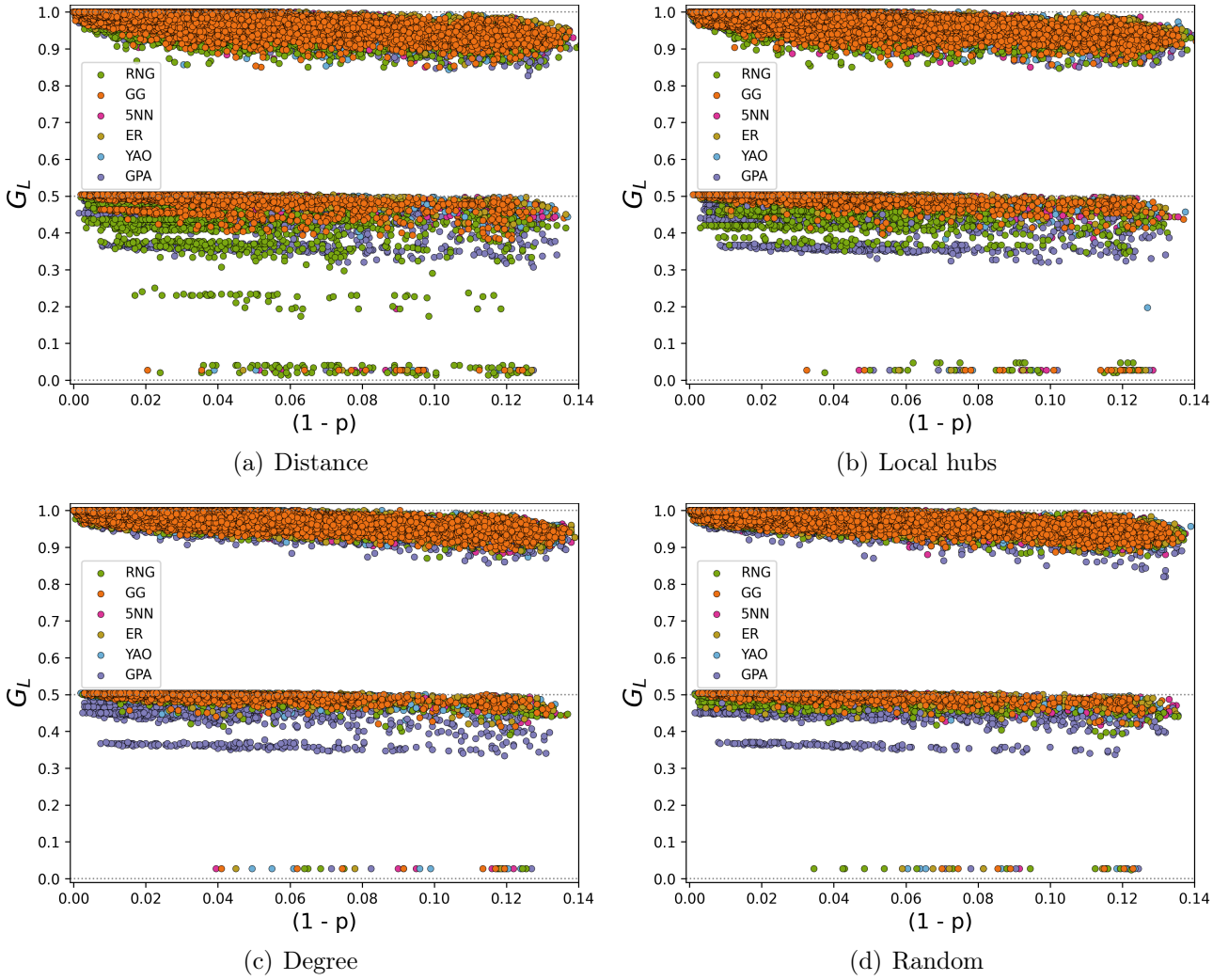
st = Original				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	3360	(5.5, 8.8)	(0.0, 0.487)	(0.82, 1.0)
GG	1963	(5.5, 8.8)	(0.027, 0.503)	(0.84, 1.0)
GPA	3889	(5.5, 8.8)	(0.01, 0.493)	(0.767, 1.0)
5NN	1659	(5.5, 8.8)	(0.027, 0.503)	(0.86, 1.0)
YAO	1607	(5.5, 8.8)	(0.027, 0.503)	(0.853, 1.0)
ER	1652	(5.5, 8.8)	(0.027, 0.503)	(0.847, 1.0)
st = Distance				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	2618	(5.5, 8.8)	(0.013, 0.497)	(0.85, 1.0)
GG	1829	(5.5, 8.8)	(0.027, 0.503)	(0.85, 1.0)
GPA	2674	(5.5, 8.8)	(0.027, 0.493)	(0.827, 1.0)
5NN	1734	(5.5, 8.8)	(0.027, 0.503)	(0.85, 1.0)
YAO	1608	(5.5, 8.8)	(0.027, 0.503)	(0.843, 1.0)
ER	1588	(5.5, 8.8)	(0.027, 0.503)	(0.857, 1.0)
st = Local hubs				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	2123	(5.5, 8.8)	(0.02, 0.503)	(0.847, 1.0)
GG	1730	(5.5, 8.8)	(0.027, 0.503)	(0.857, 1.0)
GPA	2117	(5.5, 8.8)	(0.027, 0.5)	(0.85, 1.0)
5NN	1633	(5.5, 8.8)	(0.027, 0.503)	(0.85, 1.0)
YAO	1635	(5.5, 8.8)	(0.027, 0.503)	(0.857, 1.0)
ER	1562	(5.5, 8.8)	(0.027, 0.503)	(0.873, 1.0)
st = Degree				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	1564	(5.5, 8.8)	(0.027, 0.503)	(0.87, 1.0)
GG	1609	(5.5, 8.8)	(0.027, 0.503)	(0.887, 1.0)
GPA	1669	(5.5, 8.8)	(0.027, 0.503)	(0.857, 1.0)
5NN	1570	(5.5, 8.8)	(0.027, 0.503)	(0.883, 1.0)
YAO	1540	(5.5, 8.8)	(0.027, 0.503)	(0.873, 1.0)
ER	1536	(5.5, 8.8)	(0.027, 0.503)	(0.887, 1.0)
st = Random				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	1856	(5.5, 8.8)	(0.023, 0.503)	(0.877, 1.0)
GG	1618	(5.5, 8.8)	(0.027, 0.503)	(0.887, 1.0)
GPA	2745	(5.5, 8.8)	(0.027, 0.503)	(0.82, 1.0)
5NN	1619	(5.5, 8.8)	(0.027, 0.503)	(0.88, 1.0)
YAO	1597	(5.5, 8.8)	(0.027, 0.503)	(0.883, 1.0)
ER	1557	(5.5, 8.8)	(0.027, 0.503)	(0.883, 1.0)

Table 7.3: Summary of seismic attacks performed over interdependent networks with extra physical links added, and $I_{max} = 3$.

LA category for interdependent networks with $I_{max} = 3$ and extra physical links. Figures for $I_{max} \in \{5, 7, 10\}$ can be found in appendix section E.2. In Figure 7.10 we can see that seismic attacks within the **Damage SA** $>$ **Damage LA** can result in $G_L(LA) - G_L(SA) = 1$, that is, even after adding physical links, there are seismic attacks that completely destroy the logical network by removing a fraction of physical nodes comparable to localized attacks that result in no damage to the logical network. For the case of attacks within the **Damage SA** $<$ **Damage LA** category, we observe that after adding links the lowest $G_L(LA) - G_L(SA)$ values are within the range (-0.6, -0.65). This means that, regardless of the link addition strategy used, after adding physical links the difference between the damage done by a seismic attack in the **Damage SA** $<$ **Damage LA** category and a comparable localized attack is lower than before adding physical links. This happens despite there being more seismic attacks in the **Damage SA** $<$ **Damage LA** category after adding physical links. In appendix section E.2 we can see that for interdependent networks with $I_{max} \in \{5, 7, 10\}$ adding physical links in some cases can result in an increase of the lowest $G_L(LA) - G_L(SA)$ value obtained for seismic attacks in the **Damage SA** $<$ **Damage LA**. This is the case of interdependent networks built using $I_{max} \in \{5, 7\}$ after adding physical links using either Degree or Random strategies. We also observe that after adding physical links using Degree strategy to interdependent networks built using $I_{max} = 10$ the highest $G_L(LA) - G_L(SA)$ value obtained for seismic attacks in the **Damage SA** $>$ **Damage LA** significantly decreases. These results suggest that adding extra physical links using Degree strategies can reduce the differences between the G_L values obtained for seismic attacks and the G_L values obtained for comparable localized attacks.

st = Original							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	52.3%	37.6%	33.9%	34.2%	33.3%	32.4%	37.3%
Damage SA ∼ Damage LA	41.7%	51.4%	50.2%	52.7%	53.2%	52.7%	50.3%
Damage SA < Damage LA	6.0%	11.0%	16.0%	13.1%	13.5%	14.9%	12.4%
st = Distance							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	45.9%	35.5%	34.2%	33.2%	33.1%	32.5%	35.7%
Damage SA ∼ Damage LA	46.3%	52.2%	50.7%	53.1%	53.0%	52.7%	51.3%
Damage SA < Damage LA	7.8%	12.3%	15.1%	13.7%	13.9%	14.9%	12.9%
st = Local hubs							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	40.4%	34.7%	33.3%	32.9%	32.9%	32.2%	34.4%
Damage SA ∼ Damage LA	49.5%	52.7%	51.1%	52.8%	53.1%	53.0%	52.1%
Damage SA < Damage LA	10.1%	12.6%	15.6%	14.2%	14.0%	14.8%	13.5%
st = Degree							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	33.8%	32.8%	33.3%	32.7%	32.5%	32.4%	32.9%
Damage SA ∼ Damage LA	52.7%	52.7%	51.1%	52.7%	53.1%	52.8%	52.5%
Damage SA < Damage LA	13.5%	14.5%	15.6%	14.6%	14.4%	14.8%	14.6%
st = Random							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	36.0%	33.3%	34.0%	33.0%	32.5%	32.1%	33.5%
Damage SA ∼ Damage LA	51.6%	52.7%	50.9%	52.8%	52.8%	53.1%	52.3%
Damage SA < Damage LA	12.4%	14.0%	15.2%	14.2%	14.7%	14.8%	14.2%

Table 7.4: Comparison between localized attacks and seismic attacks for interdependent networks with extra physical links added, and $I_{max} = 3$.



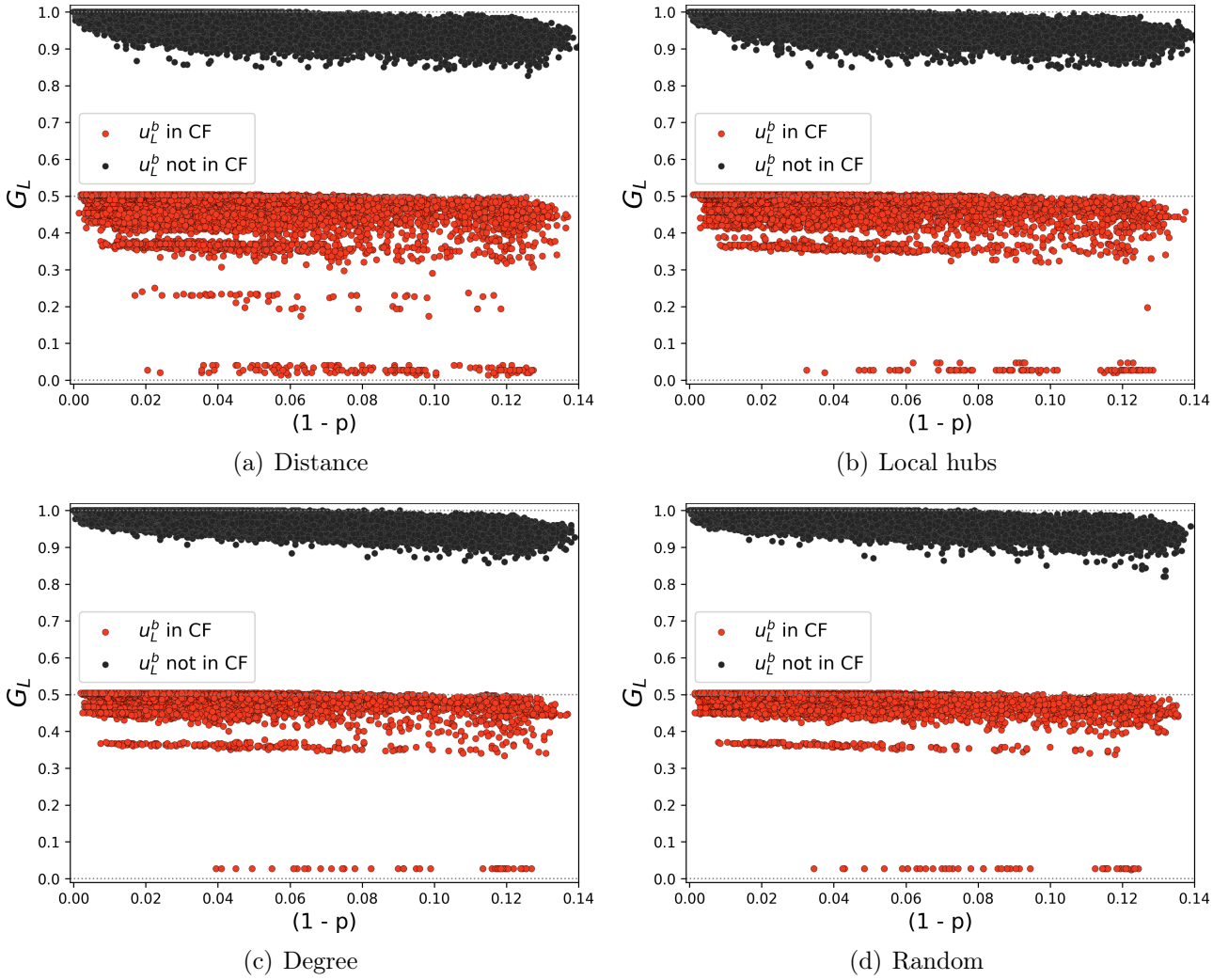
(a) Distance

(b) Local hubs

(c) Degree

(d) Random

Figure 7.7: G_L values obtained after each seismic attack tested for interdependent networks with extra physical links added, and $I_{max} = 3$. Each color represents a different physical model m.



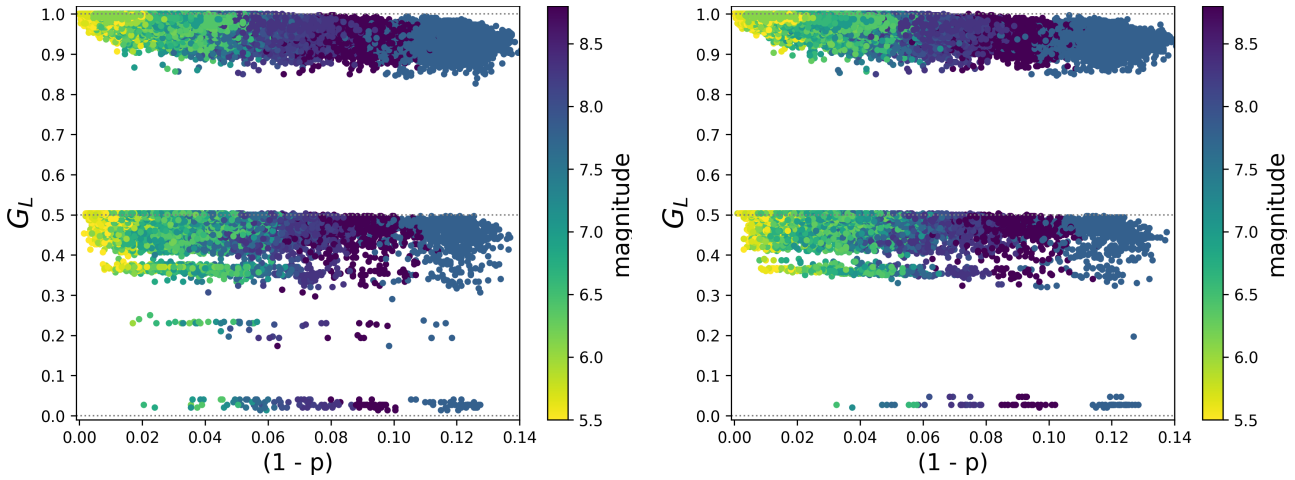
(a) Distance

(b) Local hubs

(c) Degree

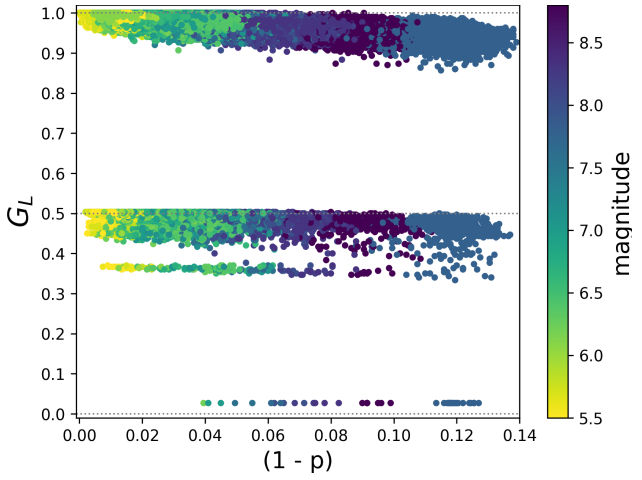
(d) Random

Figure 7.8: Each seismic attack G_L value versus $(1-p)$ for interdependent networks with extra physical links added, and $I_{max} = 3$. Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

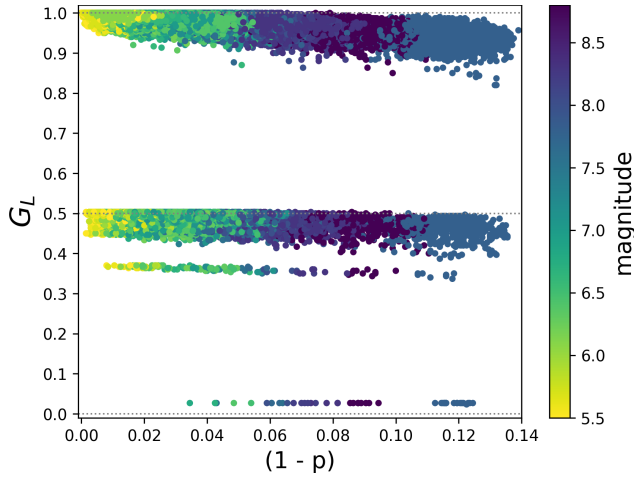


(a) Distance

(b) Local hubs

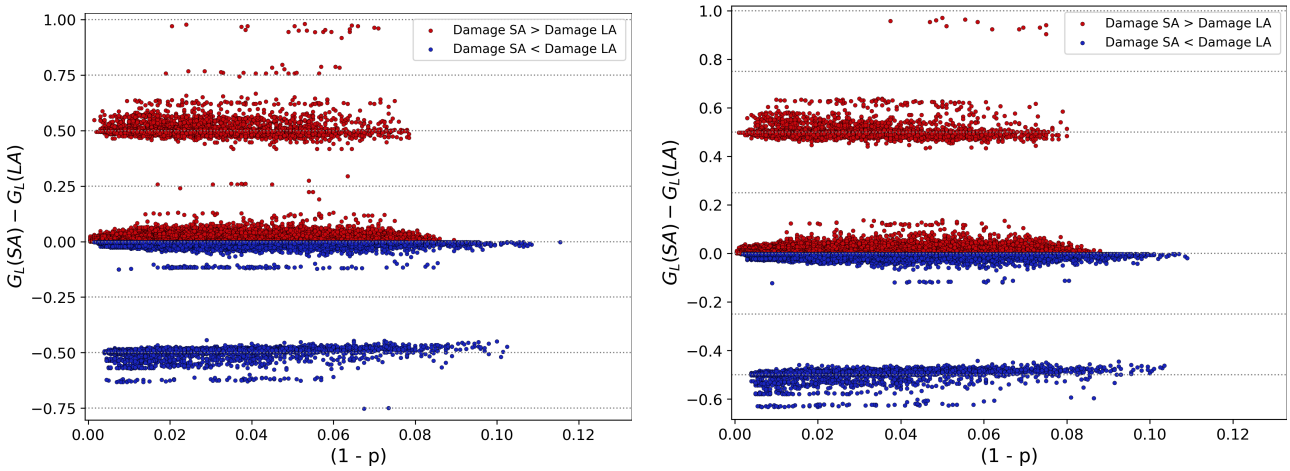


(c) Degree



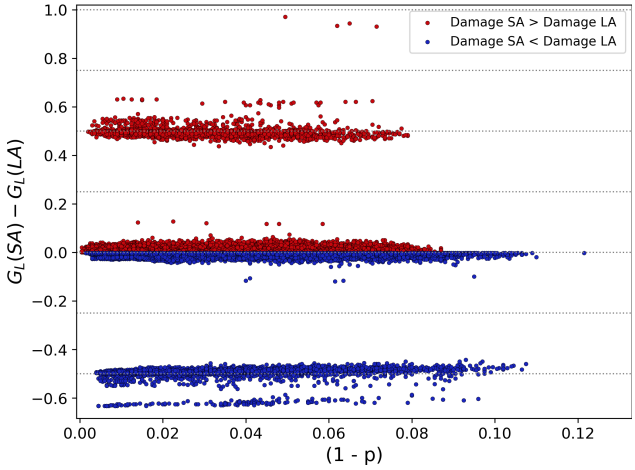
(d) Random

Figure 7.9: Each seismic attack G_L value versus $(1-p)$ for interdependent networks with extra physical links added, and $I_{max} = 3$. Colors show the moment magnitude M_w associated to each seismic attack.

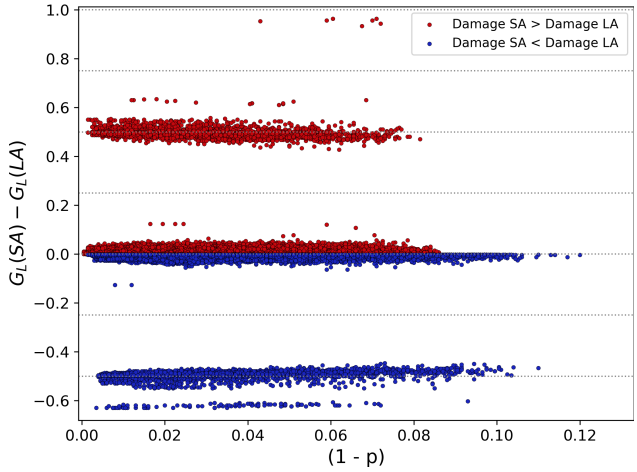


(a) Distance

(b) Local hubs



(c) Degree



(d) Random

Figure 7.10: $G_L(LA) - G_L(SA)$ values obtained for each seismic attack classified within the **Damage SA** $>$ **Damage LA** category or within the **Damage SA** $<$ **Damage LA** category. Interdependent networks have extra physical links added, and were built using $I_{max} = 3$.

7.6 Summary

In this chapter we presented a novel type of attack: Localized Attacks with Probabilistic Failures (LAPF). Here, we showed and tested an application of LAPF by using them to define "seismic attacks" or attacks that simulate the effect of seismic events over the physical network. We used the physical link addition strategies presented in Chapter 5 to test the effect of seismic attacks over the robustness of interdependent networks with and without extra physical links added, and compare it to the effect of localized attacks.

For the experiments we tested the effect of seismic attacks over the robustness of interdependent networks with and without extra physical links added. We define seismic attacks using Ground Motion Prediction Equations (GMPE) specially developed for the case of Chile. Using GMPE and real seismic data, we defined a set of seismic attacks as follows. Given space shape s we generated a set $C(s)$ of 100 localized attack centers. Centers in $C(s)$ were spread uniformly to cover the space s. For each center, a total of 103 different seismic events with different initial conditions were tested. For the experiments we considered interdependent networks with and without extra physical links added. Extra physical links were added to base interdependent networks according to the link addition strategies described in Chapter 5: Random, Distance, Local hubs, and Degree based addition. Here we use base interdependent networks tested in Chapter 5 that were built over a (1:25) space shape. Thus, for the base systems we consider space shape $s = (1{:}25)$, logical network version $q = 1$, $I_{max} \in \{3, 5, 7, 10\}$, model $m \in \{RNG, GG, 5NN, YAO, GPA, ER\}$, plus the 10 different node allocation configurations as described in Chapter 3.

For interdependent networks without extra physical links added, our results show that, similar to localized attacks, seismic attacks can cause High Damage Seismic Attacks (HDSA): seismic attacks that result in the loss of more than half of the logical network. These HDSA were observed in interdependent networks built using $I_{max} \in \{3, 10\}$. Our results show that HDSA occur because the cascading failure caused by the HDSA removes the logical bridge node u_L^b. Removing node u_L^b from the isolated logical network is enough to lose more than 45% of the logical nodes. The results show that for interdependent networks with $I_{max} = 3$ the magnitude of the event is not correlated with the occurrence of HDSA. Whereas for $I_{max} = 10$ HDSA only occur with higher magnitude events. Furthermore, we found that seismic attacks tend to cause a damage level that is similar or higher than the damage caused by comparable localized attacks.

As for interdependent networks with extra physical links added we found that link addition does improve the systems' robustness against seismic attacks. However, no physical link addition strategy is able to fully avoid catastrophic HDSA, that is, HDSA that completely destroy the logical network. As for the relation between the magnitude associated with the

seismic attack, we found that after adding extra links to the physical network the magnitude of the seismic attack is not correlated to the occurrence of HDSA for interdependent networks using $I_{max} = 3$. However, we observe that after adding physical links catastrophic HDSA only occur for seismic events with magnitude 6.5 or higher. For interdependent networks using $I_{max} = 10$ we found that physical link addition does not impact the relation between HDSA and the magnitude of the seismic attack, that is, HDSA still only occur with higher magnitude events. Our findings show that adding extra physical links does decrease the number of seismic attacks that cause more damage than comparable localized attacks. This effect is accompanied by an increase in the number of seismic attacks that cause less damage than comparable localized attacks.

These findings show that using LAPF to model seismic events as seismic attacks results in a distinct behavior that is not fully captured by common localized attacks. Here, we found that seismic attacks can cause more damage than comparable localized attacks, and that robustness against seismic attacks can be improved by adding physical links.

Chapter 8

Conclusions and Future Directions

In this Chapter we present the main conclusions of this thesis. We discuss and assess the hypothesis, and goals presented in Chapter 1. Finally, we outline future research lines that can be derived from this work.

8.1 Conclusions

In this thesis work, we have developed and tested a set of methods based on interdependent networks that allow us to analyze the robustness of a physical-logical interdependent network inspired by today's Internet, with special interest in the robustness against physical failures such as those caused by natural catastrophes.

In Chapter 3 we presented a physical-logical interdependent network model inspired by functionality features present in the logical Internet network, and the physical Internet network. We also presented a robustness measure to assess the system's robustness. Here, we tested the robustness of the proposed model against physical random attacks. In these tests we used a variety of conditions to build the physical-logical interdependent network, such as the maximum number of interlinks per logical node I_{max}, the physical model and space shape used to build the physical network, the logical network, etc. The presented results show that the same interdependent system may undergo a first order phase transition for some random attack iterations, second order phase transition for others, and even mixed phase transitions. Our results show that in most cases, most of these iterations will result in a first order phase transition. Our results also showed that a narrower space shape results in system's with a lower robustness given that the systems use physical models that do depend on physical conditions to be built. This effect was not observed in systems built using physical models

that do not depend on physical conditions. We found that the network model used to build the physical network has an impact over the system's robustness, and that this impact is not necessarily correlated to the number of links in a given physical network. We observed that a higher I_{max} tends to increase the robustness of our interdependent model. However, we also found that we can define set $U_{(q,m,s)}$ that contains I_{max} values u_1 such that a system built using $I_{max} = u_1$ is less robust than a system built using $I_{max} = (u_1 + 1)$. Furthermore, we found that this behavior could be explained by the interplay between the logical network and the interlink set.

In Chapter 4 we studied the interplay between the logical network and the interlink set to further understand the emergence of set $U_{(q,m,s)}$ found in Chapter 3. After analyzing the logical network, we found that these networks may present 'bridge nodes': nodes that connect areas that only contain logical consumer nodes with areas that contain provider nodes. Bridge nodes can be consumer nodes or provider nodes, however we found that most bridge nodes are actually consumer nodes. If a bridge node is removed, several consumer nodes will lose access to any provider node, and thus will fail. We found that, given a physical-logical system, there is an inverse correlation between the damage contribution of a bridge node and the robustness of the system. In particular, we found that bridge nodes that result in higher damage are likely to be hubs within the logical network, although not all bridge nodes are hub nodes. Furthermore, we found that bridge nodes could explain the emergence of set $U_{(q,m,s)}$, and that increasing the number of interlinks of bridge nodes can help us decrease the size of this set. We tested this by adding interlinks to bridge nodes that result in the loss of at least 10% of the logical network after being removed. We found that adding more interlinks to these bridge nodes does decrease the size of set $U_{(q,m,s)}$, and improves the average robustness of the systems. However we also found that adding interlinks only to bridge nodes that result in the loss of at least 10% of the logical network after being removed was not enough to fully avoid the emergence of set $U_{(q,m,s)}$.

With the information gathered in Chapter 4, we continued the testing of the proposed model. In Chapter 5 we tested the effect of adding physical links over the robustness of the proposed physical-logical interdependent network model against physical random attacks. We also analyzed the cost efficiency in terms of robustness improvement of adding physical links. In our experiments we used the length of the links added by a strategy to measure its cost. We defined four physical link addition strategies: Random, Distance, Local hubs, and Degree based addition. Here, we added the same number of physical links for each system and each strategy. Our results showed that in almost every case adding links to the physical network results in an improvement in the system's robustness, the only exception being system's built using Erdös-Rényi networks as physical model. More specifically, we found that Random and Degree strategies improve the system's robustness the most, followed by Local hubs strategy in second place, and Distance strategy in third place. These results

show that the way in which physical links are added is more important than the number of physical links added. We also found that the length of the links added by a strategy has a great impact in the robustness improvement obtained after adding extra physical links. We found that restricting the maximum length of the links added by Random strategy to match maximum length of the links added by Distance strategy results in a sharp decrease in the robustness improvement obtained after adding the extra physical links. Our cost analysis showed consistent results, with higher cost strategies being also strategies that result in a greater robustness improvement. However we must note that higher cost strategies such as Degree and Random are the least cost efficient in terms of robustness improvement, whereas Distance strategy is the most cost efficient. These results suggest that adding more links using Distance strategy may be better in terms of cost than adding fewer physical links using other strategies. To test this we tested two modifications of Distance strategy. Distance+ which adds twice as many physical links as the original strategy, and Distance(B^s) which adds as many physical links as possible given the budget B^s. Here, we found that Distance+ results in a robustness improvement similar to that of Local hubs and has a lower cost than Local hubs. For the case of Distance(B^s) we used a budget B^s for RNG systems that matches the cost of GG systems. We found that despite RNG + Distance(B^s) having the same cost as GG systems, RNG + Distance(B^s) systems are less robust than GG systems. This suggests that to improve RNG systems using Distance strategy we would need a bigger budget.

In Chapter 6, to better represent a natural catastrophe scenario, we tested the robustness of our physical-logical interdependent model against localized attacks. To do this we studied the robustness against localized attacks of each system tested in Chapter 5. Thus, we tested physical-logical systems with and without extra physical links added. Our results showed that on average localized attacks damage the physical-logical systems as much as random attacks do. However, for systems with $I_{max} = 3$, some localized attacks can damage more than half of the logical network, even causing total system failure. We found that these high damage localized attacks happen because during their cascading failure process they remove logic bridge node u_L^b. We must note that node u_L^b is not a provider node, but a consumer node that connects roughly half of logic consumer nodes to any other provider node. We found that adding physical links does decrease the damage caused by high damage localized attacks, and the number of high damage localized attacks. Furthermore, after adding links to the physical network no localized attack caused total system failure ($G_L = 0$). However, high damage localized attacks that affect more than half of the logic network still happen. These results, along with the results obtained in Chapter 4, suggest that in order to further decrease the occurrence of high damage localized attacks we would need to add interlinks to logical node u_L^b such that the physical nodes are sufficiently far apart from each other so as to not be removed by a single localized attack. We must note that another solution is to add links in the logical network to avoid the existence of bridge nodes. However this may be much more difficult than adding interlinks or physical links for systems like the Internet, since

logical links in this case are added through economic agreement between different parties, whereas interlinks and physical links can be added by a single entity.

Finally in Chapter 7 we presented a novel way to test the robustness in physical environments: Localized Attacks with Probabilistic Failures (LAPF). These attacks allow us to model adverse events that affect a physical area, but do not necessarily affect the entire area in the same way. Thus, these attacks can be used to model the effect of natural catastrophes such as tsunamis, earthquakes, tornadoes, etc. Here, we showed an application of LAPF to model seismic events or "seismic attacks". We used these attacks to test the robustness against seismic attacks of each system tested in Chapter 5. Thus, we tested physical-logical systems with and without extra physical links added. We found that seismic attacks can result in high damage seismic attacks that damage more than half of the logic network. Our results show that only a small percentage of the seismic attacks tested result in high damage seismic attacks. We found that, similar to high damage localized attacks from Chapter 6, all high damage seismic attacks remove the logic bridge node u_L^b during the cascading failure process. We also found that compared to localized attacks, in most cases, seismic attacks tend to result in a similar or higher damage level. This tendency was observed even after adding extra physical links. However, adding extra physical links did result in a decrease of the number of seismic attacks that result in a higher damage than comparable localized attacks. Furthermore we found that, similar to the case of localized attacks, adding physical links does improve the robustness of physical-logical systems against seismic attacks, with Degree strategy resulting in the greatest improvement, followed by Random strategy in second place, Local hubs in third place, and Distance in fourth place.

In the present work we have shown a physical-logical interdependent network inspired by the Internet. We have studied its robustness against physical attacks such as physical random attacks, and localized attacks. We have also presented a novel way to model physical adverse events and applied it to model seismic events. Our analysis has shown that when studying the robustness of systems like our proposed model, we must pay especial attention to the presence of "bridge nodes" as we have seen throughout our experiments that bridge nodes are related to events that can damage a great part of the system, even resulting in total system failure. Our results have shown that adding more links to the physical network can be very useful to reduce the impact of bridge nodes. However, these results also show that physical link addition is not enough and that adding more interlinks far apart from each other may be a better solution. Another solution is to add logical links, however this is likely to be much more difficult for the case of the actual Internet network, since logical links are added through economic agreement between different parties.

8.2 Assessment of the thesis' goals

For this thesis we proposed the following hypothesis "It is possible to increase the expressiveness of complex network's models oriented to study the Internet robustness using interdependent networks to model the interactions of the different elements that compose the Internet. Here we consider the expressiveness of such a model is measured by the number of characteristics and/or behaviors of the object being modeled that it captures". In the presented work we have used interdependent networks to create a model inspired by today's Internet. This model specifically considers a logical network inspired by the logical Internet network, and its interactions with a physical network inspired by the physical Internet network. In this model we have considered a consumer-provider approach to capture access to the Internet service for each network. We have integrated this behavior into the functionality conditions. We defined interdependencies considering broad characteristics of the interactions between the physical Internet network and the logical Internet network.

This model has allowed us to identify weak points, that we have called bridge nodes, specific to networks that present a consumer-provider behavior. Our model has also allowed us to represent the fact that it is possible to divide the physical Internet network of a country in two connected components in such a way that each component remains fully functional. Our tests have shown that bridge nodes play an important role in the robustness of the proposed model against physical damage. We have been able to study the effect that damaging the physical network can have over logical bridge nodes, and thus the entire network. Here, we have shown and proposed ways to identify bridge nodes, as well as ways to minimize the damage caused by them.

Existing Internet models proposed by the complex network area have mostly considered single isolated networks or interdependent networks that do not consider multiple Internet layers. Whereas in our model we have considered two interdependent networks, each inspired by the Internet. Thus, we have indeed increased the expressiveness of models oriented to study the Internet robustness using interdependent networks, as we have incorporated more characteristics and/or behaviors presented by the Internet. However, the model we have presented, although inspired by the Internet, still should be further refined to be considered an accurate representation of the Internet network. In the future, we hope to further develop our model, as well as other of the presented tools such as Localized Attacks with Probabilistic failures.

In the following, we review the thesis' goals and assess the level of accomplishment achieved for each item.

(**A**) **Perform a survey of the study of the robustness of interdependent networks:**

A comprehensive survey was performed at the beginning of this thesis work. The main findings were presented in Chapter 2, and the complete survey has been published [10].

(**B**) **Generate an initial model that captures the Internet's behavior considering interactions between the Internet Backbone and the BGP network:** In Chapter 3 we presented a physical-logical interdependent model that represents the interactions between a logical network inspired by the AS-level network, and a physical network inspired by the Internet backbone. We must note that in Chapter 3 we presented the refined initial model.

(**C**) **Establish indexes or measures that capture the robustness of the generated model:** In Chapter 3 we presented our definition of what we consider as a robust Internet, and a way to measure the robustness of the presented model accordingly.

(**D**) **Generate a set of tests that include failures and attacks to the system considered to observe its behavior:** In Chapter 3 we defined an initial set of tests to observe the behavior of our model against physical random attacks.

(**E**) **Perform tests to measure the robustness of the interdependent system and understand the behavior of the system under different adverse scenarios:** In Chapter 3 we performed the initial tests defined. Based on the results obtained, in Chapter 4 we performed a different set of tests to better understand the results obtained in Chapter 3.

(**F**) **Establish and generate a refined version of the initial model that captures more precisely the Internet's behavior:** The model presented in Chapter 3 already contained refinements. However, we must note that further refinements are possible. This will be discussed in section 8.3.

(**G**) **Refine the robustness measurement tests to simulate events that are closer to real world failure scenarios:** In Chapter 5 we refined our tests by testing the model's robustness against physical random attacks after adding extra links to the physical network according to different link addition strategies. In Chapter 6 we further refined our tests by testing the effect of localized attacks over the model's robustness for systems with and without added extra physical links. Finally, in Chapter 7 we proposed Localized Attacks with Probabilistic Failure (LAPF), and used them to further refine our tests by testing a LAPF application: seismic attacks. Here, we considered systems with and without added extra physical links.

(**H**) **Test the refined model using the refined tests:** Each of the test refinements were tested in the Chapters they were presented. That is, in Chapter 5 we performed

experiments to study the effect of adding extra physical links, in Chapter 6 we studied the effect of localized attacks, and in Chapter 7 we studied the effect of seismic attacks.

8.3 Future Work

In this thesis work we have developed and tested a set of methods based on interdependent networks that allow us to analyze the robustness of a physical-logical interdependent network inspired by today's Internet, with special interest in the robustness against physical failures such as those caused by natural catastrophes. Here, we defined a simple way to measure Internet robustness, tested the effect of physical adverse events over the model presented, and proposed a novel type of physical attack. The work we have presented can be further developed to increase the expressiveness of the presented interdependent network model, and improve the testing methods.

During this thesis, the logical network of our model was generated using Scale-Free networks [42]. Here, the logical network is inspired by the AS-level network. However, this approach has been criticized before [37, 67, 115]. A better representation might be achieved using highly organized/optimized tolerances/tradeoffs networks or HOT-Nets [41, 24]. HOT-Nets allow to incorporate the optimized aspects that engineered networks, such as the BGP network, present. Flexible models such as those based on HOT-Nets could allow to test the effect of changing budgets, economic incentives, restrictions, and objective functions over the logical Internet network. Furthermore, the logical network representation can be modified to incorporate the relationships found between nodes in the BGP network: Peer-to-peer (p2p), and customer-to-provider (c2p) [73].

Another interesting thing to study is the existence of bridge nodes in the actual AS-level network. In this work we found bridge nodes in our logical network. We observed that, in some cases, removing these nodes during the cascading failure process can greatly damage the physical-logical interdependent network. In our experiments we found that in most cases logical bridge nodes are not provider nodes. However, given the business relationships that influence the link structure in the actual AS-level network, bridge nodes are likely to be ISP nodes or "provider nodes". Furthermore, it is yet to be tested whether the actual AS-level network has bridge nodes or not.

For the case of the physical network, it would be interesting to incorporate physical allocations for the physical links, such that the concept of Shared Risk Link Groups (SRLG) can be considered within the physical-logical interdependent networks model. By considering physical allocations for the links, we would be able to represent the case in which there is more than one bundle connecting two points, and those bundles do not share risk. Furthermore, by incorporating SRLGs, we could represent the dependencies between logical links and

physical links, and incorporate backup routes in the logical network.

Another interesting thing to incorporate to the physical network would be Internet exchange points (IXPs). Exchange points allow Internet Service Providers (ISPs) to exchange data destined for their respective networks. They do this by operating physical infrastructure to connect different ISPs, and thus play a major role in the proper functioning of provider nodes as described in the model we have proposed.

It would also be interesting to test the effect that interlink configuration might have over the system robustness. In this thesis we focused on adding interlinks uniformly at random. Here, we defined a maximum number of interlinks per logical node I_{max}. Logical consumer nodes can have between 1 and I_{max} interlinks, whereas logical provider nodes have exactly I_{max} interlinks. However, we could refine the interlink allocation to follow different probability distributions, or to be allocated in function of characteristics of the logical network. As we have shown in this work, changing the interlink set can greatly impact the effect that existing bridge nodes might have over the robustness of physical-logical systems.

Another research venue is that of the effect of adding links to the physical network following some strategy. The strategies we have presented here were selected to be simple enough to remain useful even in scenarios where the information regarding the physical network structure is incomplete or not accurate enough to use more complex strategies. However, more complex strategies may prove to be better in terms of cost efficiency and robustness improvement. An interesting way to add physical links would be by using community detection algorithms as they have been shown to be useful in single isolated networks [109]. We must note that given the lack of granularity consistency usually found in PoP data (physical network data) [116], in order to use community detection we would need to first define and develop a way to ensure that the communities obtained have a real meaning.

As for Localized Attacks with Probabilistic Failures (LAPF), there are several other applications to be tested. These attacks can be adapted to affect areas of various shapes and sizes. Thus, LAPF could be used to model the damage caused by other natural catastrophes such as landslides, floods, volcanic eruptions, tornadoes, tsunamis, etc. Furthermore, the seismic attacks we have presented here can be improved by including more complete, and more accurate information regarding soil characteristics, and damage caused by seismic events.

Finally, it would be interesting to incorporate other robustness measures. In this work we have used a simple robustness measure as we were interested in pure node functionality. However, there are many other measurements [93] that can be used to further understand

and improve the interdependent networks' robustness. Using other measures may help us develop better physical links additions strategies by incorporating information that we may have not considered in this work.

Chapter 9

Bibliography

[1] Autonomous system. https://tools.ietf.org/html/rfc1930. Accessed: August 2^{nd} 2021.

[2] Border gateway protocol. https://tools.ietf.org/html/rfc4271. Accessed: August 2^{nd} 2021.

[3] Border gateway protocol. https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/. Accessed: October 6^{th} 2021.

[4] Charles O Adler and Cihan H Dagli. Study of the use of a genetic algorithm to improve networked system-of-systems resilience. *Procedia Computer Science*, 36:49–56, 2014.

[5] Abdulaziz Alashaikh, Teresa Gomes, and David Tipper. The spine concept for improving network availability. *Computer Networks*, 82:4–19, 2015.

[6] Number of autonomous system. https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html, Accessed: October 5^{th} 2021.

[7] Dominic Assimaki, Christian Ledezma, Gonzalo A Montalva, Andres Tassara, George Mylonakis, and Ruben Boroschek. Site effects and damage patterns. *Earthquake Spectra*, 28(1_suppl1):55–74, 2012.

[8] Ivana Bachmann and Javier Bustos-Jiménez. Improving the chilean internet robustness: Increase the interdependencies or change the shape of the country? In *International Conference on Complex Networks and their Applications*, pages 646–657. Springer, 2017.

[9] Ivana Bachmann and Javier Bustos-Jiménez. Using localized attacks with probabilistic failures to model seismic events over physical-logical interdependent networks. In *International Conference on Network Science*, pages 1–14. Springer, 2022.

[10] Ivana Bachmann, Javier Bustos-Jiménez, and Benjamin Bustos. A survey on frameworks used for robustness analysis on interdependent networks. *Complexity*, 2020, 2020.

[11] Ivana Bachmann and Felipe Espinoza. Modelling the interactions between the internet backbone and the bgp network. 2018.

[12] Ivana Bachmann, Francisco Sanhueza, and Javier Bustos-Jiménez. Space geometry effect over the internet as a physical-logical interdependent network. In *International Conference on Network Science*, pages 213–227. Springer, 2020.

[13] Ivana Bachmann, Valeria Valdés, Javier Bustos-Jiménez, and Benjamin Bustos. Effect of adding physical links on the robustness of the internet modeled as a physical-logical interdependent network using simple strategies. *International Journal of Critical Infrastructure Protection*, page 100483, 2021.

[14] Albert-László Barabási and Réka Albert. Emergence of scaling in random networks. *science*, 286(5439):509–512, 1999.

[15] Albert-László Barabási and Eric Bonabeau. Scale-free networks. *Scientific american*, 288(5):60–69, 2003.

[16] Amir Bashan, Yehiel Berezin, Sergey V Buldyrev, and Shlomo Havlin. The extreme vulnerability of interdependent spatially embedded networks. *Nature Physics*, 9(10):667–672, 2013.

[17] Yehiel Berezin, Amir Bashan, Michael M Danziger, Daqing Li, and Shlomo Havlin. Localized attacks on spatially embedded networks with dependencies. *Scientific reports*, 5, 2015.

[18] Ginestra Bianconi. *Multilayer Networks: Structure and Function*. Oxford university press, 2018.

[19] Daniel K Blandford, Guy E Blelloch, and Ian A Kash. Compact representations of separable graphs. 2003.

[20] Prosenjit Bose, Pat Morin, Ivan Stojmenović, and Jorge Urrutia. Routing with guaranteed delivery in ad hoc wireless networks. *Wireless networks*, 7(6):609–616, 2001.

[21] Sergey V Buldyrev, Roni Parshani, Gerald Paul, H Eugene Stanley, and Shlomo Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025–1028, 2010.

[22] Ye Cai, Yong Li, Yijia Cao, Wenguo Li, and Xiangjun Zeng. Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids. *International Journal of Electrical Power & Energy Systems*, 89:106–114, 2017.

[23] Alessio Cardillo, Salvatore Scellato, Vito Latora, and Sergio Porta. Structural properties of planar graphs of urban street patterns. *Physical Review E*, 73(6):066107, 2006.

[24] Jean M Carlson and John Doyle. Complexity and robustness. *Proceedings of the national academy of sciences*, 99(suppl 1):2538–2545, 2002.

[25] Wei Koong Chai, Vaios Kyritsis, K Katsaros, and George Pavlou. Resilience of interdependent communication and power distribution networks against cascading failures. *15th IFIP Networking, Vienna, Austria*, 2016.

[26] Srinjoy Chattopadhyay and Huaiyu Dai. Towards optimal link patterns for robustness of interdependent networks against cascading failures. In *2015 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2015.

[27] Zhenhao Chen, Jiajing Wu, Yongxiang Xia, and Xi Zhang. Robustness of interdependent power grids and communication networks: A complex network perspective. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 65(1):115–119, 2017.

[28] Zunshui Cheng and Jinde Cao. Cascade of failures in interdependent networks coupled by different type networks. *Physica A: Statistical Mechanics and its Applications*, 430:193–200, 2015.

[29] James H Cowie, Andy T Ogielski, B Premore, Eric A Smith, and Todd Underwood. Impact of the 2003 blackouts on internet communications. *Preliminary Report, Renesys Corporation (updated March 1, 2004)*, 2003.

[30] CB Crouse. Ground-motion attenuation equations for earthquakes on the cascadia subduction zone. *Earthquake spectra*, 7(2):201–236, 1991.

[31] Michael M Danziger, Amir Bashan, Yehiel Berezin, and Shlomo Havlin. Interdependent spatially embedded networks: dynamics at percolation threshold. In *Signal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference*

on, pages 619–625. IEEE, 2013.

[32] Jian-Xun Ding, Rui-Ke Qin, Ning Guo, and Jian-Cheng Long. Urban road network growth model based on rng proximity graph and angle restriction. *Nonlinear Dynamics*, 96(4):2281–2292, 2019.

[33] Rui Ding, Norsidah Ujang, Hussain bin Hamid, Mohd Shahrudin Abd Manan, Rong Li, and Jianjun Wu. Heuristic urban transportation network design method, a multilayer coevolution approach. *Physica A: Statistical Mechanics and its Applications*, 479:71–83, 2017.

[34] Snoop Dogg. Hollywood walk of fame speech, October 2018.

[35] Gaogao Dong, Lixin Tian, Ruijin Du, Min Fu, and H Eugene Stanley. Analysis of percolation behaviors of clustered networks with partial support–dependence relations. *Physica A: Statistical Mechanics and its Applications*, 394:370–378, 2014.

[36] Shangjia Dong, Haizhong Wang, Ali Mostafavi, and Jianxi Gao. Robust component: a robustness measure that incorporates access to critical facilities under disruptions. *Journal of the Royal Society Interface*, 16(157):20190149, 2019.

[37] John C Doyle, David L Alderson, Lun Li, Steven Low, Matthew Roughan, Stanislav Shalunov, Reiko Tanaka, and Walter Willinger. The "robust yet fragile" nature of the internet. *Proceedings of the National Academy of Sciences*, 102(41):14497–14502, 2005.

[38] Ruijin Du, Gaogao Dong, Lixin Tian, and Runran Liu. Targeted attack on networks coupled by connectivity and dependency links. *Physica A: Statistical Mechanics and its Applications*, 450:687–699, 2016.

[39] David Eppstein, Michael S Paterson, and F Frances Yao. On nearest-neighbor graphs. *Discrete & Computational Geometry*, 17(3):263–282, 1997.

[40] Paul Erdös and Alfréd Rényi. On the evolution of random graphs. *Publ. Math. Inst. Hung. Acad. Sci*, 5(1):17–60, 1960.

[41] Alex Fabrikant, Elias Koutsoupias, and Christos H Papadimitriou. Heuristically optimized trade-offs: A new paradigm for power laws in the internet. In *International Colloquium on Automata, Languages, and Programming*, pages 110–122. Springer, 2002.

[42] Michalis Faloutsos, Petros Faloutsos, and Christos Faloutsos. On power-law relationships of the internet topology. In *ACM SIGCOMM computer communication review*, volume 29, pages 251–262. ACM, 1999.

[43] Abraham D Flaxman, Alan M Frieze, and Juan Vera. A geometric preferential attachment model of networks. *Internet Mathematics*, 3(2):187–205, 2006.

[44] K Ruben Gabriel and Robert R Sokal. A new statistical approach to geographic variation analysis. *Systematic Zoology*, 18(3):259–278, 1969.

[45] Jianxi Gao, Sergey V Buldyrev, Shlomo Havlin, and H Eugene Stanley. Robustness of a network formed by n interdependent networks with a one-to-one correspondence of dependent nodes. *Physical Review E*, 85(6):066134, 2012.

[46] Jianxi Gao, Sergey V Buldyrev, H Eugene Stanley, Xiaoming Xu, and Shlomo Havlin. Percolation of a general network of networks. *Physical Review E*, 88(6):062816, 2013.

[47] Lixin Gao. On inferring autonomous system relationships in the internet. *IEEE/ACM Transactions on networking*, 9(6):733–745, 2001.

[48] Edgar N Gilbert. Random graphs. *The Annals of Mathematical Statistics*, 30(4):1141–1144, 1959.

[49] Yuqi Han, Zhi Li, Chuangxin Guo, and Yuezhong Tang. Improved percolation theory incorporating power flow analysis to model cascading failures in cyber-physical power system. In *Power and Energy Society General Meeting (PESGM), 2016*, pages 1–5. IEEE, 2016.

[50] Yanqing Hu, Dong Zhou, Rui Zhang, Zhangang Han, Céline Rozenblat, and Shlomo Havlin. Percolation of interdependent networks with intersimilarity. *Physical Review E*, 88(5):052805, 2013.

[51] Xuqing Huang, Jianxi Gao, Sergey V Buldyrev, Shlomo Havlin, and H Eugene Stanley. Robustness of interdependent networks under targeted attack. *Physical Review E*, 83(6):065101, 2011.

[52] Zhen Huang, Cheng Wang, Amiya Nayak, and Ivan Stojmenovic. Small cluster in cyber physical systems: Network topology, interdependence and cascading failures. *IEEE Transactions on Parallel and Distributed Systems*, 26(8):2340–2351, 2014.

[53] Zhen Huang, Cheng Wang, Tieying Zhu, and Amiya Nayak. Cascading failures in smart grid: Joint effect of load propagation and interdependence. *Access, IEEE*, 3:2520–2530, 2015.

[54] Benjamín Idini, Fabián Rojas, Sergio Ruiz, and César Pastén. Ground motion prediction equations for the chilean subduction zone. *Bulletin of Earthquake Engineering*,

15(5):1853–1880, 2017.

[55] Xingpei Ji, Bo Wang, Dichen Liu, Guo Chen, Fei Tang, Daqian Wei, and Lian Tu. Improving interdependent networks robustness by adding connectivity links. *Physica A: Statistical Mechanics and its Applications*, 444:9–19, 2016.

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

[57] Japanese meteorological agency seismic intensity scale calculation method. https://www.data.jma.go.jp/svd/eqev/data/kyoshin/kaisetsu/calc_sindo.htm#gosei, Accessed on November 15^{th}, 2021.

[58] Brad Karp and Hsiang-Tsung Kung. Gpsr: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254, 2000.

[59] Yui Kazawa and Sho Tsugawa. On the effectiveness of link addition for improving robustness of multiplex networks against layer node-based attack. In *Computer Software and Applications Conference (COMPSAC), 2017 IEEE 41st Annual*, volume 1, pages 697–700. IEEE, 2017.

[60] Barbara Kitchenham. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26, 2004.

[61] Mert Korkali, Jason G Veneman, Brian F Tivnan, James P Bagrow, and Paul DH Hines. Reducing cascading failure risk by increasing infrastructure network interdependence. *Scientific reports*, 7:44499, 2017.

[62] Bhushan Kotnis and Joy Kuri. Percolation on networks with antagonistic and dependent interactions. *Physical Review E*, 91(3):032805, 2015.

[63] Philip M Lankford. Regionalization: theory and alternative algorithms. *Geographical Analysis*, 1(2):196–212, 1969.

[64] Vito Latora, Vincenzo Nicosia, and Giovanni Russo. *Complex networks: principles, methods and applications*. Cambridge University Press, 2017.

[65] Deokjae Lee, S Choi, M Stippinger, J Kertész, and B Kahng. Hybrid phase transition into an absorbing state: Percolation and avalanches. *Physical Review E*, 93(4):042109, 2016.

[66] F Leyton, C Pastén, S Ruiz, B Idini, and F Rojas. Empirical site classification of csn network using strong-motion records. *Seismological Research Letters*, 89(2A):512–518, 2018.

[67] Lun Li, David Alderson, John C Doyle, and Walter Willinger. Towards a theory of scale-free graphs: Definition, properties, and implications. *Internet Mathematics*, 2(4):431–523, 2005.

[68] Wei Li, Amir Bashan, Sergey V Buldyrev, H Eugene Stanley, and Shlomo Havlin. Cascading failures in interdependent lattice networks: The critical role of the length of dependency links. *Physical review letters*, 108(22):228702, 2012.

[69] Xiang-Yang Li, Peng-Jun Wan, and Yu Wang. Power efficient and sparse spanner for wireless ad hoc networks. In *Proceedings Tenth International Conference on Computer Communications and Networks (Cat. No. 01EX495)*, pages 564–567. IEEE, 2001.

[70] Xin Li, Haotian Wu, Caterina Scoglio, and Don Gruenbacher. Robust allocation of weighted dependency links in cyber–physical networks. *Physica A: Statistical Mechanics and its Applications*, 433:316–327, 2015.

[71] Dong Liu, Xi Zhang, and K Tse Chi. A stochastic model for cascading failures in smart grid under cyber attack. In *Future Energy Electronics Conference and ECCE Asia (IFEEC 2017-ECCE Asia), 2017 IEEE 3rd International*, pages 783–788. IEEE, 2017.

[72] Steven Lowinger, Gabriel A Cwilich, and Sergey V Buldyrev. Interdependent lattice networks in high dimensions. *Physical Review E*, 94(5):052306, 2016.

[73] Matthew Luckie, Bradley Huffaker, Amogh Dhamdhere, Vasileios Giotsas, and KC Claffy. As relationships, customer cones, and validation. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 243–256, 2013.

[74] Luke Mathieson and Pablo Moscato. An introduction to proximity graphs. In *Business and Consumer Analytics: New Ideas*, pages 213–233. Springer, 2019.

[75] Yuki Matsui, Hideharu Kojima, and Tatsuhiro Tsuchiya. Modeling the interaction of power line and scada networks. In *2014 IEEE 15th International Symposium on High-Assurance Systems Engineering*, pages 261–262. IEEE, 2014.

[76] David W Matula and Robert R Sokal. Properties of gabriel graphs relevant to geographic variation research and the clustering of points in the plane. *Geographical*

analysis, 12(3):205–222, 1980.

[77] Saburoh Midorikawa. Semi-empirical estimation of peak ground acceleration from large earthquakes. *Tectonophysics*, 218(1-3):287–295, 1993.

[78] Fernando G Morales, Marcia HM Paiva, and Javier A Bustos-Jiménez. Measuring and improving network robustness: A chilean case study. *IEEE Communications Letters*, 23(1):44–47, 2018.

[79] Sebastian Neumayer, Gil Zussman, Reuven Cohen, and Eytan Modiano. Assessing the vulnerability of the fiber infrastructure to disasters. *IEEE/ACM Transactions on Networking*, 19(6):1610–1623, 2011.

[80] Duy T Nguyen, Yilin Shen, and My T Thai. Detecting critical nodes in interdependent power networks for vulnerability assessment. *Smart Grid, IEEE Transactions on*, 4(1):151–159, 2013.

[81] TM Ouboter, DTH Worm, RE Kooij, and Huijuan Wang. Design of robust dependent networks against flow-based cascading failures. In *Reliable Networks Design and Modeling (RNDM), 2014 6th International Workshop on*, pages 54–60. IEEE, 2014.

[82] Nagendra K Panduranga, Jianxi Gao, Xin Yuan, H Eugene Stanley, and Shlomo Havlin. Generalized model for k-core percolation and interdependent networks. *Physical Review E*, 96(3):032317, 2017.

[83] Marzieh Parandehgheibi and Eytan Modiano. Robustness of interdependent networks: The case of communication networks and the power grid. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 2164–2169. IEEE, 2013.

[84] Roni Parshani, Sergey V Buldyrev, and Shlomo Havlin. Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition. *Physical review letters*, 105(4):048701, 2010.

[85] Yuzhuo Qiu. The effect of clustering-based and degree-based weighting on robustness in symmetrically coupled heterogeneous interdependent networks. In *2013 IEEE International Conference on Systems, Man, and Cybernetics*, pages 3984–3988. IEEE, 2013.

[86] Yuzhuo Qiu. Optimal weighting scheme and the role of coupling strength against load failures in degree-based weighted interdependent networks. *Physica A: Statistical Mechanics and its Applications*, 392(8):1920–1924, 2013.

[87] Filippo Radicchi. Percolation in real interdependent networks. *Nature Physics*, 11(7):597–602, 2015.

[88] V Ramiro, J Piquer, T Barros, and P Sepúlveda. The chilean internet: Did it survive the earthquake? *WIT Transactions on State-of-the-art in Science and Engineering*, 58, 2012.

[89] Rodrigo Rauld, Francisco Medina, Felipe Leyton, and Sergio Ruiz. Mapa de microzonificación sismo-geológica para chile. In *Congreso Geológico Chileno*, pages 106–109, 2015.

[90] Saulo DS Reis, Yanqing Hu, Andrés Babino, José S Andrade Jr, Santiago Canals, Mariano Sigman, and Hernán A Makse. Avoiding catastrophic failure in correlated networks of networks. *Nature Physics*, 10(10):762–767, 2014.

[91] Vittorio Rosato, L Issacharoff, F Tiriticco, Sandro Meloni, S Porcellinis, and Roberto Setola. Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures*, 4(1-2):63–79, 2008.

[92] Diego F Rueda, Eusebi Calle, Xiangrong Wang, and Robert E Kooij. Enhanced interconnection model in geographically interdependent networks. *INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL*, 13(4):537–549, 2018.

[93] SE Schaeffer, V Valdés, J Figols, I Bachmann, F Morales, and J Bustos-Jiménez. Characterization of robustness and resilience in graphs: a mini-review. *Journal of Complex Networks*, 9(2):cnab018, 2021.

[94] Christian M Schneider, André A Moreira, José S Andrade, Shlomo Havlin, and Hans J Herrmann. Mitigation of malicious attacks on networks. *Proceedings of the National Academy of Sciences*, 108(10):3838–3841, 2011.

[95] Christian M Schneider, Nuri Yazdani, Nuno AM Araújo, Shlomo Havlin, and Hans J Herrmann. Towards designing robust coupled networks. *Scientific reports*, 3, 2013.

[96] Yilun Shang. Attack robustness and stability of generalized k-cores. *New Journal of Physics*, 21(9):093013, 2019.

[97] Yilun Shang. Subgraph robustness of complex networks under attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(4):821–832, 2019.

[98] Yilun Shang. Generalized k-core percolation in networks with community structure.

SIAM Journal on Applied Mathematics, 80(3):1272–1289, 2020.

[99] Jia Shao, Sergey V Buldyrev, Shlomo Havlin, and H Eugene Stanley. Cascade of failures in coupled network systems with multiple support-dependence relations. *Physical Review E*, 83(3):036116, 2011.

[100] Shuai Shao, Xuqing Huang, H Eugene Stanley, and Shlomo Havlin. Robustness of a partially interdependent network formed of clustered networks. *Physical Review E*, 89(3):032812, 2014.

[101] Shuai Shao, Xuqing Huang, H Eugene Stanley, and Shlomo Havlin. Percolation of localized attack on complex networks. *New Journal of Physics*, 17(2):023049, 2015.

[102] Dietrich Stauffer and Ammon Aharony. *Introduction to percolation theory*. CRC press, 1994.

[103] Fei Tan, Yongxiang Xia, and Zhi Wei. Robust-yet-fragile nature of interdependent networks. *Physical Review E*, 91(5):052809, 2015.

[104] Liang Tang, Ke Jing, Jie He, and H Eugene Stanley. Complex interdependent supply chain networks: Cascading failure and robustness. *Physica A: Statistical Mechanics and its Applications*, 443:58–69, 2016.

[105] David Tipper. Resilient network design: challenges and future directions. *Telecommunication Systems*, 56(1):5–16, 2014.

[106] Godfried T Toussaint. The relative neighbourhood graph of a finite planar set. *Pattern recognition*, 12(4):261–268, 1980.

[107] Adam Tyra, Jingtao Li, Yilun Shang, Shuo Jiang, Yanjun Zhao, and Shouhuai Xu. Robustness of non-interdependent and interdependent networks against dependent and adaptive attacks. *Physica A: Statistical Mechanics and its Applications*, 482:713–727, 2017.

[108] KS Vipin, P Anbazhagan, and TG Sitharam. Estimation of peak ground acceleration and spectral acceleration for south india with local site effects: probabilistic approach. *Natural Hazards and Earth System Sciences*, 9(3):865–878, 2009.

[109] Sebastian Wandelt, Xing Shi, and Xiaoqian Sun. Estimation and improvement of transportation network robustness by exploiting communities. *Reliability Engineering & System Safety*, 206:107307, 2021.

[110] Jianwei Wang, Yun Li, and Qiaofang Zheng. Cascading load model in interdependent networks with coupled strength. *Physica A: Statistical Mechanics and its Applications*, 430:242–253, 2015.

[111] Xiangrong Wang, Robert E Kooij, and Piet Van Mieghem. Modeling region-based interconnection for interdependent networks. *Physical Review E*, 94(4):042315, 2016.

[112] Xingyuan Wang, Jianye Cao, Rui Li, and Tianfang Zhao. A preferential attachment strategy for connectivity link addition strategy in improving the robustness of interdependent networks. *Physica A: Statistical Mechanics and its Applications*, 483:412–422, 2017.

[113] Yu Wang. Topology control for wireless sensor networks. In *Wireless sensor networks and applications*, pages 113–147. Springer, 2008.

[114] Shunsuke Watanabe and Yoshiyuki Kabashima. Cavity-based robustness analysis of interdependent networks: Influences of intranetwork and internetwork degree-degree correlations. *Physical Review E*, 89(1):012808, 2014.

[115] Walter Willinger, David Alderson, and John C Doyle. Mathematics and the internet: A source of enormous confusion and great potential. *Notices of the American Mathematical Society*, 56(5):586–599, 2009.

[116] Walter Willinger and Matthew Roughan. Internet topology research redux. *ACM SIGCOMM eBook: Recent Advances in Networking*, 2013.

[117] A. C. C. Yao. On constructing minimum spanning trees in k-dimensional spaces and related problems. *SIAM Journal on Computing*, 11(4):721–736, 1982.

[118] Xin Yuan, Yang Dai, H Eugene Stanley, and Shlomo Havlin. k-core percolation on complex networks: Comparing random, localized, and targeted attacks. *Physical Review E*, 93(6):062302, 2016.

[119] Xin Yuan, Shuai Shao, H Eugene Stanley, and Shlomo Havlin. How breadth of degree distribution influences network robustness: Comparing localized and random attacks. *Physical Review E*, 92(3):032122, 2015.

[120] Hang Zhang, Jie Zhou, Yong Zou, Ming Tang, Gaoxi Xiao, and H Eugene Stanley. Asymmetric interdependent networks with multiple-dependence relation. *Physical Review E*, 101(2):022314, 2020.

[121] Xian Zhang, Chris Phillips, and Xiuzhong Chen. An overlay mapping model for achiev-

ing enhanced qos and resilience performance. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on*, pages 1–7. IEEE, 2011.

[122] Da-wei Zhao, Lian-hai Wang, Yong-feng Zhi, Jun Zhang, and Zhen Wang. The robustness of multiplex networks under layer node-based attack. *Scientific reports*, 6, 2016.

[123] Fangxia Zhao, Jianjun Wu, Huijun Sun, Ziyou Gao, and Ronghui Liu. Population-driven urban road evolution dynamic model. *Networks and Spatial Economics*, 16(4):997–1018, 2016.

[124] Zhuang Zhao, Peng Zhang, and Hujiang Yang. Cascading failures in interconnected networks with dynamical redistribution of loads. *Physica A: Statistical Mechanics and its Applications*, 433:204–210, 2015.

[125] Di Zhou, Jianxi Gao, H Eugene Stanley, and Shlomo Havlin. Percolation of partially interdependent scale-free networks. *Physical Review E*, 87(5):052812, 2013.

[126] Di Zhou, H Eugene Stanley, Gregorio D'Agostino, and Antonio Scala. Assortativity decreases the robustness of interdependent networks. *Physical Review E*, 86(6):066103, 2012.

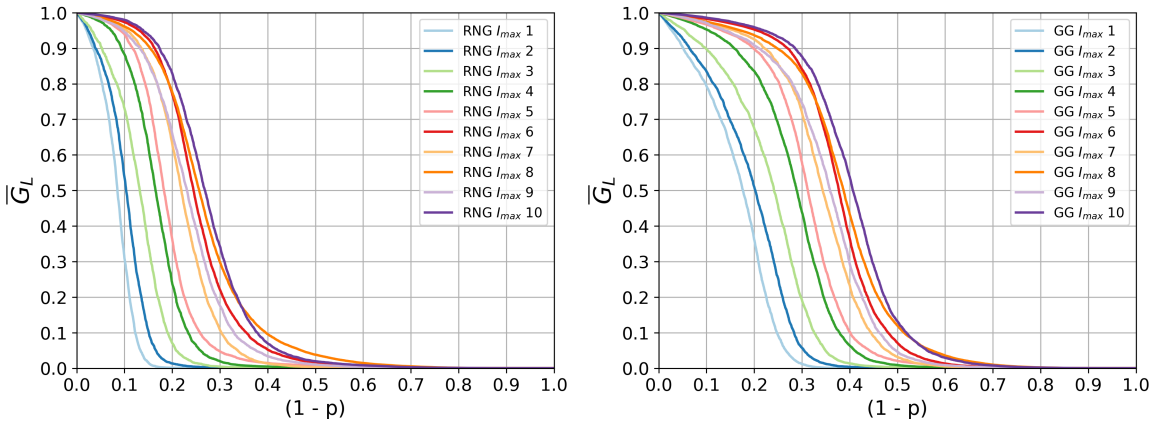
[127] Dong Zhou, Amir Bashan, Reuven Cohen, Yehiel Berezin, Nadav Shnerb, and Shlomo Havlin. Simultaneous first-and second-order percolation transitions in interdependent networks. *Physical Review E*, 90(1):012803, 2014.

[128] Dong Zhou and Ahmed Elmokashfi. Overload-based cascades on multiplex networks and effects of inter-similarity. *PloS one*, 12(12):e0189624, 2017.

Annexed A

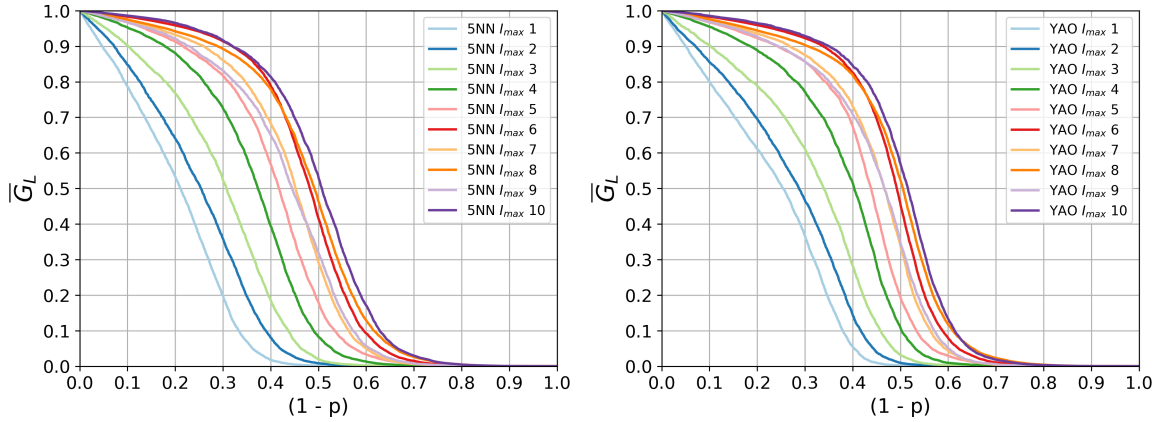
Chapter 3: Initial interdependent model and testing

A.1 General robustness behavior figures



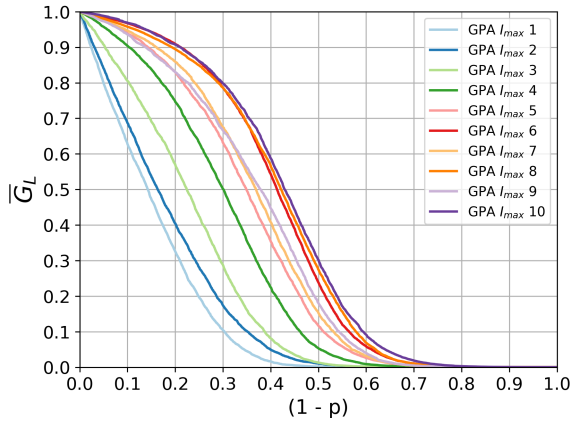
(a) RNG (b) GG

Figure A.1: Average robustness by model for systems built over a (1:25) space, logical network version $q = 1$, and $m \in \{\text{RNG, GG}\}$.

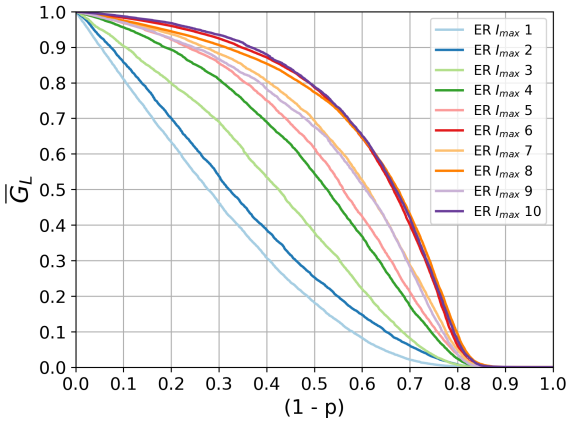


(a) 5NN

(b) YAO

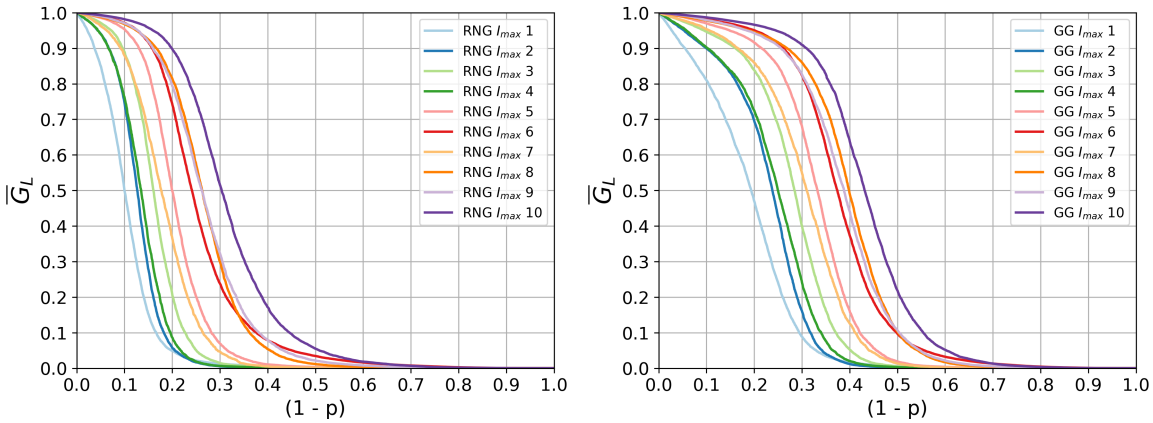


(c) GPA



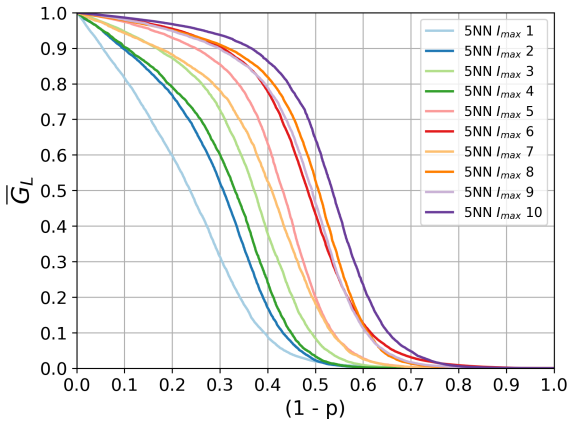
(d) ER

Figure A.2: Average robustness by model for systems built over a (1:25) space, logical network version $q = 1$, and $m \in \{5\text{NN,YAO,GPA,ER}\}$.

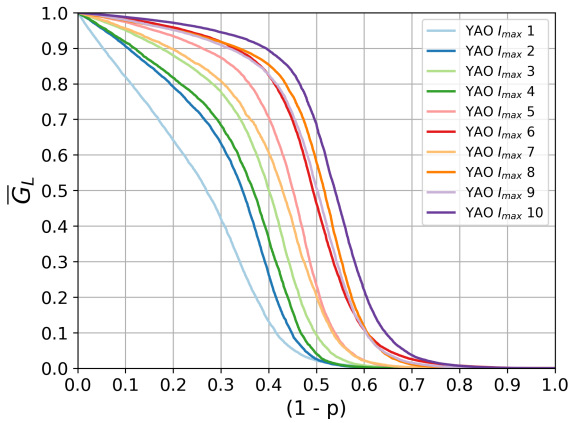


(a) RNG

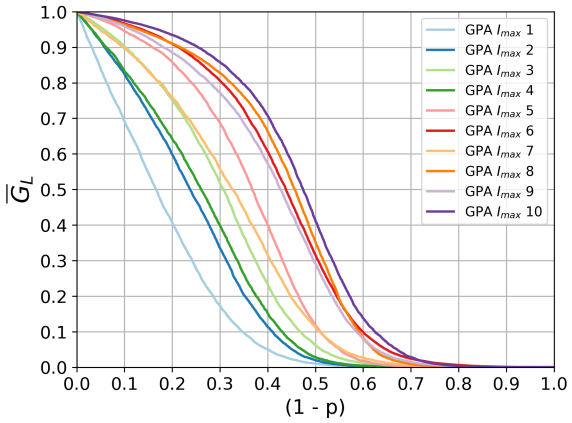
(b) GG



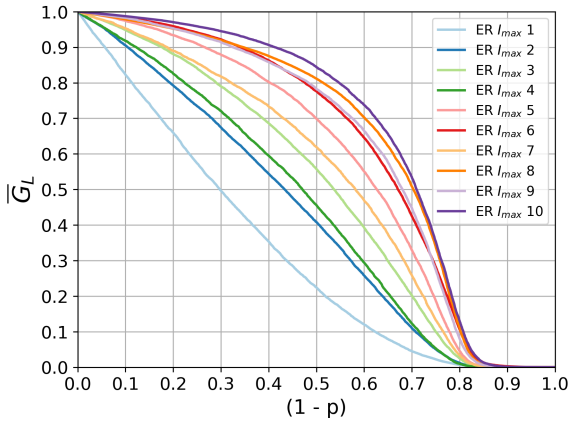
(c) 5NN



(d) YAO

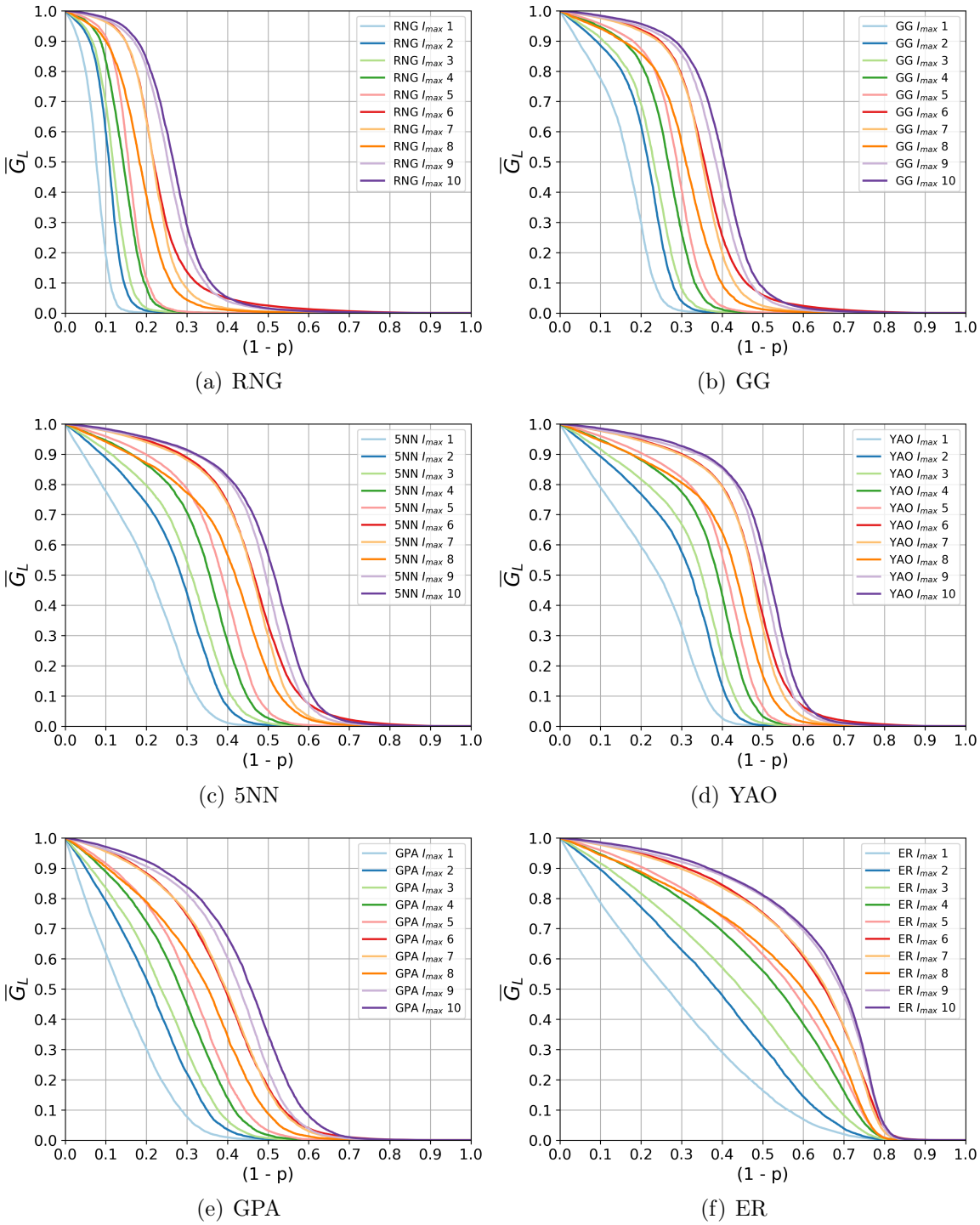


(e) GPA



(f) ER

Figure A.3: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 2$.

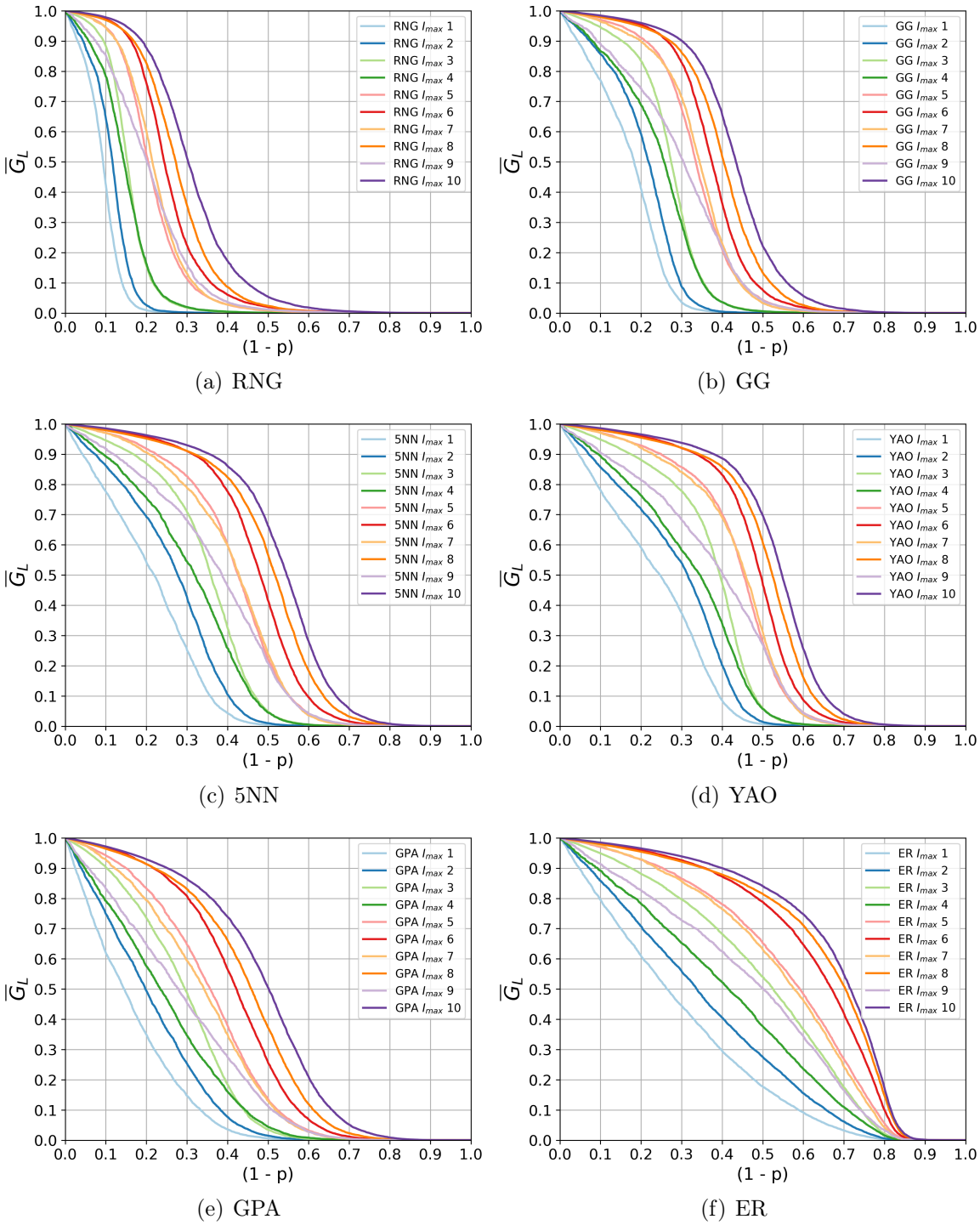


(a) RNG (b) GG

(c) 5NN (d) YAO

(e) GPA (f) ER

Figure A.4: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 3$.

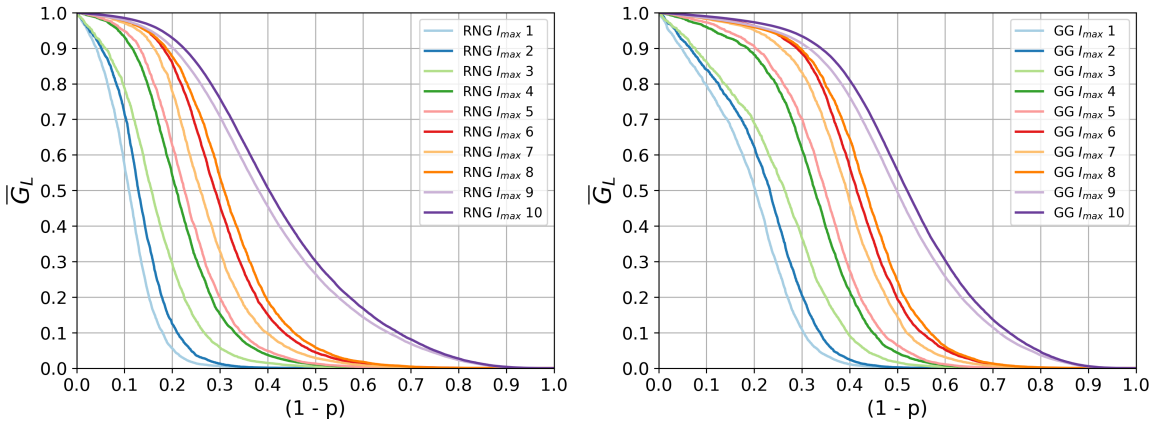


(a) RNG (b) GG

(c) 5NN (d) YAO

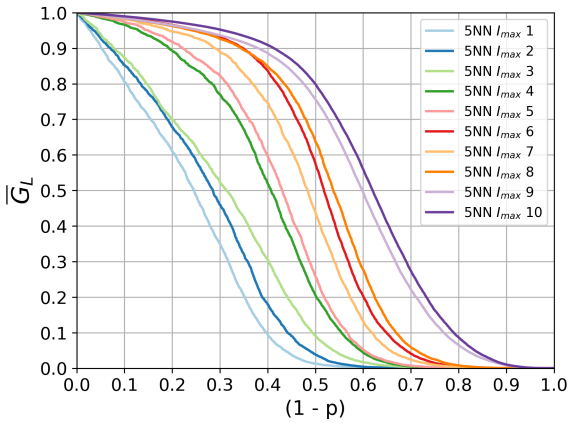
(e) GPA (f) ER

Figure A.5: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 4$.

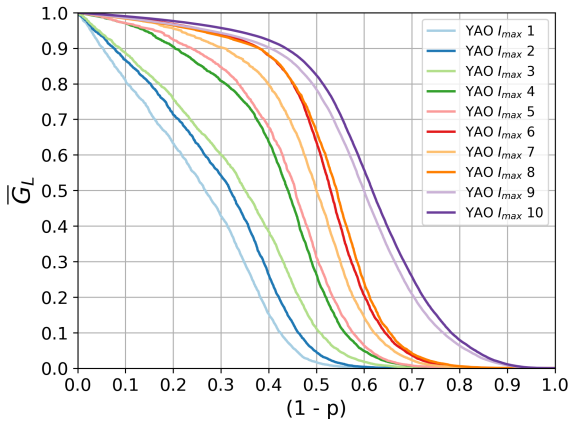


(a) RNG

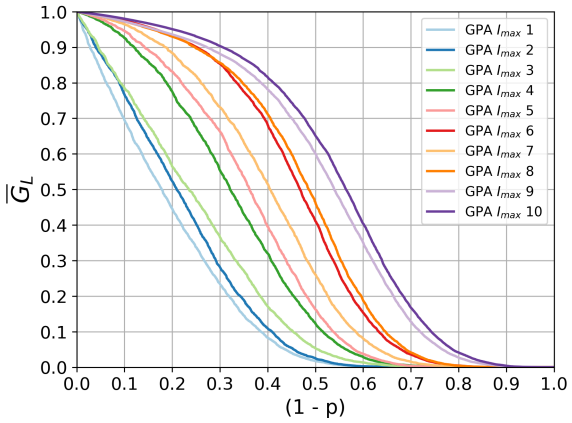
(b) GG



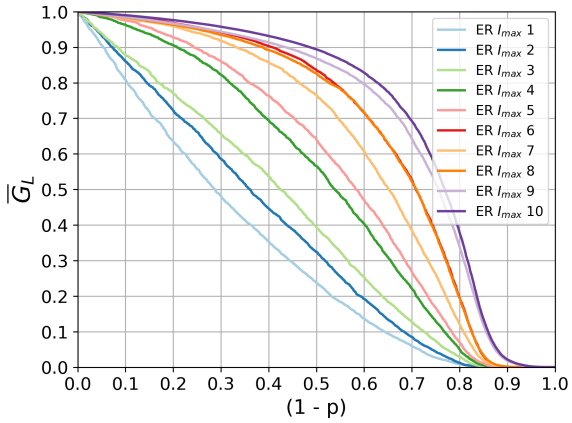
(c) 5NN



(d) YAO

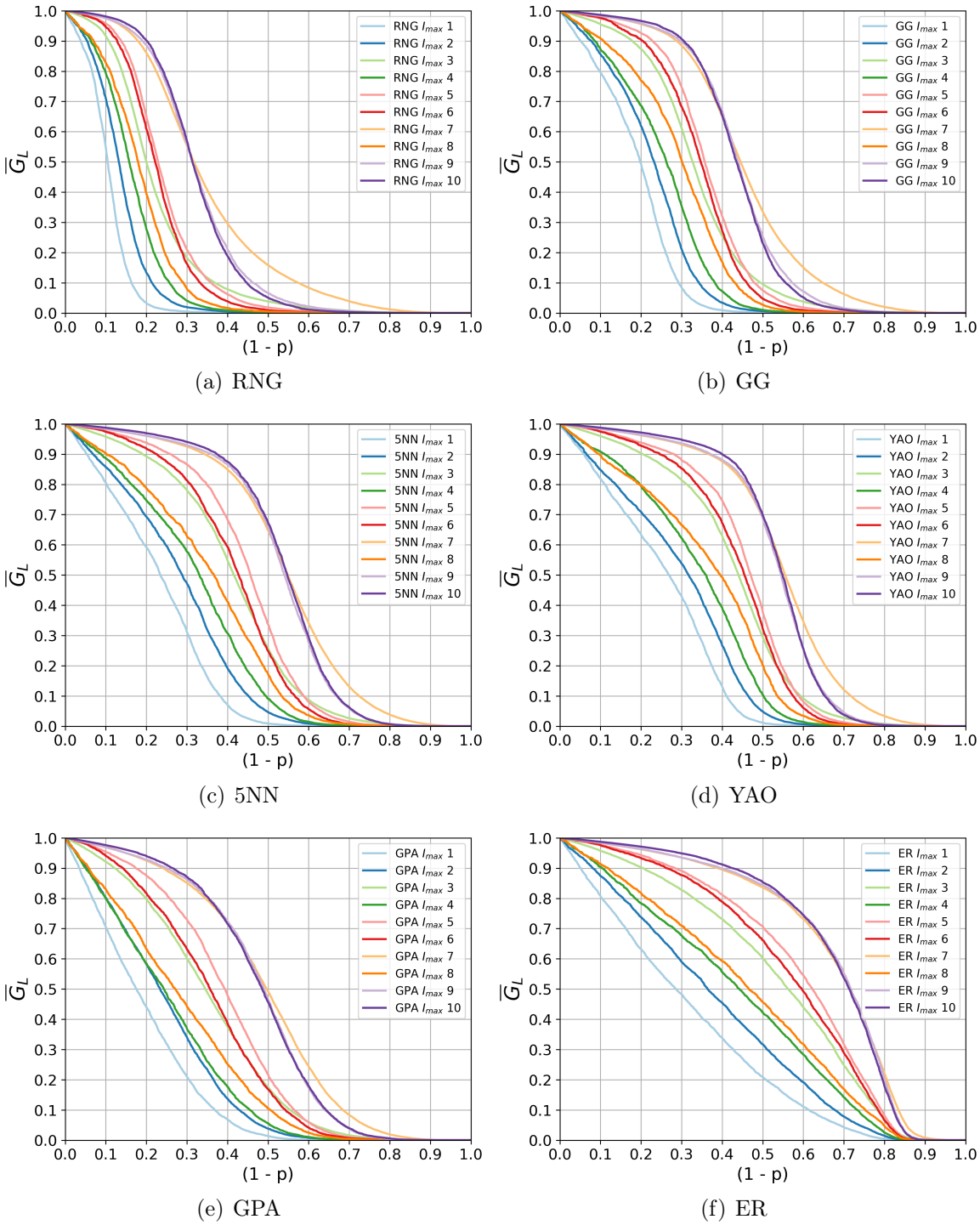


(e) GPA



(f) ER

Figure A.6: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 5$.

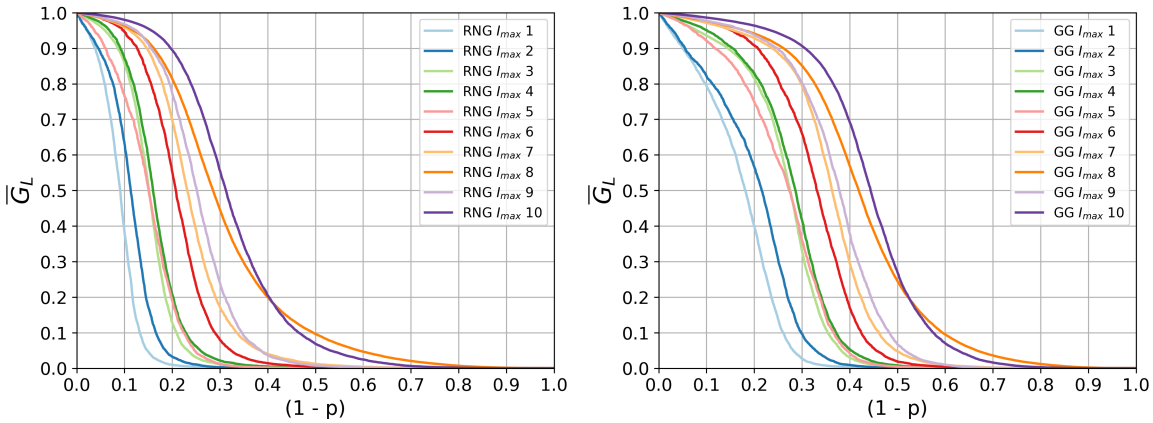


(a) RNG (b) GG

(c) 5NN (d) YAO

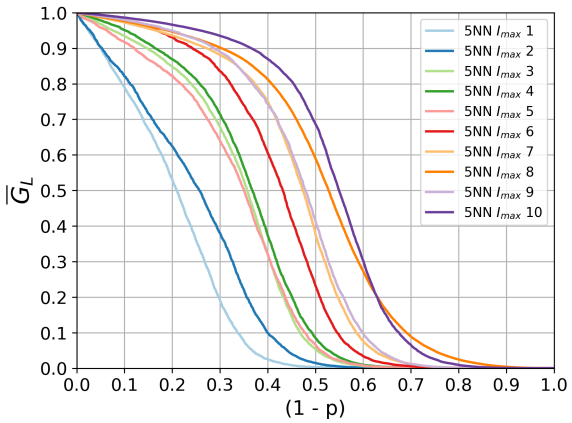
(e) GPA (f) ER

Figure A.7: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 6$.

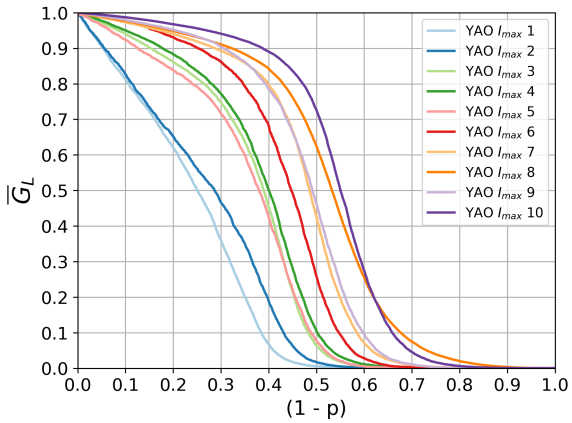


(a) RNG

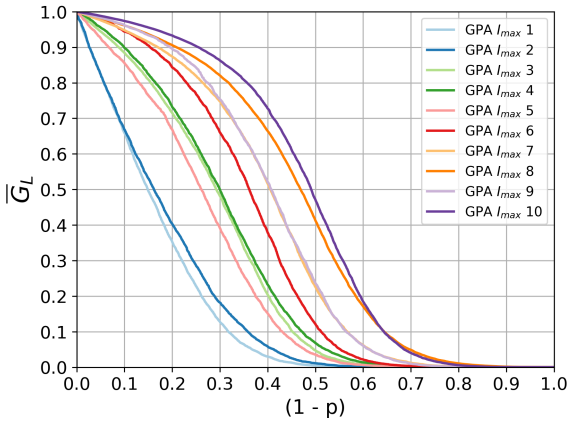
(b) GG



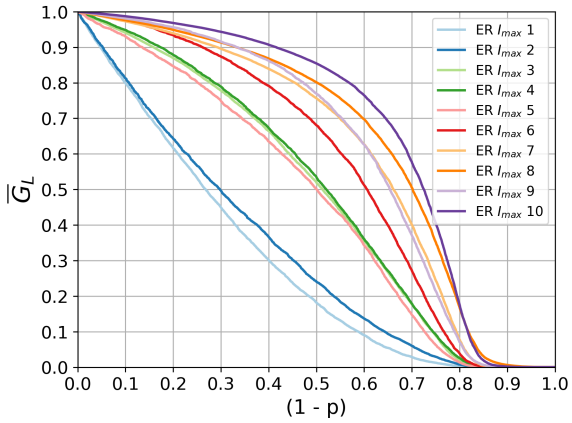
(c) 5NN



(d) YAO

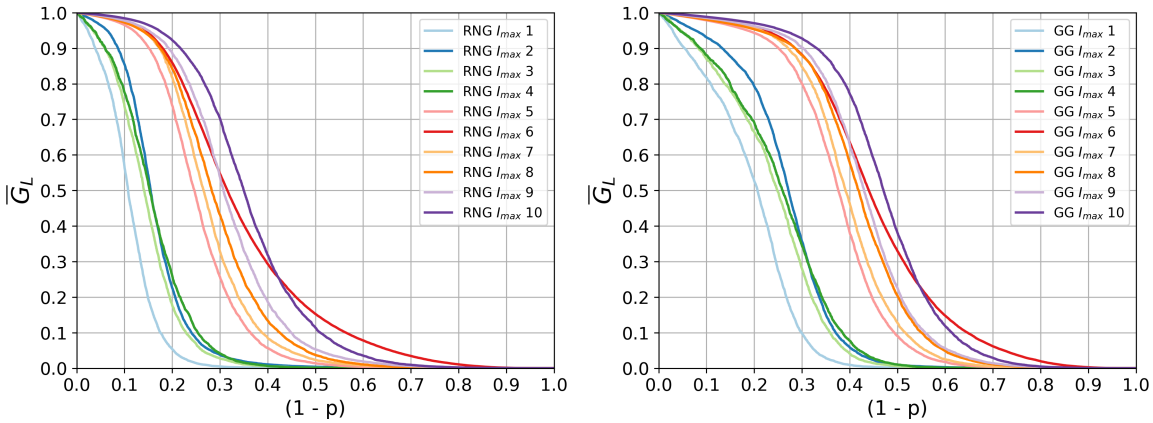


(e) GPA



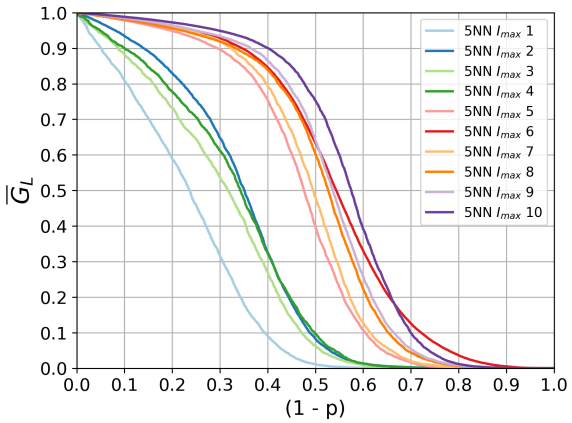
(f) ER

Figure A.8: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 7$.

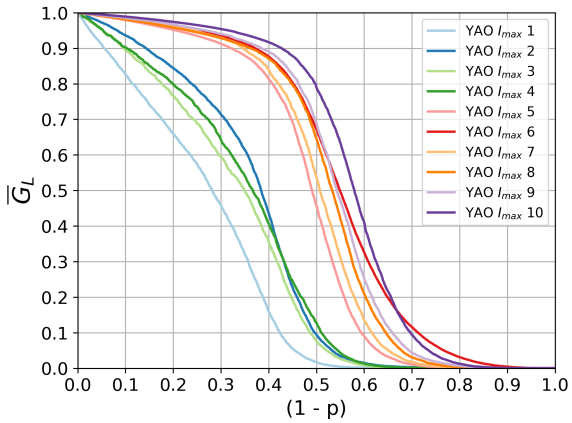


(a) RNG

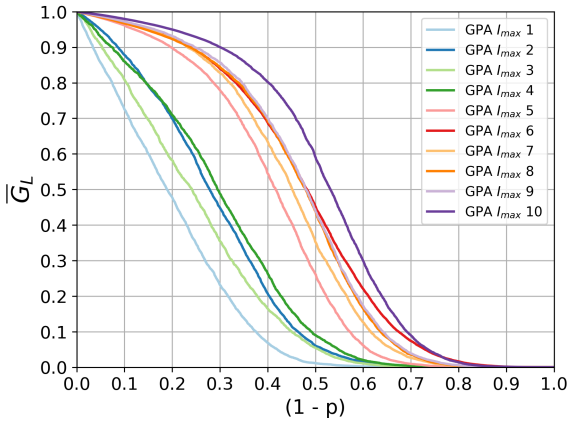
(b) GG



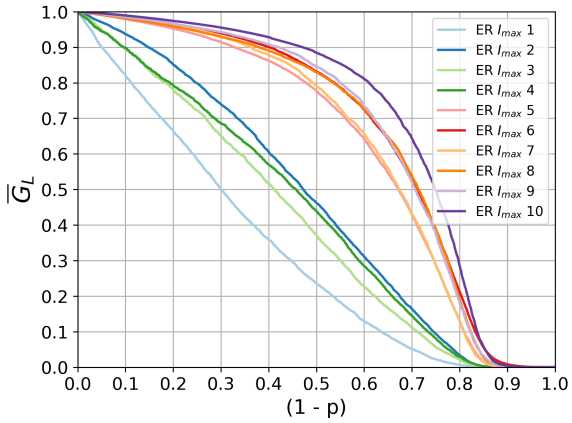
(c) 5NN



(d) YAO

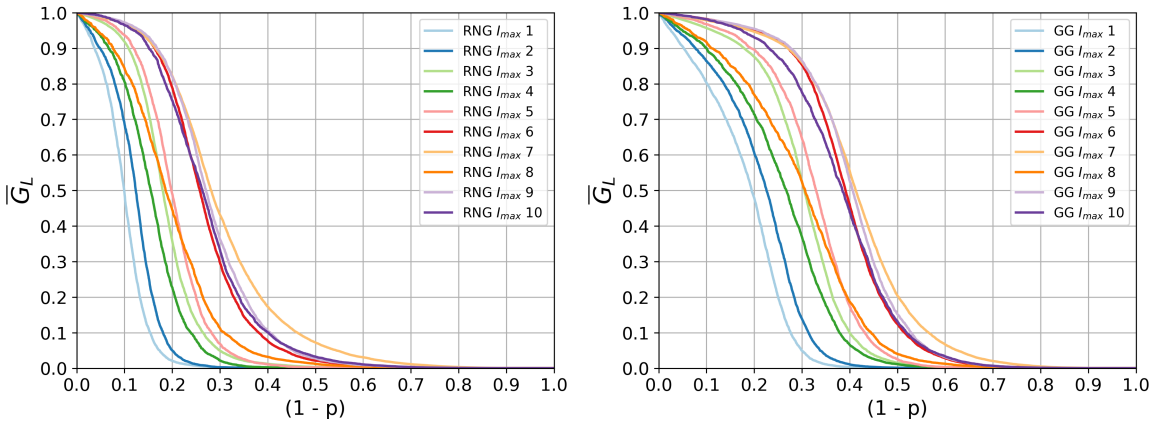


(e) GPA



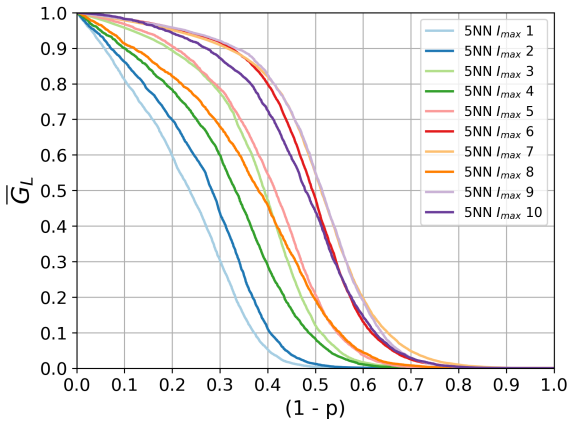
(f) ER

Figure A.9: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 8$.

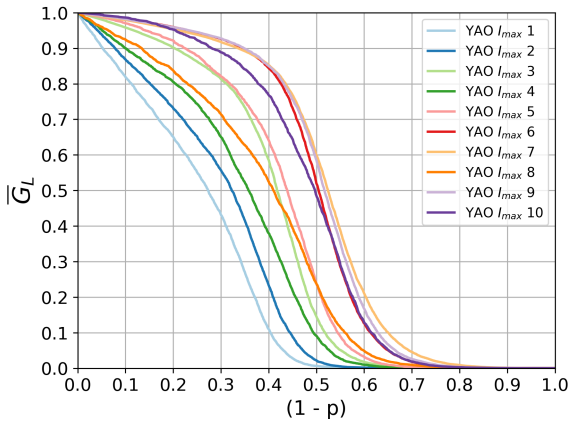


(a) RNG

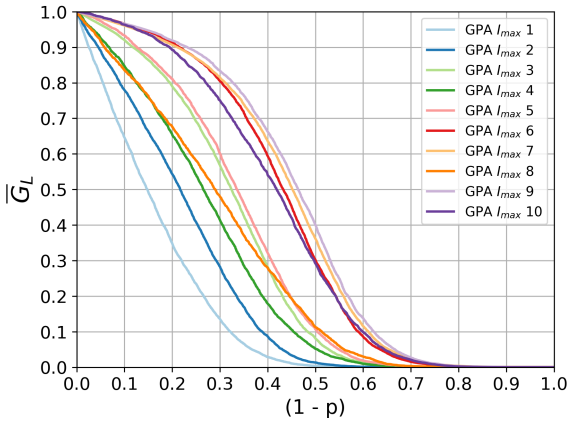
(b) GG



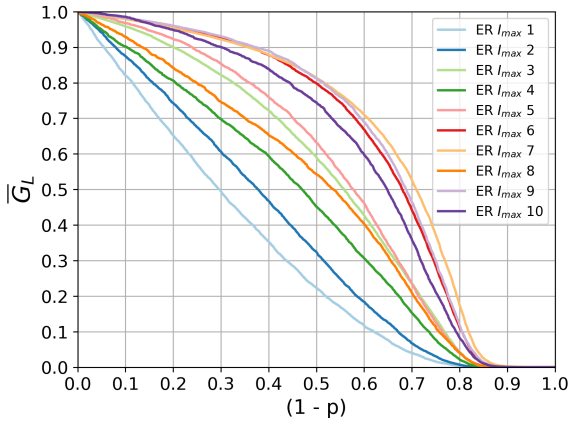
(c) 5NN



(d) YAO

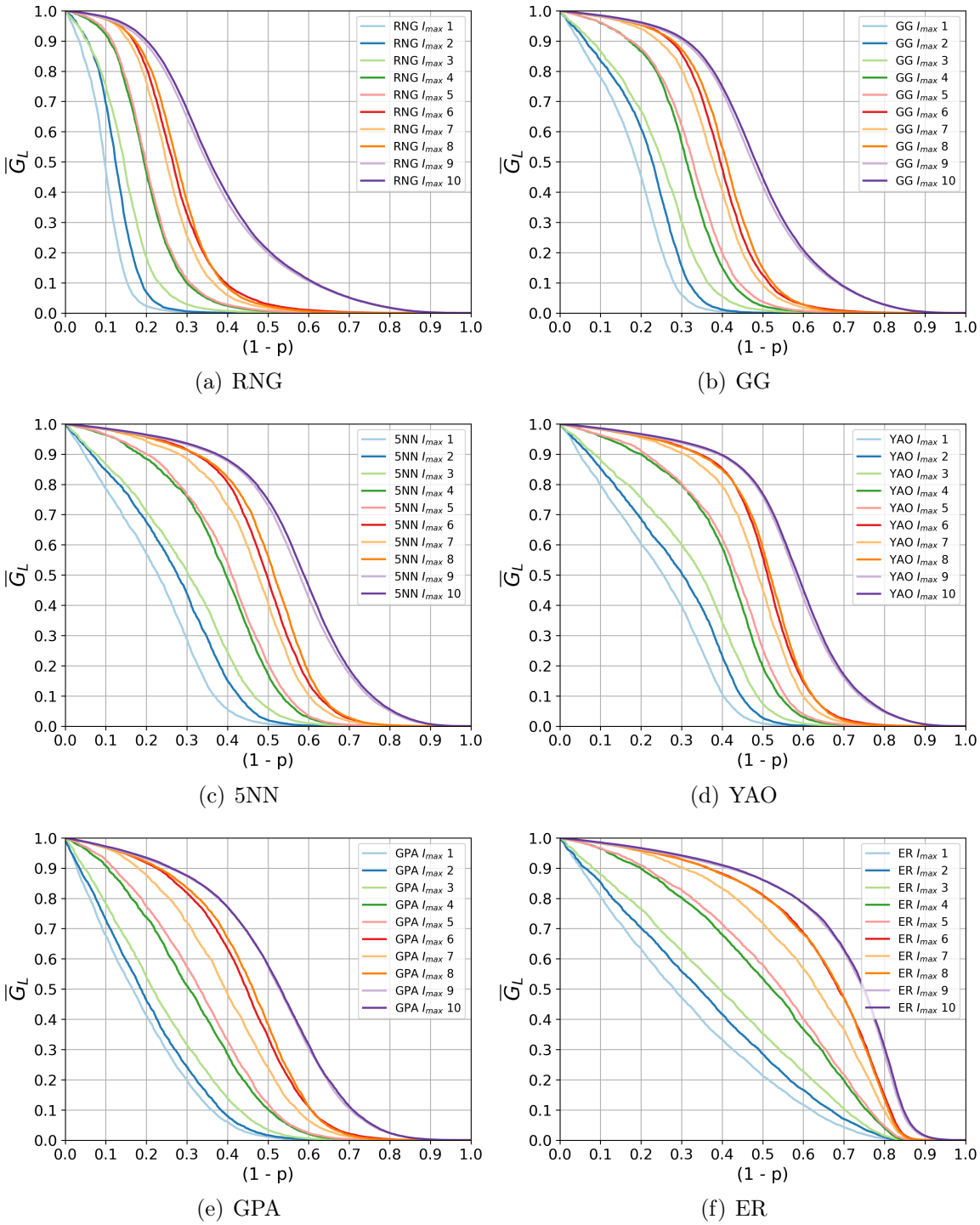


(e) GPA



(f) ER

Figure A.10: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 9$.

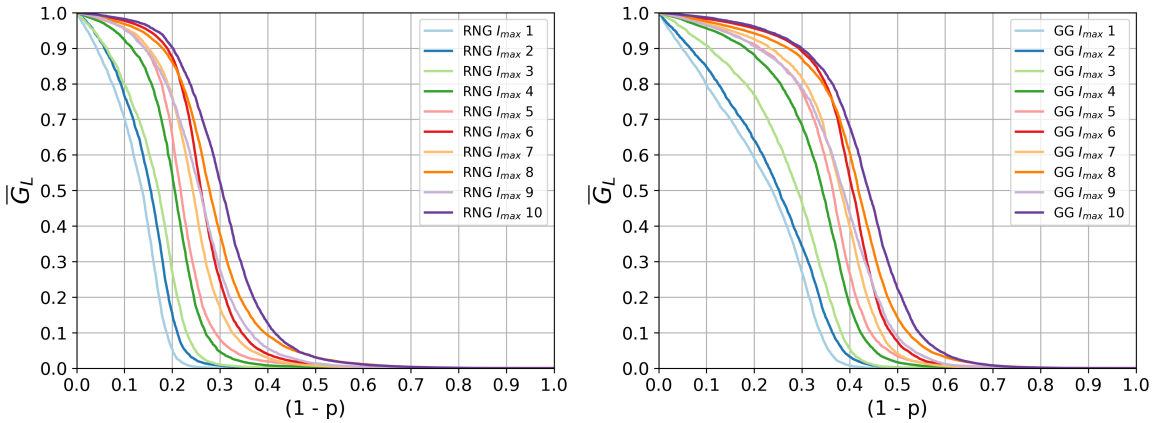


(a) RNG (b) GG

(c) 5NN (d) YAO

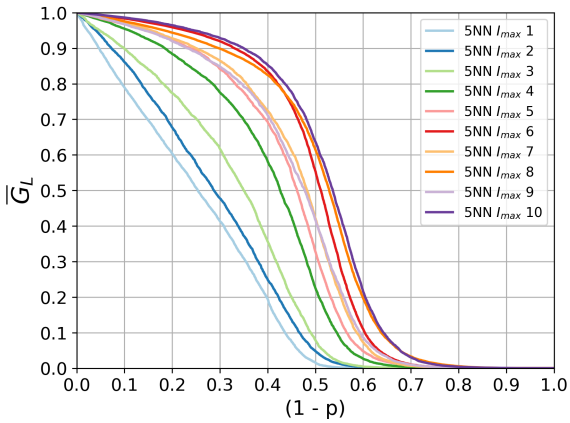
(e) GPA (f) ER

Figure A.11: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 10$.

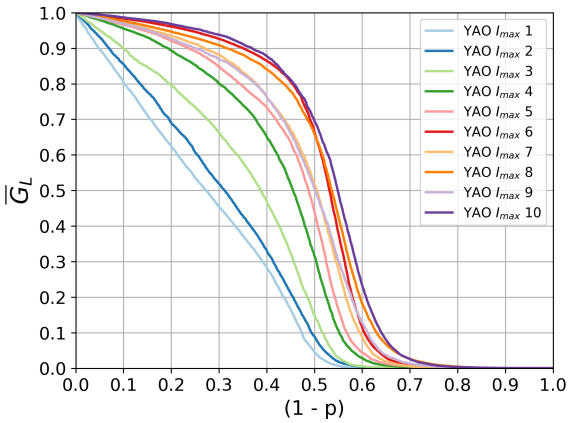


(a) RNG

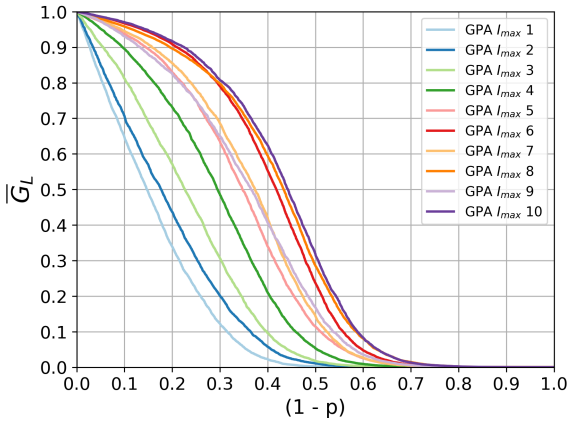
(b) GG



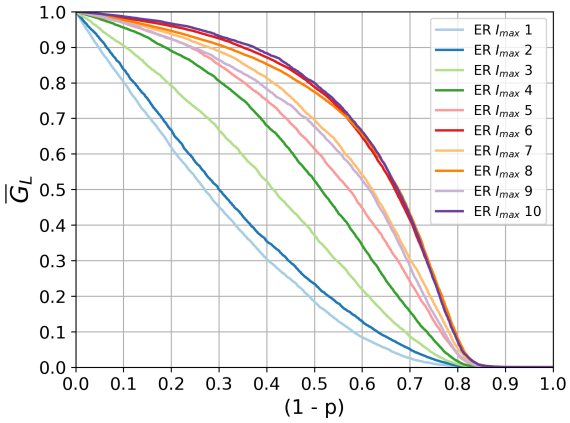
(c) 5NN



(d) YAO

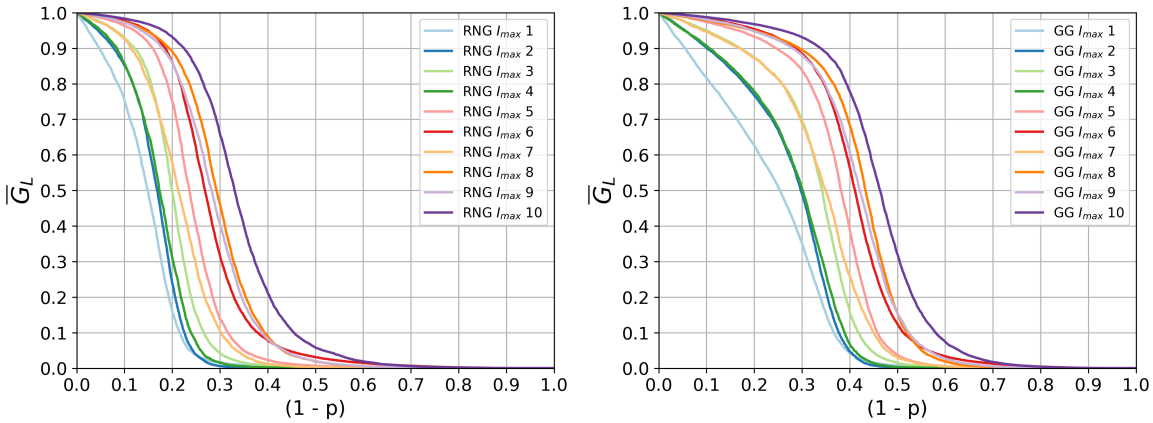


(e) GPA



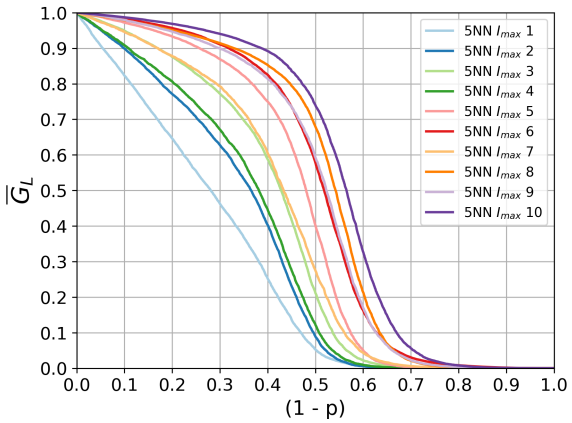
(f) ER

Figure A.12: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 1$.

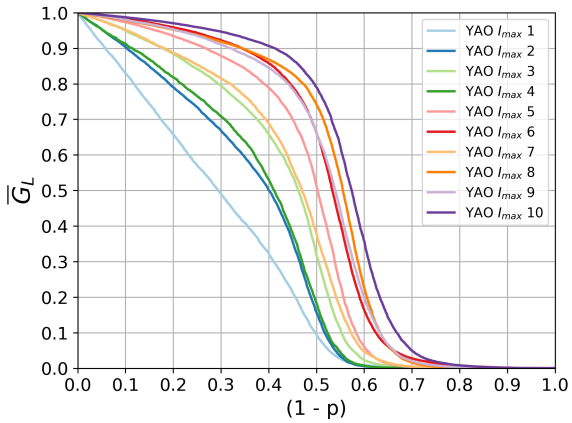


(a) RNG

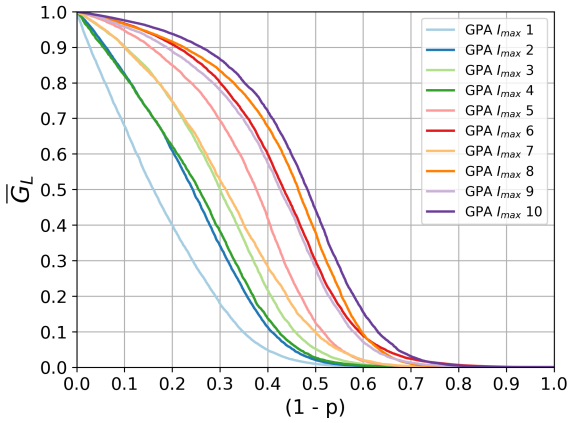
(b) GG



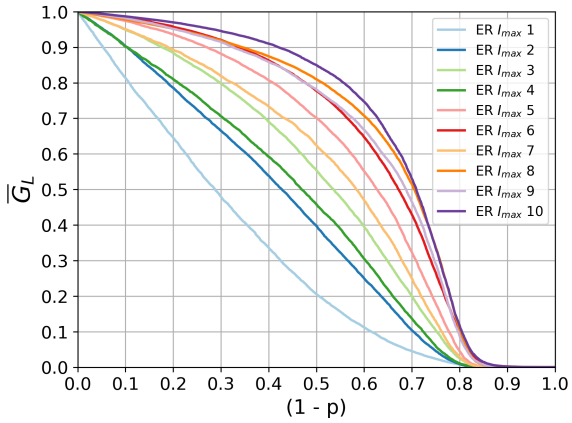
(c) 5NN



(d) YAO

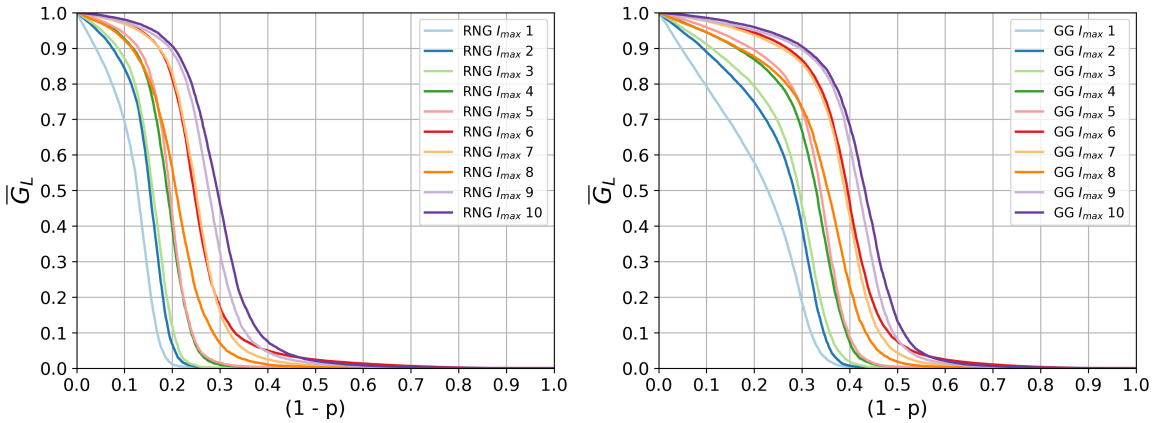


(e) GPA



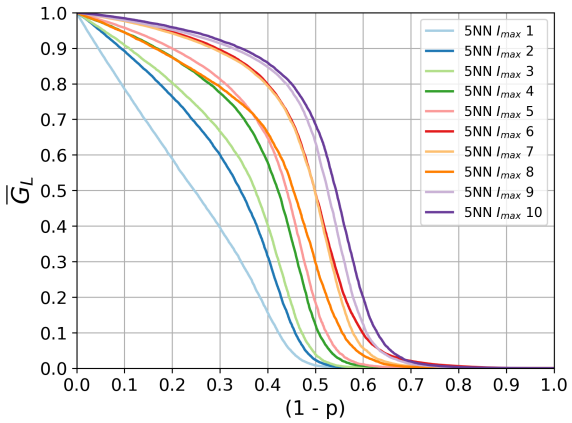
(f) ER

Figure A.13: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 2$.

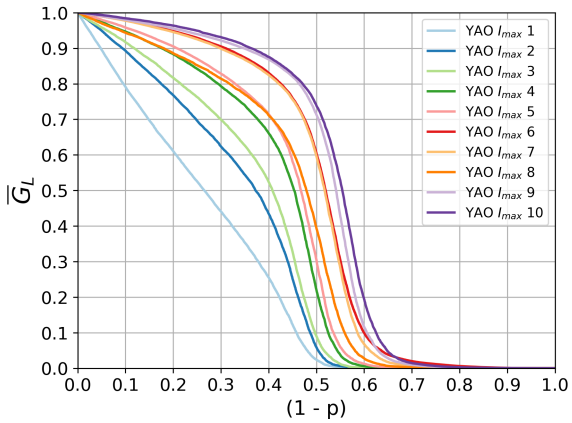


(a) RNG

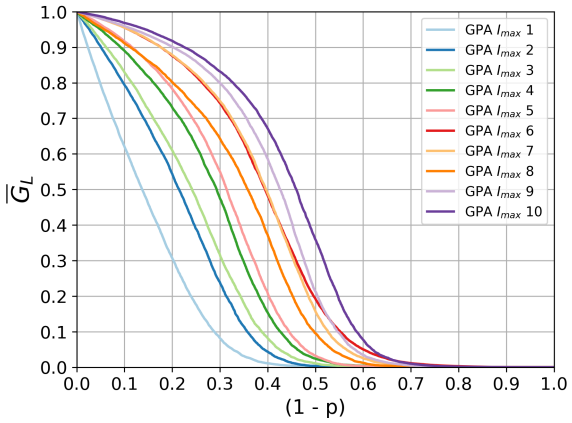
(b) GG



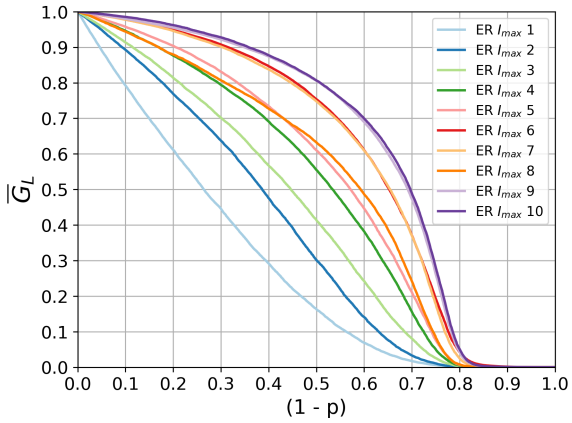
(c) 5NN



(d) YAO

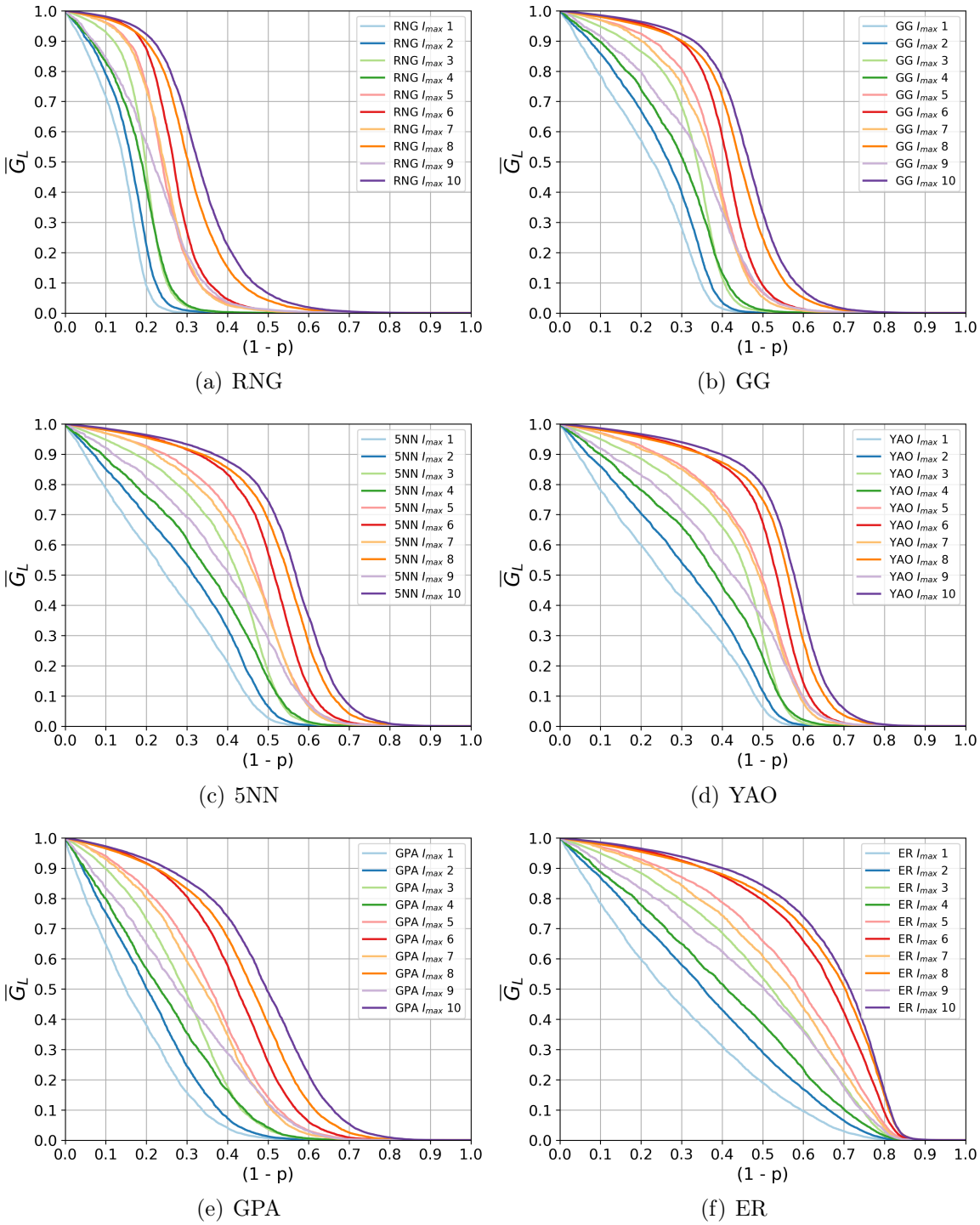


(e) GPA



(f) ER

Figure A.14: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 3$.

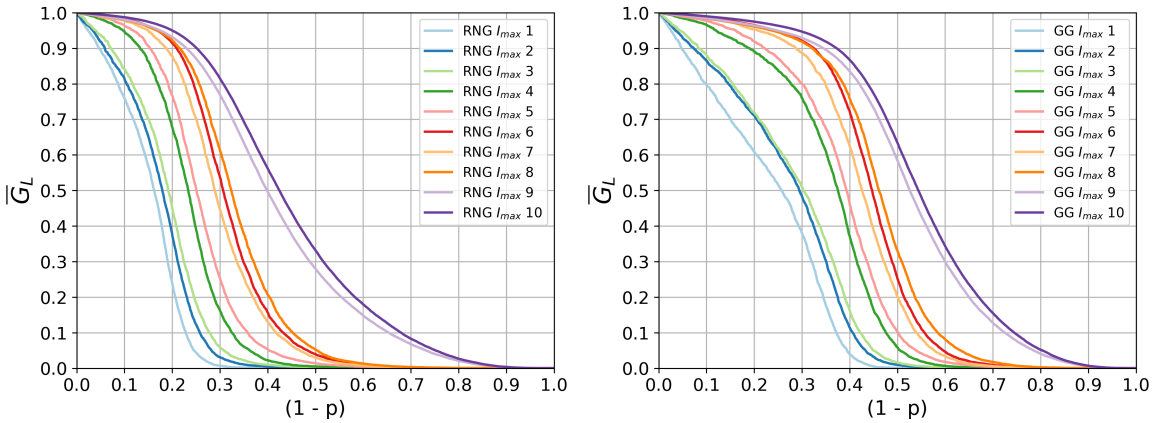


(a) RNG (b) GG

(c) 5NN (d) YAO

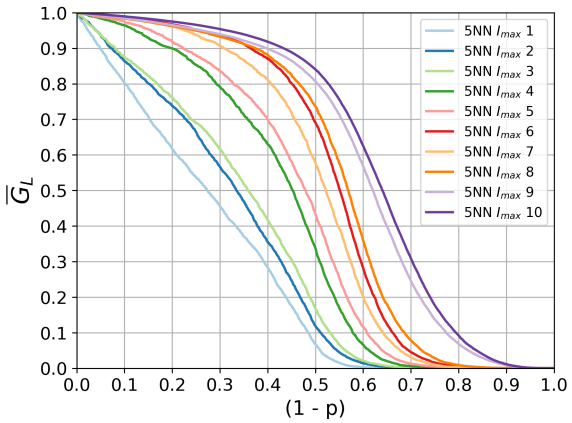
(e) GPA (f) ER

Figure A.15: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 4$.

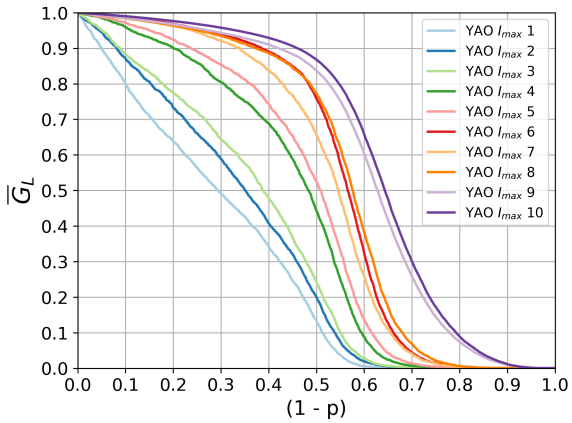


(a) RNG

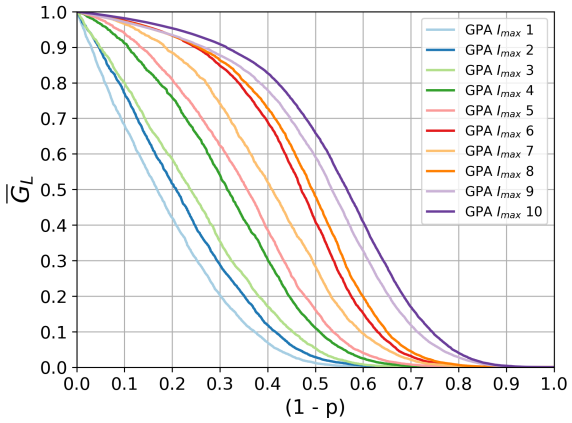
(b) GG



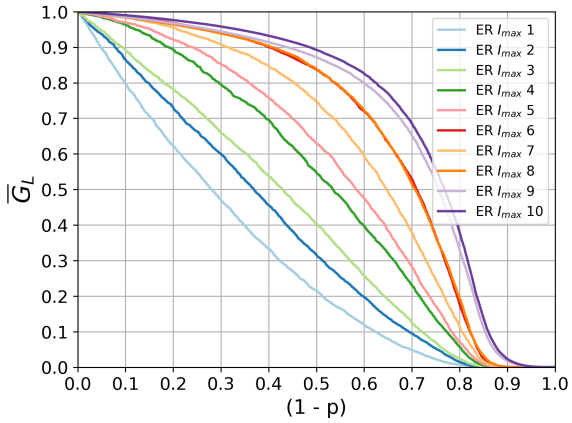
(c) 5NN



(d) YAO

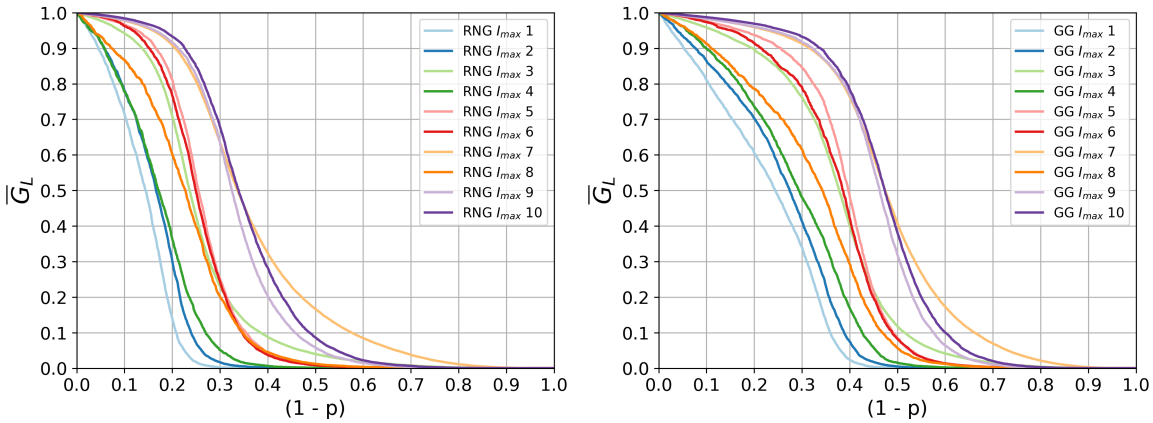


(e) GPA



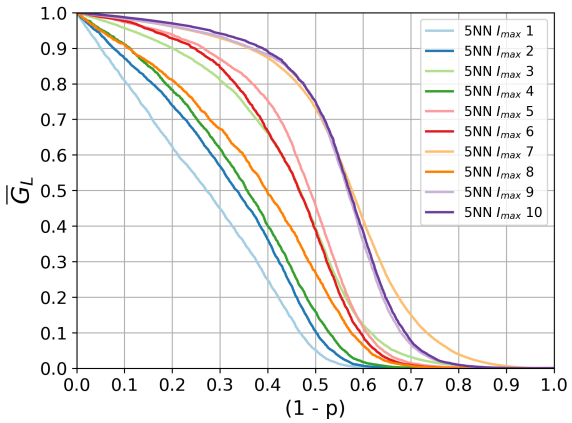
(f) ER

Figure A.16: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 5$.

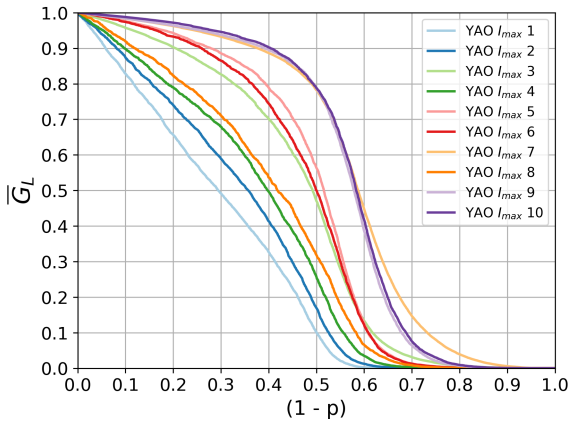


(a) RNG

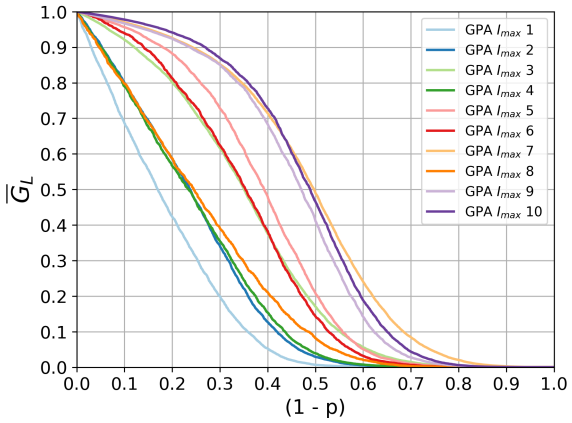
(b) GG



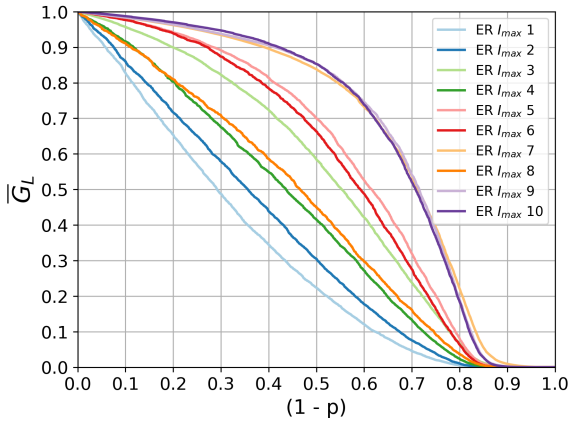
(c) 5NN



(d) YAO

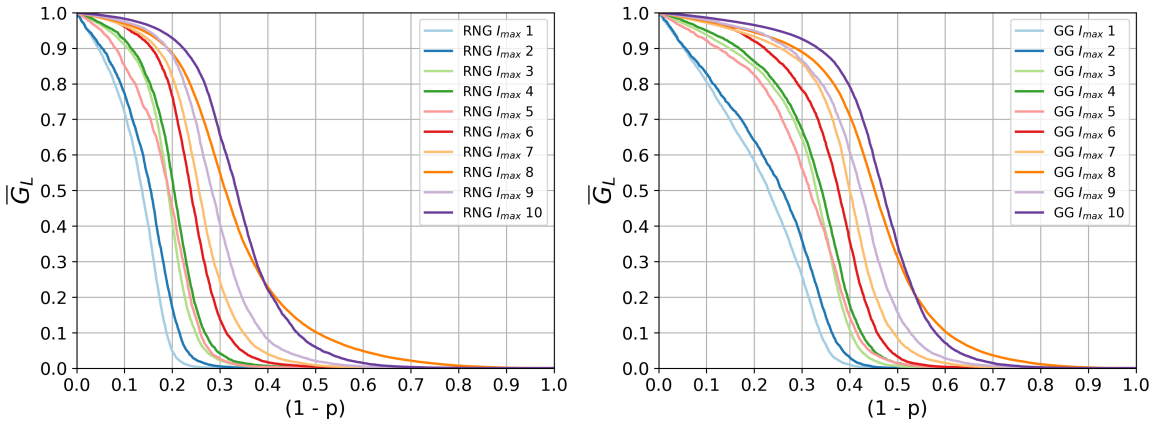


(e) GPA



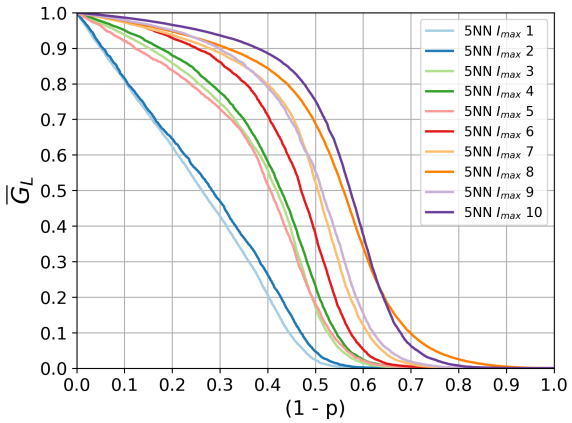
(f) ER

Figure A.17: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 6$.

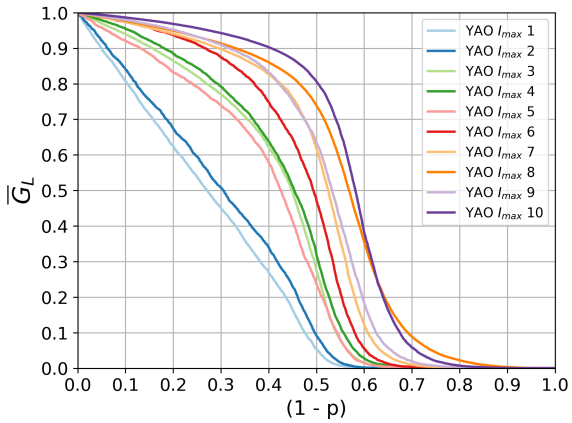


(a) RNG

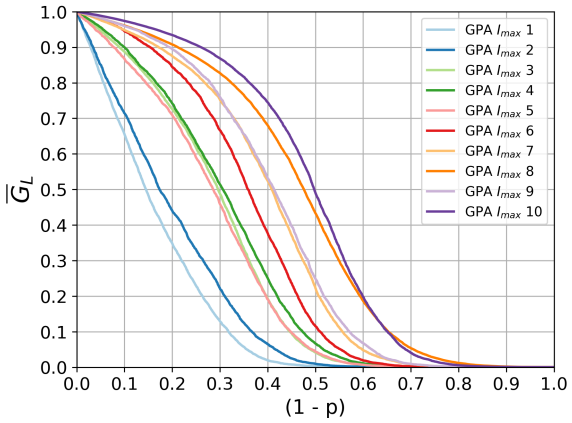
(b) GG



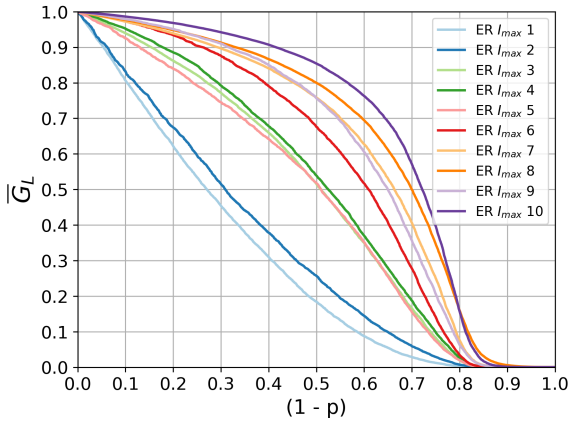
(c) 5NN



(d) YAO

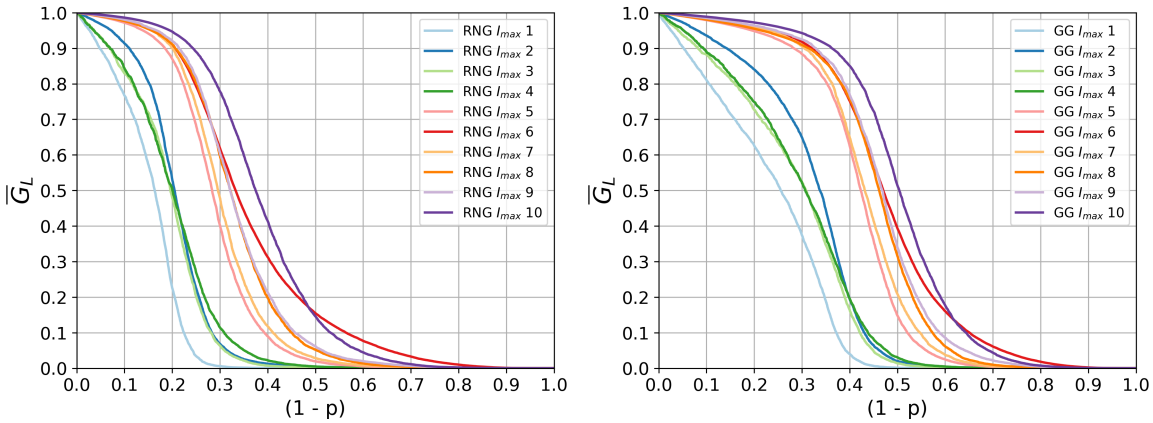


(e) GPA



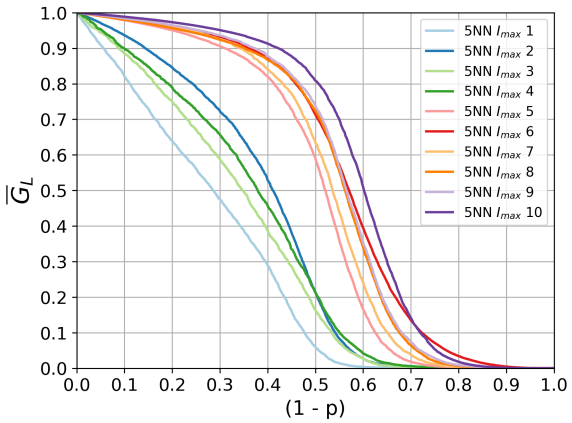
(f) ER

Figure A.18: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 7$.

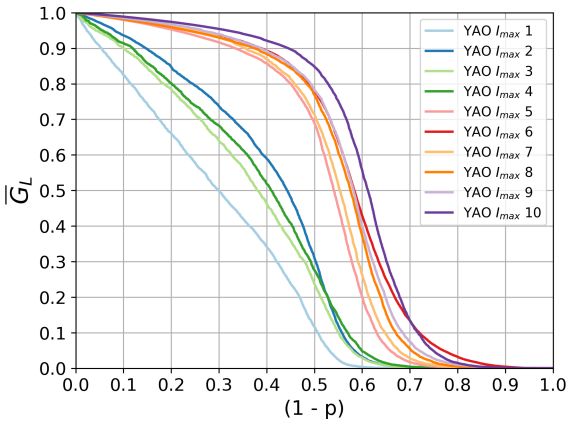


(a) RNG

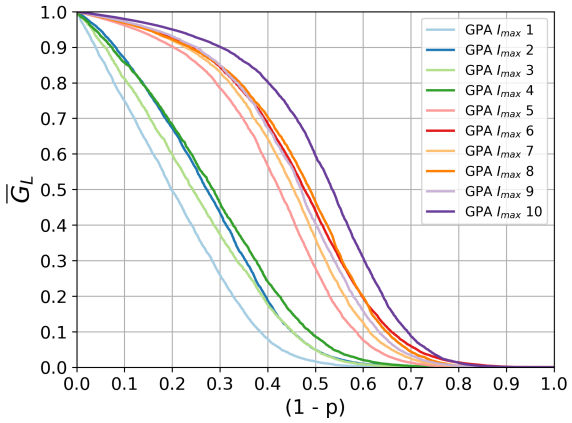
(b) GG



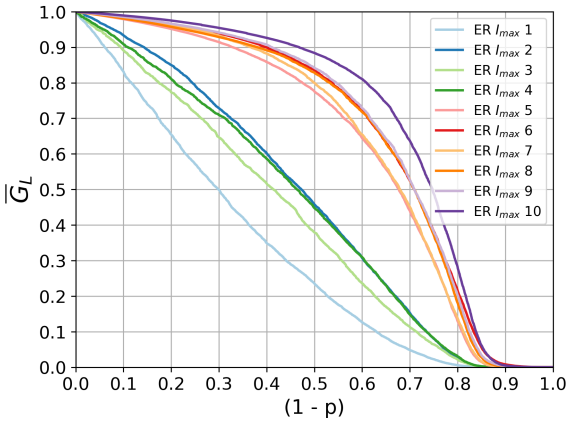
(c) 5NN



(d) YAO

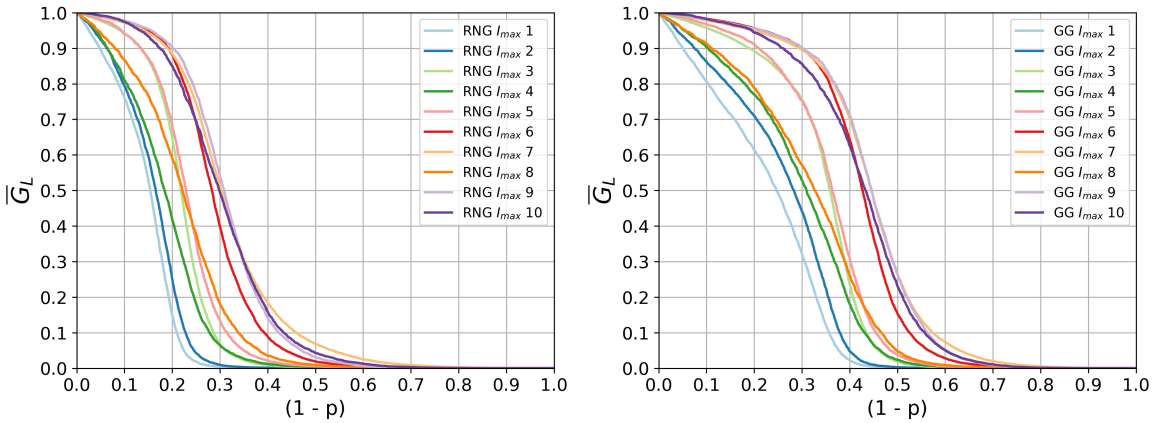


(e) GPA



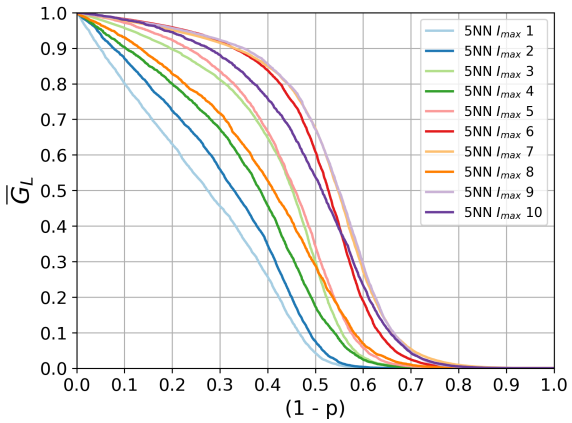
(f) ER

Figure A.19: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 8$.

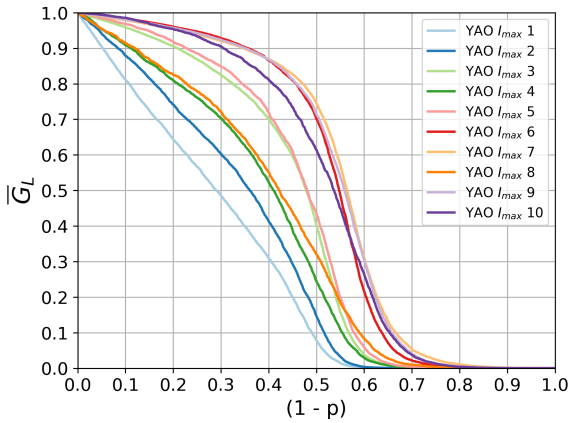


(a) RNG

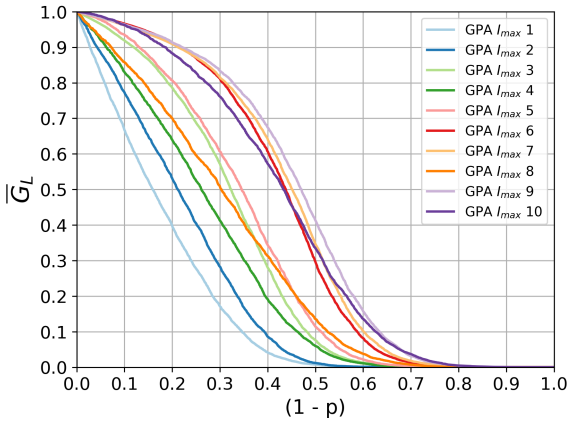
(b) GG



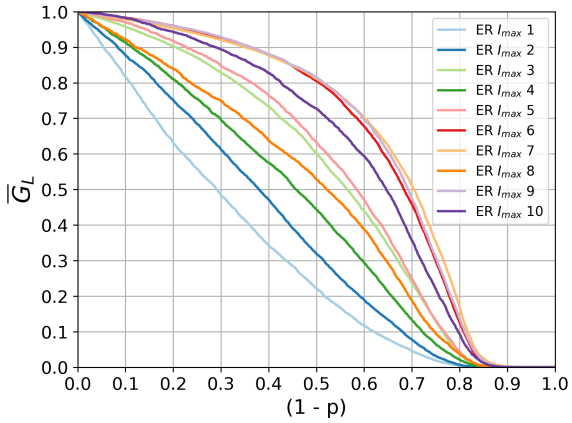
(c) 5NN



(d) YAO

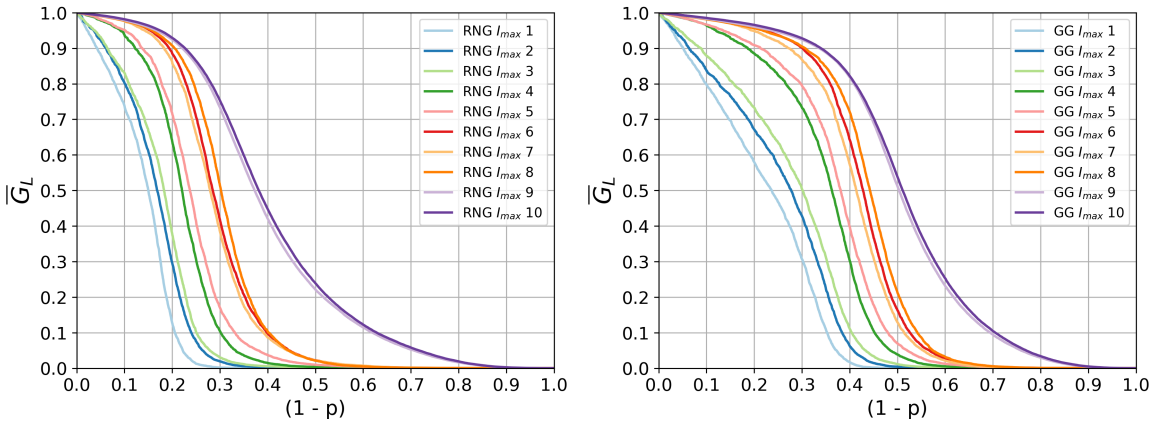


(e) GPA



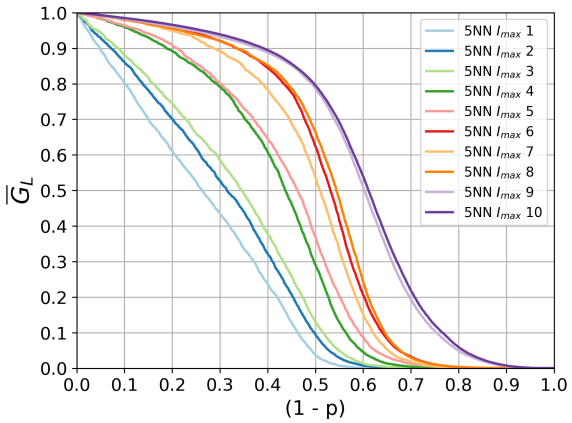
(f) ER

Figure A.20: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 9$.

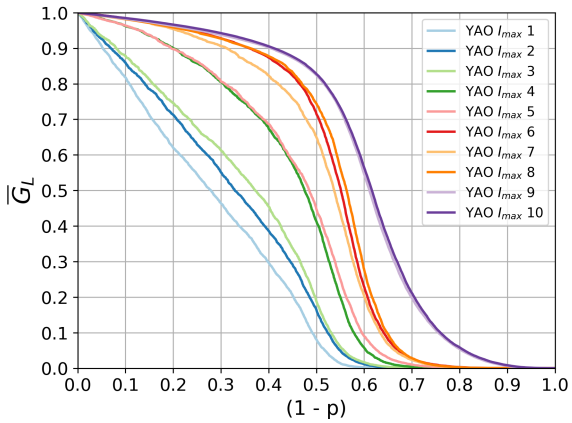


(a) RNG

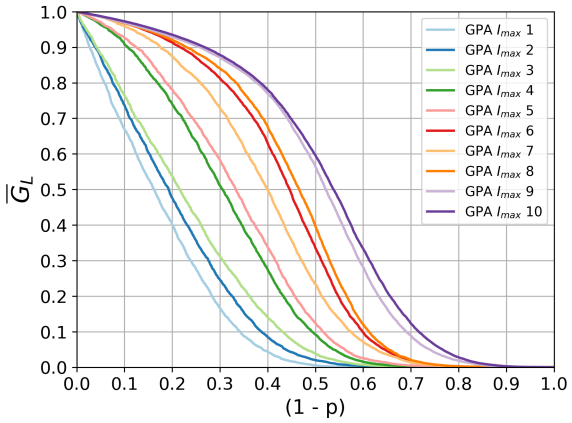
(b) GG



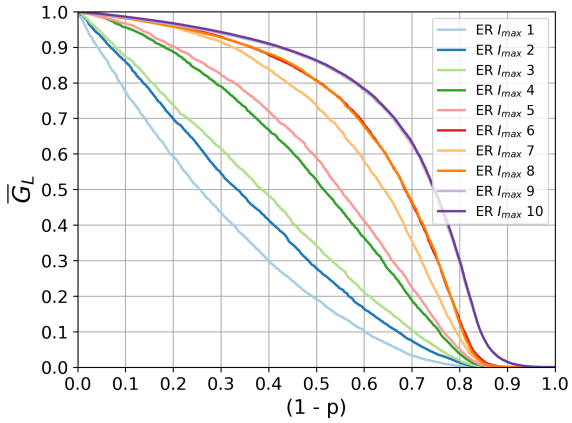
(c) 5NN



(d) YAO

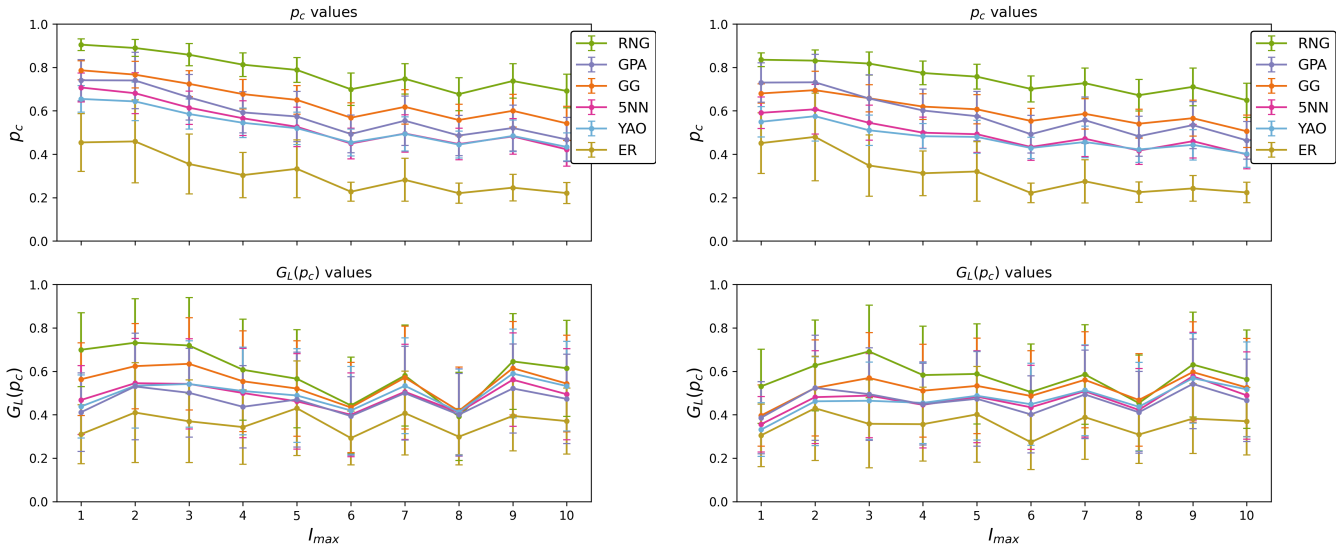


(e) GPA



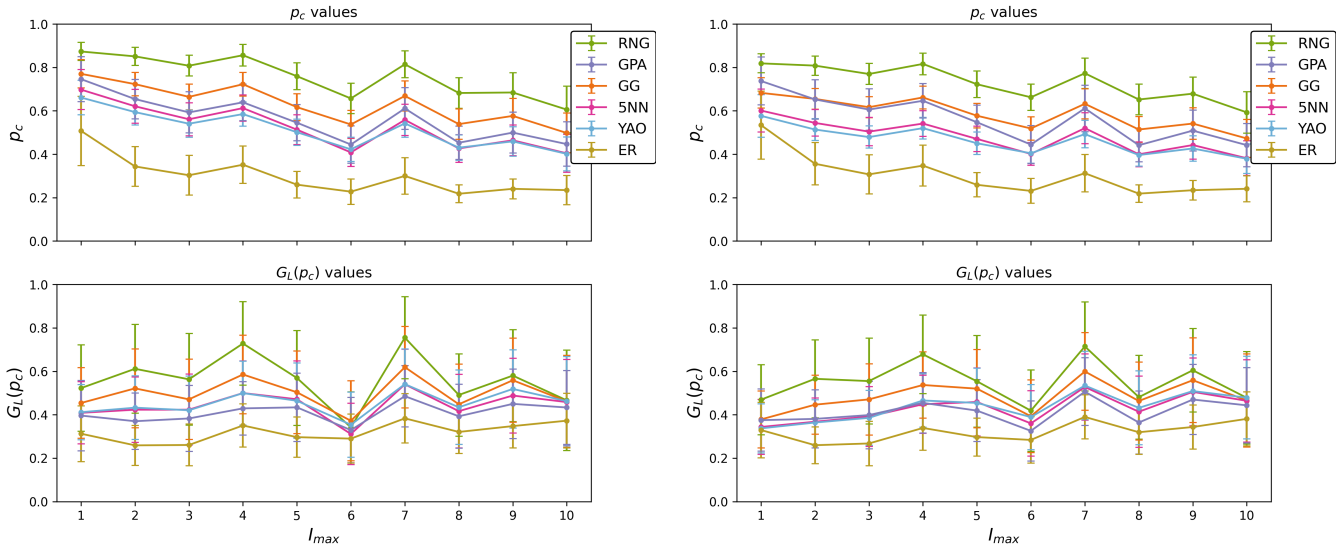
(f) ER

Figure A.21: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 10$.



(a) $q = 1$, s =(1:25)

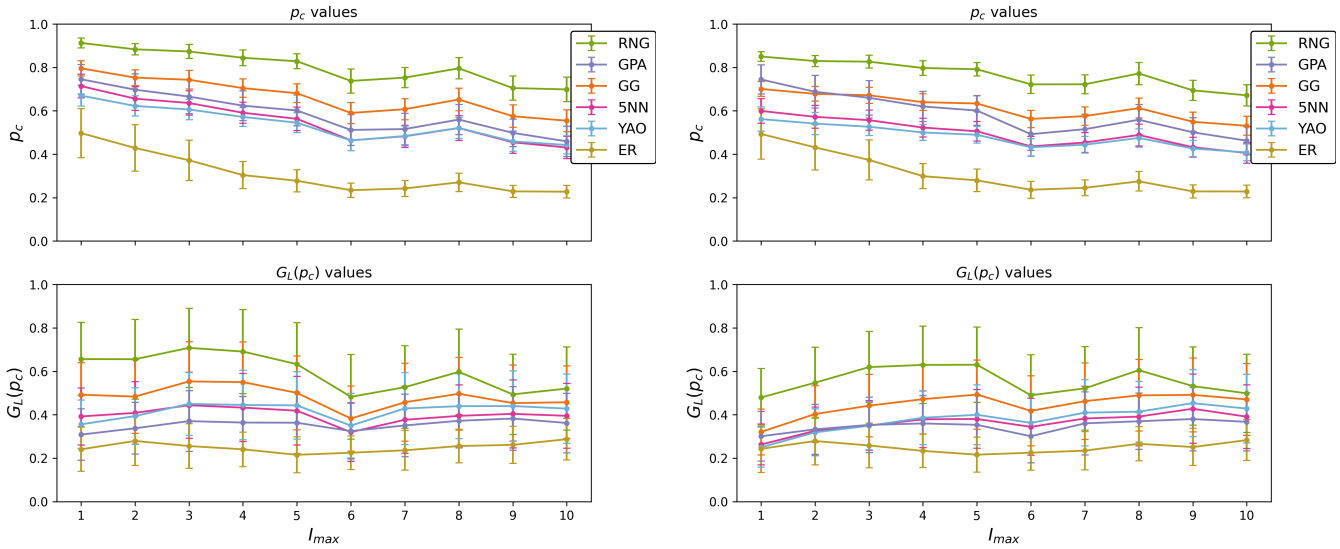
(b) $q = 1$, s =(1:1)



(c) $q = 2$, s =(1:25)

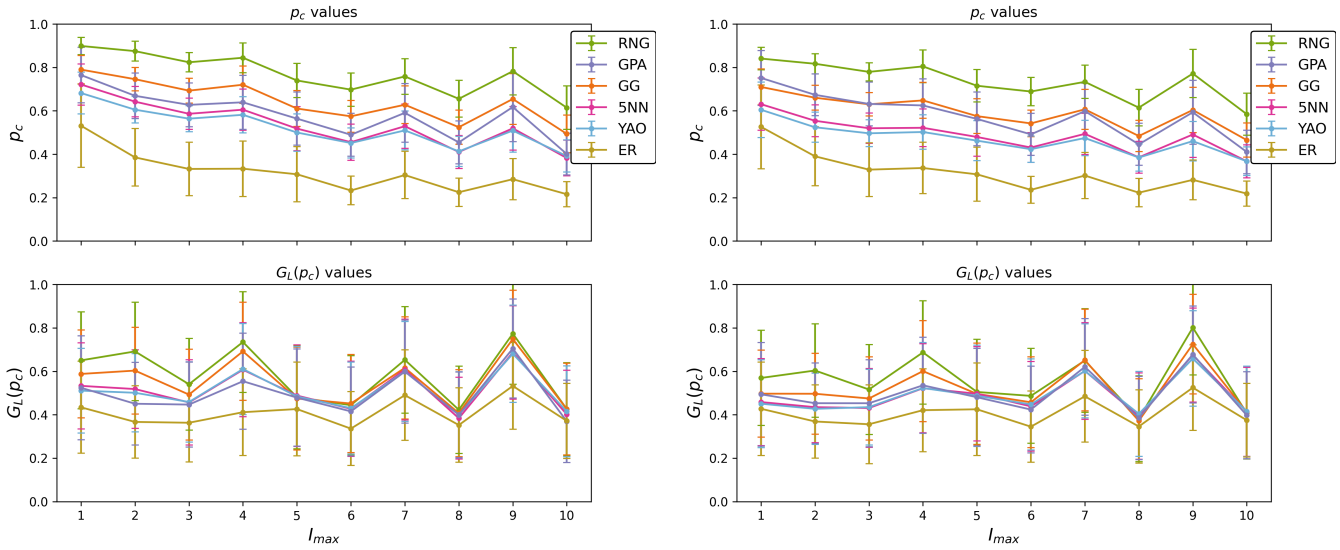
(d) $q = 2$, s =(1:1)

Figure A.22: Average values of p_c and $G_L(p_c)$ for each model m, space s, I_{max} value, and logical network version $q \in \{1, 2\}$. Bars represent the standard deviation.



(a) $q = 3$, s =(1:25)

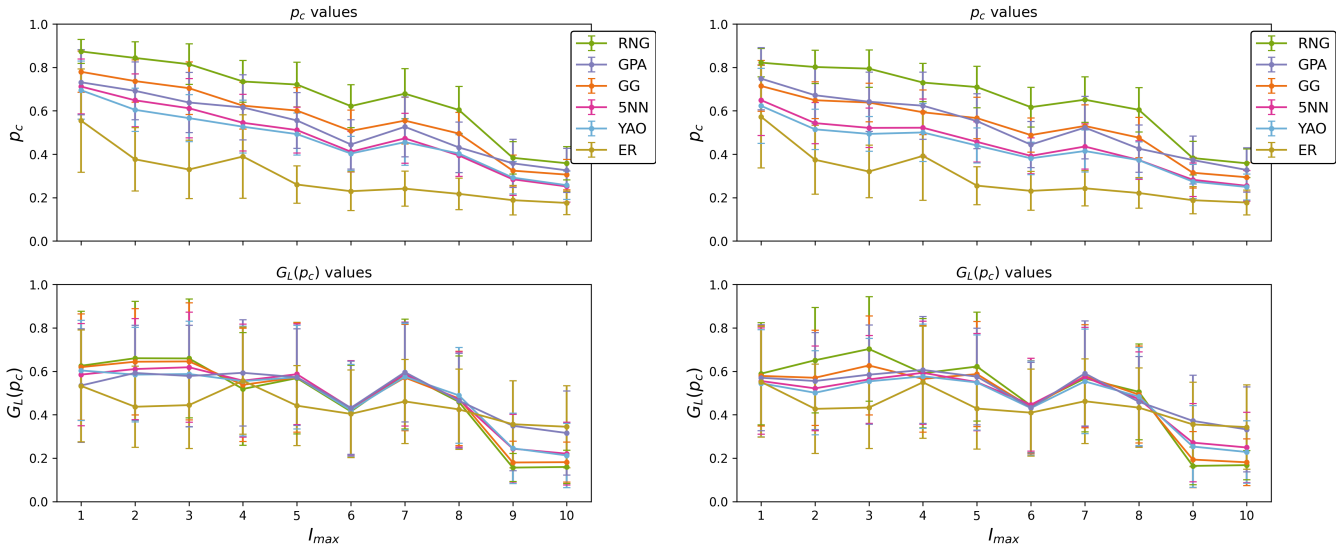
(b) $q = 3$, s =(1:1)



(c) $q = 4$, s =(1:25)

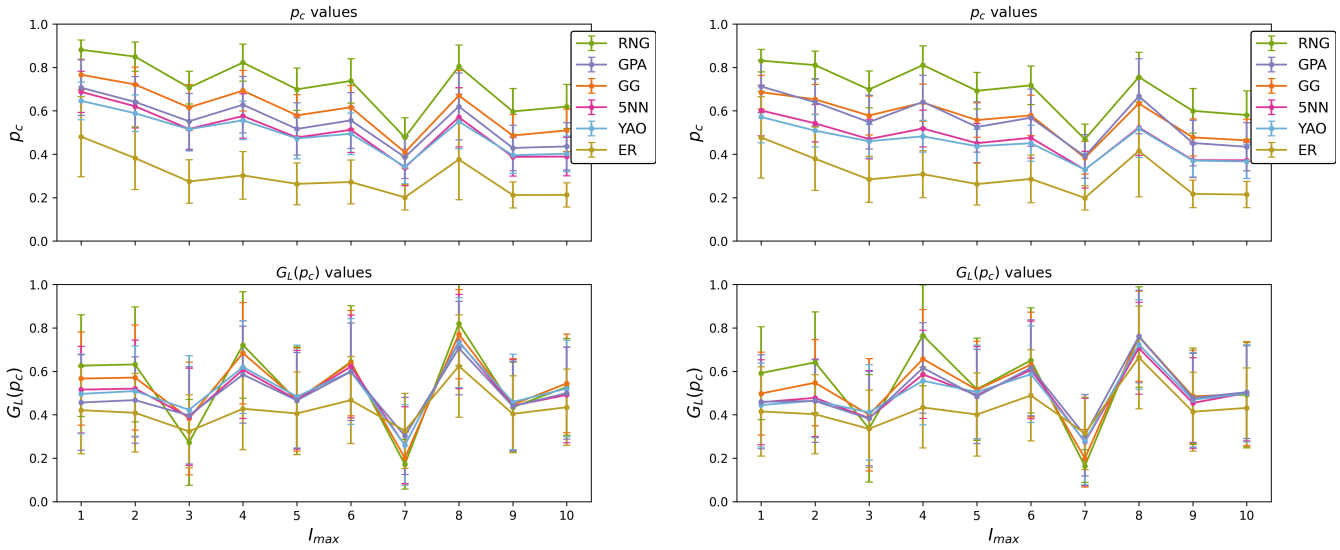
(d) $q = 4$, s =(1:1)

Figure A.23: Average values of p_c and $G_L(p_c)$ for each model m, space s, I_{max} value, and logical network version $q \in \{3, 4\}$. Bars represent the standard deviation.



(a) $q = 5$, s =(1:25)

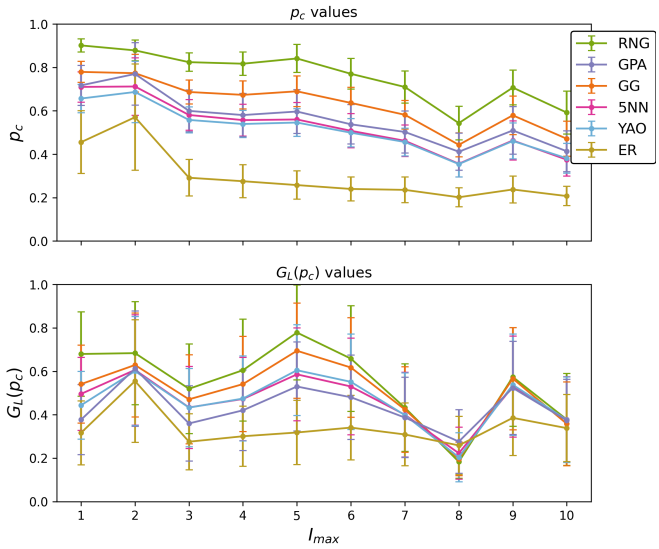
(b) $q = 5$, s =(1:1)



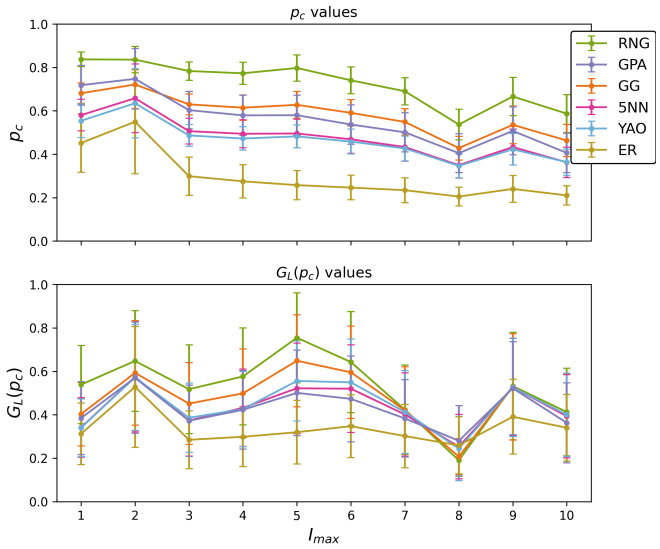
(c) $q = 6$, s =(1:25)

(d) $q = 6$, s =(1:1)

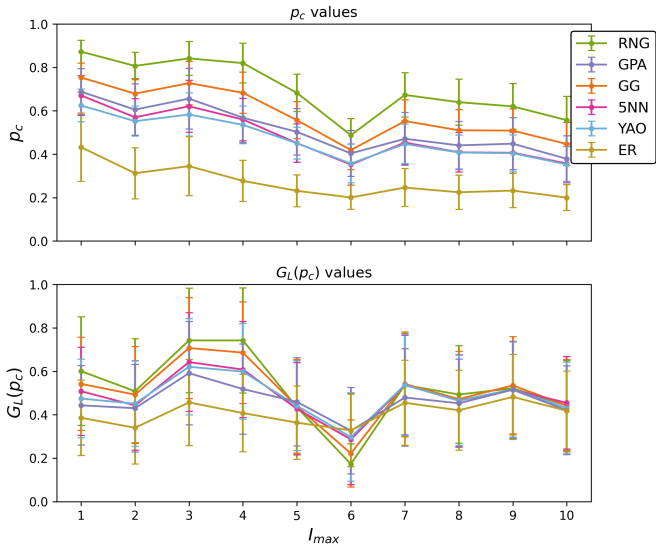
Figure A.24: Average values of p_c and $G_L(p_c)$ for each model m, space s, I_{max} value, and logical network version $q \in \{5, 6\}$. Bars represent the standard deviation.



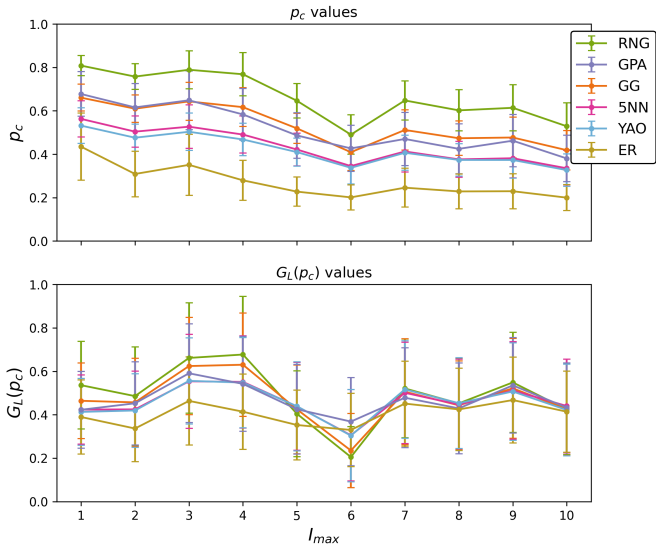
(a) $q = 7$, s =(1:25)



(b) $q = 7$, s =(1:1)

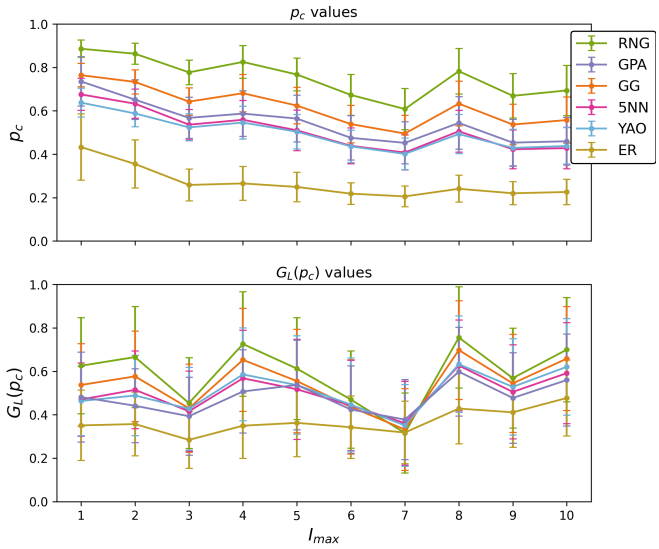


(c) $q = 8$, s =(1:25)

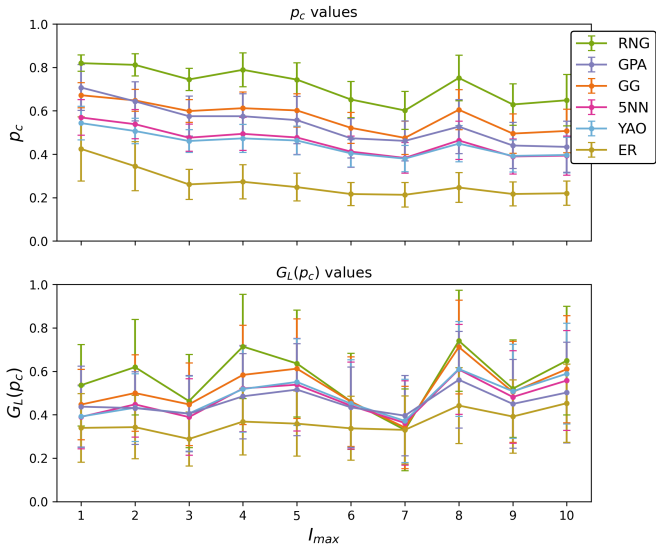


(d) $q = 8$, s =(1:1)

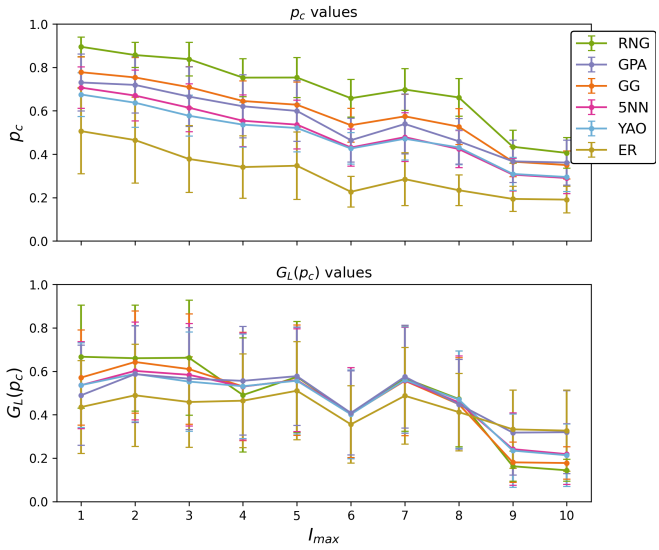
Figure A.25: Average values of p_c and $G_L(p_c)$ for each model m, space s, I_{max} value, and logical network version $q \in \{7, 8\}$. Bars represent the standard deviation.



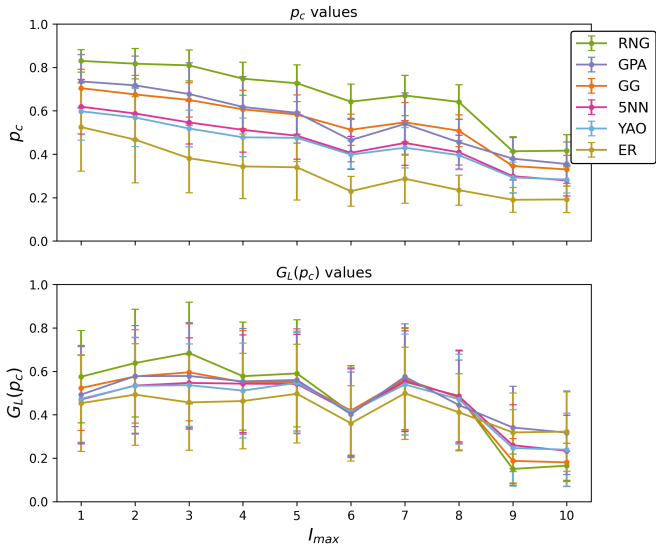
(a) $q = 9$, s =(1:25)



(b) $q = 9$, s =(1:1)



(c) $q = 10$, s =(1:25)



(d) $q = 10$, s =(1:1)

Figure A.26: Average values of p_c and $G_L(p_c)$ for each model m, space s, I_{max} value, and logical network version $q \in \{9, 10\}$. Bars represent the standard deviation.

A.2 General robustness behavior tables

s =(1:25)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.766	0.86	0.848	0.888	0.813	0.705	0.9	0.399	0.841	0.787
GG	0.652	0.765	0.708	0.81	0.844	0.72	0.884	0.486	0.817	0.719
5NN	0.514	0.744	0.606	0.768	0.837	0.699	0.842	0.537	0.679	0.595
YAO	0.556	0.695	0.552	0.749	0.82	0.711	0.867	0.552	0.746	0.676
GPA	0.592	0.73	0.545	0.686	0.809	0.652	0.847	0.696	0.669	0.54
ER	0.585	0.651	0.411	0.618	0.861	0.646	0.766	0.703	0.471	0.539
s =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.757	0.804	0.765	0.824	0.811	0.707	0.866	0.482	0.824	0.736
GG	0.654	0.708	0.662	0.76	0.801	0.783	0.883	0.536	0.784	0.669
5NN	0.641	0.674	0.5	0.7	0.838	0.752	0.839	0.554	0.67	0.621
YAO	0.598	0.662	0.537	0.701	0.853	0.757	0.833	0.56	0.659	0.648
GPA	0.646	0.772	0.56	0.704	0.816	0.725	0.837	0.663	0.599	0.576
ER	0.549	0.634	0.418	0.644	0.854	0.64	0.762	0.725	0.473	0.535

Table A.1: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 1$.

s =(1:25)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.361	0.607	0.673	0.675	0.597	0.271	0.733	0.62	0.441	0.455
GG	0.346	0.521	0.544	0.586	0.485	0.269	0.693	0.558	0.461	0.465
5NN	0.329	0.405	0.438	0.521	0.448	0.239	0.535	0.546	0.443	0.457
YAO	0.371	0.454	0.493	0.522	0.498	0.281	0.602	0.591	0.5	0.423
GPA	0.461	0.389	0.425	0.41	0.424	0.289	0.404	0.572	0.37	0.44
ER	0.487	0.298	0.391	0.296	0.42	0.42	0.349	0.597	0.403	0.52
s =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.506	0.714	0.643	0.711	0.529	0.351	0.739	0.6	0.456	0.471
GG	0.462	0.579	0.514	0.621	0.57	0.332	0.614	0.585	0.428	0.425
5NN	0.472	0.461	0.491	0.472	0.509	0.308	0.553	0.564	0.452	0.485
YAO	0.457	0.48	0.508	0.51	0.574	0.331	0.566	0.603	0.456	0.511
GPA	0.424	0.402	0.446	0.396	0.429	0.263	0.469	0.538	0.433	0.494
ER	0.48	0.28	0.403	0.284	0.412	0.412	0.365	0.611	0.453	0.543

Table A.2: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 2$.

s =(1:25)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.811	0.742	0.814	0.761	0.777	0.247	0.545	0.559	0.499	0.423
GG	0.639	0.734	0.71	0.643	0.721	0.226	0.523	0.55	0.539	0.392
5NN	0.563	0.69	0.615	0.531	0.632	0.218	0.557	0.428	0.519	0.436
YAO	0.58	0.737	0.655	0.58	0.688	0.234	0.542	0.545	0.554	0.451
GPA	0.486	0.692	0.568	0.457	0.615	0.353	0.53	0.48	0.553	0.464
ER	0.436	0.699	0.455	0.377	0.547	0.496	0.635	0.375	0.696	0.537
s =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.743	0.821	0.864	0.773	0.775	0.325	0.535	0.609	0.547	0.397
GG	0.636	0.798	0.76	0.689	0.753	0.32	0.553	0.588	0.584	0.423
5NN	0.534	0.806	0.624	0.588	0.71	0.318	0.559	0.495	0.557	0.479
YAO	0.558	0.786	0.71	0.661	0.697	0.377	0.583	0.635	0.637	0.509
GPA	0.454	0.765	0.492	0.488	0.611	0.31	0.547	0.523	0.527	0.477
ER	0.419	0.722	0.406	0.382	0.579	0.457	0.64	0.366	0.67	0.515

Table A.3: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 3$.

s =(1:25)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.72	0.876	0.582	0.9	0.839	0.697	0.891	0.876	0.931	0.858
GG	0.689	0.72	0.673	0.832	0.84	0.747	0.897	0.879	0.789	0.842
5NN	0.693	0.623	0.745	0.714	0.866	0.782	0.85	0.817	0.611	0.86
YAO	0.662	0.595	0.738	0.668	0.829	0.769	0.869	0.853	0.62	0.844
GPA	0.84	0.626	0.839	0.63	0.858	0.801	0.847	0.803	0.668	0.79
ER	0.84	0.526	0.899	0.482	0.875	0.795	0.742	0.877	0.348	0.894
s =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.846	0.769	0.737	0.909	0.851	0.841	0.91	0.778	0.927	0.88
GG	0.806	0.662	0.803	0.752	0.833	0.834	0.896	0.761	0.748	0.862
5NN	0.846	0.598	0.815	0.598	0.844	0.82	0.845	0.798	0.598	0.837
YAO	0.824	0.545	0.82	0.583	0.821	0.834	0.834	0.81	0.555	0.853
GPA	0.868	0.615	0.83	0.635	0.841	0.818	0.88	0.796	0.61	0.776
ER	0.842	0.582	0.887	0.478	0.865	0.829	0.695	0.887	0.372	0.887

Table A.4: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 4$.

s =(1:25)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.817	0.97	0.884	0.865	0.931	0.859	0.936	0.926	0.123	0.157
GG	0.822	0.909	0.863	0.906	0.934	0.847	0.93	0.911	0.182	0.184
5NN	0.864	0.811	0.742	0.919	0.881	0.873	0.913	0.899	0.288	0.295
YAO	0.874	0.75	0.698	0.895	0.866	0.875	0.924	0.919	0.244	0.228
GPA	0.907	0.795	0.68	0.904	0.855	0.836	0.907	0.907	0.601	0.598
ER	0.948	0.552	0.488	0.971	0.598	0.914	0.722	0.839	0.686	0.659
s =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.903	0.917	0.946	0.962	0.936	0.901	0.95	0.951	0.147	0.153
GG	0.956	0.758	0.747	0.943	0.887	0.893	0.944	0.894	0.196	0.194
5NN	0.947	0.64	0.631	0.936	0.802	0.865	0.934	0.916	0.297	0.314
YAO	0.952	0.592	0.619	0.928	0.794	0.881	0.904	0.9	0.257	0.244
GPA	0.931	0.694	0.685	0.937	0.787	0.858	0.898	0.882	0.6	0.622
ER	0.968	0.571	0.482	0.97	0.605	0.947	0.724	0.836	0.669	0.622

Table A.5: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 5$.

s =(1:25)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.767	0.81	0.097	0.943	0.835	0.963	0.098	0.993	0.885	0.939
GG	0.691	0.703	0.143	0.798	0.854	0.921	0.136	0.907	0.885	0.935
5NN	0.683	0.619	0.28	0.662	0.85	0.814	0.229	0.733	0.877	0.878
YAO	0.677	0.583	0.225	0.655	0.865	0.855	0.205	0.752	0.898	0.934
GPA	0.801	0.686	0.518	0.603	0.864	0.761	0.445	0.68	0.866	0.844
ER	0.733	0.552	0.709	0.439	0.792	0.666	0.695	0.561	0.84	0.784
s =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.829	0.88	0.096	0.947	0.952	0.957	0.08	0.95	0.946	0.914
GG	0.766	0.716	0.182	0.72	0.926	0.878	0.137	0.848	0.928	0.903
5NN	0.745	0.66	0.301	0.556	0.866	0.791	0.228	0.719	0.893	0.877
YAO	0.763	0.592	0.279	0.553	0.88	0.78	0.215	0.729	0.894	0.852
GPA	0.809	0.735	0.482	0.622	0.852	0.777	0.429	0.712	0.864	0.839
ER	0.742	0.542	0.672	0.42	0.785	0.681	0.694	0.594	0.848	0.783

Table A.6: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 6$.

s =(1:25)										
$m\|I_{max}$	1	2	3	4	5	6	7	8	9	10
RNG	0.706	0.825	0.725	0.84	0.905	0.84	0.769	0.042	0.932	0.72
GG	0.629	0.873	0.747	0.825	0.735	0.767	0.815	0.09	0.92	0.77
5NN	0.547	0.886	0.742	0.705	0.498	0.649	0.751	0.138	0.834	0.748
YAO	0.546	0.888	0.743	0.722	0.577	0.688	0.786	0.16	0.849	0.774
GPA	0.59	0.902	0.745	0.628	0.399	0.583	0.726	0.379	0.765	0.772
ER	0.597	0.922	0.704	0.555	0.287	0.484	0.829	0.635	0.641	0.809
s =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.772	0.892	0.762	0.84	0.83	0.839	0.748	0.049	0.895	0.87
GG	0.647	0.929	0.779	0.806	0.611	0.78	0.766	0.111	0.827	0.848
5NN	0.619	0.957	0.723	0.709	0.447	0.671	0.801	0.187	0.809	0.824
YAO	0.646	0.94	0.754	0.702	0.464	0.691	0.814	0.155	0.793	0.815
GPA	0.644	0.937	0.758	0.653	0.404	0.603	0.774	0.365	0.791	0.793
ER	0.588	0.931	0.721	0.574	0.297	0.513	0.802	0.606	0.628	0.818

Table A.7: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 7$.

s =(1:25)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.749	0.791	0.935	0.97	0.881	0.121	0.923	0.93	0.954	0.903
GG	0.689	0.803	0.903	0.77	0.876	0.135	0.923	0.909	0.957	0.907
5NN	0.613	0.742	0.773	0.647	0.859	0.241	0.927	0.895	0.93	0.923
YAO	0.624	0.711	0.741	0.622	0.881	0.243	0.934	0.913	0.933	0.897
GPA	0.756	0.763	0.729	0.633	0.865	0.481	0.876	0.88	0.909	0.864
ER	0.631	0.695	0.506	0.348	0.836	0.68	0.846	0.917	0.884	0.897
q =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.813	0.82	0.926	0.881	0.873	0.097	0.91	0.919	0.956	0.893
GG	0.684	0.783	0.756	0.686	0.847	0.166	0.922	0.914	0.912	0.855
5NN	0.622	0.735	0.586	0.52	0.845	0.267	0.91	0.903	0.919	0.872
YAO	0.621	0.722	0.6	0.524	0.855	0.225	0.897	0.902	0.913	0.907
GPA	0.714	0.743	0.75	0.6	0.833	0.54	0.897	0.889	0.91	0.883
ER	0.617	0.699	0.532	0.378	0.865	0.679	0.844	0.91	0.853	0.867

Table A.8: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 8$.

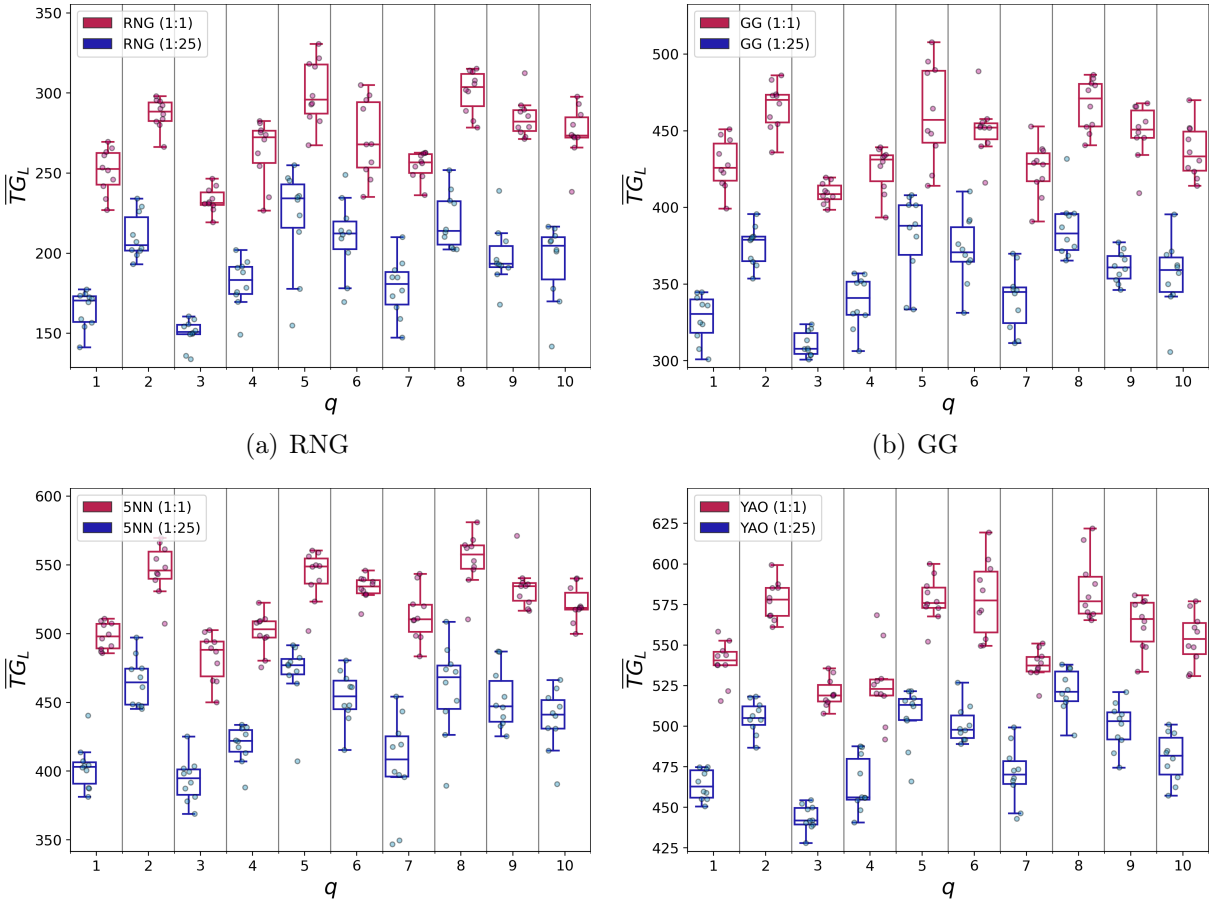
s =(1:25)										
$m\|I_{max}$	1	2	3	4	5	6	7	8	9	10
RNG	0.713	0.836	0.742	0.953	0.977	0.929	0.525	0.903	0.945	0.901
GG	0.669	0.649	0.75	0.742	0.913	0.888	0.575	0.718	0.915	0.813
5NN	0.619	0.591	0.735	0.526	0.79	0.835	0.662	0.521	0.888	0.628
YAO	0.614	0.568	0.761	0.536	0.807	0.871	0.657	0.591	0.889	0.714
GPA	0.637	0.576	0.754	0.478	0.729	0.788	0.766	0.486	0.842	0.572
ER	0.626	0.48	0.686	0.353	0.48	0.722	0.81	0.321	0.695	0.48
s =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.759	0.794	0.783	0.802	0.906	0.937	0.549	0.922	0.97	0.909
GG	0.633	0.644	0.81	0.594	0.863	0.885	0.602	0.692	0.927	0.82
5NN	0.611	0.555	0.768	0.494	0.747	0.857	0.675	0.524	0.871	0.656
YAO	0.596	0.54	0.746	0.481	0.752	0.866	0.626	0.497	0.853	0.711
GPA	0.615	0.572	0.749	0.463	0.713	0.829	0.783	0.503	0.804	0.598
ER	0.587	0.464	0.701	0.317	0.52	0.748	0.805	0.295	0.724	0.47

Table A.9: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 9$.

s =(1:25)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.691	0.945	0.853	0.839	0.926	0.797	0.928	0.868	0.083	0.063
GG	0.67	0.918	0.775	0.87	0.945	0.833	0.924	0.861	0.116	0.112
5NN	0.711	0.843	0.688	0.881	0.909	0.838	0.906	0.855	0.215	0.177
YAO	0.708	0.802	0.682	0.833	0.892	0.781	0.916	0.856	0.188	0.153
GPA	0.824	0.819	0.73	0.866	0.918	0.805	0.901	0.901	0.477	0.511
ER	0.815	0.776	0.61	0.797	0.832	0.864	0.842	0.88	0.676	0.64
s =(1:1)										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.883	0.891	0.875	0.921	0.919	0.869	0.904	0.916	0.094	0.079
GG	0.847	0.809	0.746	0.889	0.892	0.872	0.921	0.867	0.141	0.096
5NN	0.821	0.779	0.651	0.858	0.833	0.834	0.91	0.86	0.261	0.206
YAO	0.836	0.75	0.629	0.855	0.85	0.831	0.887	0.878	0.211	0.177
GPA	0.883	0.802	0.735	0.884	0.877	0.828	0.91	0.883	0.561	0.483
ER	0.796	0.746	0.573	0.796	0.819	0.858	0.862	0.871	0.645	0.654

Table A.10: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks with logical network version $q = 10$.

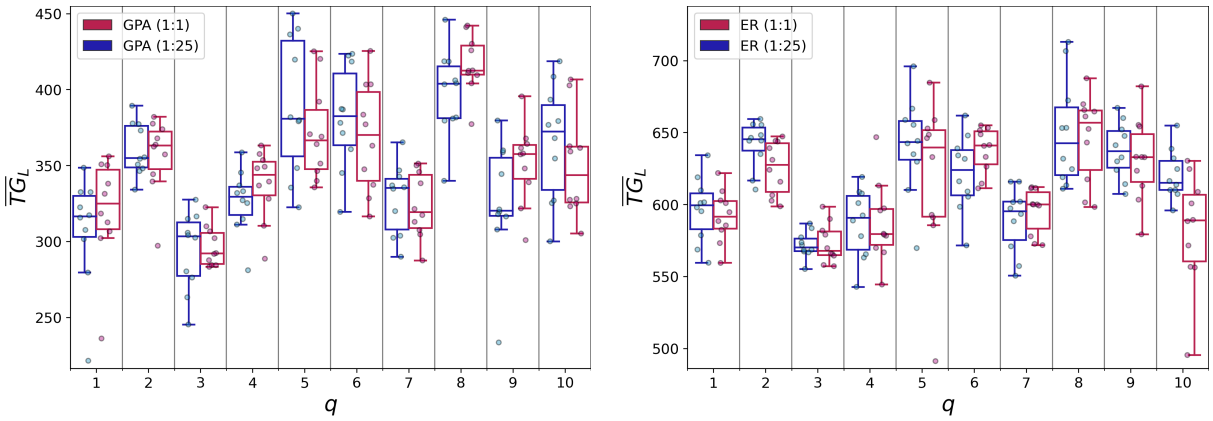
A.3 Space shape effect figures



(a) RNG (b) GG

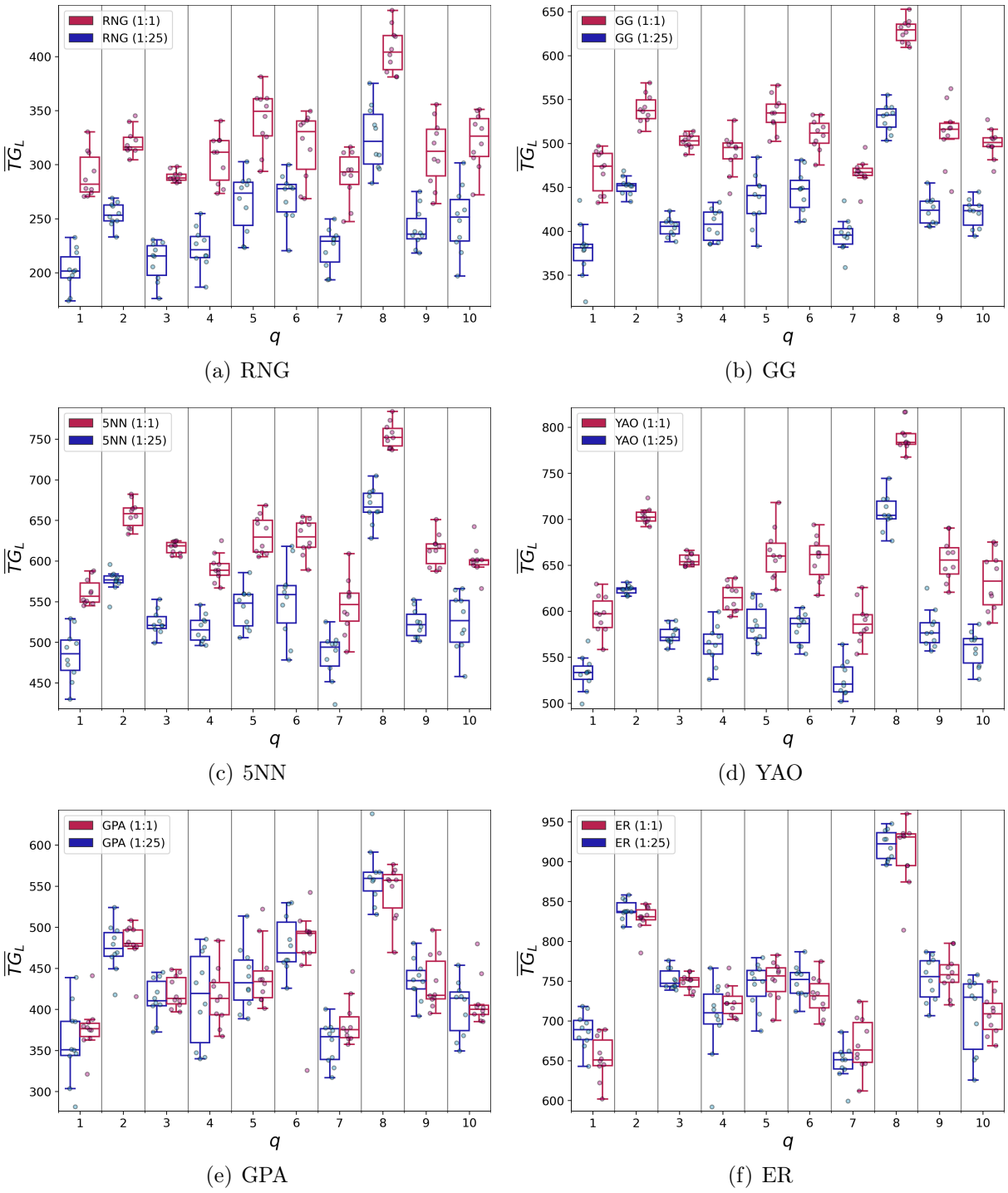
(c) 5NN (d) YAO

Figure A.27: $\overline{TG}_L$ values obtained for physical-logical interdependent networks with $I_{max} = 1$ and $m \in \{\text{RNG,GG,5NN,YAO}\}$, versus the logical network version q used to build the system.



(a) GPA (b) ER

Figure A.28: $\overline{TG}_L$ values obtained physical-logical interdependent networks with $I_{max} = 1$ and $m \in \{\text{GPA,ER}\}$, versus the logical network version q used to build the system.

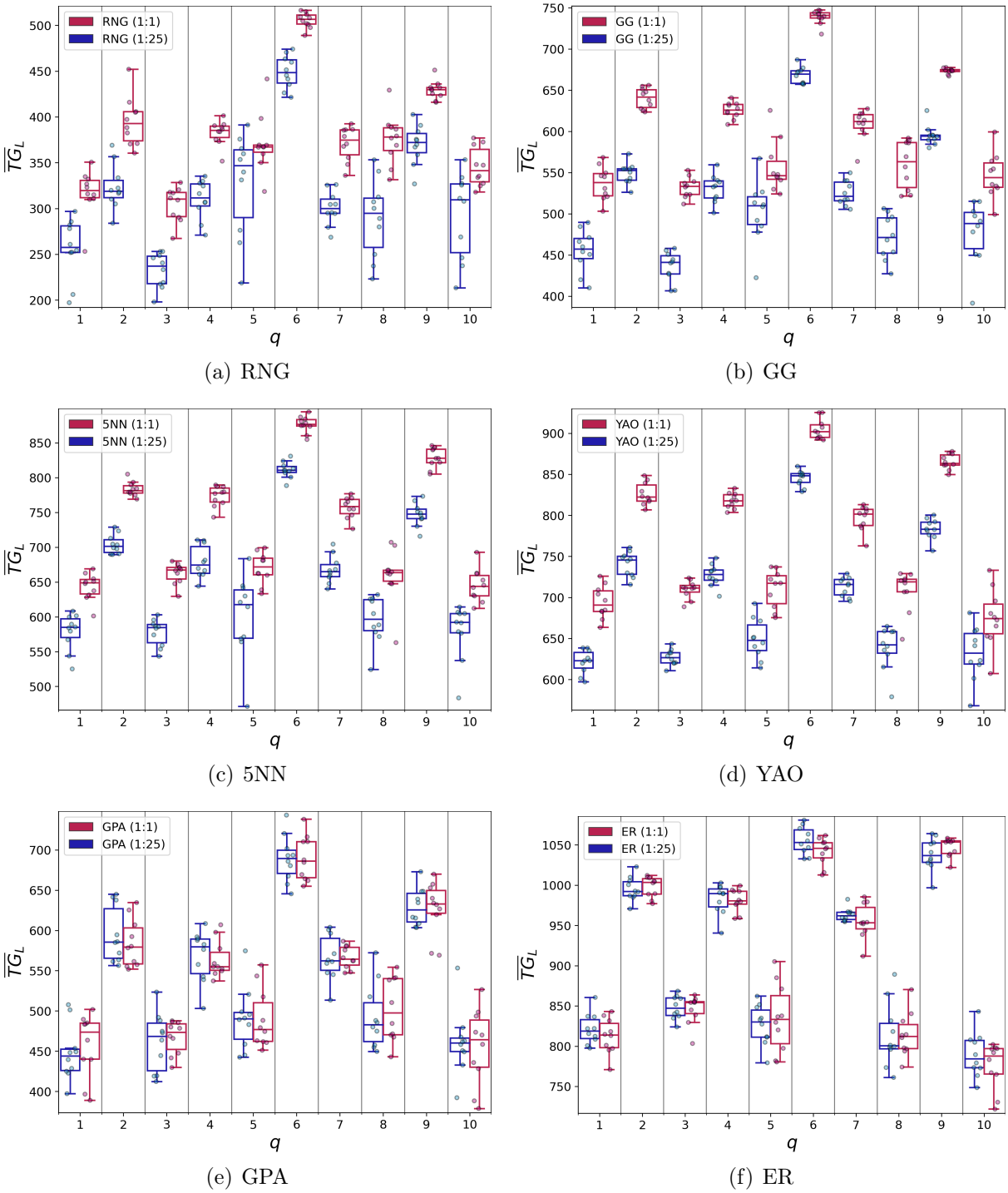


(a) RNG (b) GG

(c) 5NN (d) YAO

(e) GPA (f) ER

Figure A.29: $\overline{TG}_L$ values obtained for each physical-logical interdependent network for $I_{max} = 2$, versus the logical network version q used to build the system.

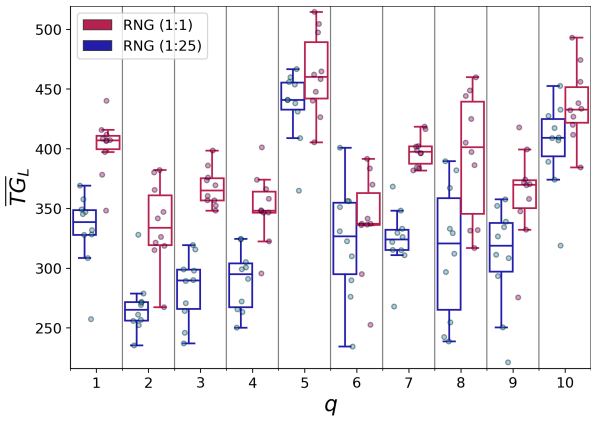


(a) RNG (b) GG

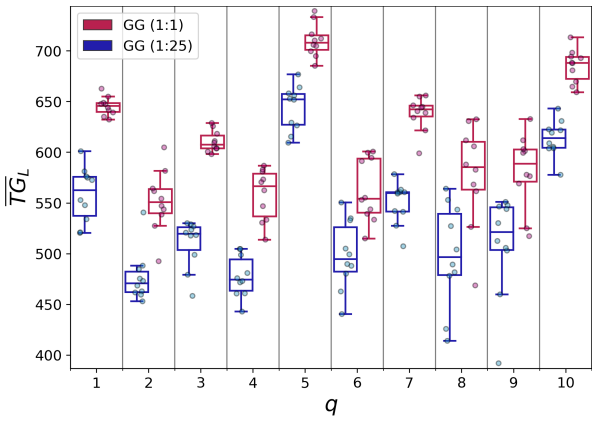
(c) 5NN (d) YAO

(e) GPA (f) ER

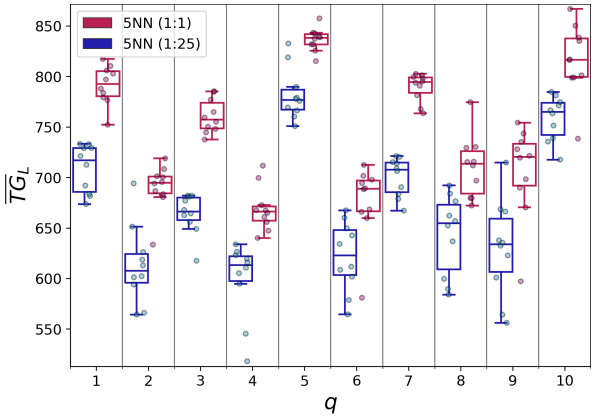
Figure A.30: $\overline{TG}_L$ values obtained for each physical-logical interdependent network for $I_{max} = 3$, versus the logical network version q used to build the system.



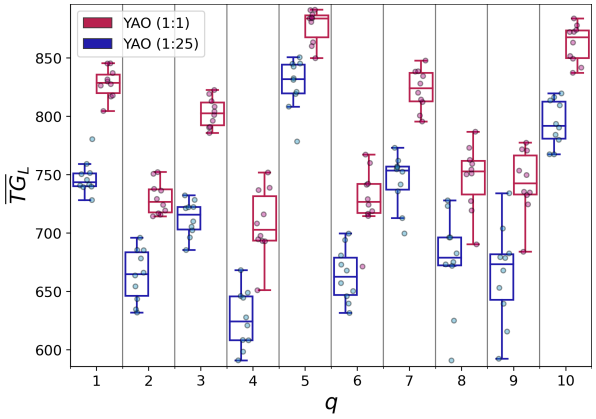
(a) RNG



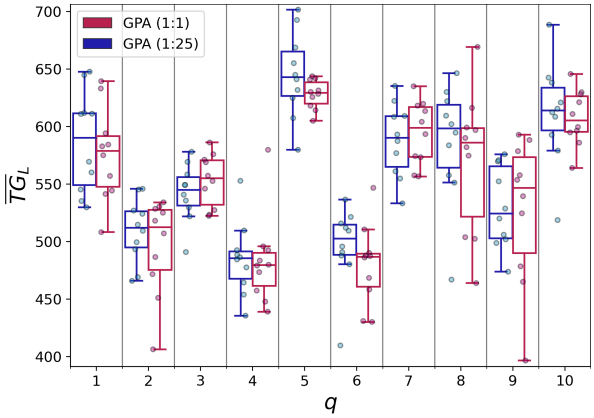
(b) GG



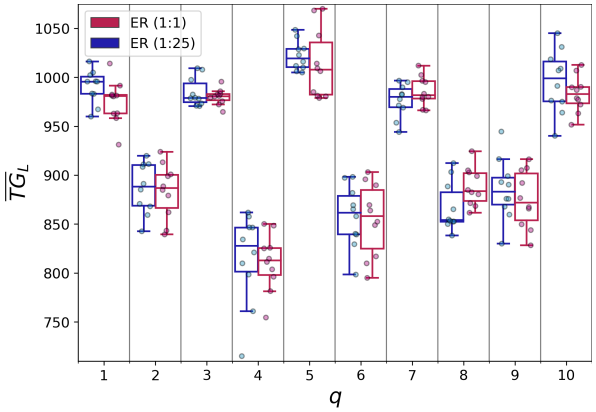
(c) 5NN



(d) YAO

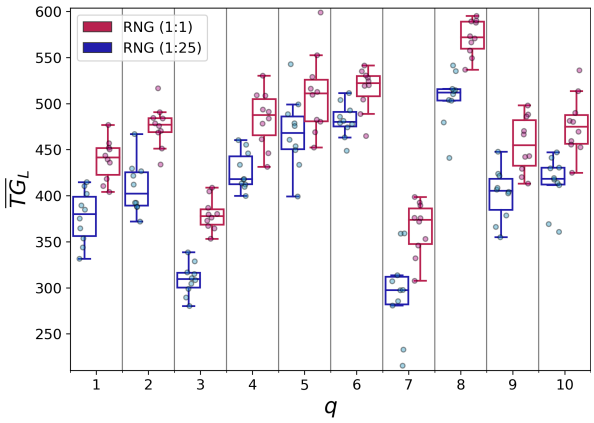


(e) GPA

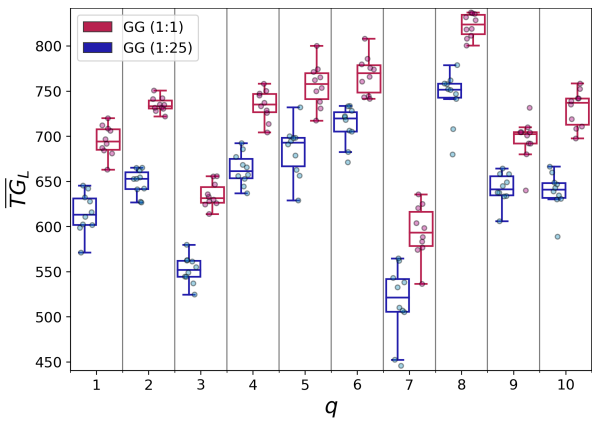


(f) ER

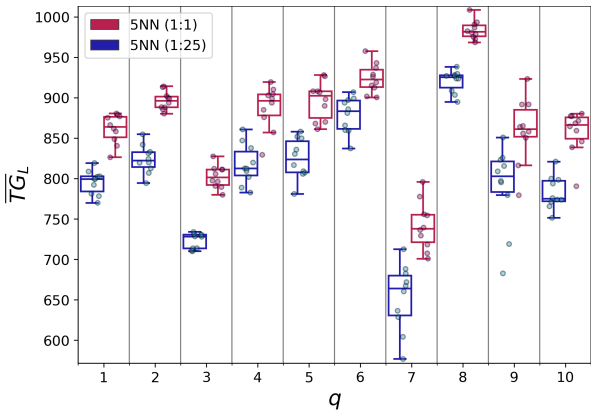
Figure A.31: $\overline{TG}_L$ values obtained for each physical-logical interdependent network for $I_{max} = 4$, versus the logical network version q used to build the system.



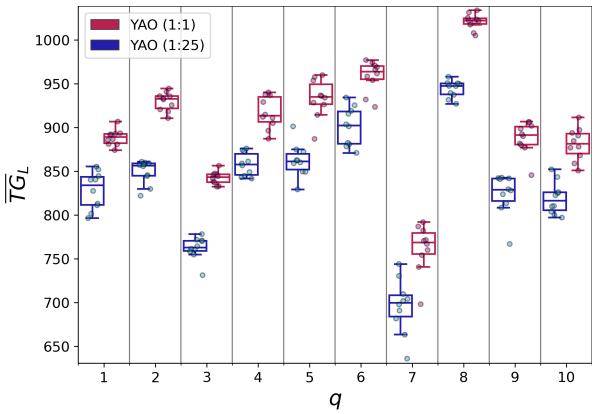
(a) RNG



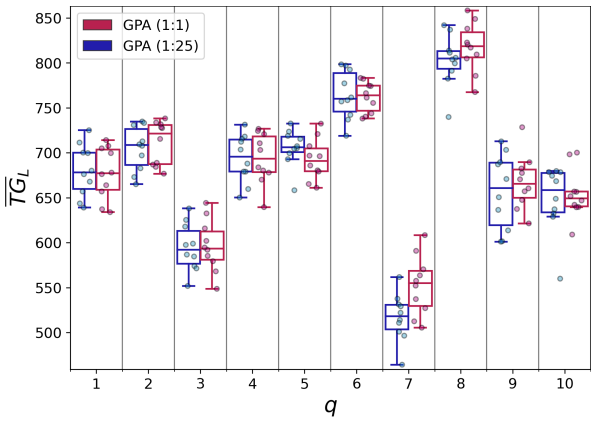
(b) GG



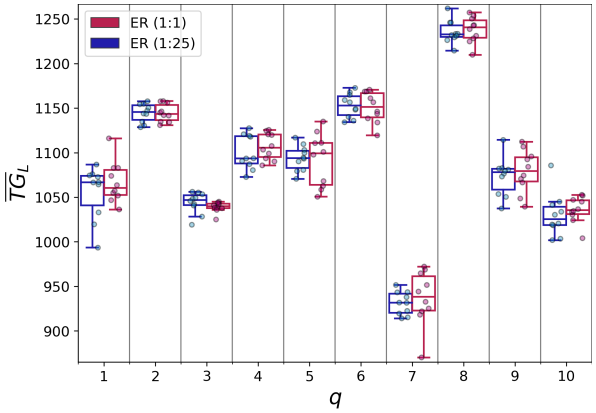
(c) 5NN



(d) YAO

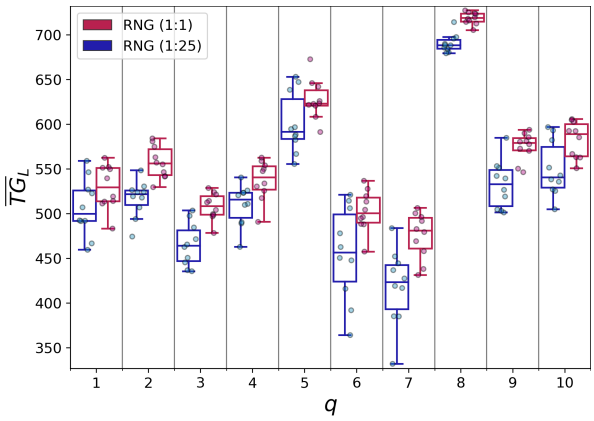


(e) GPA

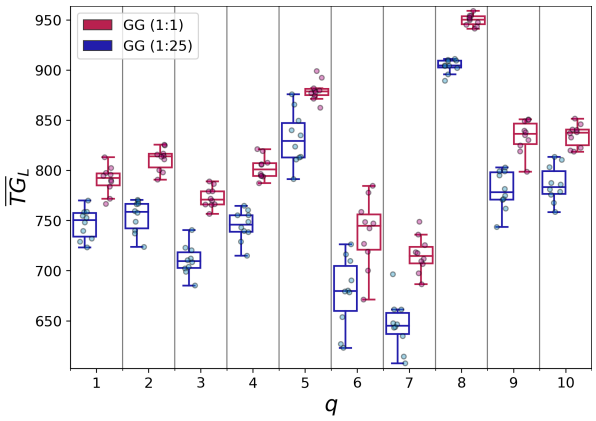


(f) ER

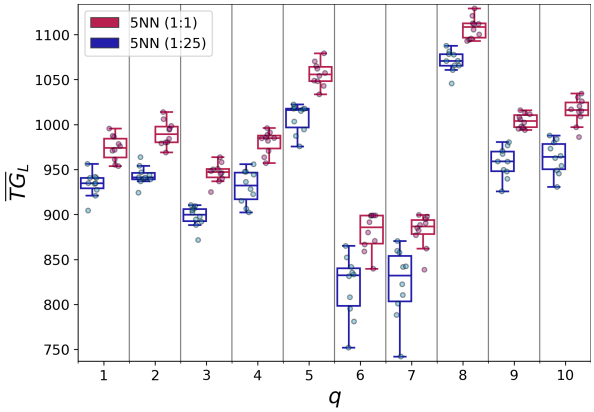
Figure A.32: $\overline{TG}_L$ values obtained for each physical-logical interdependent network for $I_{max} = 5$, versus the logical network version q used to build the system.



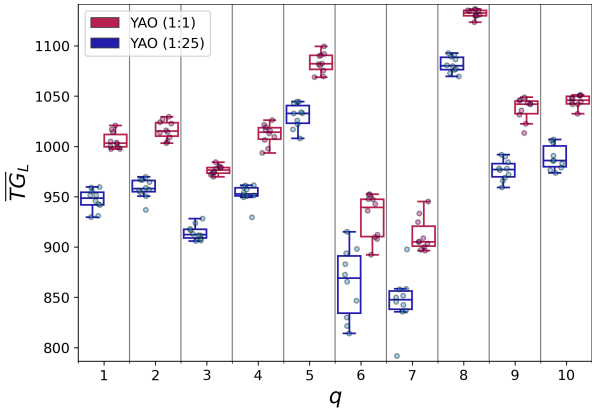
(a) RNG



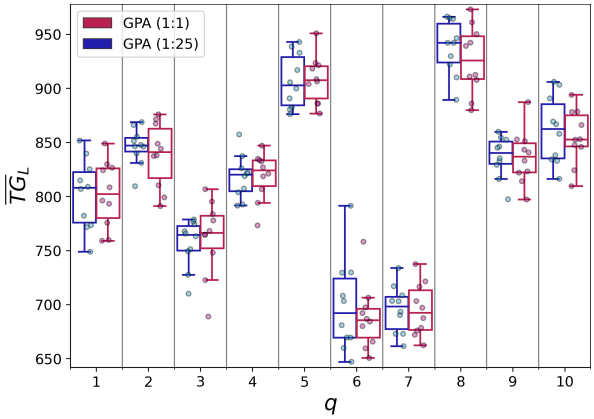
(b) GG



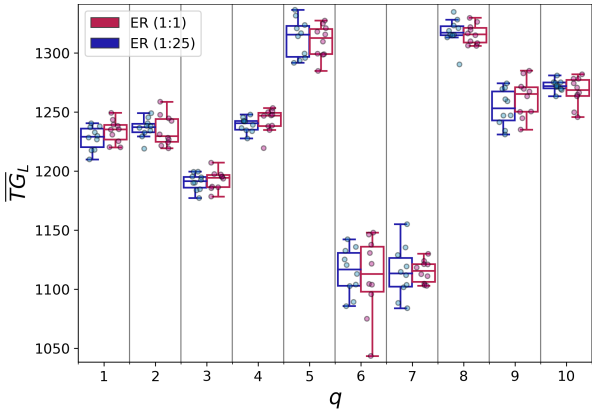
(c) 5NN



(d) YAO

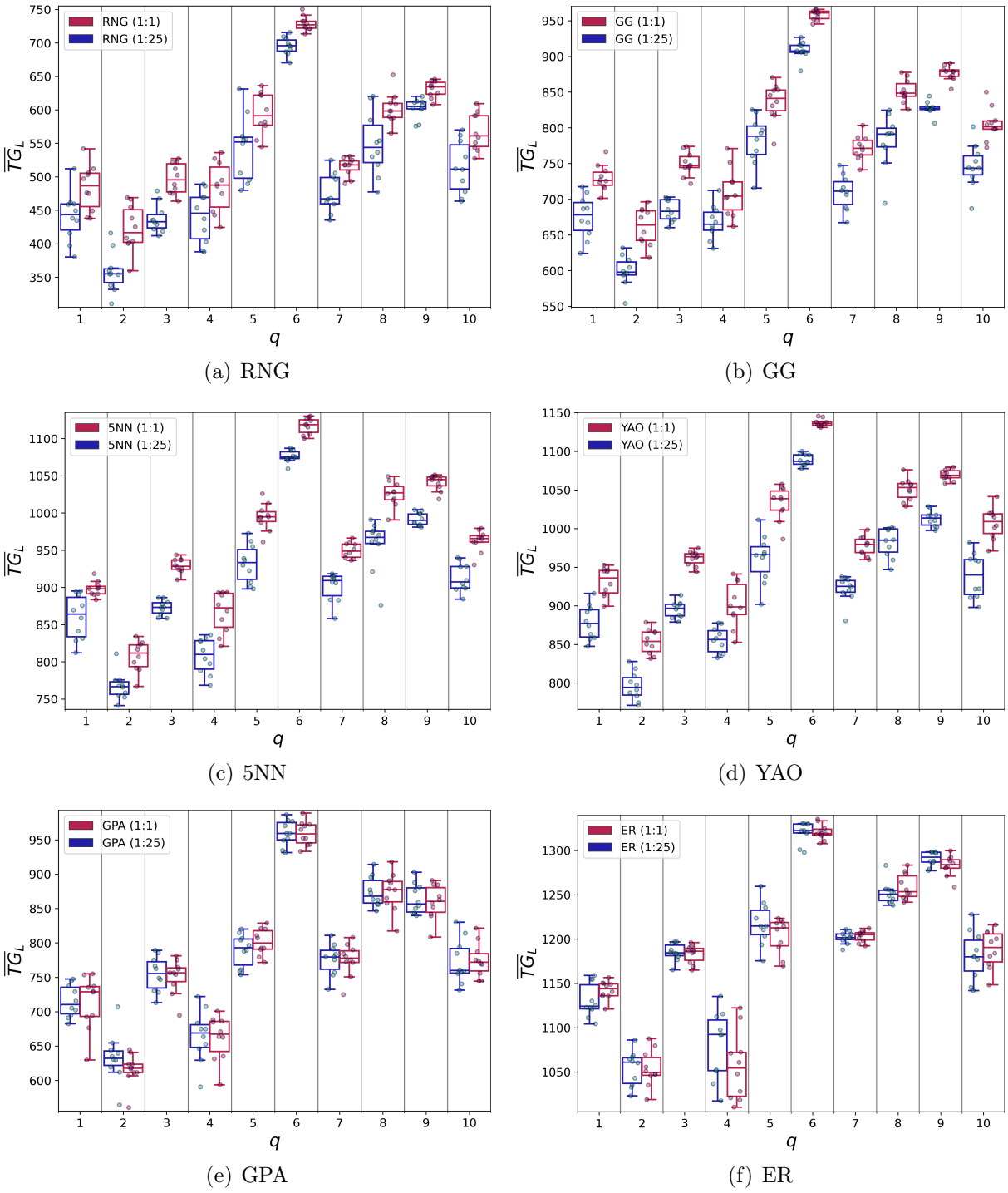


(e) GPA



(f) ER

Figure A.33: $\overline{TG}_L$ values obtained for each physical-logical interdependent network for $I_{max} = 6$, versus the logical network version q used to build the system.

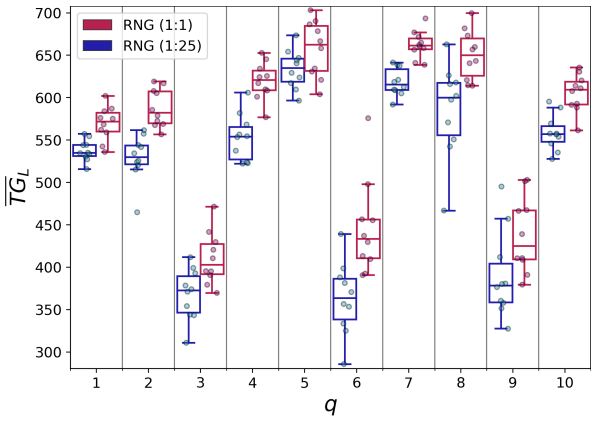


(a) RNG (b) GG

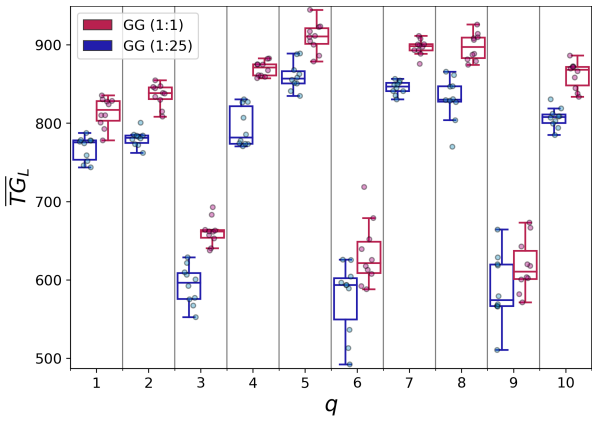
(c) 5NN (d) YAO

(e) GPA (f) ER

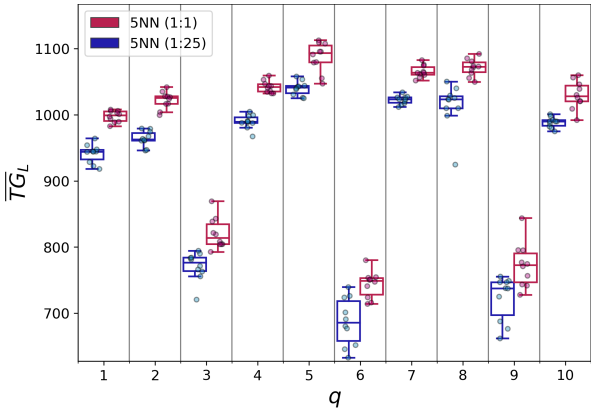
Figure A.34: $\overline{TG}_L$ values obtained for each physical-logical interdependent network for $I_{max} = 7$, versus the logical network version q used to build the system.



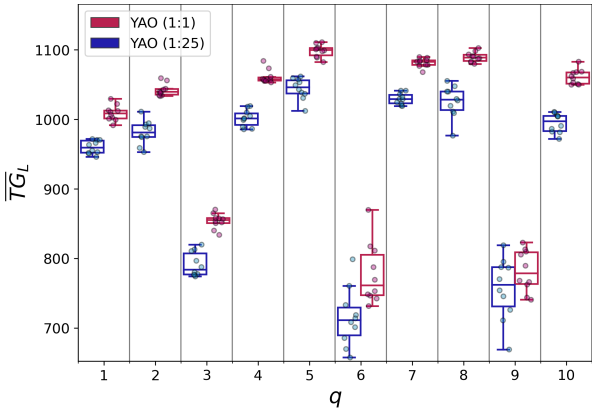
(a) RNG



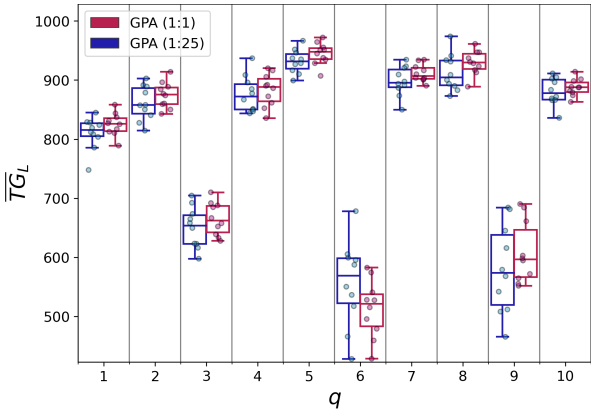
(b) GG



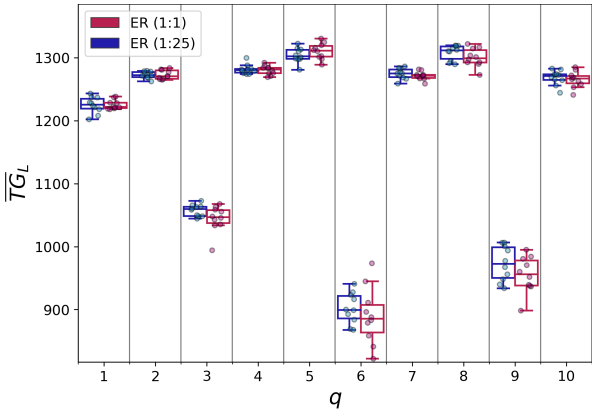
(c) 5NN



(d) YAO

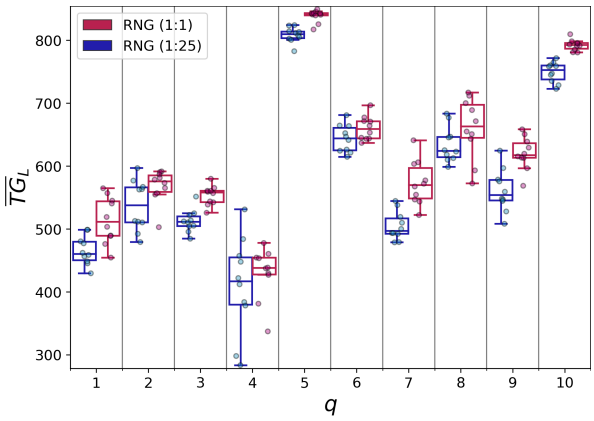


(e) GPA

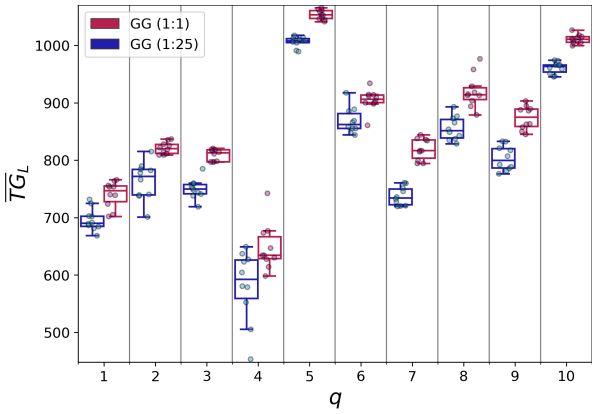


(f) ER

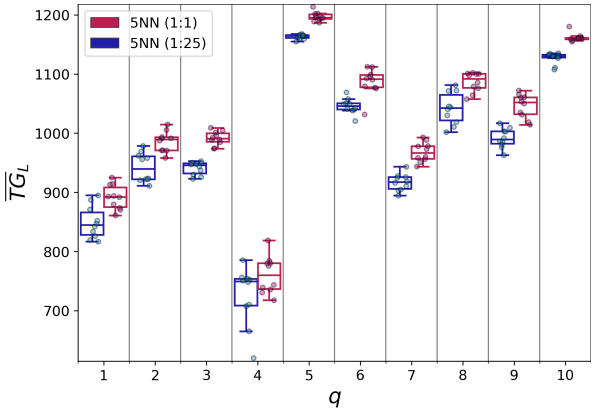
Figure A.35: $\overline{TG}_L$ values obtained for each physical-logical interdependent network for $I_{max} = 8$, versus the logical network version q used to build the system.



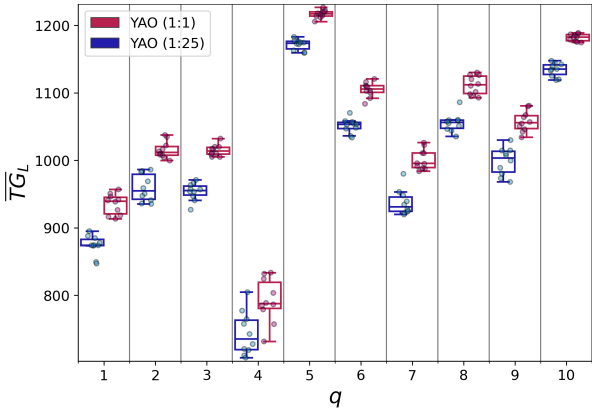
(a) RNG



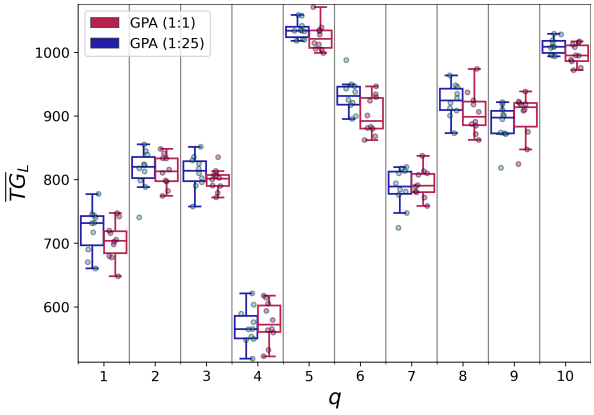
(b) GG



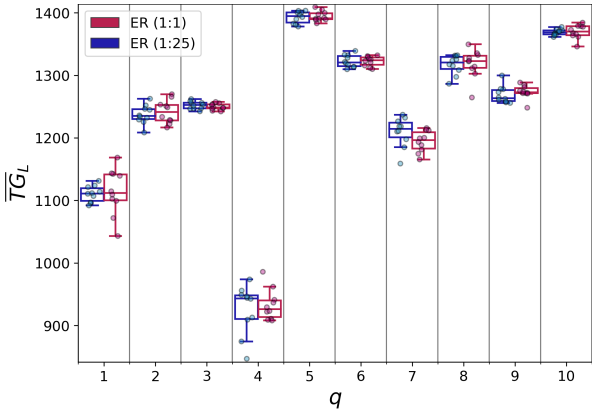
(c) 5NN



(d) YAO

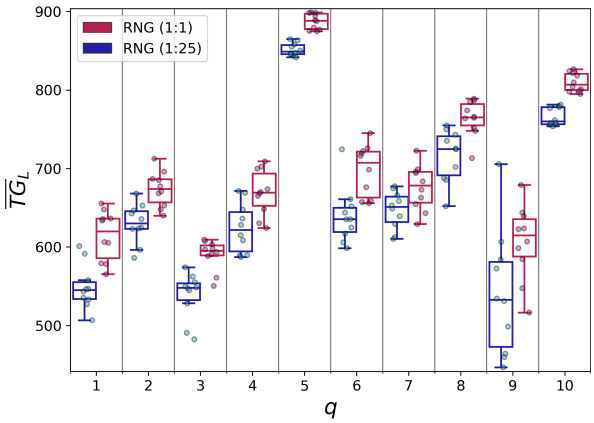


(e) GPA

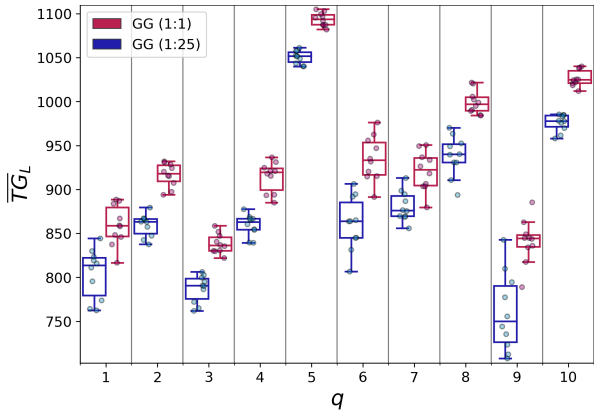


(f) ER

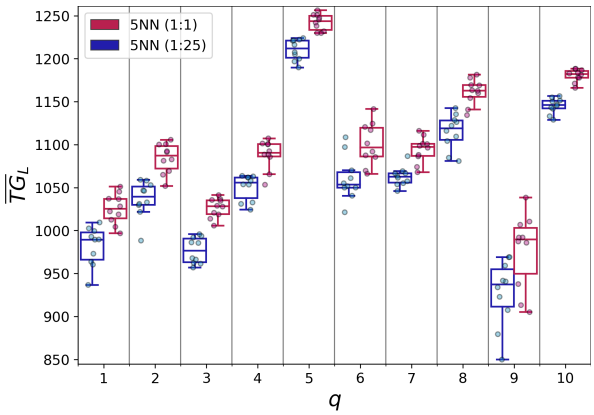
Figure A.36: $\overline{TG}_L$ values obtained for each physical-logical interdependent network for $I_{max} = 9$, versus the logical network version q used to build the system.



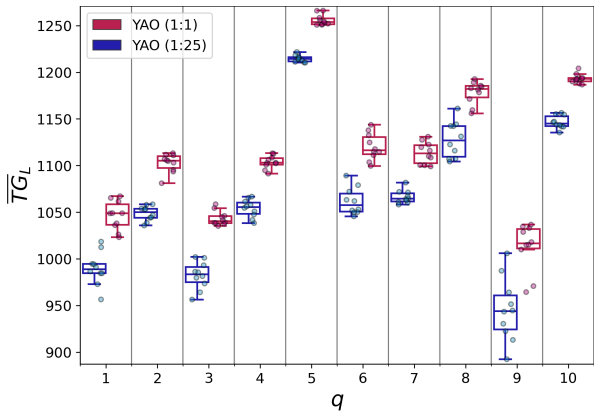
(a) RNG



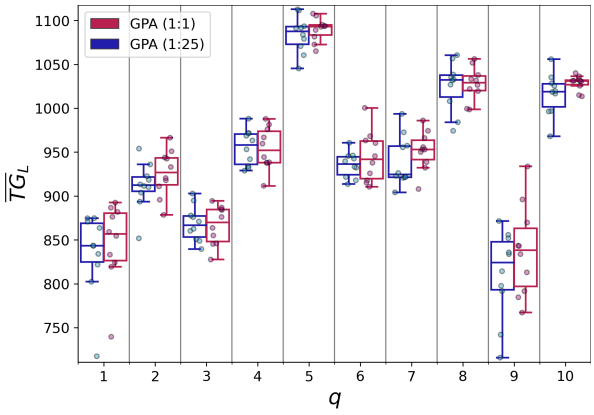
(b) GG



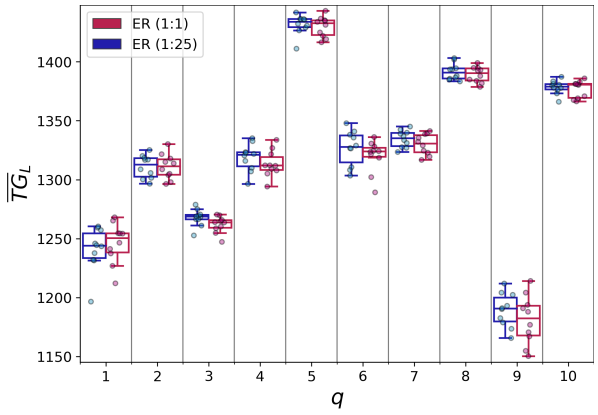
(c) 5NN



(d) YAO



(e) GPA



(f) ER

Figure A.37: $\overline{TG_L}$ values obtained for each physical-logical interdependent network for $I_{max} = 10$, versus the logical network version q used to build the system.

A.4 Average $\overline{TG}_L$ tables

$I_{max} = 1$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	164.83 (11.07)	307.93 (33.96)	327.53 (14.72)	402.73 (15.78)	463.75 (8.68)	596.58 (21.47)
	(1:1)	251.2 (13.4)	320.25 (33.47)	427.98 (15.56)	498.08 (9.26)	539.36 (12.29)	591.88 (17.19)
2	(1:25)	210.51 (13.43)	360.64 (16.66)	374.82 (12.18)	464.89 (17.09)	505.23 (9.48)	641.57 (15.57)
	(1:1)	286.89 (8.95)	356.58 (23.6)	465.68 (14.59)	546.24 (17.52)	577.5 (11.38)	625.31 (17.52)
3	(1:25)	149.85 (8.37)	293.65 (24.88)	310.71 (7.65)	393.41 (15.08)	443.33 (7.53)	571.96 (8.6)
	(1:1)	233.08 (7.39)	296.55 (12.57)	409.24 (6.51)	482.64 (16.56)	520.42 (8.44)	573.04 (13.1)
4	(1:25)	181.3 (14.53)	326.52 (20.01)	338.42 (16.34)	419.14 (13.16)	463.82 (16.05)	586.74 (22.86)
	(1:1)	263.78 (18.47)	337.52 (21.89)	424.88 (14.18)	500.63 (13.56)	525.57 (21.72)	587.14 (26.74)
5	(1:25)	221.95 (30.48)	389.31 (43.23)	380.66 (26.46)	470.95 (22.79)	505.88 (17.06)	640.79 (32.26)
	(1:1)	300.56 (19.22)	371.43 (30.11)	461.65 (30.68)	542.13 (17.29)	578.03 (12.94)	618.44 (52.65)
6	(1:25)	209.99 (22.44)	381.32 (32.52)	372.07 (21.19)	453.55 (18.04)	501.11 (11.02)	621.52 (25.22)
	(1:1)	271.46 (23.17)	368.56 (34.25)	450.78 (17.09)	533.22 (8.26)	578.61 (22.74)	637.58 (15.04)
7	(1:25)	178.41 (17.22)	327.83 (22.13)	339.99 (19.3)	404.92 (33.77)	470.41 (16.86)	589.33 (21.62)
	(1:1)	254.8 (8.05)	323.69 (20.62)	424.64 (16.64)	513.41 (17.79)	537.81 (8.7)	595.68 (15.0)
8	(1:25)	220.1 (16.57)	397.88 (27.47)	386.31 (18.66)	459.41 (32.12)	521.81 (12.71)	649.79 (35.32)
	(1:1)	300.77 (12.62)	416.6 (18.27)	466.69 (15.96)	553.55 (18.43)	584.31 (19.04)	646.16 (28.95)
9	(1:25)	197.83 (17.71)	325.92 (38.13)	361.08 (9.67)	452.23 (20.81)	499.92 (13.61)	637.64 (18.53)
	(1:1)	284.42 (11.6)	351.4 (24.81)	449.01 (16.74)	533.67 (14.71)	563.28 (14.54)	630.96 (27.49)
10	(1:25)	194.91 (23.01)	365.15 (36.42)	355.59 (22.27)	437.52 (21.25)	480.42 (14.11)	620.38 (16.5)
	(1:1)	275.21 (15.66)	350.18 (32.73)	436.47 (16.66)	521.16 (12.36)	553.75 (15.12)	582.24 (37.71)

Table A.11: Average $\overline{TG}_L$ results for $I_{max} = 1$, standard deviation in parenthesis. Variable q indicates the logical network version used. Averages were obtained across the 10 physical network instances for a given space and physical model.

$I_{max} = 2$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	202.29 (17.89)	359.78 (45.08)	378.51 (29.48)	484.42 (30.19)	532.64 (17.85)	687.58 (21.5)
	(1:1)	290.41 (19.84)	376.78 (27.84)	468.93 (22.61)	561.79 (15.35)	596.08 (19.78)	653.17 (26.63)
2	(1:25)	253.93 (10.42)	475.21 (27.84)	451.44 (9.5)	575.33 (12.83)	623.23 (4.49)	839.48 (11.49)
	(1:1)	321.22 (12.01)	480.56 (24.36)	539.4 (15.67)	657.37 (15.65)	703.83 (8.33)	828.69 (16.45)
3	(1:25)	210.46 (17.1)	412.54 (23.59)	404.5 (10.08)	524.36 (14.47)	574.39 (9.49)	752.27 (12.11)
	(1:1)	289.17 (4.81)	420.63 (18.38)	502.52 (7.55)	616.24 (7.08)	655.56 (6.09)	749.14 (9.43)
4	(1:25)	223.09 (18.16)	414.03 (53.83)	407.28 (17.09)	516.42 (16.18)	563.3 (20.41)	703.35 (46.6)
	(1:1)	305.94 (21.47)	415.2 (33.57)	489.22 (22.04)	591.1 (16.2)	614.75 (14.48)	723.88 (18.85)
5	(1:25)	264.66 (26.12)	437.72 (36.68)	435.76 (28.43)	542.22 (24.18)	585.45 (20.78)	744.37 (27.41)
	(1:1)	341.55 (26.35)	441.78 (36.64)	533.9 (19.32)	631.97 (22.29)	662.52 (26.43)	751.16 (23.14)
6	(1:25)	269.84 (21.58)	478.88 (33.13)	444.94 (23.39)	551.54 (44.05)	581.02 (15.97)	749.19 (20.36)
	(1:1)	317.5 (29.17)	474.18 (54.62)	510.13 (17.22)	628.82 (20.61)	657.06 (22.44)	731.01 (23.0)
7	(1:25)	222.56 (18.07)	358.84 (24.9)	395.65 (18.89)	483.57 (27.84)	526.51 (18.2)	648.1 (21.5)
	(1:1)	289.19 (21.98)	384.33 (26.7)	467.01 (14.48)	545.05 (32.85)	588.32 (20.85)	670.03 (32.15)
8	(1:25)	324.51 (28.49)	561.74 (32.92)	528.84 (15.07)	668.06 (21.1)	707.4 (18.34)	920.56 (17.77)
	(1:1)	406.32 (20.29)	542.85 (32.09)	628.26 (12.62)	754.62 (14.87)	789.56 (15.01)	910.42 (40.22)
9	(1:25)	240.88 (17.68)	435.49 (23.96)	423.73 (15.49)	523.33 (16.7)	580.45 (19.61)	752.52 (26.58)
	(1:1)	311.65 (29.25)	432.62 (31.59)	511.52 (32.89)	613.81 (18.85)	656.1 (22.59)	759.26 (24.41)
10	(1:25)	249.1 (29.52)	402.12 (32.17)	420.54 (15.43)	524.59 (33.56)	558.93 (18.06)	708.42 (45.95)
	(1:1)	322.31 (24.3)	409.05 (28.21)	499.99 (15.78)	600.91 (17.81)	632.89 (29.94)	707.6 (24.13)

Table A.12: Average $\overline{TG}_L$ results for $I_{max} = 2$, standard deviation in parenthesis. Variable q indicates the logical network version used. Averages were obtained across the 10 physical network instances for a given space and physical model.

$I_{max} = 3$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	256.55 (31.17)	447.33 (32.6)	455.07 (24.21)	578.39 (25.02)	621.42 (13.73)	821.26 (18.12)
	(1:1)	317.2 (24.44)	457.31 (37.63)	536.91 (19.43)	643.34 (18.63)	694.08 (19.04)	812.3 (20.94)
2	(1:25)	323.51 (23.32)	594.27 (32.84)	549.32 (12.01)	703.99 (13.17)	740.46 (14.35)	995.28 (14.06)
	(1:1)	394.88 (25.46)	584.35 (28.25)	640.37 (11.79)	783.58 (9.74)	826.11 (12.95)	997.92 (12.19)
3	(1:25)	232.38 (18.13)	461.01 (34.74)	435.92 (17.54)	577.37 (18.43)	626.92 (9.15)	848.05 (13.66)
	(1:1)	304.29 (17.97)	467.13 (19.62)	532.26 (11.9)	662.3 (14.48)	709.53 (10.45)	845.78 (17.08)
4	(1:25)	310.1 (20.03)	567.9 (30.27)	530.5 (15.93)	679.03 (21.98)	727.06 (12.68)	982.54 (17.82)
	(1:1)	382.69 (12.81)	563.68 (21.71)	625.65 (9.37)	773.28 (13.95)	817.97 (8.83)	981.1 (13.28)
5	(1:25)	327.44 (53.26)	489.94 (36.75)	502.79 (35.86)	601.04 (56.5)	649.54 (23.39)	826.43 (23.74)
	(1:1)	370.81 (30.1)	489.67 (35.15)	556.94 (29.49)	669.93 (21.32)	710.49 (21.65)	834.47 (40.27)
6	(1:25)	448.87 (17.16)	688.81 (27.49)	668.26 (9.49)	811.13 (11.1)	845.07 (9.18)	1055.35 (16.14)
	(1:1)	505.45 (8.0)	689.71 (26.36)	738.85 (8.22)	876.37 (11.22)	904.87 (11.7)	1041.73 (16.06)
7	(1:25)	300.62 (17.31)	566.18 (26.87)	525.37 (14.14)	667.8 (18.62)	712.94 (11.03)	963.15 (7.8)
	(1:1)	370.71 (17.8)	566.47 (13.25)	608.52 (17.29)	756.89 (14.54)	796.28 (14.53)	954.98 (20.89)
8	(1:25)	289.33 (40.52)	492.39 (38.22)	471.68 (25.94)	595.9 (31.77)	638.6 (24.66)	813.46 (37.36)
	(1:1)	375.55 (25.92)	502.16 (37.57)	559.6 (27.46)	659.11 (37.25)	708.28 (23.79)	814.29 (25.94)
9	(1:25)	369.78 (20.53)	629.09 (22.01)	595.23 (11.62)	747.03 (15.85)	783.38 (12.01)	1038.47 (19.22)
	(1:1)	429.24 (9.58)	627.28 (31.85)	673.47 (3.17)	828.27 (13.7)	865.21 (8.83)	1046.99 (11.08)
10	(1:25)	292.5 (45.01)	460.77 (38.3)	477.74 (36.04)	579.01 (38.09)	632.16 (31.17)	789.27 (26.18)
	(1:1)	345.43 (20.24)	455.22 (45.2)	546.58 (26.05)	645.23 (22.38)	674.94 (33.51)	775.26 (27.44)

Table A.13: Average $\overline{TG}_L$ results for $I_{max} = 3$, standard deviation in parenthesis. Variable q indicates the logical network version used. Averages were obtained across the 10 physical network instances for a given space and physical model.

$I_{max} = 4$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	332.13 (29.83)	586.43 (41.86)	558.14 (25.86)	708.9 (22.5)	747.63 (13.52)	990.42 (16.36)
	(1:1)	401.97 (23.1)	575.79 (38.58)	645.27 (8.64)	791.28 (18.39)	828.19 (12.16)	974.69 (21.08)
2	(1:25)	267.91 (23.2)	509.21 (26.55)	476.72 (23.73)	613.1 (36.67)	663.86 (21.35)	886.77 (24.67)
	(1:1)	336.46 (32.98)	495.71 (39.86)	551.54 (28.85)	690.23 (21.88)	729.64 (13.38)	883.43 (26.68)
3	(1:25)	282.8 (26.39)	542.12 (23.71)	510.23 (22.82)	663.95 (18.89)	712.53 (14.37)	984.78 (13.93)
	(1:1)	367.74 (15.13)	552.93 (21.79)	610.46 (9.97)	760.66 (16.03)	803.11 (11.94)	980.0 (7.8)
4	(1:25)	289.48 (24.49)	484.37 (30.27)	477.34 (19.36)	599.26 (35.89)	626.17 (23.88)	815.21 (44.3)
	(1:1)	350.64 (26.96)	482.63 (36.83)	558.08 (24.1)	668.77 (20.8)	708.07 (27.84)	811.12 (27.75)
5	(1:25)	436.04 (28.46)	644.61 (35.22)	643.9 (21.19)	782.04 (24.3)	827.35 (20.75)	1022.05 (14.28)
	(1:1)	462.1 (33.16)	627.76 (12.05)	710.06 (15.63)	836.31 (10.76)	877.53 (13.69)	1013.63 (33.56)
6	(1:25)	322.72 (45.23)	495.75 (33.03)	498.35 (32.27)	621.91 (32.78)	663.91 (21.8)	857.72 (29.92)
	(1:1)	338.02 (38.9)	479.47 (33.38)	562.53 (29.68)	675.88 (35.48)	728.49 (25.62)	854.53 (35.5)
7	(1:25)	323.54 (24.8)	587.99 (30.42)	550.01 (19.65)	700.58 (18.14)	744.48 (21.65)	976.21 (16.3)
	(1:1)	397.94 (12.04)	594.4 (26.37)	637.93 (16.04)	789.39 (13.2)	822.97 (16.42)	985.98 (14.3)
8	(1:25)	314.47 (53.29)	586.23 (48.96)	498.05 (48.3)	643.42 (37.56)	676.18 (39.59)	867.07 (23.87)
	(1:1)	394.59 (49.73)	569.66 (58.59)	577.58 (47.7)	710.53 (29.09)	747.4 (26.65)	888.06 (18.49)
9	(1:25)	309.34 (41.8)	529.61 (33.85)	509.2 (47.43)	629.89 (45.56)	664.64 (39.39)	885.24 (29.93)
	(1:1)	361.55 (36.73)	527.34 (59.82)	581.33 (34.96)	705.77 (43.49)	743.36 (26.44)	875.25 (28.07)
10	(1:25)	403.68 (35.12)	611.51 (42.11)	613.62 (17.04)	758.53 (20.84)	794.14 (18.7)	995.73 (30.7)
	(1:1)	436.96 (29.56)	607.48 (22.98)	684.79 (15.73)	816.1 (33.84)	862.3 (15.42)	982.92 (17.65)

Table A.14: Average $\overline{TG}_L$ results for $I_{max} = 4$, standard deviation in parenthesis. Variable q indicates the logical network version used. Averages were obtained across the 10 physical network instances for a given space and physical model.

$I_{max} = 5$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	376.92 (26.95)	679.97 (27.39)	614.65 (21.6)	795.38 (14.25)	828.23 (20.28)	1055.31 (28.33)
	(1:1)	438.67 (21.34)	677.22 (27.62)	694.89 (16.23)	861.36 (17.21)	888.48 (8.59)	1066.59 (21.9)
2	(1:25)	408.83 (26.6)	704.61 (23.69)	648.84 (13.47)	823.87 (16.54)	849.26 (12.96)	1144.5 (9.84)
	(1:1)	475.28 (21.15)	711.11 (22.87)	734.63 (7.73)	896.41 (10.77)	929.73 (10.13)	1144.58 (9.46)
3	(1:25)	308.98 (16.41)	594.58 (25.22)	551.96 (14.78)	723.11 (9.13)	762.18 (12.31)	1043.82 (11.37)
	(1:1)	379.3 (16.32)	596.24 (27.42)	634.71 (13.08)	802.16 (13.27)	842.35 (7.0)	1039.02 (5.47)
4	(1:25)	426.49 (19.84)	693.61 (25.37)	663.51 (16.81)	817.32 (23.59)	857.85 (12.51)	1100.24 (18.23)
	(1:1)	483.24 (28.76)	693.66 (26.73)	734.2 (15.97)	887.69 (25.83)	916.98 (17.4)	1106.96 (14.11)
5	(1:25)	468.04 (36.99)	705.76 (19.4)	683.9 (27.21)	824.6 (23.53)	862.09 (17.91)	1093.7 (13.55)
	(1:1)	510.19 (40.95)	692.51 (21.79)	756.14 (22.64)	896.49 (22.53)	933.37 (20.78)	1091.83 (28.19)
6	(1:25)	481.69 (17.36)	763.99 (25.67)	712.02 (20.05)	878.62 (21.12)	901.18 (20.97)	1152.77 (12.81)
	(1:1)	515.52 (22.26)	761.91 (16.17)	767.72 (20.22)	924.13 (17.27)	958.63 (16.92)	1150.67 (16.33)
7	(1:25)	294.73 (43.78)	516.8 (25.12)	515.99 (38.99)	652.91 (39.17)	695.97 (29.48)	931.06 (12.32)
	(1:1)	364.16 (27.65)	552.5 (31.24)	594.07 (27.69)	741.56 (28.55)	762.27 (25.89)	936.95 (29.1)
8	(1:25)	505.77 (27.01)	802.59 (27.24)	743.48 (27.35)	920.44 (12.87)	943.88 (9.19)	1235.3 (12.33)
	(1:1)	571.54 (18.47)	817.23 (26.17)	822.52 (12.44)	983.73 (11.12)	1020.93 (8.61)	1237.91 (13.89)
9	(1:25)	401.34 (26.6)	656.63 (39.91)	642.14 (16.0)	789.78 (48.82)	823.78 (22.24)	1073.03 (20.39)
	(1:1)	455.57 (28.63)	667.2 (28.47)	695.81 (22.62)	859.57 (38.17)	887.92 (17.36)	1079.06 (22.6)
10	(1:25)	413.95 (26.92)	648.65 (35.28)	638.59 (20.1)	782.51 (19.34)	819.04 (17.38)	1029.95 (23.01)
	(1:1)	476.18 (30.26)	654.02 (25.96)	730.28 (19.26)	857.34 (25.76)	881.03 (17.47)	1035.97 (13.9)

Table A.15: Average $\overline{TG}_L$ results for $I_{max} = 5$, standard deviation in parenthesis. Variable q indicates the logical network version used. Averages were obtained across the 10 physical network instances for a given space and physical model.

$I_{max} = 6$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	506.27 (30.75)	802.33 (31.0)	746.52 (14.35)	933.58 (13.19)	946.75 (10.11)	1227.81 (9.5)
	(1:1)	529.49 (23.77)	802.16 (29.25)	790.35 (13.11)	973.67 (13.28)	1005.75 (8.03)	1233.68 (9.16)
2	(1:25)	516.43 (19.53)	846.17 (16.22)	753.89 (15.17)	943.08 (10.01)	958.11 (9.22)	1236.24 (7.98)
	(1:1)	557.32 (17.31)	838.3 (28.36)	811.0 (10.84)	990.06 (13.15)	1016.4 (8.67)	1234.41 (12.41)
3	(1:25)	465.19 (22.86)	756.46 (21.32)	710.41 (14.31)	897.73 (11.21)	914.27 (6.94)	1190.67 (6.81)
	(1:1)	507.69 (14.52)	762.0 (33.11)	772.88 (9.7)	946.45 (10.33)	976.42 (4.25)	1192.26 (7.67)
4	(1:25)	509.49 (21.68)	817.79 (19.17)	744.84 (14.47)	930.65 (17.66)	952.53 (8.78)	1239.1 (5.78)
	(1:1)	536.96 (20.99)	818.82 (20.87)	802.55 (10.73)	980.43 (11.92)	1011.84 (9.79)	1242.57 (9.67)
5	(1:25)	600.87 (32.06)	906.59 (23.76)	831.73 (25.14)	1007.0 (15.22)	1030.38 (11.66)	1312.32 (15.49)
	(1:1)	627.38 (21.0)	908.13 (20.8)	879.49 (9.7)	1056.17 (12.85)	1082.99 (9.5)	1309.75 (13.2)
6	(1:25)	455.07 (49.94)	698.87 (40.98)	678.32 (33.43)	819.52 (33.14)	863.94 (32.97)	1115.05 (18.5)
	(1:1)	502.52 (21.81)	688.07 (28.55)	737.5 (32.84)	880.27 (19.72)	930.0 (21.05)	1110.63 (31.62)
7	(1:25)	418.09 (40.26)	695.66 (21.0)	645.61 (23.72)	823.58 (37.31)	846.66 (24.83)	1114.26 (20.53)
	(1:1)	475.2 (24.56)	695.19 (23.04)	715.7 (17.15)	881.57 (17.73)	911.88 (15.83)	1114.88 (8.94)
8	(1:25)	690.32 (9.7)	937.69 (24.03)	903.89 (6.56)	1070.4 (11.34)	1081.47 (7.57)	1317.44 (11.1)
	(1:1)	718.5 (6.38)	926.21 (29.91)	949.7 (5.2)	1107.46 (11.41)	1132.12 (3.86)	1315.87 (7.96)
9	(1:25)	532.41 (25.46)	836.87 (18.15)	779.89 (18.23)	957.58 (16.31)	976.39 (9.84)	1253.45 (14.75)
	(1:1)	574.68 (14.9)	836.43 (23.61)	833.45 (15.5)	1004.06 (7.57)	1037.08 (10.94)	1261.93 (15.58)
10	(1:25)	549.63 (29.44)	861.54 (29.72)	786.11 (17.12)	963.22 (17.53)	989.03 (11.77)	1272.23 (4.48)
	(1:1)	582.59 (19.18)	854.9 (24.26)	834.66 (10.63)	1014.96 (14.02)	1045.24 (5.44)	1267.26 (11.44)

Table A.16: Average $\overline{TG}_L$ results for $I_{max} = 6$, standard deviation in parenthesis. Variable q indicates the logical network version used. Averages were obtained across the 10 physical network instances for a given space and physical model.

$I_{max} = 7$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	440.65 (35.32)	714.93 (22.19)	675.17 (28.79)	859.59 (28.51)	878.59 (21.23)	1130.48 (18.09)
	(1:1)	483.67 (32.71)	713.13 (37.47)	729.64 (17.2)	898.08 (9.44)	931.17 (17.33)	1142.25 (9.79)
2	(1:25)	357.93 (28.89)	633.39 (33.86)	599.51 (20.52)	767.0 (17.7)	796.25 (17.49)	1054.16 (18.67)
	(1:1)	422.65 (32.88)	615.73 (21.85)	661.54 (24.81)	807.41 (19.63)	853.79 (15.25)	1053.77 (19.45)
3	(1:25)	437.41 (20.17)	754.45 (24.28)	684.12 (14.75)	872.8 (9.53)	895.15 (10.01)	1185.07 (9.31)
	(1:1)	496.99 (21.69)	750.95 (24.04)	749.51 (15.72)	929.27 (9.16)	961.47 (9.09)	1182.9 (9.78)
4	(1:25)	440.52 (36.73)	664.35 (35.87)	667.6 (22.54)	807.71 (22.46)	855.51 (15.88)	1080.25 (36.53)
	(1:1)	484.4 (35.68)	661.68 (31.12)	709.88 (32.1)	866.54 (26.03)	901.42 (27.67)	1056.32 (36.81)
5	(1:25)	541.86 (46.79)	789.17 (22.72)	781.96 (32.13)	932.28 (24.47)	961.26 (29.68)	1217.02 (22.98)
	(1:1)	594.31 (30.14)	801.28 (18.01)	836.17 (25.19)	994.5 (17.11)	1032.36 (20.91)	1203.68 (18.93)
6	(1:25)	695.25 (12.63)	959.64 (17.56)	908.66 (11.81)	1075.77 (7.58)	1089.04 (7.01)	1320.29 (11.33)
	(1:1)	728.87 (10.2)	959.18 (16.49)	957.98 (6.7)	1117.08 (10.25)	1136.93 (4.54)	1320.59 (8.3)
7	(1:25)	476.0 (27.62)	775.94 (21.8)	709.71 (23.04)	901.17 (18.81)	921.82 (15.83)	1201.67 (6.52)
	(1:1)	514.8 (13.17)	775.36 (22.46)	771.68 (16.51)	949.74 (9.96)	977.66 (11.63)	1203.06 (6.1)
8	(1:25)	548.76 (45.03)	874.17 (20.82)	781.33 (35.66)	957.51 (32.51)	981.92 (18.17)	1251.61 (11.99)
	(1:1)	601.55 (22.11)	873.84 (26.63)	851.49 (15.39)	1025.21 (16.01)	1050.75 (13.65)	1258.88 (13.8)
9	(1:25)	602.16 (13.93)	863.62 (20.73)	827.26 (9.05)	991.93 (8.27)	1012.88 (9.91)	1290.61 (7.77)
	(1:1)	631.1 (11.87)	858.98 (23.93)	876.41 (9.88)	1040.77 (9.99)	1069.31 (6.67)	1282.72 (10.9)
10	(1:25)	513.97 (37.1)	772.68 (30.37)	746.31 (29.05)	912.84 (18.23)	939.14 (27.67)	1181.15 (26.16)
	(1:1)	567.27 (26.71)	774.7 (23.64)	804.93 (21.47)	962.28 (13.92)	1006.72 (19.22)	1188.08 (20.28)

Table A.17: Average $\overline{TG}_L$ results for $I_{max} = 7$, standard deviation in parenthesis. Variable q indicates the logical network version used. Averages were obtained across the 10 physical network instances for a given space and physical model.

$I_{max} = 8$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	537.49 (11.93)	810.24 (25.83)	767.22 (14.86)	941.13 (13.49)	959.89 (9.11)	1224.65 (12.37)
	(1:1)	569.08 (19.17)	825.15 (18.37)	813.66 (17.83)	997.47 (8.11)	1008.82 (10.64)	1225.18 (7.07)
2	(1:25)	528.77 (25.9)	861.02 (27.6)	780.31 (9.62)	963.95 (11.01)	981.21 (16.44)	1272.52 (5.02)
	(1:1)	587.75 (21.42)	874.62 (20.87)	835.52 (13.84)	1021.9 (12.43)	1042.16 (8.44)	1272.78 (6.81)
3	(1:25)	367.88 (28.8)	650.34 (33.06)	593.09 (23.46)	770.92 (20.51)	791.27 (16.6)	1057.38 (8.79)
	(1:1)	410.31 (29.4)	665.12 (26.42)	661.32 (16.03)	820.5 (22.18)	853.81 (10.19)	1044.38 (19.91)
4	(1:25)	552.48 (26.17)	876.24 (29.17)	794.52 (23.99)	989.38 (9.91)	1001.54 (11.42)	1281.39 (7.28)
	(1:1)	619.37 (21.05)	883.22 (26.23)	869.5 (9.08)	1042.18 (8.52)	1061.22 (9.29)	1280.05 (7.07)
5	(1:25)	633.33 (21.64)	931.77 (19.12)	859.76 (16.97)	1039.99 (10.25)	1044.2 (14.53)	1303.93 (11.04)
	(1:1)	657.14 (31.58)	944.64 (17.74)	909.81 (18.08)	1087.18 (21.14)	1098.48 (8.64)	1310.3 (12.16)
6	(1:25)	363.14 (40.61)	556.44 (69.4)	576.85 (44.14)	686.83 (34.5)	714.77 (39.87)	902.03 (23.46)
	(1:1)	445.72 (53.29)	513.19 (46.15)	633.17 (38.54)	743.15 (19.24)	777.75 (41.43)	889.66 (43.17)
7	(1:25)	618.29 (15.5)	898.04 (23.91)	845.27 (8.05)	1022.4 (6.22)	1029.53 (7.78)	1274.49 (8.08)
	(1:1)	662.22 (15.29)	911.58 (13.92)	896.66 (9.53)	1065.44 (8.96)	1081.45 (6.05)	1271.28 (6.25)
8	(1:25)	585.16 (52.34)	912.83 (29.72)	830.95 (26.69)	1013.36 (32.8)	1025.56 (21.74)	1307.98 (11.18)
	(1:1)	650.25 (27.73)	929.35 (19.52)	897.43 (16.52)	1071.27 (12.33)	1089.51 (6.83)	1300.24 (13.92)
9	(1:25)	389.8 (48.67)	580.17 (71.55)	588.86 (41.5)	722.36 (32.31)	756.46 (42.71)	972.89 (26.42)
	(1:1)	437.64 (42.32)	607.59 (49.79)	617.87 (32.03)	772.55 (31.92)	782.2 (28.31)	955.37 (27.35)
10	(1:25)	558.61 (20.1)	880.69 (22.06)	806.59 (12.07)	988.43 (7.52)	994.73 (13.12)	1268.25 (11.0)
	(1:1)	605.13 (21.08)	887.62 (13.8)	861.19 (16.34)	1029.84 (20.02)	1061.03 (10.24)	1265.45 (12.21)

Table A.18: Average $\overline{TG}_L$ results for $I_{max} = 8$, standard deviation in parenthesis. Variable q indicates the logical network version used. Averages were obtained across the 10 physical network instances for a given space and physical model.

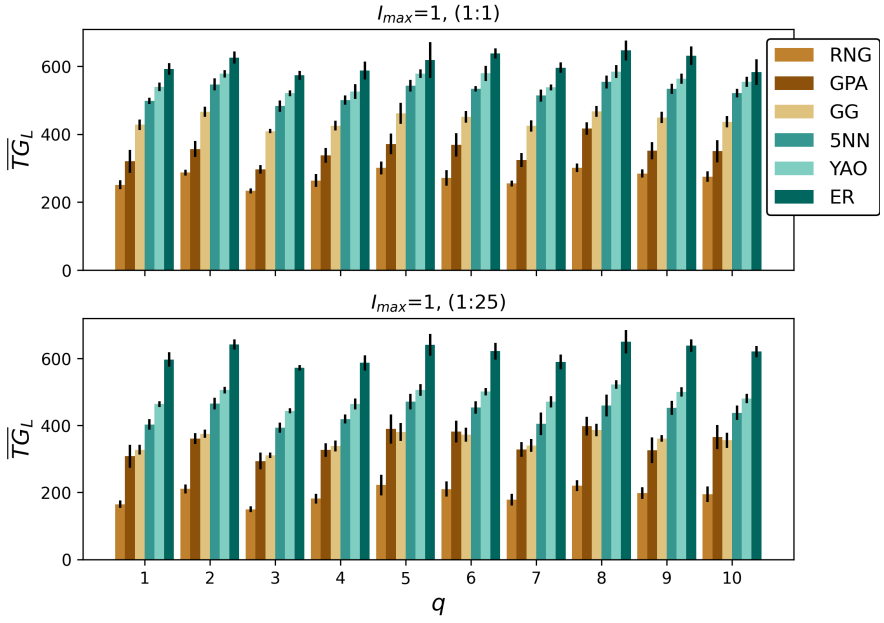
$I_{max} = 9$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	465.61 (21.66)	720.65 (34.82)	696.2 (18.54)	848.95 (26.03)	873.83 (14.53)	1110.41 (12.29)
	(1:1)	513.94 (35.24)	703.52 (28.62)	740.22 (21.88)	891.53 (19.86)	935.01 (14.51)	1113.46 (35.29)
2	(1:25)	537.32 (38.33)	814.31 (31.24)	763.37 (31.68)	942.26 (23.34)	959.18 (19.14)	1237.14 (14.36)
	(1:1)	568.16 (25.03)	813.37 (24.05)	820.97 (9.81)	985.4 (16.65)	1015.39 (11.93)	1241.71 (17.51)
3	(1:25)	512.47 (17.22)	811.48 (25.37)	749.73 (16.31)	940.63 (10.39)	953.76 (12.32)	1252.16 (5.9)
	(1:1)	553.35 (14.77)	799.62 (17.1)	808.79 (9.75)	991.41 (11.22)	1014.63 (7.97)	1249.67 (4.79)
4	(1:25)	409.82 (73.6)	568.78 (28.31)	581.08 (59.25)	725.06 (47.54)	743.35 (30.43)	925.55 (37.53)
	(1:1)	429.79 (39.35)	575.19 (31.18)	647.81 (38.86)	760.55 (30.08)	792.22 (31.01)	932.84 (23.77)
5	(1:25)	808.53 (11.44)	1035.11 (13.57)	1006.1 (8.77)	1162.91 (3.68)	1171.33 (7.61)	1392.87 (9.1)
	(1:1)	838.78 (9.3)	1024.04 (20.61)	1053.5 (7.89)	1196.83 (7.28)	1216.9 (5.66)	1394.59 (7.71)
6	(1:25)	643.65 (20.8)	932.2 (25.63)	868.61 (21.42)	1045.78 (12.19)	1051.11 (10.14)	1322.72 (9.3)
	(1:1)	660.31 (18.07)	900.81 (28.77)	904.55 (17.66)	1086.47 (22.08)	1104.84 (10.41)	1322.55 (7.46)
7	(1:25)	504.91 (21.66)	786.72 (29.91)	737.35 (15.22)	916.77 (13.56)	937.41 (17.79)	1209.52 (22.4)
	(1:1)	573.47 (33.44)	793.92 (21.96)	818.75 (17.69)	967.83 (15.66)	1001.26 (14.4)	1194.36 (16.12)
8	(1:25)	634.05 (27.03)	923.42 (25.13)	855.34 (19.84)	1041.47 (25.7)	1055.39 (12.75)	1316.9 (14.61)
	(1:1)	660.41 (45.86)	905.55 (31.93)	919.89 (27.39)	1086.26 (15.6)	1111.47 (13.36)	1318.37 (21.91)
9	(1:25)	561.1 (32.18)	888.25 (29.14)	803.38 (20.27)	991.51 (15.58)	998.72 (19.22)	1268.8 (13.01)
	(1:1)	620.41 (24.82)	898.18 (35.11)	873.95 (19.43)	1046.06 (19.06)	1057.72 (14.71)	1273.75 (10.34)
10	(1:25)	749.28 (15.43)	1009.99 (12.17)	960.75 (9.67)	1126.65 (9.15)	1134.18 (9.45)	1368.82 (4.65)
	(1:1)	792.11 (8.21)	996.34 (15.48)	1011.12 (7.4)	1161.4 (6.7)	1181.87 (5.03)	1369.73 (10.64)

Table A.19: Average $\overline{TG}_L$ results for $I_{max} = 9$, standard deviation in parenthesis. Variable q indicates the logical network version used. Averages were obtained across the 10 physical network instances for a given space and physical model.

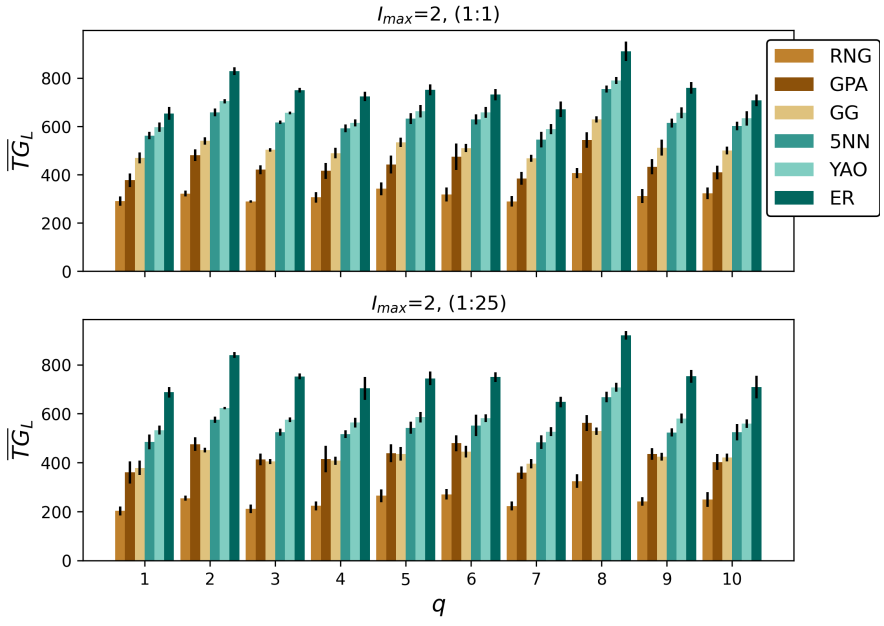
$I_{max} = 10$							
q	space	RNG	GG	GPA	5NN	YAO	ER
1	(1:25)	548.84 (27.08)	834.6 (45.24)	803.96 (27.17)	981.66 (21.56)	989.59 (16.85)	1240.85 (17.8)
	(1:1)	614.24 (30.33)	846.73 (43.52)	859.16 (22.1)	1025.24 (16.73)	1046.43 (14.7)	1246.08 (16.37)
2	(1:25)	629.88 (23.68)	911.5 (25.54)	858.97 (12.19)	1036.6 (20.18)	1048.68 (7.49)	1311.03 (9.26)
	(1:1)	673.69 (21.43)	926.05 (25.3)	916.51 (12.74)	1083.97 (16.61)	1102.66 (9.47)	1311.06 (10.14)
3	(1:25)	538.27 (28.31)	868.43 (19.13)	786.95 (14.83)	976.76 (14.39)	982.36 (14.03)	1267.78 (6.8)
	(1:1)	589.89 (18.45)	866.39 (21.11)	838.27 (10.73)	1026.32 (10.78)	1043.44 (7.31)	1261.98 (6.67)
4	(1:25)	624.11 (30.08)	955.33 (19.28)	859.3 (11.86)	1050.26 (14.29)	1054.05 (9.03)	1318.56 (11.12)
	(1:1)	669.06 (27.68)	954.21 (22.9)	913.96 (16.43)	1088.3 (16.1)	1103.6 (6.67)	1313.45 (10.75)
5	(1:25)	851.55 (7.83)	1084.03 (20.07)	1050.39 (6.98)	1210.33 (11.59)	1214.55 (3.48)	1431.55 (8.0)
	(1:1)	887.27 (9.49)	1089.72 (12.67)	1093.4 (7.27)	1242.28 (9.04)	1255.88 (5.54)	1429.72 (8.2)
6	(1:25)	639.74 (33.79)	935.34 (13.83)	861.3 (29.18)	1060.48 (24.52)	1061.61 (13.68)	1326.69 (14.18)
	(1:1)	697.44 (31.32)	944.5 (27.24)	934.94 (24.41)	1100.52 (23.5)	1120.05 (13.7)	1319.83 (13.25)
7	(1:25)	646.89 (22.66)	939.63 (27.01)	880.84 (16.26)	1062.59 (10.43)	1066.31 (6.67)	1334.56 (6.82)
	(1:1)	675.78 (27.26)	951.75 (20.94)	920.74 (21.57)	1094.01 (14.43)	1113.5 (11.04)	1329.95 (8.29)
8	(1:25)	715.95 (31.51)	1024.91 (26.83)	938.03 (21.98)	1114.97 (19.39)	1127.84 (18.4)	1391.5 (6.63)
	(1:1)	764.16 (21.59)	1027.72 (18.13)	999.18 (12.78)	1161.22 (14.18)	1178.14 (11.6)	1389.12 (6.31)
9	(1:25)	540.25 (75.93)	811.02 (47.81)	760.3 (42.46)	927.27 (36.94)	945.53 (32.26)	1189.36 (13.71)
	(1:1)	606.17 (45.23)	837.62 (49.25)	840.66 (24.23)	976.81 (41.47)	1012.65 (24.21)	1181.09 (19.72)
10	(1:25)	765.94 (10.93)	1016.12 (22.97)	975.83 (9.31)	1145.18 (8.46)	1146.61 (6.52)	1378.32 (5.5)
	(1:1)	809.76 (11.32)	1028.71 (8.06)	1026.38 (8.96)	1180.37 (6.95)	1193.05 (4.83)	1376.59 (6.91)

Table A.20: Average $\overline{TG}_L$ results for $I_{max} = 10$, standard deviation in parenthesis. Variable q indicates the logical network version used. Averages were obtained across the 10 physical network instances for a given space and physical model.

A.5 Physical network model effect figures

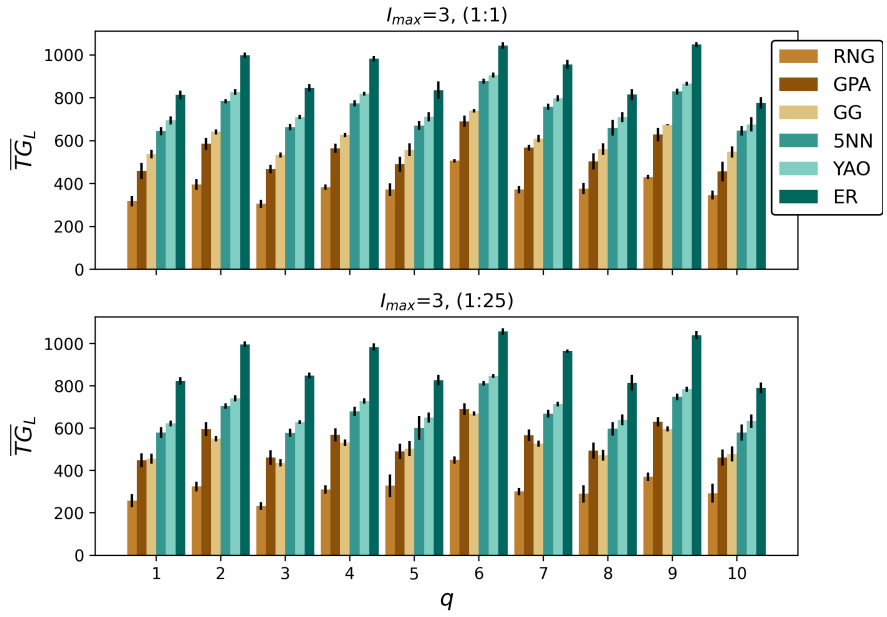


(a)

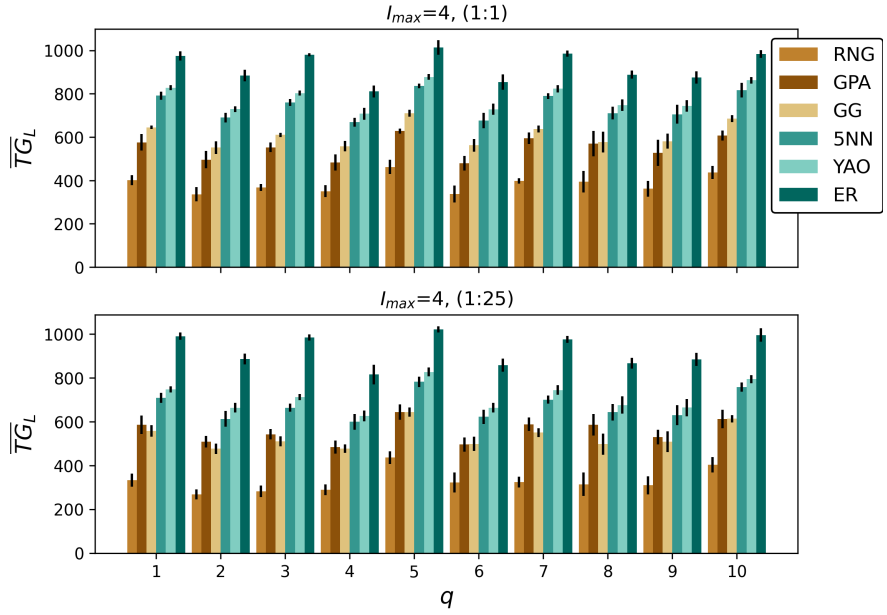


(b)

Figure A.38: Comparison of the average $\overline{TG}_L$ for a given physical network model, for $I_{max} \in \{1, 2\}$. Black line on top shows the $\overline{TG}_L$ standard deviation.

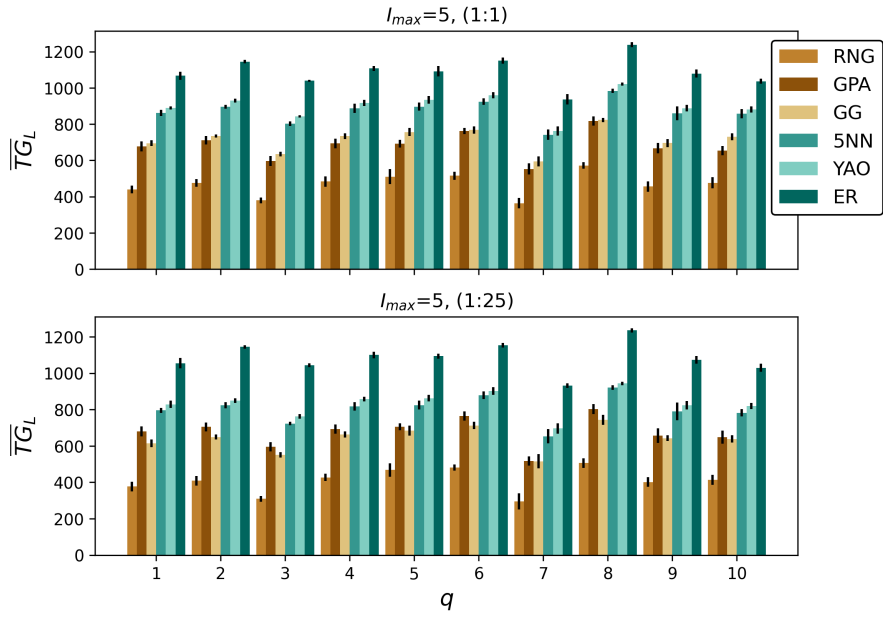


(a)

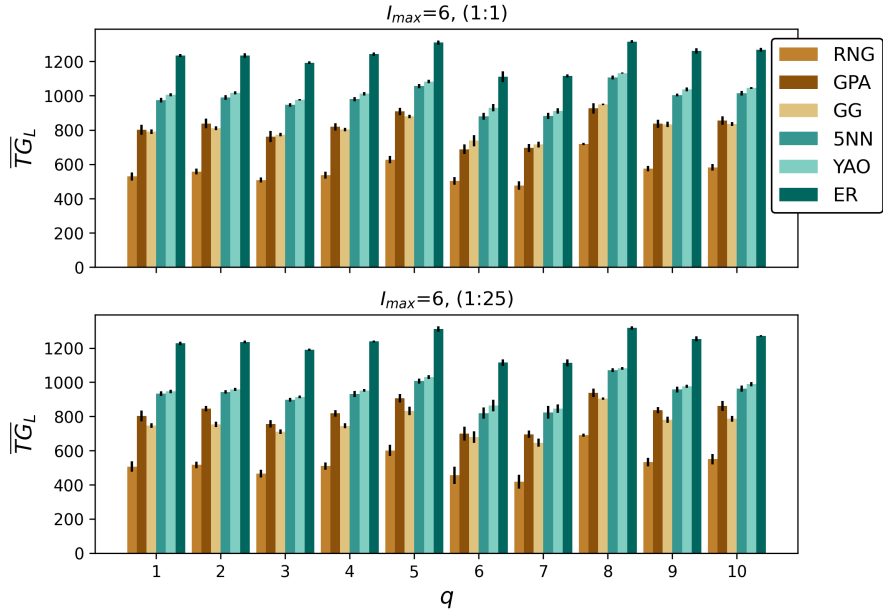


(b)

Figure A.39: Comparison of the average $\overline{TG_L}$ for a given physical network model, for $I_{max} \in \{3, 4\}$. Black line on top shows the $\overline{TG_L}$ standard deviation.

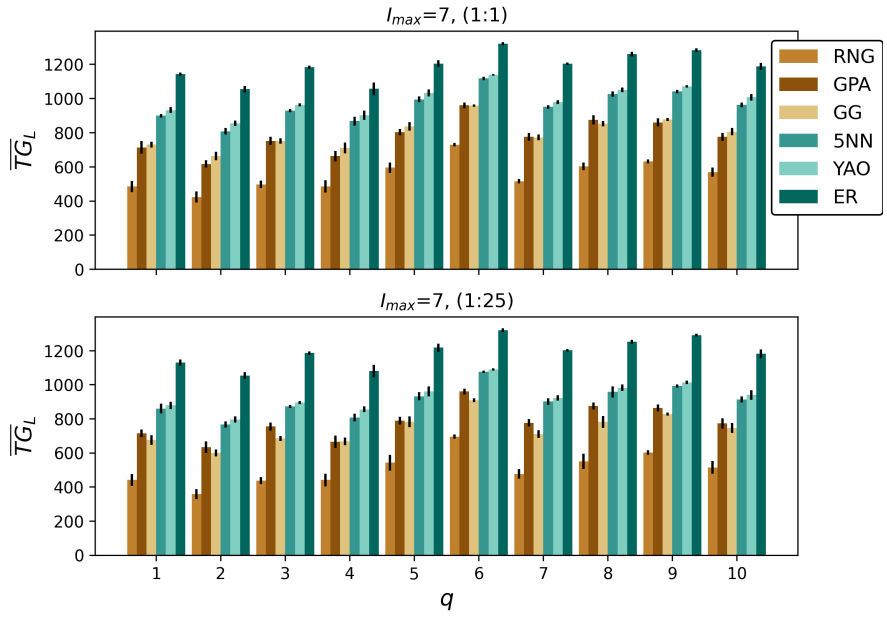


(a)

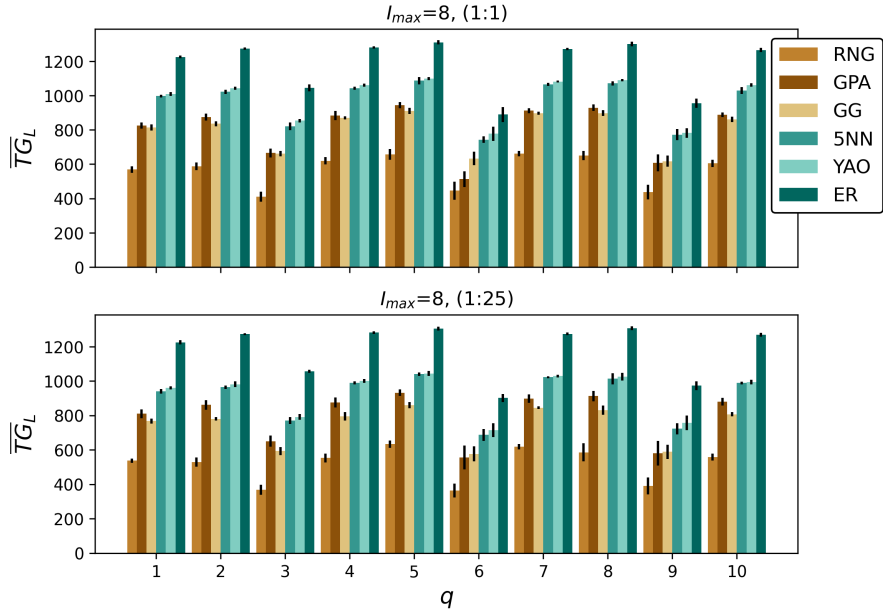


(b)

Figure A.40: Comparison of the average $\overline{TG_L}$ for a given physical network model, for $I_{max} \in \{5, 6\}$. Black line on top shows the $\overline{TG_L}$ standard deviation.

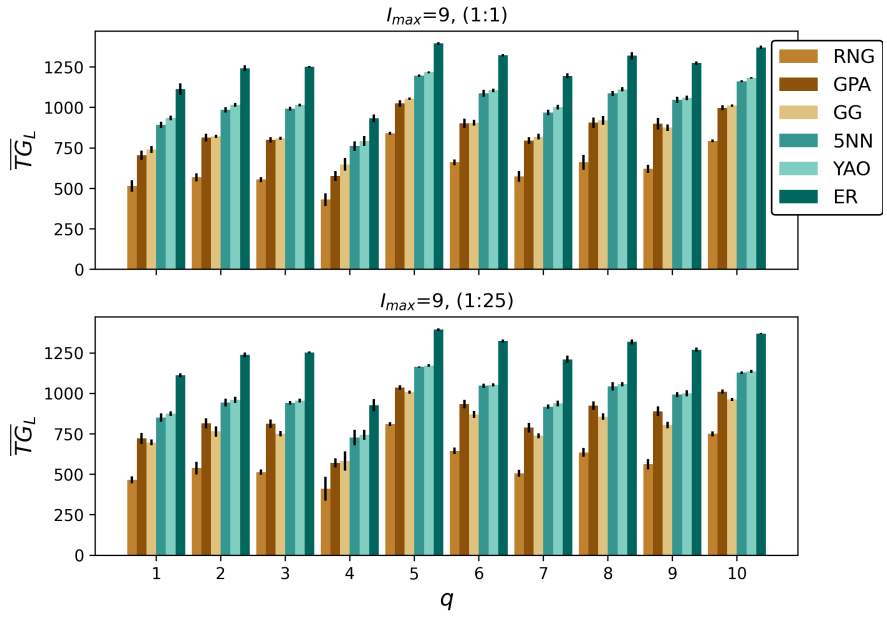


(a)

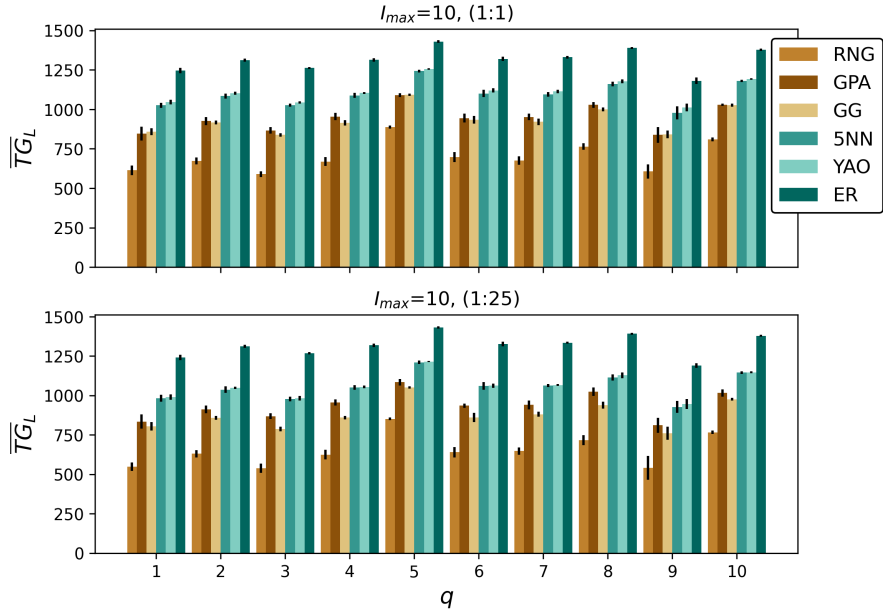


(b)

Figure A.41: Comparison of the average $\overline{TG}_L$ for a given physical network model, for $I_{max} \in \{7, 8\}$. Black line on top shows the $\overline{TG}_L$ standard deviation.



(a)



(b)

Figure A.42: Comparison of the average $\overline{TG}_L$ for a given physical network model, for $I_{max} \in \{9, 10\}$. Black line on top shows the $\overline{TG}_L$ standard deviation.

A.6 I_{max} effect figures

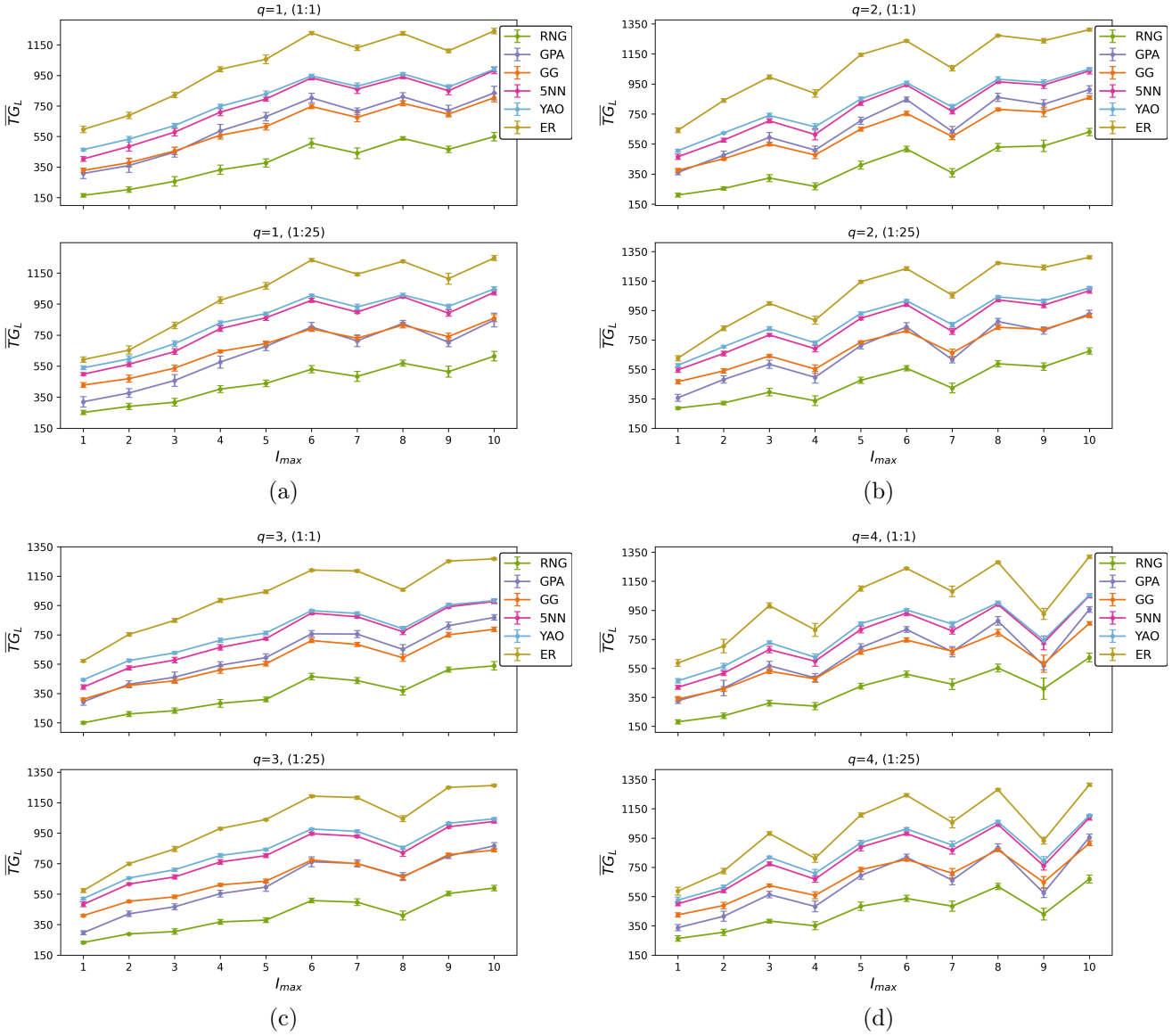


Figure A.43: Average $\overline{TG}_L$ versus I_{max} for logic network versions $q \in \{1, 2, 3, 4\}$.

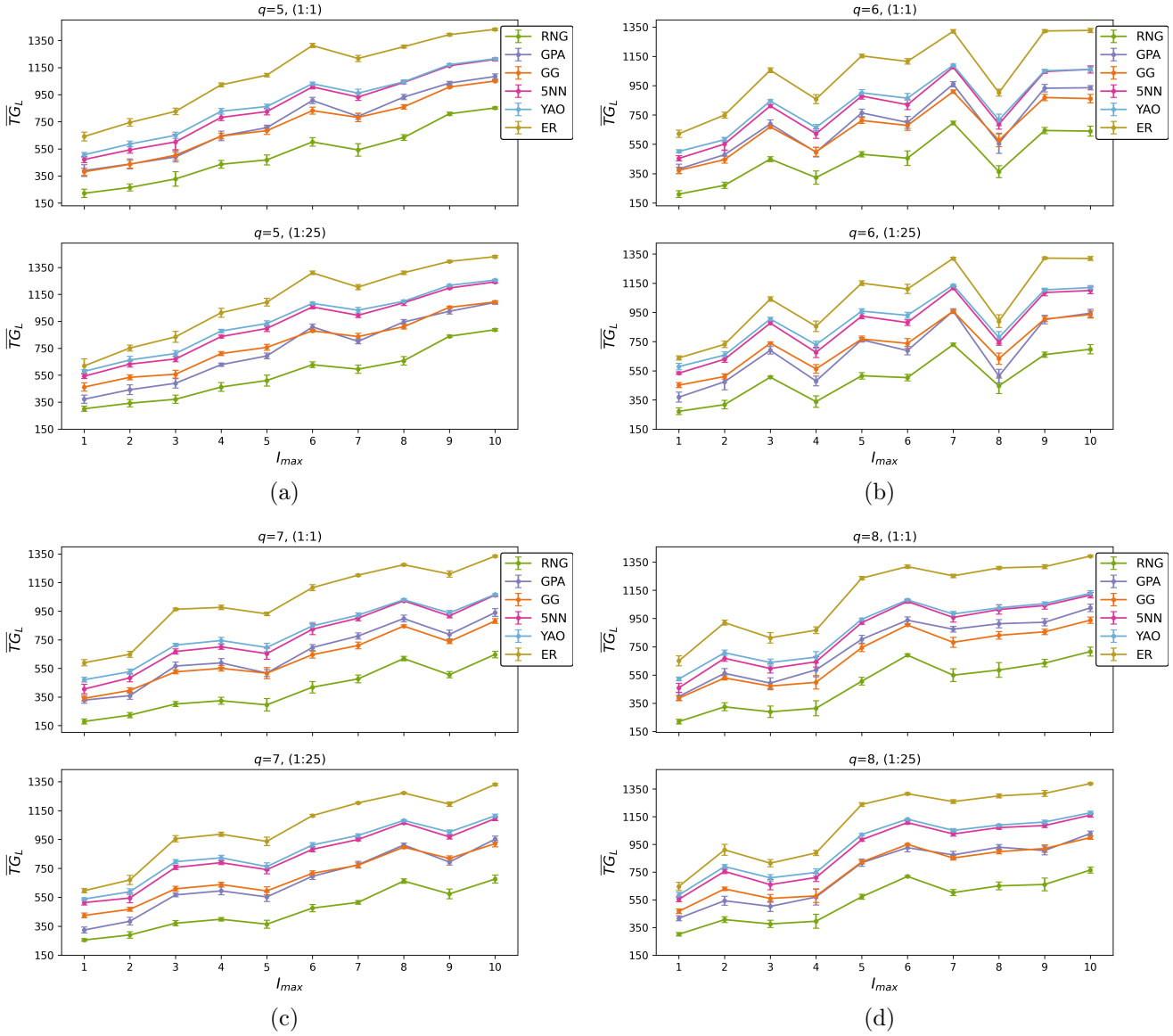


Figure A.44: Average $\overline{TG}_L$ versus I_{max} for logic network versions $q \in \{5, 6, 7, 8\}$.

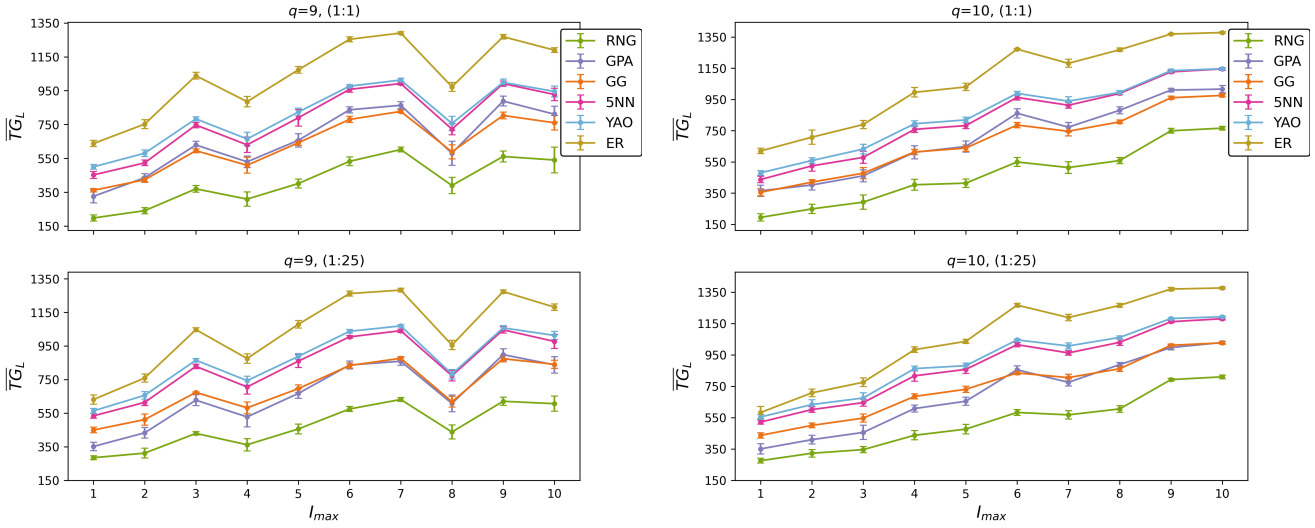


Figure A.45: Average TG_L versus I_{max} for logic network versions $q \in \{9, 10\}$.

Annexed B

Chapter 4: Interplay between the logical network and the interlinks

B.1 Robustness comparison tables

$q = 1$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	164.83 (11.07)	327.53 (14.72)	307.93 (33.96)	402.73 (15.78)	463.75 (8.68)	596.58 (21.47)
	✓	164.86 (13.7)	325.43 (8.99)	308.07 (27.87)	409.96 (16.86)	464.31 (7.33)	592.63 (16.49)
2	×	202.29 (17.89)	378.51 (29.48)	359.78 (45.08)	484.42 (30.19)	532.64 (17.85)	687.58 (21.5)
	✓	235.81 (13.92)	438.24 (19.11)	453.74 (34.15)	566.87 (17.3)	611.95 (14.61)	810.06 (23.25)
3	×	256.55 (31.17)	455.07 (24.21)	447.33 (32.6)	578.39 (25.02)	621.42 (13.73)	821.26 (18.12)
	✓	315.61 (15.43)	542.27 (14.27)	575.83 (20.42)	693.24 (17.59)	735.49 (8.28)	984.9 (12.36)
4	×	332.13 (29.83)	558.14 (25.86)	586.43 (41.86)	708.9 (22.5)	747.63 (13.52)	990.42 (16.36)
	✓	367.16 (19.05)	604.43 (11.92)	667.08 (29.4)	766.94 (10.95)	802.57 (11.79)	1065.87 (12.7)
5	×	376.92 (26.95)	614.65 (21.6)	679.97 (27.39)	795.38 (14.25)	828.23 (20.28)	1055.31 (28.33)
	✓	397.32 (21.16)	643.85 (24.03)	729.05 (25.21)	834.42 (17.07)	851.58 (13.81)	1124.32 (11.11)
6	×	506.27 (30.75)	746.52 (14.35)	802.33 (31.0)	933.58 (13.19)	946.75 (10.11)	1227.81 (9.5)
	✓	509.79 (28.63)	759.14 (12.06)	819.77 (24.49)	943.82 (13.48)	957.37 (10.94)	1241.04 (6.96)
7	×	440.65 (35.32)	675.17 (28.79)	714.93 (22.19)	859.59 (28.51)	878.59 (21.23)	1130.48 (18.09)
	✓	484.48 (20.85)	729.65 (17.44)	790.6 (9.12)	916.67 (18.64)	940.15 (14.2)	1220.38 (6.77)
8	×	537.49 (11.93)	767.22 (14.86)	810.24 (25.83)	941.13 (13.49)	959.89 (9.11)	1224.65 (12.37)
	✓	548.37 (10.91)	778.8 (12.36)	838.54 (31.89)	965.58 (8.77)	973.07 (9.52)	1246.7 (7.16)
9	×	465.61 (21.66)	696.2 (18.54)	720.65 (34.82)	848.95 (26.03)	873.83 (14.53)	1110.41 (12.29)
	✓	559.66 (17.17)	798.11 (13.36)	877.2 (17.25)	975.6 (13.7)	997.05 (6.71)	1274.64 (6.73)
10	×	548.84 (27.08)	803.96 (27.17)	834.6 (45.24)	981.66 (21.56)	989.59 (16.85)	1240.85 (17.8)
	✓	665.24 (20.89)	891.26 (12.03)	951.28 (23.93)	1077.56 (14.58)	1081.07 (6.38)	1345.49 (7.05)

Table B.1: Average $\overline{TG_L}$ of systems with $q = 1$, and $s = (1 : 25)$. Column $+I$ shows whether the systems has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

$q = 2$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	210.51 (13.43)	374.82 (12.18)	360.64 (16.66)	464.89 (17.09)	505.23 (9.48)	641.57 (15.57)
	✓	212.97 (11.35)	375.38 (17.36)	357.92 (22.25)	457.97 (15.13)	509.14 (12.92)	645.19 (17.02)
2	×	253.93 (10.42)	451.44 (9.5)	475.21 (27.84)	575.33 (12.83)	623.23 (4.49)	839.48 (11.49)
	✓	274.18 (10.76)	477.26 (8.69)	514.55 (25.04)	623.33 (9.07)	659.2 (9.74)	889.95 (11.53)
3	×	323.51 (23.32)	549.32 (12.01)	594.27 (32.84)	703.99 (13.17)	740.46 (14.35)	995.28 (14.06)
	✓	333.0 (21.17)	565.26 (17.35)	622.81 (26.0)	728.49 (17.88)	763.42 (13.64)	1025.89 (11.78)
4	×	267.91 (23.2)	476.72 (23.73)	509.21 (26.55)	613.1 (36.67)	663.86 (21.35)	886.77 (24.67)
	✓	369.27 (17.46)	614.14 (13.77)	687.42 (25.58)	784.48 (11.03)	818.59 (11.96)	1117.85 (7.53)
5	×	408.83 (26.6)	648.84 (13.47)	704.61 (23.69)	823.87 (16.54)	849.26 (12.96)	1144.5 (9.84)
	✓	448.23 (25.9)	691.83 (16.23)	758.78 (28.21)	871.59 (16.0)	899.91 (9.09)	1205.11 (6.68)
6	×	516.43 (19.53)	753.89 (15.17)	846.17 (16.22)	943.08 (10.01)	958.11 (9.22)	1236.24 (7.98)
	✓	553.87 (18.38)	790.94 (15.17)	872.51 (18.64)	975.86 (11.09)	988.52 (6.87)	1272.78 (7.22)
7	×	357.93 (28.89)	599.51 (20.52)	633.39 (33.86)	767.0 (17.7)	796.25 (17.49)	1054.16 (18.67)
	✓	565.39 (21.76)	805.78 (15.07)	864.48 (20.06)	991.54 (5.5)	1011.08 (12.01)	1299.68 (5.64)
8	×	528.77 (25.9)	780.31 (9.62)	861.02 (27.6)	963.95 (11.01)	981.21 (16.44)	1272.52 (5.02)
	✓	557.26 (21.73)	797.75 (14.09)	882.01 (22.45)	979.67 (13.07)	996.89 (11.06)	1293.58 (5.09)
9	×	537.32 (38.33)	763.37 (31.68)	814.31 (31.24)	942.26 (23.34)	959.18 (19.14)	1237.14 (14.36)
	✓	607.74 (27.21)	844.34 (24.48)	943.31 (21.68)	1038.43 (19.24)	1047.76 (16.99)	1336.87 (7.42)
10	×	629.88 (23.68)	858.97 (12.19)	911.5 (25.54)	1036.6 (20.18)	1048.68 (7.49)	1311.03 (9.26)
	✓	685.71 (17.52)	905.75 (15.79)	980.59 (24.01)	1095.24 (12.09)	1098.0 (7.65)	1372.9 (7.35)

Table B.2: Average $\overline{TG_L}$ of systems with $q = 2$, and $s = (1 : 25)$. Column $+I$ shows whether the systems has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

$q = 3$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	149.85 (8.37)	310.71 (7.65)	293.65 (24.88)	393.41 (15.08)	443.33 (7.53)	571.96 (8.6)
	✓	151.37 (7.03)	312.15 (5.92)	293.15 (19.32)	391.87 (12.86)	450.08 (8.15)	576.37 (6.08)
2	×	210.46 (17.1)	404.5 (10.08)	412.54 (23.59)	524.36 (14.47)	574.39 (9.49)	752.27 (12.11)
	✓	224.79 (12.62)	422.69 (6.86)	444.45 (24.14)	558.39 (11.64)	601.09 (7.88)	797.95 (10.74)
3	×	232.38 (18.13)	435.92 (17.54)	461.01 (34.74)	577.37 (18.43)	626.92 (9.15)	848.05 (13.66)
	✓	267.99 (17.97)	490.67 (13.89)	526.64 (26.6)	643.27 (15.28)	681.58 (9.14)	928.99 (3.95)
4	×	282.8 (26.39)	510.23 (22.82)	542.12 (23.71)	663.95 (18.89)	712.53 (14.37)	984.78 (13.93)
	✓	347.48 (21.18)	584.91 (17.06)	641.16 (15.1)	756.13 (20.67)	794.68 (13.75)	1078.19 (5.48)
5	×	308.98 (16.41)	551.96 (14.78)	594.58 (25.22)	723.11 (9.13)	762.18 (12.31)	1043.82 (11.37)
	✓	330.71 (16.54)	578.4 (18.99)	625.09 (27.08)	752.83 (8.85)	786.79 (11.68)	1075.76 (6.81)
6	×	465.19 (22.86)	710.41 (14.31)	756.46 (21.32)	897.73 (11.21)	914.27 (6.94)	1190.67 (6.81)
	✓	471.97 (19.71)	714.87 (13.96)	767.54 (21.55)	902.28 (6.75)	921.79 (9.38)	1200.64 (5.61)
7	×	437.41 (20.17)	684.12 (14.75)	754.45 (24.28)	872.8 (9.53)	895.15 (10.01)	1185.07 (9.31)
	✓	446.88 (19.02)	695.94 (14.19)	766.52 (18.35)	887.41 (11.17)	907.26 (9.79)	1202.62 (4.5)
8	×	367.88 (28.8)	593.09 (23.46)	650.34 (33.06)	770.92 (20.51)	791.27 (16.6)	1057.38 (8.79)
	✓	489.05 (10.23)	741.79 (15.09)	820.26 (25.9)	935.7 (10.21)	948.17 (11.79)	1229.3 (3.78)
9	×	512.47 (17.22)	749.73 (16.31)	811.48 (25.37)	940.63 (10.39)	953.76 (12.32)	1252.16 (5.9)
	✓	532.03 (17.79)	769.99 (15.54)	839.31 (24.26)	964.63 (4.52)	976.77 (5.16)	1275.27 (3.35)
10	×	538.27 (28.31)	786.95 (14.83)	868.43 (19.13)	976.76 (14.39)	982.36 (14.03)	1267.78 (6.8)
	✓	589.01 (15.62)	834.66 (9.47)	912.94 (13.85)	1031.52 (11.66)	1034.74 (10.2)	1327.45 (4.74)

Table B.3: Average $\overline{TG_L}$ of systems with $q = 3$, and $s = (1 : 25)$. Column $+I$ shows whether the systems has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

$q = 4$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	181.3 (14.53)	338.42 (16.34)	326.52 (20.01)	419.14 (13.16)	463.82 (16.05)	586.74 (22.86)
	✓	180.51 (16.59)	338.25 (12.25)	329.61 (17.64)	418.84 (11.35)	464.39 (13.05)	575.18 (34.64)
2	×	223.09 (18.16)	407.28 (17.09)	414.03 (53.83)	516.42 (16.18)	563.3 (20.41)	703.35 (46.6)
	✓	259.61 (15.43)	461.73 (13.67)	486.67 (35.67)	594.13 (14.3)	639.72 (12.87)	843.42 (17.49)
3	×	310.1 (20.03)	530.5 (15.93)	567.9 (30.27)	679.03 (21.98)	727.06 (12.68)	982.54 (17.82)
	✓	310.19 (19.32)	530.21 (11.96)	569.17 (26.04)	681.92 (14.5)	724.24 (12.78)	973.9 (19.0)
4	×	289.48 (24.49)	477.34 (19.36)	484.37 (30.27)	599.26 (35.89)	626.17 (23.88)	815.21 (44.3)
	✓	378.58 (21.37)	617.26 (20.28)	682.71 (22.25)	783.44 (12.7)	810.98 (12.51)	1081.64 (11.87)
5	×	426.49 (19.84)	663.51 (16.81)	693.61 (25.37)	817.32 (23.59)	857.85 (12.51)	1100.24 (18.23)
	✓	445.81 (19.95)	690.54 (17.13)	745.94 (22.96)	865.69 (19.32)	892.18 (6.24)	1171.11 (15.76)
6	×	509.49 (21.68)	744.84 (14.47)	817.79 (19.17)	930.65 (17.66)	952.53 (8.78)	1239.1 (5.78)
	✓	511.69 (23.46)	751.17 (15.89)	834.17 (22.18)	944.95 (19.89)	960.62 (9.48)	1260.06 (7.79)
7	×	440.52 (36.73)	667.6 (22.54)	664.35 (35.87)	807.71 (22.46)	855.51 (15.88)	1080.25 (36.53)
	✓	514.37 (20.01)	761.38 (19.41)	822.94 (25.24)	933.96 (19.89)	961.13 (13.65)	1256.09 (6.01)
8	×	552.48 (26.17)	794.52 (23.99)	876.24 (29.17)	989.38 (9.91)	1001.54 (11.42)	1281.39 (7.28)
	✓	567.51 (22.28)	800.59 (24.64)	882.14 (29.07)	994.65 (12.69)	1005.43 (11.44)	1293.82 (3.57)
9	×	409.82 (73.6)	581.08 (59.25)	568.78 (28.31)	725.06 (47.54)	743.35 (30.43)	925.55 (37.53)
	✓	613.0 (18.76)	847.71 (15.32)	932.37 (23.0)	1030.8 (11.5)	1044.0 (8.67)	1328.55 (8.41)
10	×	624.11 (30.08)	859.3 (11.86)	955.33 (19.28)	1050.26 (14.29)	1054.05 (9.03)	1318.56 (11.12)
	✓	648.82 (31.6)	884.07 (13.11)	965.95 (20.15)	1069.64 (12.28)	1069.71 (8.14)	1339.51 (5.35)

Table B.4: Average $\overline{TG_L}$ of systems with $q = 4$, and $s = (1 : 25)$. Column $+I$ shows whether the systems has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

$q = 5$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	221.95 (30.48)	380.66 (26.46)	389.31 (43.23)	470.95 (22.79)	505.88 (17.06)	640.79 (32.26)
	✓	221.51 (29.1)	381.78 (25.42)	392.76 (45.25)	463.06 (22.51)	508.91 (25.42)	632.18 (26.36)
2	×	264.66 (26.12)	435.76 (28.43)	437.72 (36.68)	542.22 (24.18)	585.45 (20.78)	744.37 (27.41)
	✓	305.95 (22.73)	518.71 (18.67)	575.4 (29.41)	655.54 (15.29)	702.47 (13.88)	920.04 (19.28)
3	×	327.44 (53.26)	502.79 (35.86)	489.94 (36.75)	601.04 (56.5)	649.54 (23.39)	826.43 (23.74)
	✓	408.27 (28.14)	634.17 (17.76)	664.44 (30.12)	786.35 (12.14)	818.08 (13.82)	1069.61 (13.06)
4	×	436.04 (28.46)	643.9 (21.19)	644.61 (35.22)	782.04 (24.3)	827.35 (20.75)	1022.05 (14.28)
	✓	471.42 (24.19)	702.71 (20.0)	757.02 (33.26)	859.22 (16.16)	893.21 (13.9)	1162.01 (16.97)
5	×	468.04 (36.99)	683.9 (27.21)	705.76 (19.4)	824.6 (23.53)	862.09 (17.91)	1093.7 (13.55)
	✓	531.78 (20.73)	771.27 (15.26)	830.56 (24.49)	937.86 (15.63)	969.01 (9.42)	1248.35 (9.46)
6	×	600.87 (32.06)	831.73 (25.14)	906.59 (23.76)	1007.0 (15.22)	1030.38 (11.66)	1312.32 (15.49)
	✓	596.82 (32.58)	831.9 (17.3)	904.44 (26.05)	1008.73 (14.37)	1029.82 (15.07)	1312.86 (11.36)
7	×	541.86 (46.79)	781.96 (32.13)	789.17 (22.72)	932.28 (24.47)	961.26 (29.68)	1217.02 (22.98)
	✓	666.15 (16.74)	879.71 (15.29)	934.35 (23.29)	1044.2 (17.92)	1065.23 (8.67)	1331.18 (5.16)
8	×	633.33 (21.64)	859.76 (16.97)	931.77 (19.12)	1039.99 (10.25)	1044.2 (14.53)	1303.93 (11.04)
	✓	659.15 (26.04)	892.36 (20.47)	974.08 (25.34)	1076.14 (12.76)	1077.27 (10.53)	1348.84 (6.04)
9	×	808.53 (11.44)	1006.1 (8.77)	1035.11 (13.57)	1162.91 (3.68)	1171.33 (7.61)	1392.87 (9.1)
	✓	807.88 (11.92)	1007.34 (7.36)	1037.01 (14.49)	1164.4 (7.96)	1172.01 (6.26)	1396.34 (5.99)
10	×	851.55 (7.83)	1050.39 (6.98)	1084.03 (20.07)	1210.33 (11.59)	1214.55 (3.48)	1431.55 (8.0)
	✓	849.03 (9.45)	1050.44 (6.67)	1081.87 (17.43)	1212.17 (9.34)	1214.72 (6.7)	1434.79 (4.54)

Table B.5: Average $\overline{TG_L}$ of systems with $q = 5$, and $s = (1 : 25)$. Column $+I$ shows whether the systems has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

$q = 6$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	209.99 (22.44)	372.07 (21.19)	381.32 (32.52)	453.55 (18.04)	501.11 (11.02)	621.52 (25.22)
	✓	211.09 (21.63)	374.63 (22.64)	383.14 (35.66)	457.7 (21.66)	499.03 (11.92)	629.06 (25.34)
2	×	269.84 (21.58)	444.94 (23.39)	478.88 (33.13)	551.54 (44.05)	581.02 (15.97)	749.19 (20.36)
	✓	301.81 (19.67)	502.69 (17.04)	554.4 (20.37)	638.41 (23.45)	684.11 (12.72)	893.08 (24.76)
3	×	448.87 (17.16)	668.26 (9.49)	688.81 (27.49)	811.13 (11.1)	845.07 (9.18)	1055.35 (16.14)
	✓	449.73 (14.76)	665.53 (11.63)	689.51 (35.95)	809.22 (12.35)	845.06 (10.07)	1037.75 (16.62)
4	×	322.72 (45.23)	498.35 (32.27)	495.75 (33.03)	621.91 (32.78)	663.91 (21.8)	857.72 (29.92)
	✓	436.1 (26.07)	662.04 (22.06)	724.54 (29.4)	833.66 (20.52)	864.03 (16.3)	1123.36 (21.65)
5	×	481.69 (17.36)	712.02 (20.05)	763.99 (25.67)	878.62 (21.12)	901.18 (20.97)	1152.77 (12.81)
	✓	514.79 (16.55)	742.6 (10.06)	810.7 (23.13)	916.48 (10.99)	940.08 (10.28)	1216.96 (14.02)
6	×	455.07 (49.94)	678.32 (33.43)	698.87 (40.98)	819.52 (33.14)	863.94 (32.97)	1115.05 (18.5)
	✓	553.04 (23.61)	789.09 (12.23)	863.02 (26.87)	974.81 (16.43)	987.14 (9.17)	1280.7 (7.97)
7	×	695.25 (12.63)	908.66 (11.81)	959.64 (17.56)	1075.77 (7.58)	1089.04 (7.01)	1320.29 (11.33)
	✓	692.73 (10.98)	909.12 (11.57)	955.49 (22.22)	1075.43 (7.1)	1091.3 (8.78)	1316.98 (10.14)
8	×	363.14 (40.61)	576.85 (44.14)	556.44 (69.4)	686.83 (34.5)	714.77 (39.87)	902.03 (23.46)
	✓	594.17 (23.41)	826.33 (21.87)	905.75 (31.3)	1019.05 (18.67)	1023.65 (13.09)	1320.85 (7.55)
9	×	643.65 (20.8)	868.61 (21.42)	932.2 (25.63)	1045.78 (12.19)	1051.11 (10.14)	1322.72 (9.3)
	✓	667.8 (21.18)	893.57 (14.48)	963.48 (25.63)	1074.22 (15.23)	1082.99 (6.94)	1358.63 (5.22)
10	×	639.74 (33.79)	861.3 (29.18)	935.34 (13.83)	1060.48 (24.52)	1061.61 (13.68)	1326.69 (14.18)
	✓	685.8 (26.13)	922.82 (22.53)	1007.37 (24.49)	1113.32 (14.83)	1115.36 (11.89)	1387.37 (6.7)

Table B.6: Average $\overline{TG_L}$ of systems with $q = 6$, and $s = (1 : 25)$. Column $+I$ shows whether the systems has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

$q = 7$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	178.41 (17.22)	339.99 (19.3)	327.83 (22.13)	404.92 (33.77)	470.41 (16.86)	589.33 (21.62)
	✓	175.41 (19.92)	333.95 (18.23)	328.05 (24.0)	404.93 (32.17)	467.08 (13.16)	592.73 (36.17)
2	×	222.56 (18.07)	395.65 (18.89)	358.84 (24.9)	483.57 (27.84)	526.51 (18.2)	648.1 (21.5)
	✓	256.7 (11.65)	464.52 (16.62)	456.83 (33.68)	575.33 (11.26)	634.34 (11.96)	812.7 (25.53)
3	×	300.62 (17.31)	525.37 (14.14)	566.18 (26.87)	667.8 (18.62)	712.94 (11.03)	963.15 (7.8)
	✓	299.59 (18.95)	519.03 (14.26)	565.47 (25.95)	673.0 (12.83)	711.09 (16.26)	966.07 (9.33)
4	×	323.54 (24.8)	550.01 (19.65)	587.99 (30.42)	700.58 (18.14)	744.48 (21.65)	976.21 (16.3)
	✓	356.58 (24.69)	594.08 (19.99)	649.46 (29.02)	756.17 (15.54)	793.83 (10.6)	1067.2 (11.7)
5	×	294.73 (43.78)	515.99 (38.99)	516.8 (25.12)	652.91 (39.17)	695.97 (29.48)	931.06 (12.32)
	✓	404.94 (25.05)	650.35 (22.1)	727.84 (21.03)	832.1 (23.38)	867.35 (16.64)	1168.41 (7.23)
6	×	418.09 (40.26)	645.61 (23.72)	695.66 (21.0)	823.58 (37.31)	846.66 (24.83)	1114.26 (20.53)
	✓	488.36 (29.11)	733.96 (16.65)	797.15 (21.13)	914.75 (21.69)	938.55 (13.24)	1235.89 (11.96)
7	×	476.0 (27.62)	709.71 (23.04)	775.94 (21.8)	901.17 (18.81)	921.82 (15.83)	1201.67 (6.52)
	✓	486.57 (31.55)	724.15 (20.32)	784.62 (21.43)	909.96 (22.35)	929.75 (15.87)	1212.43 (8.58)
8	×	618.29 (15.5)	845.27 (8.05)	898.04 (23.91)	1022.4 (6.22)	1029.53 (7.78)	1274.49 (8.08)
	✓	620.68 (12.91)	847.24 (9.78)	898.26 (26.38)	1023.62 (7.28)	1031.55 (5.5)	1279.75 (9.58)
9	×	504.91 (21.66)	737.35 (15.22)	786.72 (29.91)	916.77 (13.56)	937.41 (17.79)	1209.52 (22.4)
	✓	606.68 (17.39)	830.37 (15.15)	895.63 (18.61)	1018.56 (8.74)	1024.48 (12.49)	1304.05 (5.19)
10	×	646.89 (22.66)	880.84 (16.26)	939.63 (27.01)	1062.59 (10.43)	1066.31 (6.67)	1334.56 (6.82)
	✓	660.93 (16.6)	888.25 (15.18)	952.97 (19.99)	1075.66 (8.56)	1078.2 (8.51)	1341.26 (5.26)

Table B.7: Average $\overline{TG_L}$ of systems with $q = 7$, and $s = (1 : 25)$. Column $+I$ shows whether the systems has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

$q = 8$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	220.1 (16.57)	386.31 (18.66)	397.88 (27.47)	459.41 (32.12)	521.81 (12.71)	649.79 (35.32)
	✓	221.22 (16.9)	387.83 (9.88)	415.0 (36.36)	460.56 (41.69)	516.18 (18.01)	633.95 (16.22)
2	×	324.51 (28.49)	528.84 (15.07)	561.74 (32.92)	668.06 (21.1)	707.4 (18.34)	920.56 (17.77)
	✓	324.9 (29.77)	535.92 (14.59)	556.82 (34.99)	665.25 (24.8)	707.96 (19.29)	932.24 (18.06)
3	×	289.33 (40.52)	471.68 (25.94)	492.39 (38.22)	595.9 (31.77)	638.6 (24.66)	813.46 (37.36)
	✓	386.66 (41.12)	605.55 (31.74)	651.36 (32.24)	766.26 (20.28)	809.03 (21.43)	1052.91 (17.4)
4	×	314.47 (53.29)	498.05 (48.3)	586.23 (48.96)	643.42 (37.56)	676.18 (39.59)	867.07 (23.87)
	✓	448.75 (17.74)	678.96 (19.88)	740.07 (32.1)	849.45 (14.94)	886.98 (12.4)	1158.56 (16.12)
5	×	505.77 (27.01)	743.48 (27.35)	802.59 (27.24)	920.44 (12.87)	943.88 (9.19)	1235.3 (12.33)
	✓	505.04 (30.47)	735.04 (23.6)	803.45 (21.02)	915.35 (16.7)	942.61 (14.17)	1232.14 (7.32)
6	×	690.32 (9.7)	903.89 (6.56)	937.69 (24.03)	1070.4 (11.34)	1081.47 (7.57)	1317.44 (11.1)
	✓	687.57 (10.42)	904.1 (7.06)	936.1 (32.62)	1067.66 (8.8)	1080.32 (9.91)	1316.44 (9.99)
7	×	548.76 (45.03)	781.33 (35.66)	874.17 (20.82)	957.51 (32.51)	981.92 (18.17)	1251.61 (11.99)
	✓	592.09 (33.2)	829.04 (17.85)	919.81 (18.77)	1014.05 (18.11)	1032.82 (14.56)	1315.95 (10.78)
8	×	585.16 (52.34)	830.95 (26.69)	912.83 (29.72)	1013.36 (32.8)	1025.56 (21.74)	1307.98 (11.18)
	✓	634.41 (25.41)	858.68 (19.79)	941.27 (23.84)	1040.04 (23.72)	1050.1 (16.34)	1329.97 (8.52)
9	×	634.05 (27.03)	855.34 (19.84)	923.42 (25.13)	1041.47 (25.7)	1055.39 (12.75)	1316.9 (14.61)
	✓	723.81 (22.54)	934.19 (16.9)	993.07 (21.28)	1098.45 (17.0)	1116.41 (13.78)	1374.01 (6.99)
10	×	715.95 (31.51)	938.03 (21.98)	1024.91 (26.83)	1114.97 (19.39)	1127.84 (18.4)	1391.5 (6.63)
	✓	728.74 (34.2)	960.2 (17.54)	1038.95 (18.43)	1134.45 (17.02)	1142.74 (11.88)	1403.98 (5.84)

Table B.8: Average $\overline{TG_L}$ of systems with $q = 8$, and $s = (1 : 25)$. Column $+I$ shows whether the systems has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

$q = 9$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	197.83 (17.71)	361.08 (9.67)	325.92 (38.13)	452.23 (20.81)	499.92 (13.61)	637.64 (18.53)
	✓	199.44 (13.87)	360.35 (16.65)	333.08 (38.3)	441.95 (19.12)	492.39 (22.17)	640.34 (23.35)
2	×	240.88 (17.68)	423.73 (15.49)	435.49 (23.96)	523.33 (16.7)	580.45 (19.61)	752.52 (26.58)
	✓	271.45 (21.4)	475.37 (17.18)	523.48 (25.71)	603.3 (25.03)	658.72 (13.09)	874.03 (16.89)
3	×	369.78 (20.53)	595.23 (11.62)	629.09 (22.01)	747.03 (15.85)	783.38 (12.01)	1038.47 (19.22)
	✓	367.54 (22.61)	596.62 (11.03)	631.98 (29.28)	749.31 (16.56)	791.29 (8.74)	1042.42 (11.81)
4	×	309.34 (41.8)	509.2 (47.43)	529.61 (33.85)	629.89 (45.56)	664.64 (39.39)	885.24 (29.93)
	✓	417.51 (21.13)	650.57 (20.49)	707.94 (37.82)	820.28 (15.04)	853.32 (17.65)	1133.41 (7.59)
5	×	401.34 (26.6)	642.14 (16.0)	656.63 (39.91)	789.78 (48.82)	823.78 (22.24)	1073.03 (20.39)
	✓	466.65 (13.62)	709.9 (12.93)	786.51 (24.82)	894.73 (15.62)	916.45 (11.83)	1203.91 (10.13)
6	×	532.41 (25.46)	779.89 (18.23)	836.87 (18.15)	957.58 (16.31)	976.39 (9.84)	1253.45 (14.75)
	✓	540.44 (27.81)	785.95 (17.04)	848.06 (17.37)	970.6 (13.1)	987.19 (6.07)	1272.11 (10.12)
7	×	602.16 (13.93)	827.26 (9.05)	863.62 (20.73)	991.93 (8.27)	1012.88 (9.91)	1290.61 (7.77)
	✓	601.03 (15.45)	822.58 (13.88)	858.24 (21.41)	993.59 (11.49)	1011.15 (8.48)	1287.11 (5.99)
8	×	389.8 (48.67)	588.86 (41.5)	580.17 (71.55)	722.36 (32.31)	756.46 (42.71)	972.89 (26.42)
	✓	580.49 (27.58)	813.65 (23.43)	890.98 (21.67)	994.77 (14.64)	1012.46 (11.67)	1306.61 (5.7)
9	×	561.1 (32.18)	803.38 (20.27)	888.25 (29.14)	991.51 (15.58)	998.72 (19.22)	1268.8 (13.01)
	✓	638.21 (29.47)	874.55 (19.9)	956.52 (24.62)	1055.4 (9.01)	1063.9 (9.12)	1336.37 (8.82)
10	×	540.25 (75.93)	760.3 (42.46)	811.02 (47.81)	927.27 (36.94)	945.53 (32.26)	1189.36 (13.71)
	✓	718.46 (23.47)	943.08 (14.5)	1023.25 (18.55)	1124.31 (6.93)	1126.92 (11.62)	1394.19 (3.95)

Table B.9: Average $\overline{TG_L}$ of systems with $q = 9$, and $s = (1 : 25)$. Column $+I$ shows whether the systems has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

$q = 10$							
I_{max}	$+I$	RNG	GG	GPA	5NN	YAO	ER
1	×	194.91 (23.01)	355.59 (22.27)	365.15 (36.42)	437.52 (21.25)	480.42 (14.11)	620.38 (16.5)
	✓	197.66 (26.23)	356.3 (17.3)	365.13 (36.17)	431.73 (25.62)	475.86 (16.25)	593.59 (28.76)
2	×	249.1 (29.52)	420.54 (15.43)	402.12 (32.17)	524.59 (33.56)	558.93 (18.06)	708.42 (45.95)
	✓	289.18 (12.37)	492.17 (11.02)	516.82 (40.57)	625.6 (18.25)	669.66 (12.54)	866.52 (13.56)
3	×	292.5 (45.01)	477.74 (36.04)	460.77 (38.3)	579.01 (38.09)	632.16 (31.17)	789.27 (26.18)
	✓	351.15 (31.73)	585.09 (19.21)	637.19 (35.28)	742.94 (23.88)	776.38 (12.68)	1016.23 (12.41)
4	×	403.68 (35.12)	613.62 (17.04)	611.51 (42.11)	758.53 (20.84)	794.14 (18.7)	995.73 (30.7)
	✓	438.74 (19.0)	661.29 (15.65)	699.38 (33.48)	825.26 (16.11)	857.71 (15.6)	1127.82 (16.21)
5	×	413.95 (26.92)	638.59 (20.1)	648.65 (35.28)	782.51 (19.34)	819.04 (17.38)	1029.95 (23.01)
	✓	474.45 (16.38)	713.8 (12.26)	783.03 (15.92)	886.0 (8.55)	915.16 (9.57)	1189.2 (8.08)
6	×	549.63 (29.44)	786.11 (17.12)	861.54 (29.72)	963.22 (17.53)	989.03 (11.77)	1272.23 (4.48)
	✓	545.03 (34.96)	786.75 (20.85)	867.11 (27.25)	965.41 (12.32)	986.36 (12.97)	1280.07 (5.53)
7	×	513.97 (37.1)	746.31 (29.05)	772.68 (30.37)	912.84 (18.23)	939.14 (27.67)	1181.15 (26.16)
	✓	580.73 (21.4)	819.0 (18.09)	882.87 (23.75)	996.2 (10.76)	1011.29 (10.71)	1301.01 (6.05)
8	×	558.61 (20.1)	806.59 (12.07)	880.69 (22.06)	988.43 (7.52)	994.73 (13.12)	1268.25 (11.0)
	✓	626.93 (14.14)	851.23 (10.93)	931.26 (17.79)	1033.85 (10.31)	1035.02 (9.33)	1307.54 (11.59)
9	×	749.28 (15.43)	960.75 (9.67)	1009.99 (12.17)	1126.65 (9.15)	1134.18 (9.45)	1368.82 (4.65)
	✓	752.15 (12.19)	963.47 (11.16)	1006.28 (16.98)	1125.68 (7.96)	1135.11 (8.1)	1367.68 (6.36)
10	×	765.94 (10.93)	975.83 (9.31)	1016.12 (22.97)	1145.18 (8.46)	1146.61 (6.52)	1378.32 (5.5)
	✓	768.35 (8.68)	974.93 (10.49)	1013.56 (19.76)	1144.58 (8.47)	1147.02 (7.08)	1377.36 (6.25)

Table B.10: Average $\overline{TG_L}$ of systems with $q = 10$, and $s = (1 : 25)$. Column $+I$ shows whether the systems has extra interlinks added to bridge nodes in $B_h^{(q,u)}$ or not.

$q = 1$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.762	0.685	0.669	0.757	0.725	0.703	0.745	0.321	0.737	0.463
GG	0.606	0.735	0.668	0.761	0.754	0.66	0.755	0.438	0.707	0.511
5NN	0.547	0.705	0.705	0.737	0.737	0.68	0.753	0.493	0.722	0.578
YAO	0.572	0.738	0.682	0.767	0.763	0.69	0.772	0.548	0.728	0.535
GPA	0.581	0.769	0.69	0.684	0.742	0.656	0.772	0.694	0.715	0.63
ER	0.582	0.769	0.686	0.749	0.837	0.688	0.854	0.807	0.823	0.781
$q = 2$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.364	0.649	0.641	0.694	0.665	0.424	0.469	0.579	0.444	0.471
GG	0.349	0.546	0.519	0.582	0.595	0.422	0.481	0.55	0.499	0.501
5NN	0.348	0.441	0.422	0.522	0.431	0.335	0.464	0.541	0.491	0.464
YAO	0.372	0.497	0.504	0.551	0.528	0.37	0.486	0.567	0.534	0.537
GPA	0.455	0.404	0.419	0.483	0.497	0.361	0.448	0.609	0.474	0.495
ER	0.469	0.356	0.427	0.513	0.533	0.512	0.507	0.664	0.576	0.603

Table B.11: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks built using $q \in \{1, 2\}$, after adding extra interlinks.

$q = 3$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.784	0.692	0.699	0.65	0.66	0.275	0.596	0.496	0.485	0.513
GG	0.652	0.665	0.61	0.635	0.659	0.253	0.568	0.53	0.5	0.517
5NN	0.556	0.587	0.554	0.563	0.575	0.264	0.564	0.502	0.512	0.517
YAO	0.583	0.665	0.59	0.6	0.646	0.278	0.583	0.514	0.531	0.554
GPA	0.502	0.666	0.599	0.505	0.573	0.374	0.543	0.492	0.568	0.585
ER	0.478	0.683	0.503	0.56	0.593	0.536	0.698	0.652	0.733	0.777
$q = 4$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.733	0.714	0.603	0.692	0.823	0.683	0.79	0.844	0.732	0.801
GG	0.701	0.687	0.676	0.719	0.804	0.746	0.791	0.857	0.788	0.781
5NN	0.671	0.726	0.743	0.764	0.782	0.728	0.806	0.821	0.793	0.776
YAO	0.716	0.659	0.735	0.776	0.802	0.758	0.821	0.824	0.792	0.794
GPA	0.846	0.717	0.833	0.777	0.791	0.751	0.806	0.791	0.752	0.764
ER	0.829	0.746	0.902	0.848	0.89	0.843	0.913	0.864	0.882	0.872

Table B.12: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks built using $q \in \{3, 4\}$, after adding extra interlinks.

$q = 5$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.821	0.957	0.813	0.853	0.876	0.862	0.659	0.9	0.142	0.166
GG	0.841	0.924	0.83	0.857	0.845	0.875	0.709	0.866	0.175	0.212
5NN	0.868	0.87	0.837	0.838	0.855	0.873	0.737	0.858	0.285	0.313
YAO	0.857	0.859	0.823	0.858	0.856	0.88	0.749	0.873	0.242	0.237
GPA	0.888	0.798	0.827	0.827	0.871	0.858	0.784	0.842	0.588	0.654
ER	0.957	0.784	0.803	0.935	0.85	0.924	0.841	0.898	0.666	0.623
$q = 6$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.745	0.787	0.085	0.797	0.793	0.868	0.104	0.875	0.861	0.931
GG	0.718	0.802	0.15	0.845	0.818	0.892	0.149	0.86	0.833	0.895
5NN	0.692	0.747	0.292	0.781	0.842	0.886	0.231	0.874	0.817	0.859
YAO	0.684	0.759	0.25	0.805	0.833	0.865	0.173	0.875	0.844	0.856
GPA	0.788	0.769	0.509	0.812	0.82	0.851	0.455	0.868	0.823	0.823
ER	0.738	0.764	0.653	0.802	0.852	0.873	0.676	0.905	0.872	0.882

Table B.13: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks built using $q \in \{5, 6\}$, after adding extra interlinks.

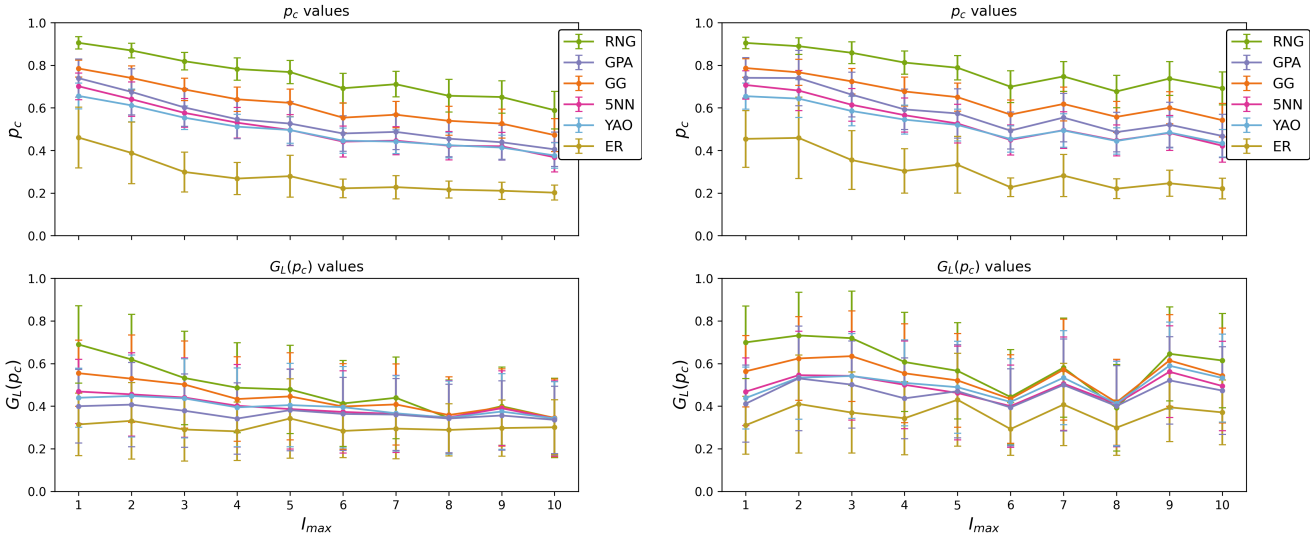
$q = 7$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.696	0.686	0.73	0.738	0.728	0.614	0.674	0.045	0.489	0.693
GG	0.618	0.718	0.738	0.791	0.729	0.644	0.736	0.097	0.6	0.74
5NN	0.547	0.77	0.725	0.718	0.694	0.68	0.737	0.144	0.632	0.713
YAO	0.542	0.74	0.756	0.758	0.739	0.689	0.725	0.149	0.622	0.731
GPA	0.568	0.877	0.738	0.716	0.739	0.734	0.744	0.369	0.732	0.752
ER	0.58	0.865	0.719	0.738	0.729	0.763	0.825	0.631	0.791	0.82
$q = 8$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.751	0.792	0.813	0.915	0.869	0.106	0.849	0.868	0.716	0.894
GG	0.689	0.771	0.853	0.915	0.883	0.151	0.87	0.874	0.74	0.867
5NN	0.627	0.728	0.831	0.855	0.876	0.252	0.851	0.865	0.794	0.901
YAO	0.602	0.742	0.831	0.846	0.883	0.228	0.884	0.866	0.738	0.87
GPA	0.778	0.756	0.856	0.843	0.848	0.494	0.82	0.863	0.838	0.853
ER	0.622	0.719	0.827	0.778	0.853	0.674	0.911	0.907	0.853	0.903

Table B.14: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks built using $q \in \{7, 8\}$, after adding extra interlinks.

$q = 9$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.737	0.798	0.752	0.796	0.875	0.932	0.532	0.806	0.856	0.842
GG	0.66	0.734	0.742	0.782	0.827	0.897	0.597	0.858	0.854	0.814
5NN	0.597	0.704	0.715	0.771	0.821	0.863	0.651	0.831	0.85	0.799
YAO	0.576	0.708	0.714	0.763	0.802	0.863	0.641	0.85	0.829	0.848
GPA	0.64	0.747	0.74	0.751	0.799	0.802	0.792	0.847	0.821	0.777
ER	0.631	0.714	0.688	0.746	0.769	0.786	0.804	0.86	0.827	0.843
$q = 10$										
m/I_{max}	1	2	3	4	5	6	7	8	9	10
RNG	0.711	0.867	0.781	0.7	0.853	0.786	0.86	0.503	0.076	0.075
GG	0.692	0.868	0.783	0.802	0.854	0.802	0.828	0.59	0.116	0.108
5NN	0.693	0.844	0.758	0.782	0.833	0.852	0.832	0.628	0.226	0.209
YAO	0.713	0.835	0.771	0.793	0.841	0.796	0.848	0.65	0.196	0.137
GPA	0.82	0.897	0.816	0.797	0.844	0.832	0.865	0.714	0.506	0.502
ER	0.825	0.881	0.823	0.903	0.895	0.871	0.895	0.877	0.659	0.667

Table B.15: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks built using $q \in \{9, 10\}$, after adding extra interlinks.

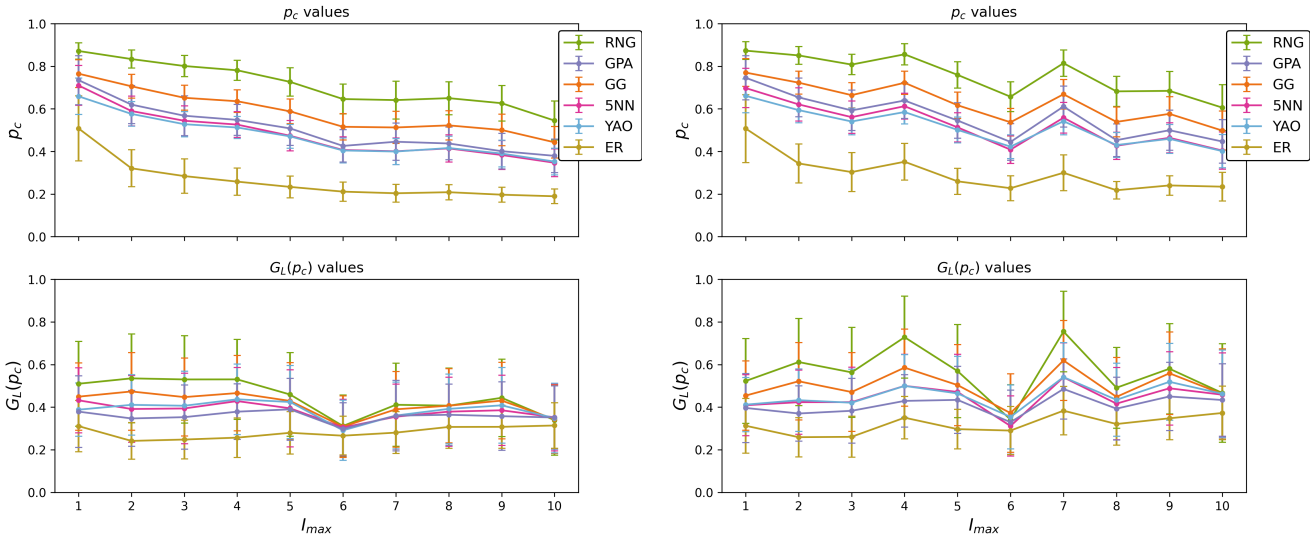
B.2 Robustness comparison figures



(a) (1:25) with extra interlinks

(b) (1:25)

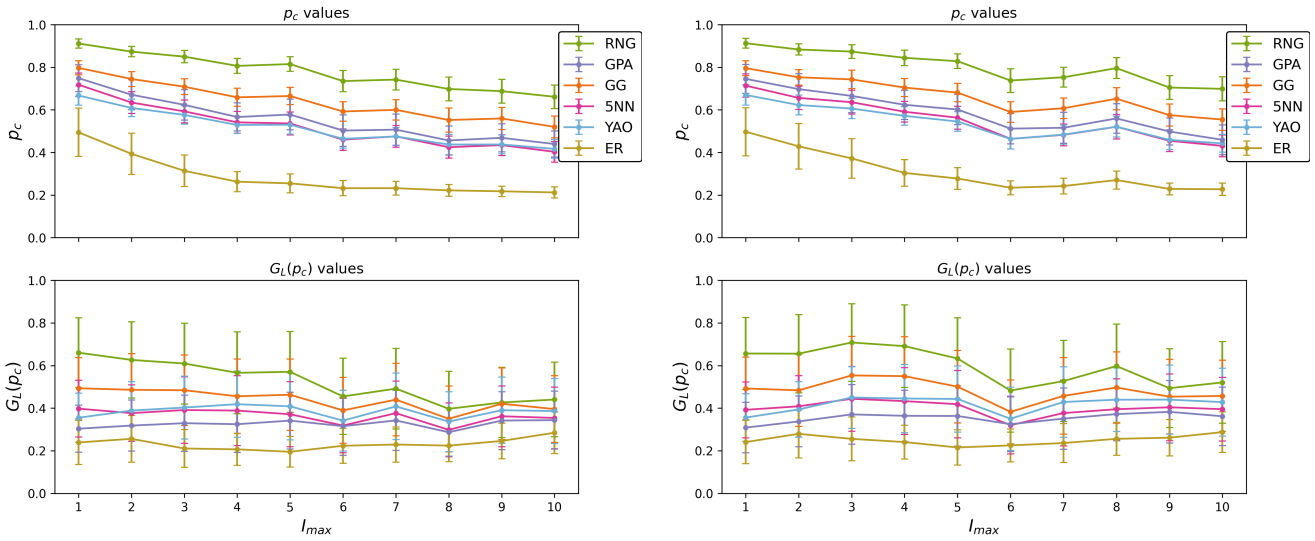
Figure B.1: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 1$.



(a) (1:25) with extra interlinks

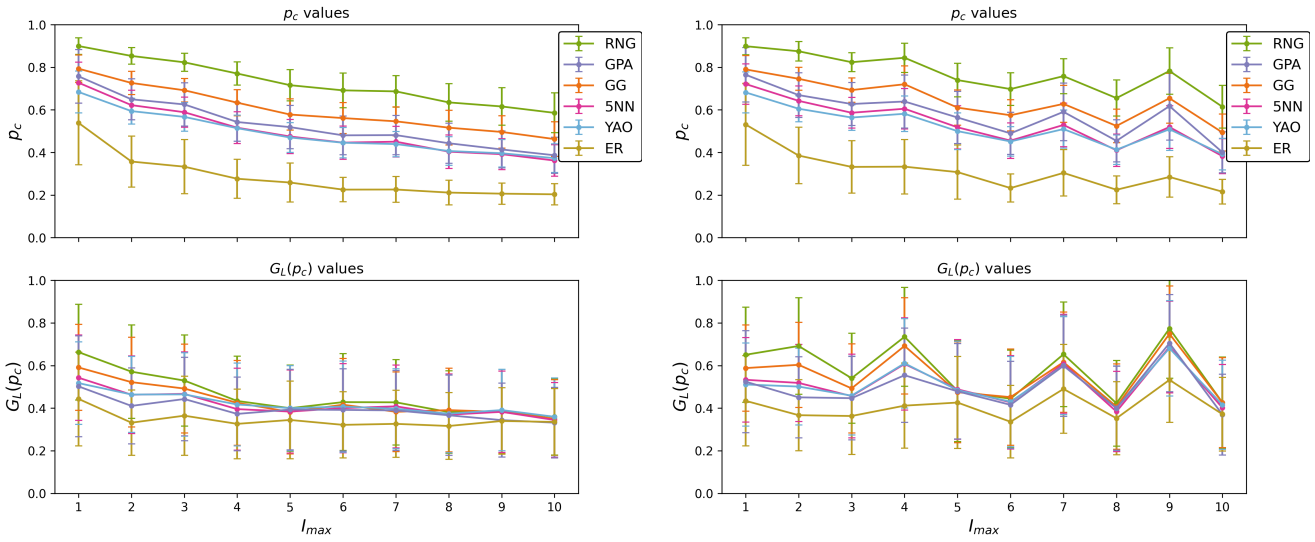
(b) (1:25)

Figure B.2: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 2$.



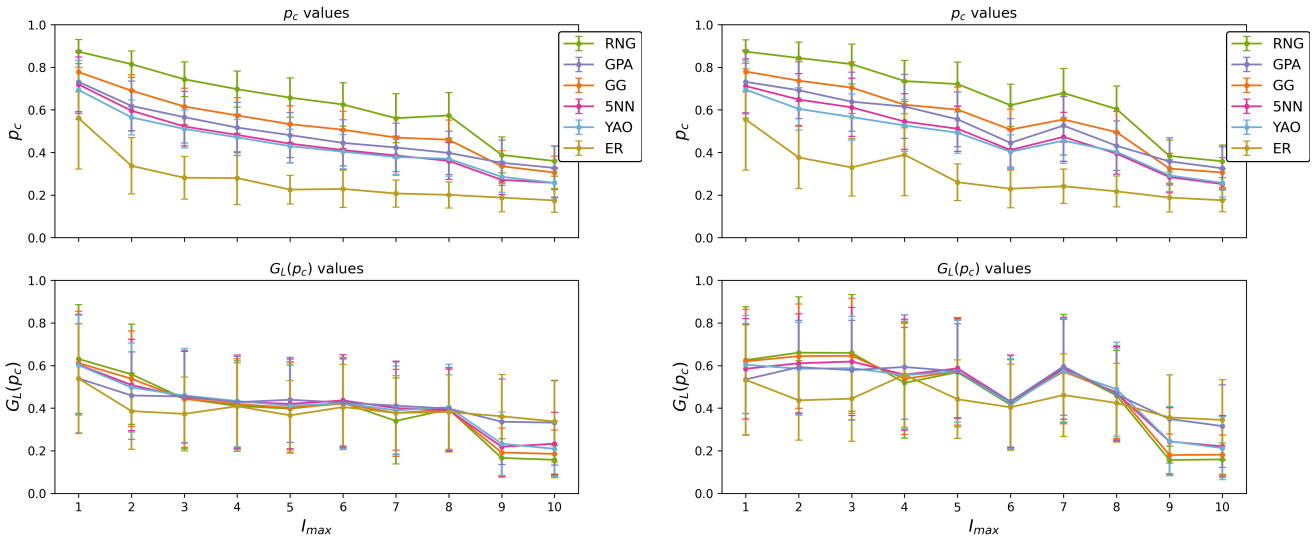
(a) (1:25) with extra interlinks (b) (1:25)

Figure B.3: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 3$.



(a) (1:25) with extra interlinks (b) (1:25)

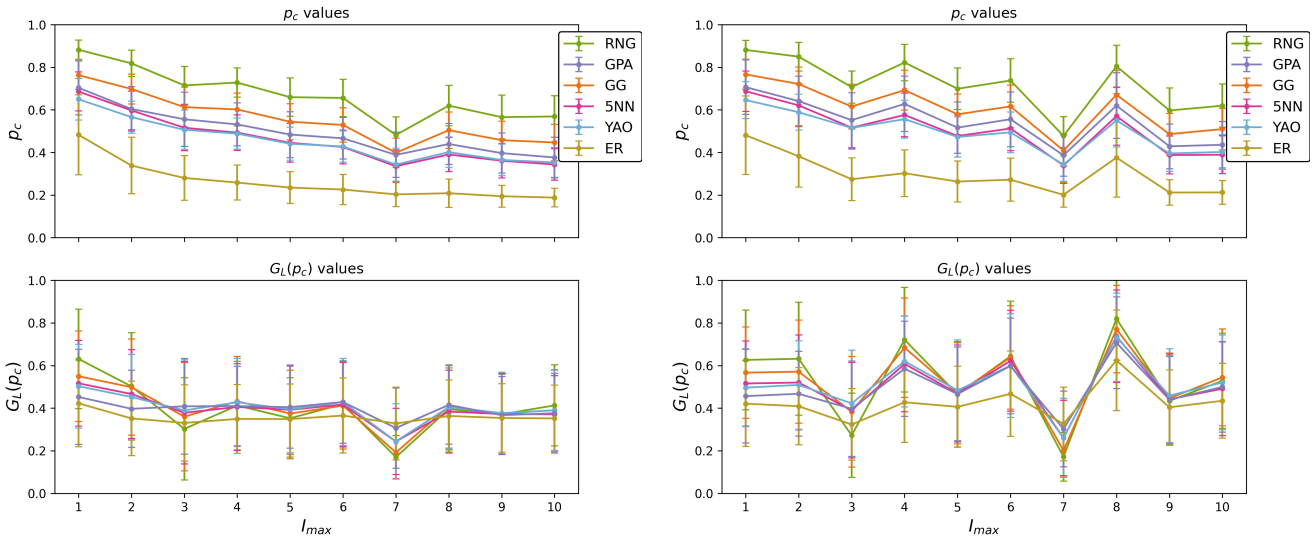
Figure B.4: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 4$.



(a) (1:25) with extra interlinks

(b) (1:25)

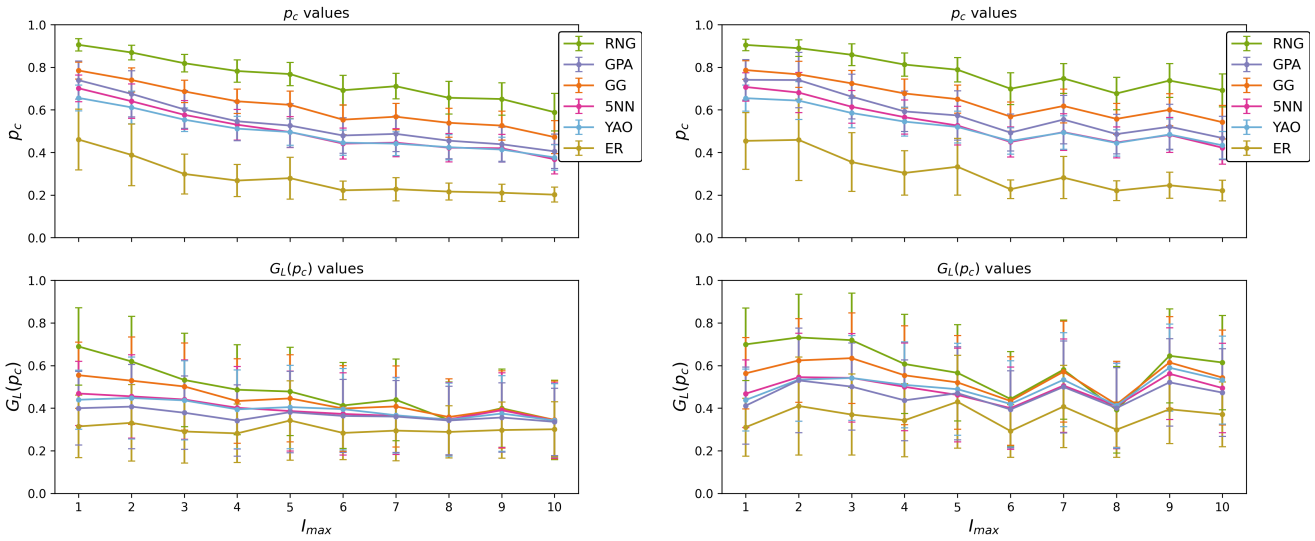
Figure B.5: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 5$.



(a) (1:25) with extra interlinks

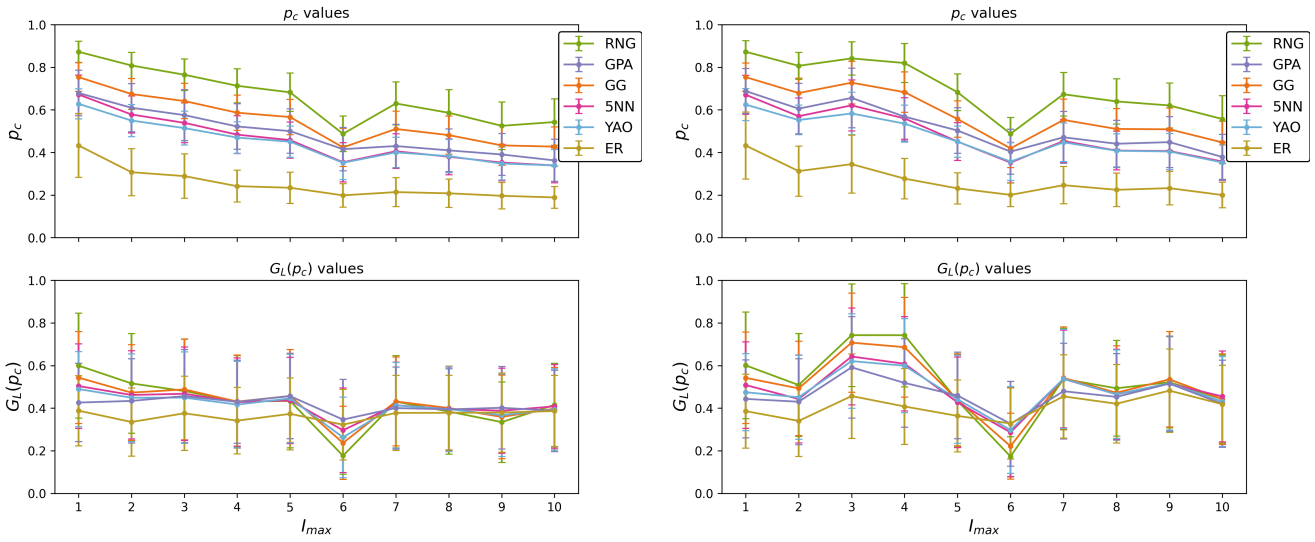
(b) (1:25)

Figure B.6: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 6$.



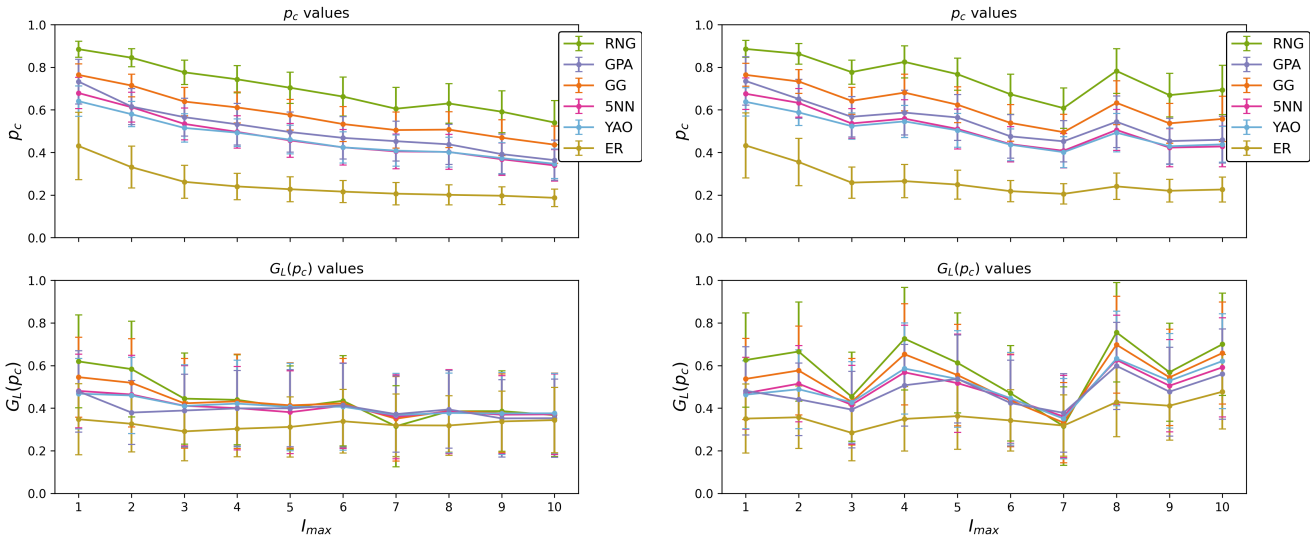
(a) (1:25) with extra interlinks (b) (1:25)

Figure B.7: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 7$.



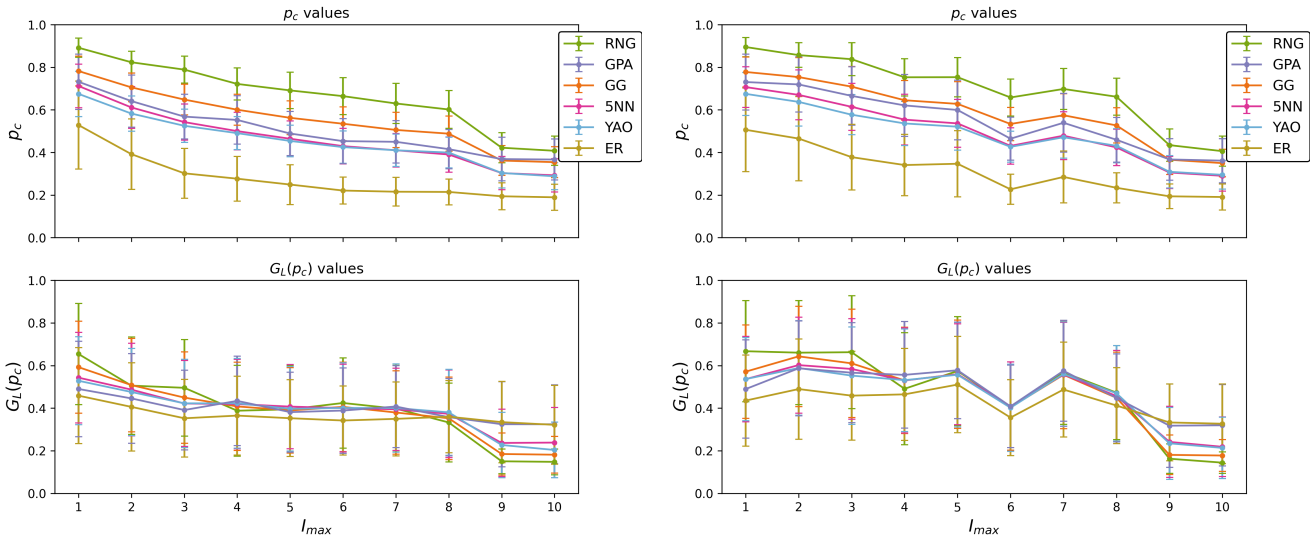
(a) (1:25) with extra interlinks (b) (1:25)

Figure B.8: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 8$.



(a) (1:25) with extra interlinks (b) (1:25)

Figure B.9: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 9$.



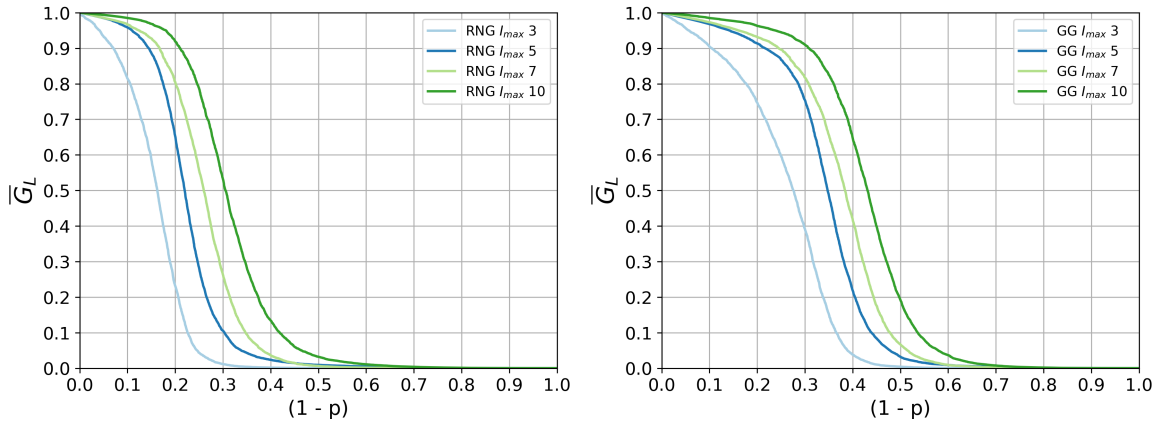
(a) (1:25) with extra interlinks (b) (1:25)

Figure B.10: Average p_c and $G_L(p_c)$ values before and after adding extra interlinks for systems with $s = (1{:}25)$ and $q = 10$.

Annexed C

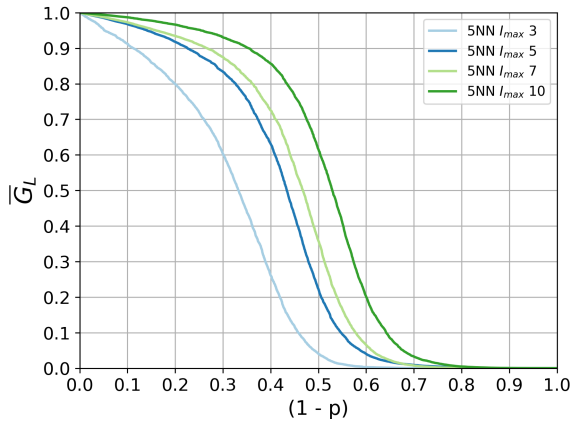
Chapter 5: Effect of adding physical links

C.1 General robustness behavior figures

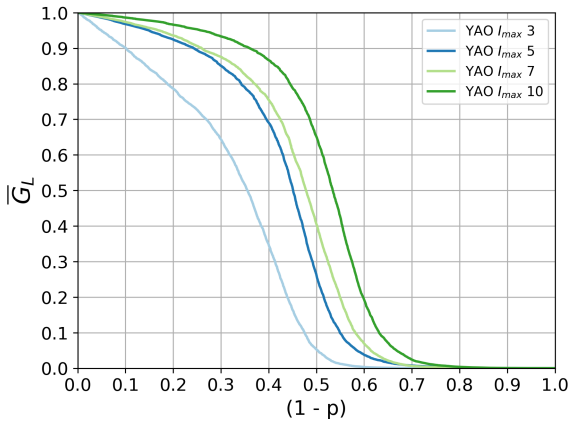


(a) RNG

(b) GG

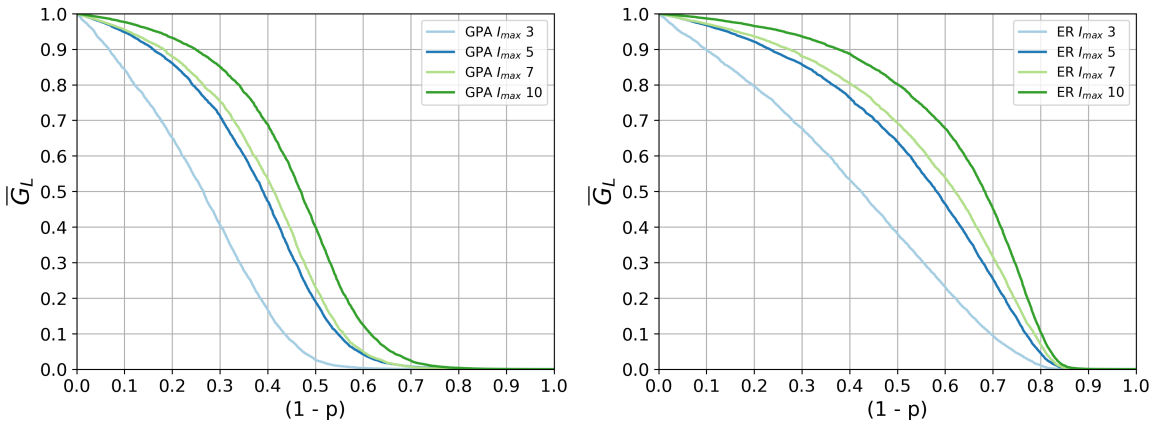


(c) 5NN



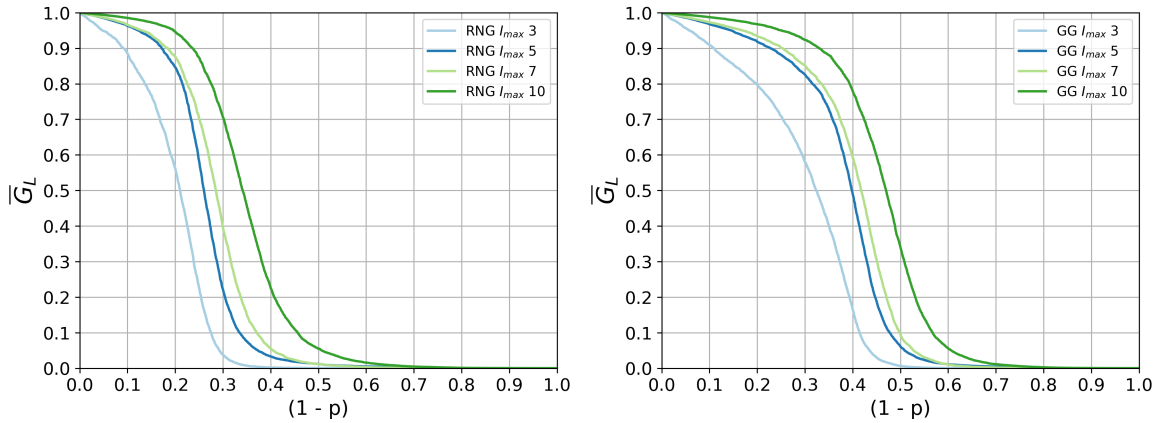
(d) YAO

Figure C.1: Average robustness by model for systems built over a (1:25) space, logical network version $q = 1$, and $m \in$ {RNG, GG, 5NN, YAO} after adding extra physical links according to Distance strategy.



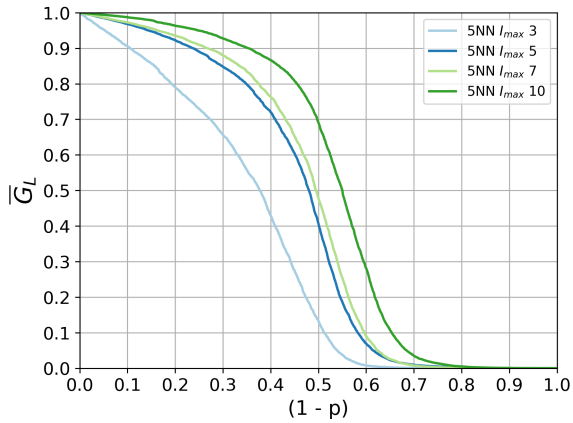
(a) GPA (b) ER

Figure C.2: Average robustness by model for systems built over a (1:25) space, logical network version $q = 1$, and $m \in \{\text{GPA, ER}\}$ after adding extra physical links according to Distance strategy.

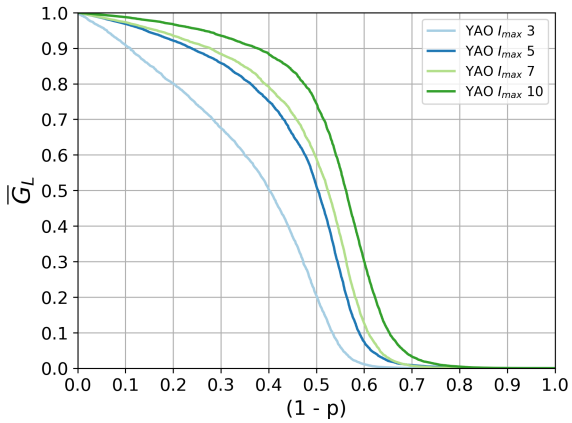


(a) RNG

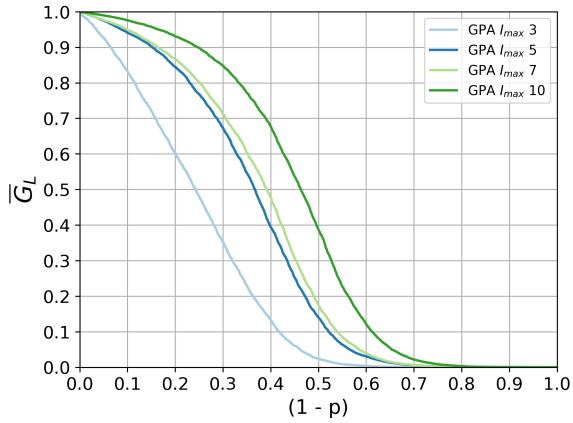
(b) GG



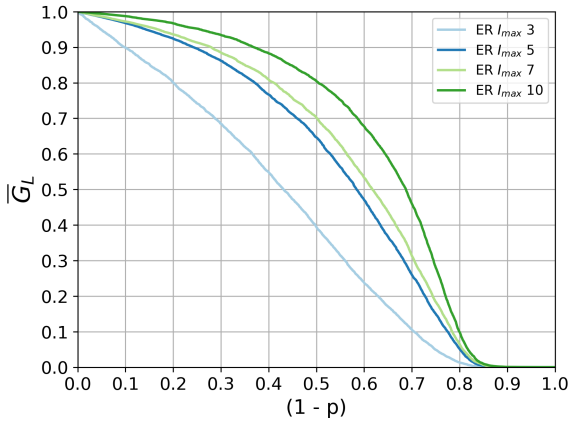
(c) 5NN



(d) YAO

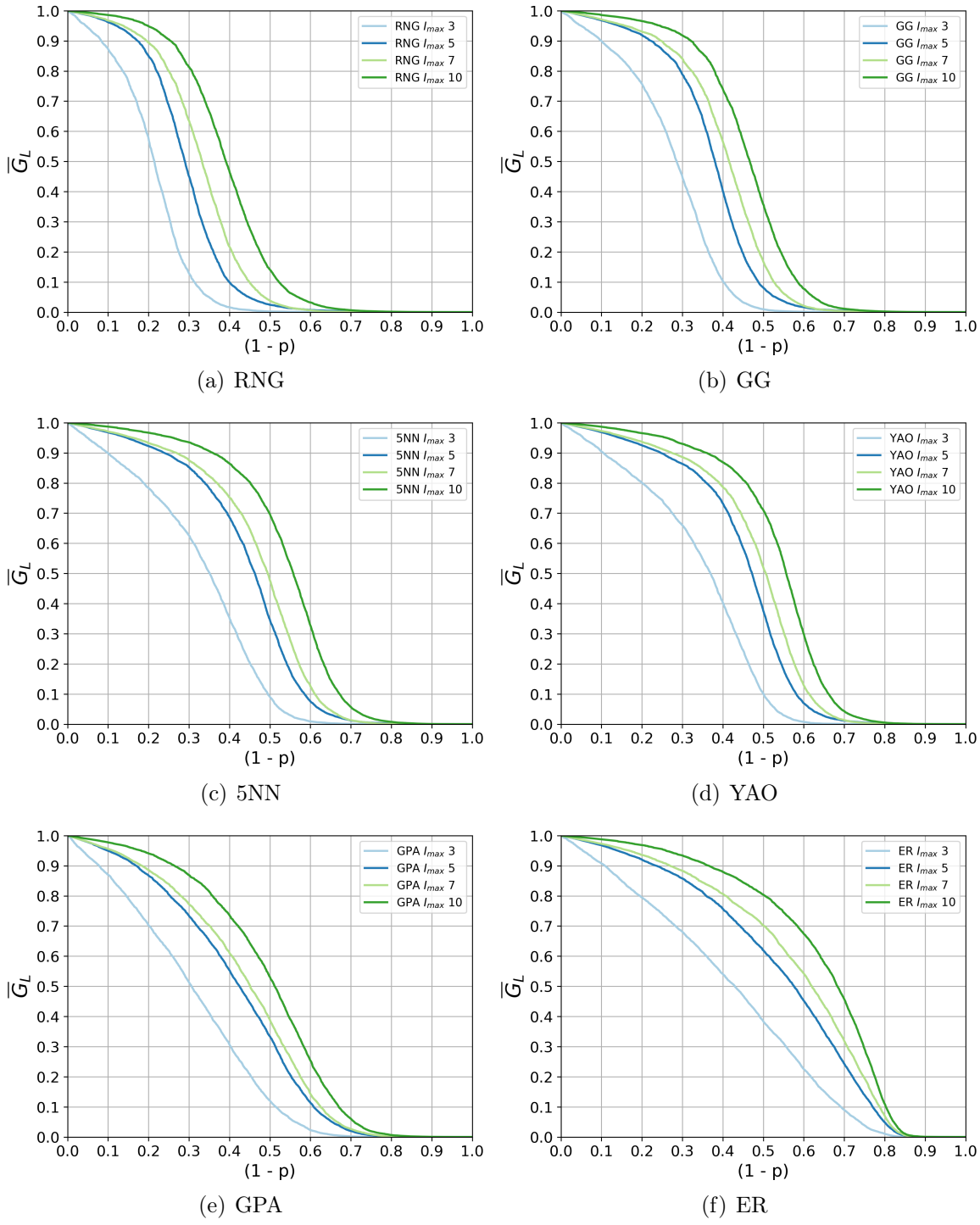


(e) GPA



(f) ER

Figure C.3: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 1$ after adding extra physical links according to Distance strategy.

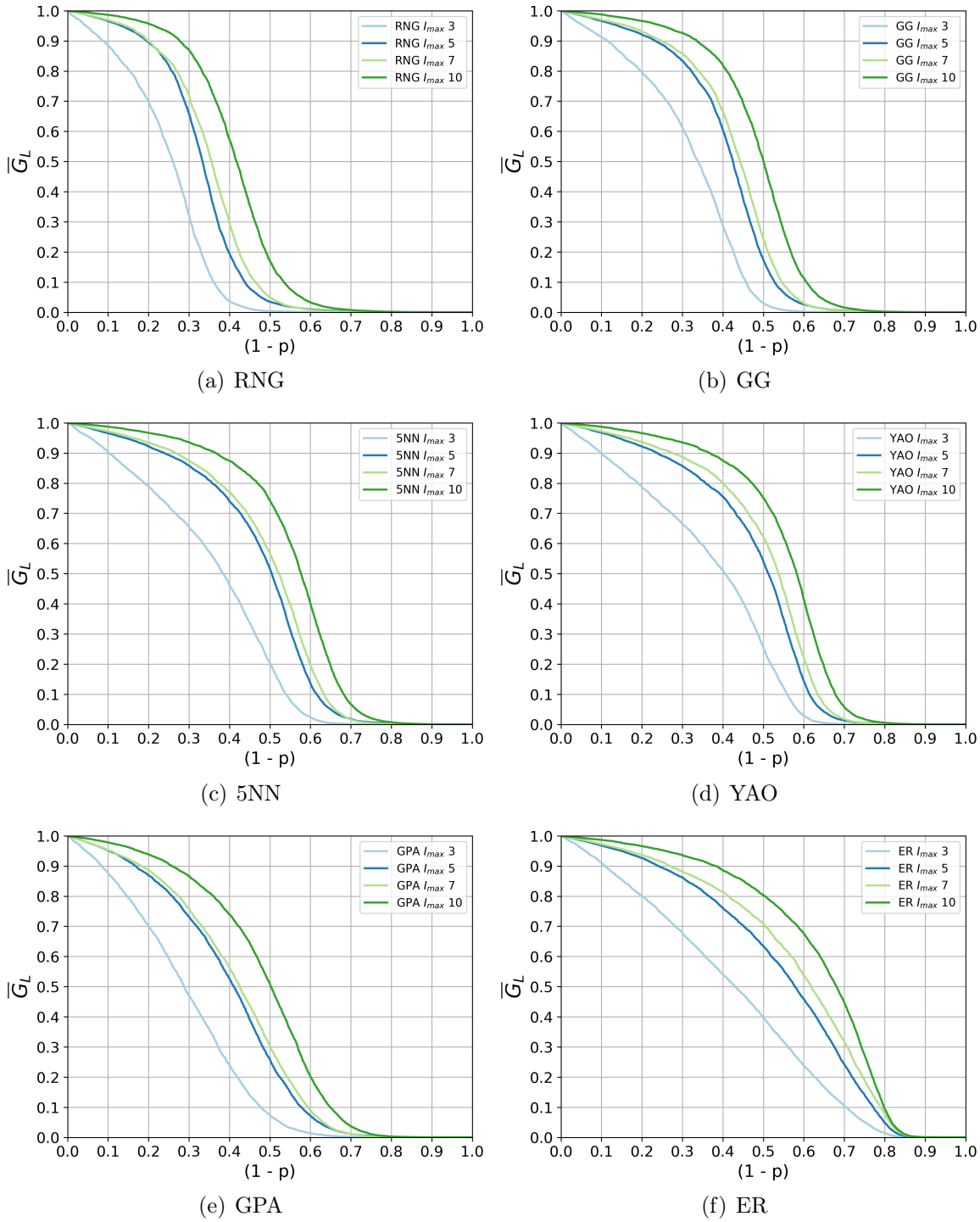


(a) RNG (b) GG

(c) 5NN (d) YAO

(e) GPA (f) ER

Figure C.4: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 1$ after adding extra physical links according to Local hubs strategy.

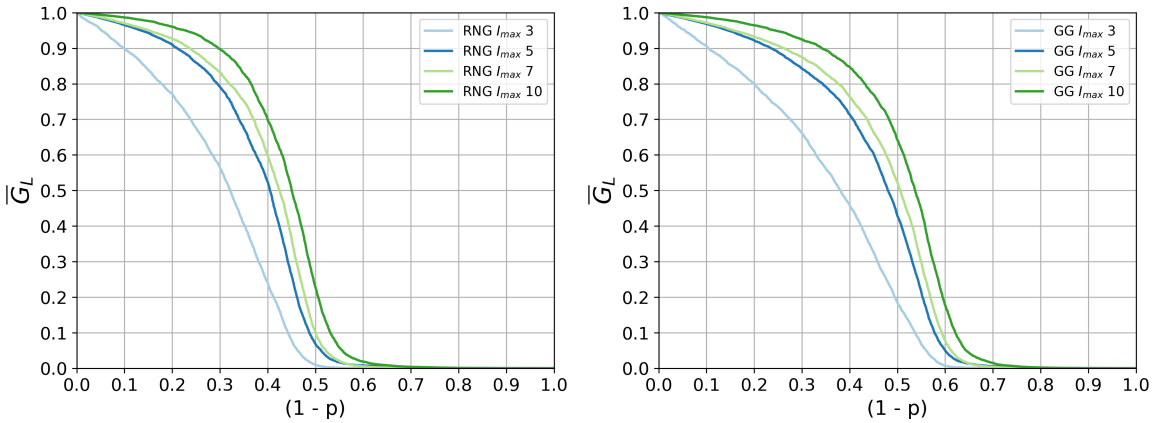


(a) RNG (b) GG

(c) 5NN (d) YAO

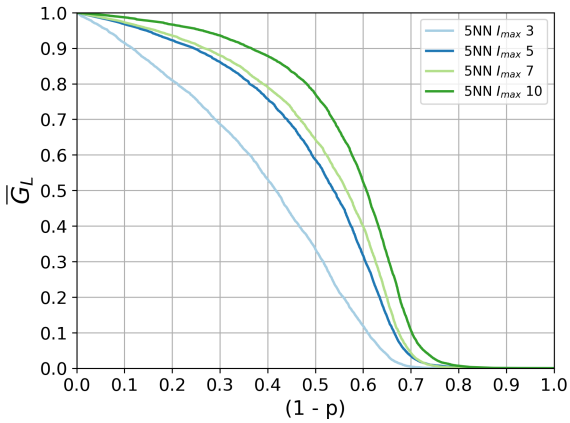
(e) GPA (f) ER

Figure C.5: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 1$ after adding extra physical links according to Local hubs strategy.

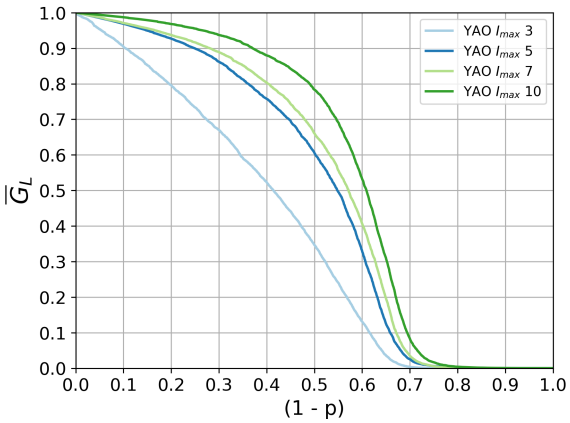


(a) RNG

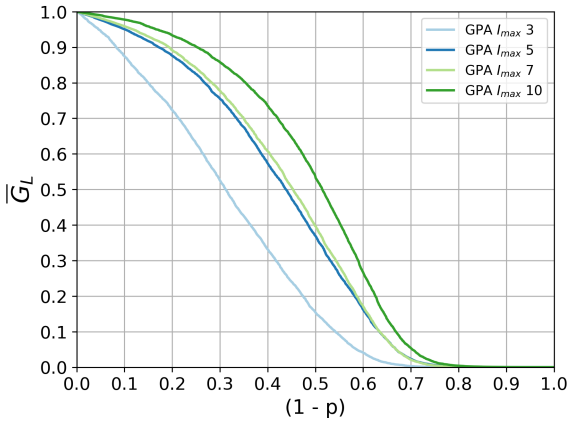
(b) GG



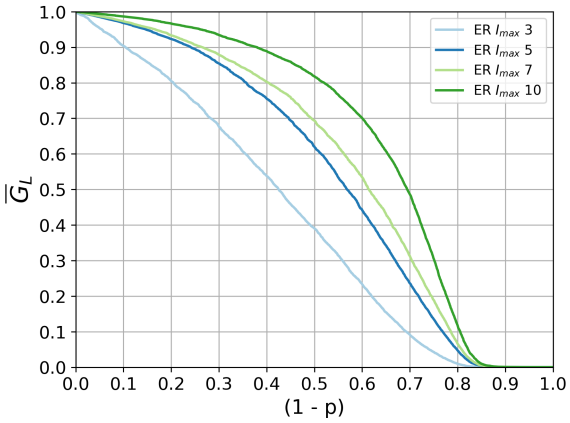
(c) 5NN



(d) YAO

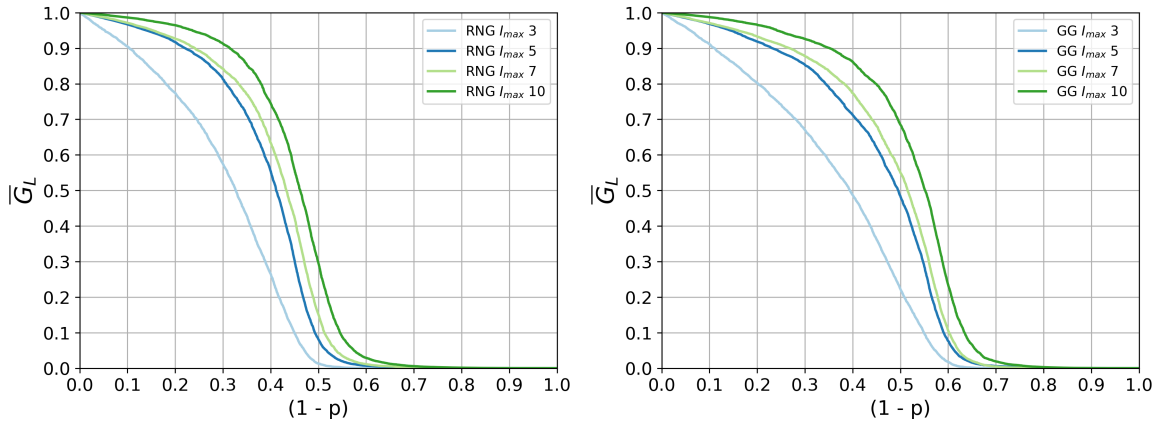


(e) GPA



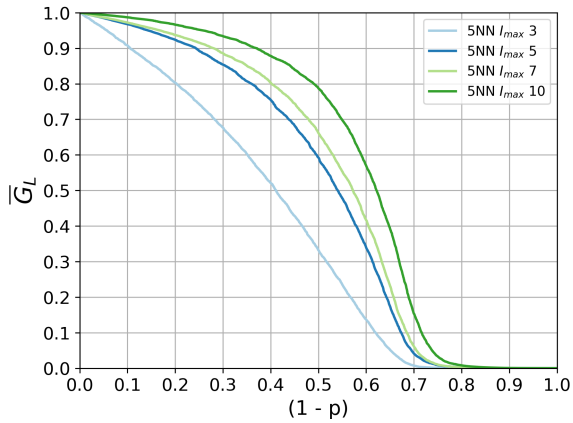
(f) ER

Figure C.6: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 1$ after adding extra physical links according to Degree strategy.

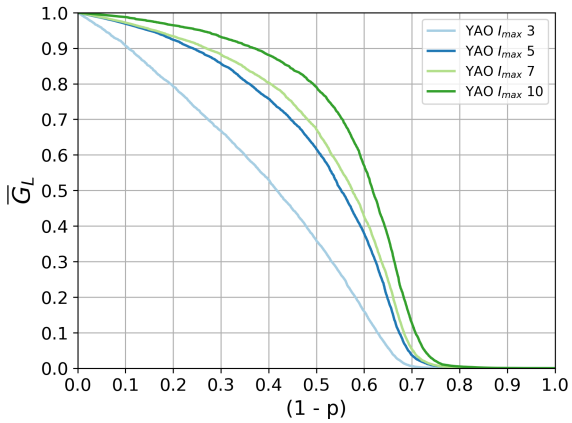


(a) RNG

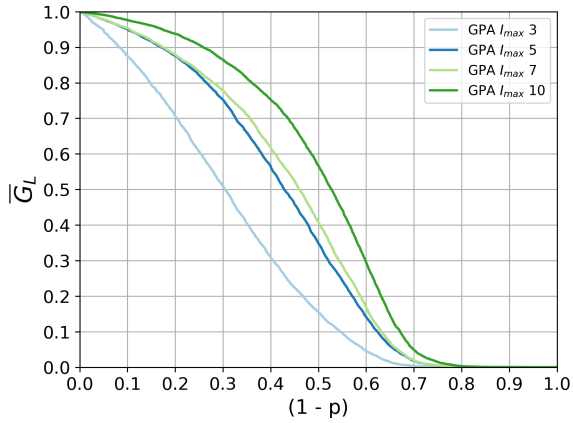
(b) GG



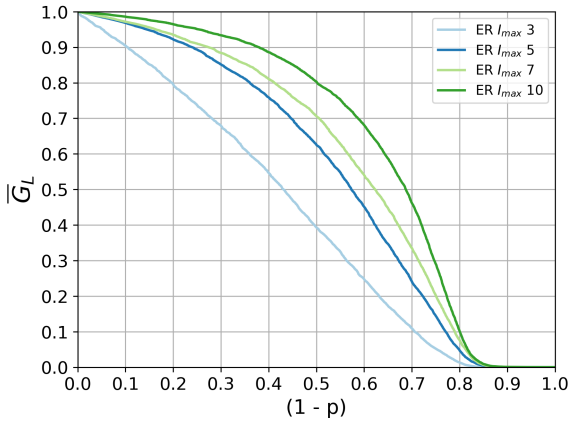
(c) 5NN



(d) YAO

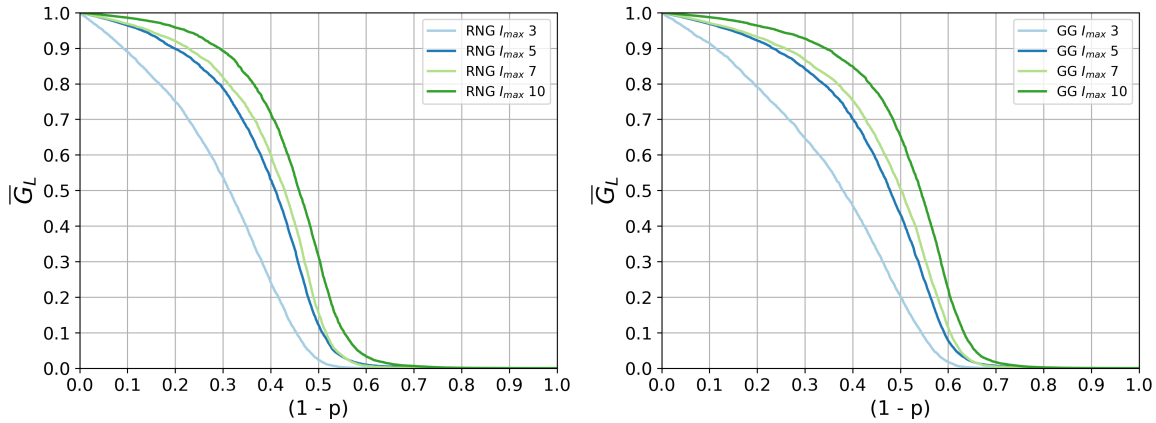


(e) GPA



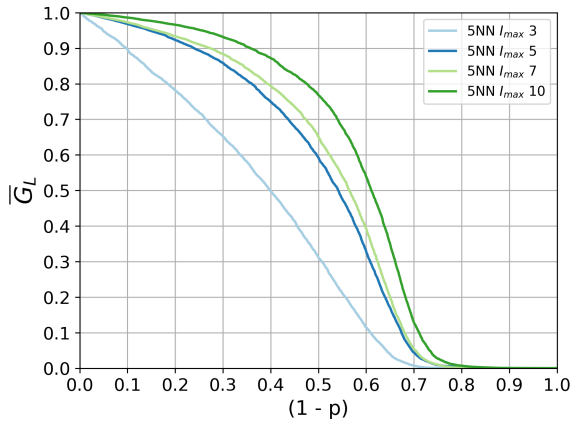
(f) ER

Figure C.7: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 1$ after adding extra physical links according to Degree strategy.

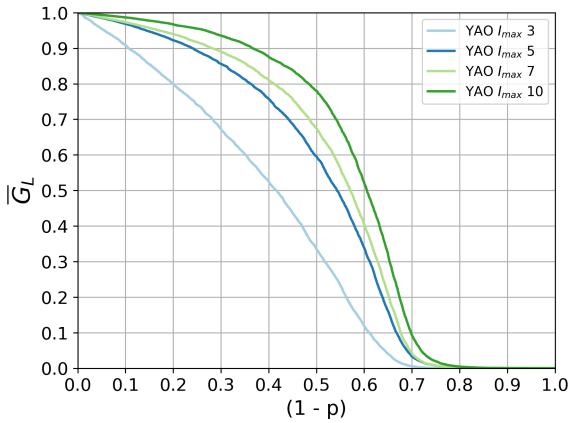


(a) RNG

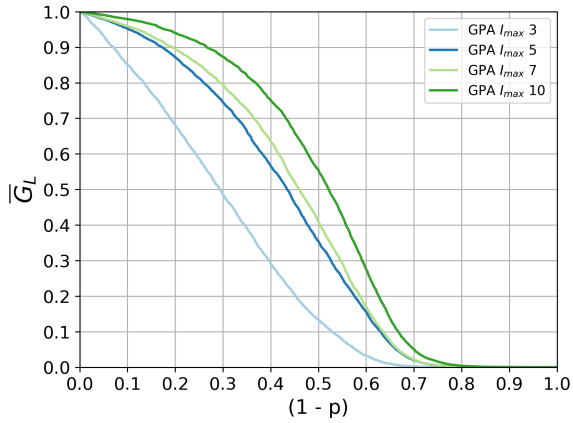
(b) GG



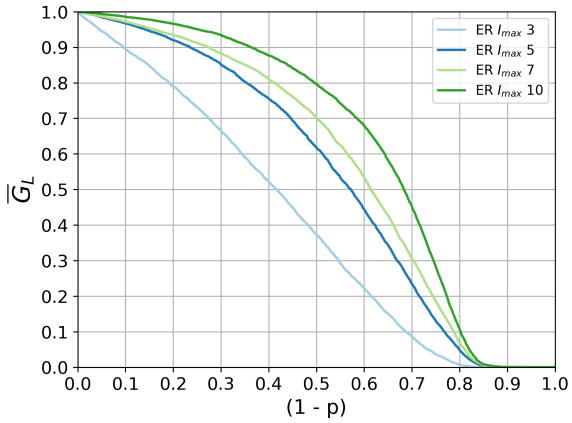
(c) 5NN



(d) YAO

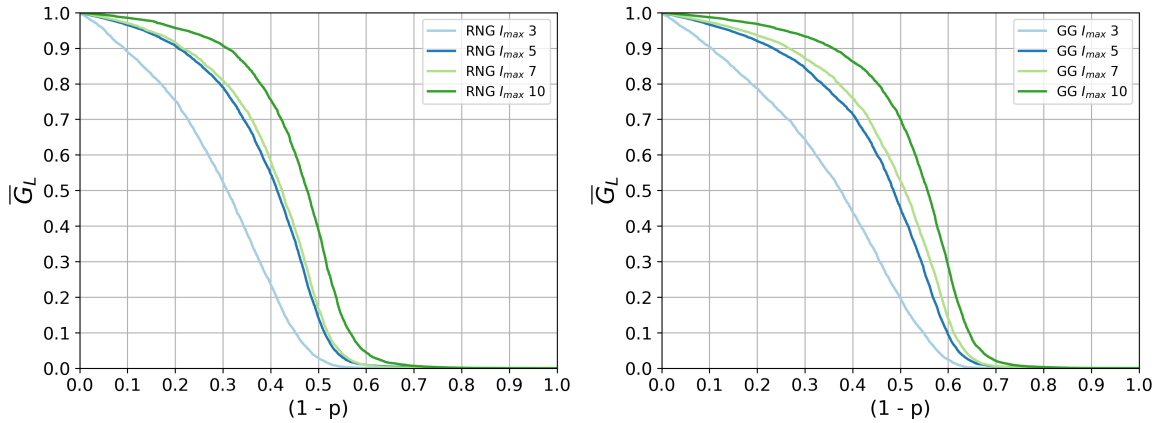


(e) GPA



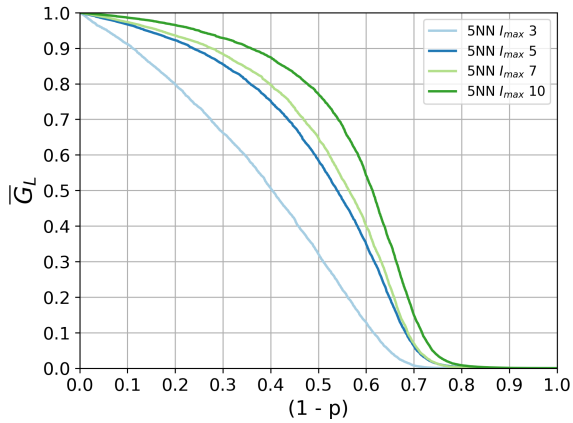
(f) ER

Figure C.8: Average robustness by model for systems built over a (1:25) space, and logical network version $q = 1$ after adding extra physical links according to Random strategy.

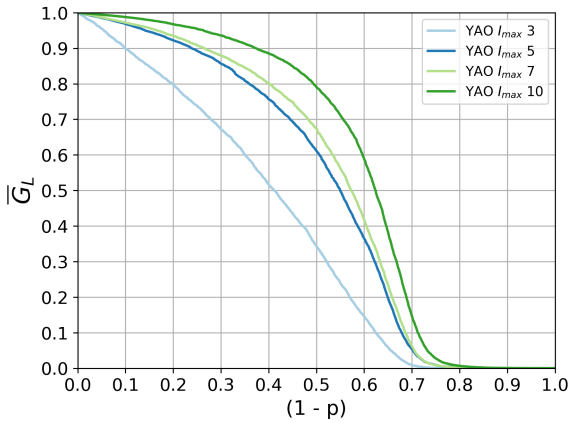


(a) RNG

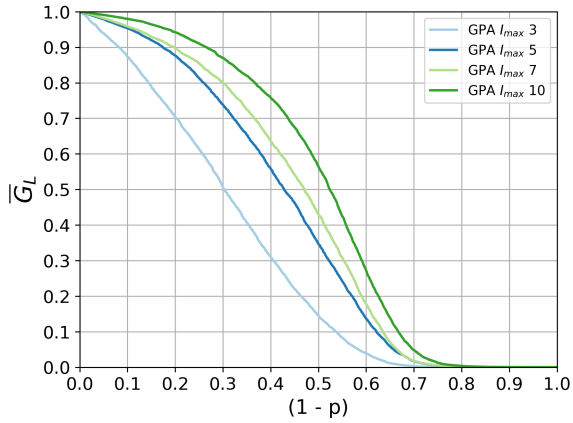
(b) GG



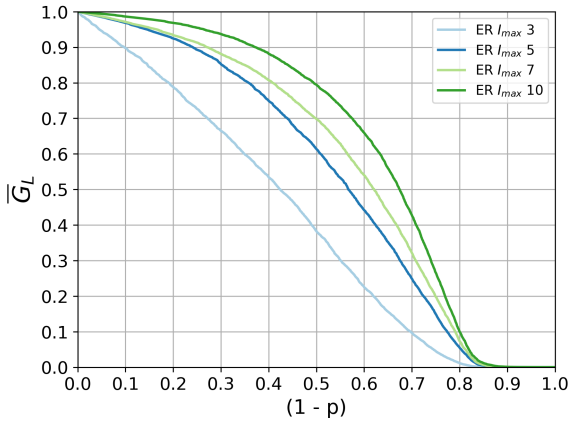
(c) 5NN



(d) YAO

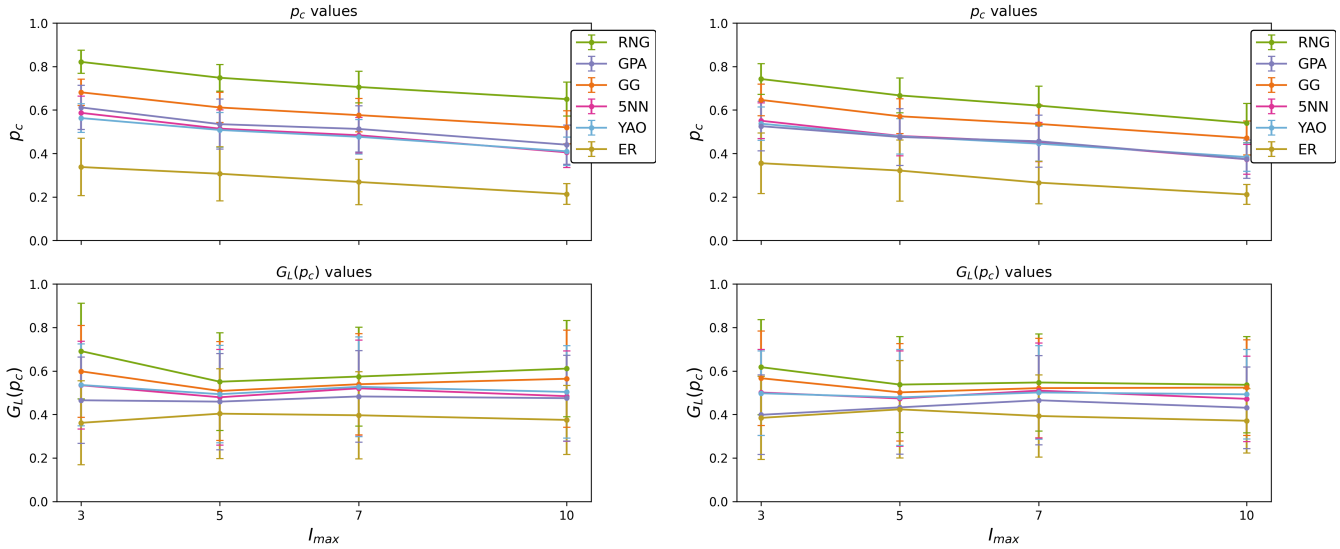


(e) GPA



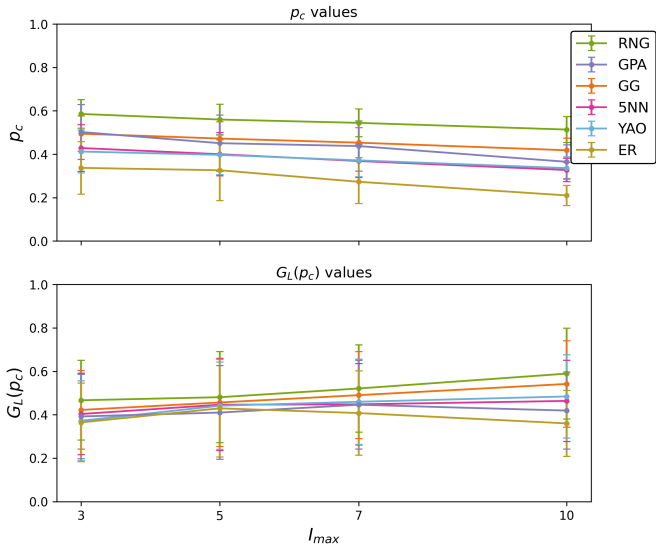
(f) ER

Figure C.9: Average robustness by model for systems built over a (1:1) space, and logical network version $q = 1$ after adding extra physical links according to Random strategy.

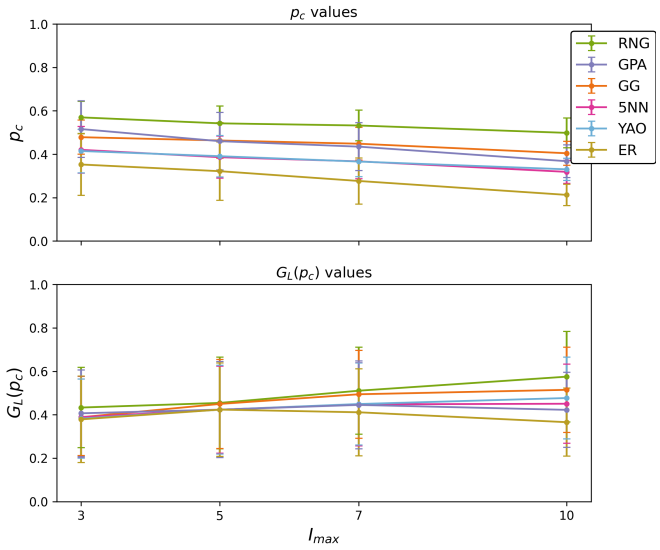


(a) Distance

(b) Local hubs

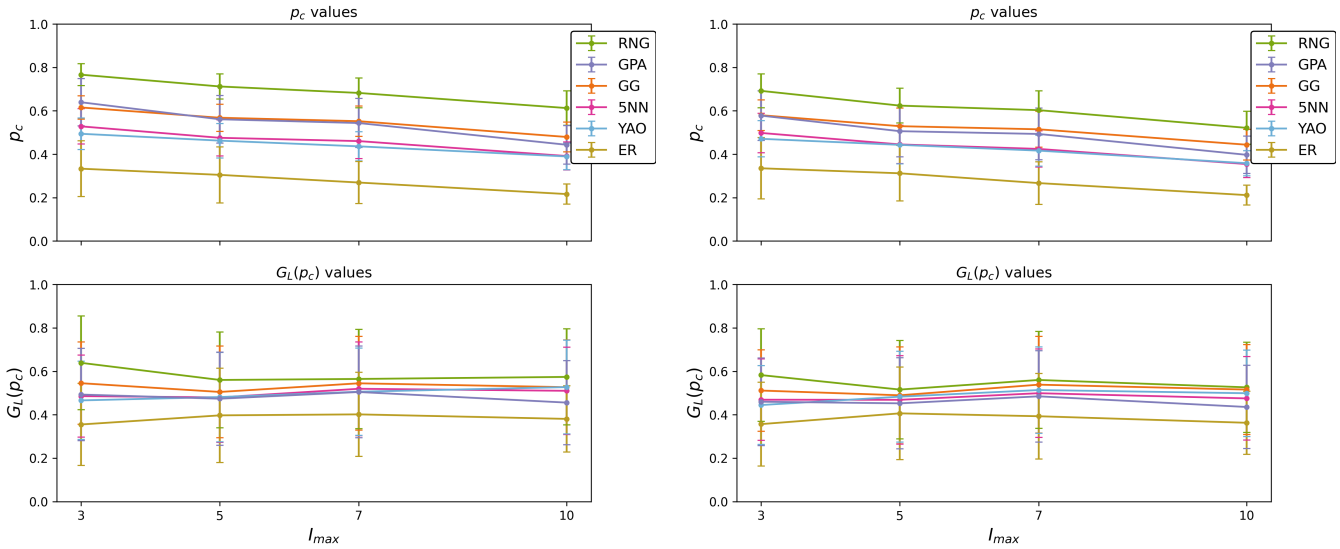


(c) Degree



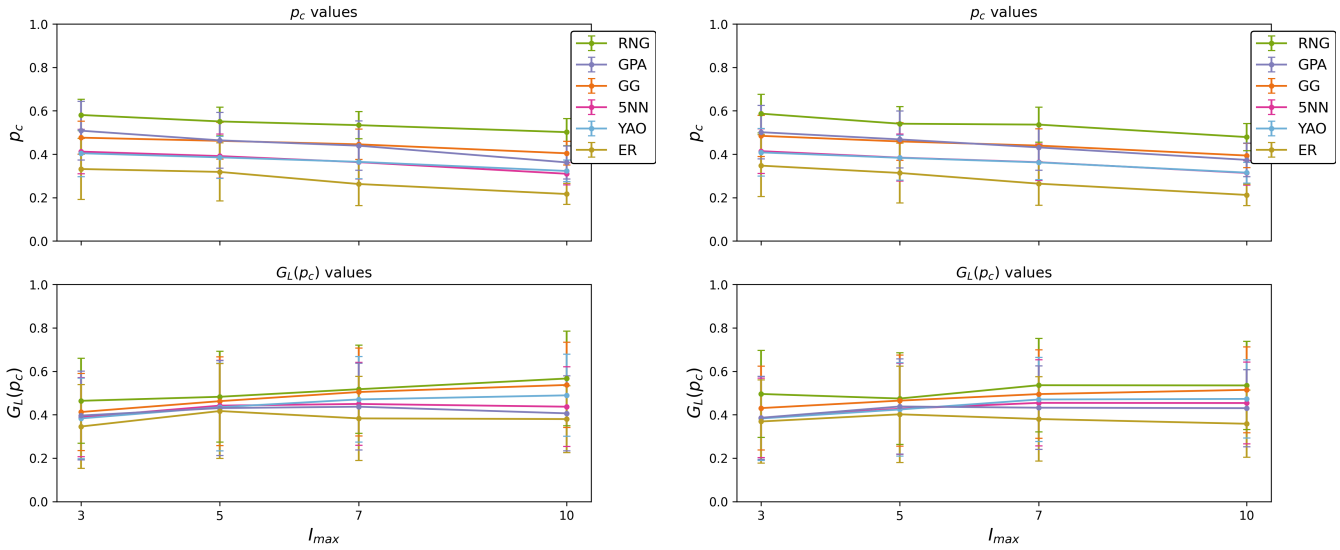
(d) Random

Figure C.10: Average values of p_c and $G_L(p_c)$ for each physical-logical interdependent network built using $s = (1{:}25)$, after adding extra physical links. Bars represent the standard deviation.



(a) Distance

(b) Local hubs



(c) Degree

(d) Random

Figure C.11: Average values of p_c and $G_L(p_c)$ for each physical-logical interdependent network built using $s = (1{:}1)$, after adding extra physical links. Bars represent the standard deviation.

C.2 General robustness behavior tables

st = Distance				
m/I_{max}	3	5	7	10
RNG	0.803	0.826	0.897	0.773
GG	0.662	0.855	0.861	0.723
5NN	0.608	0.818	0.844	0.609
YAO	0.555	0.822	0.819	0.671
GPA	0.517	0.802	0.818	0.567
ER	0.402	0.859	0.75	0.552
st = Local hubs				
m/I_{max}	3	5	7	10
RNG	0.714	0.825	0.882	0.678
GG	0.616	0.831	0.867	0.642
5NN	0.532	0.834	0.835	0.594
YAO	0.537	0.811	0.834	0.618
GPA	0.512	0.838	0.8	0.514
ER	0.433	0.866	0.76	0.536
st = Degree				
m/I_{max}	3	5	7	10
RNG	0.573	0.857	0.861	0.771
GG	0.501	0.843	0.852	0.683
5NN	0.492	0.857	0.795	0.606
YAO	0.453	0.856	0.823	0.67
GPA	0.513	0.878	0.803	0.566
ER	0.413	0.87	0.762	0.577
st = Random				
m/I_{max}	3	5	7	10
RNG	0.537	0.881	0.882	0.753
GG	0.494	0.841	0.835	0.676
5NN	0.429	0.848	0.819	0.65
YAO	0.446	0.856	0.811	0.624
GPA	0.458	0.853	0.81	0.547
ER	0.418	0.84	0.766	0.529

Table C.1: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks built using $s = (1{:}25)$, after adding extra physical links.

st = Distance				
m/I_{max}	3	5	7	10
RNG	0.78	0.802	0.86	0.71
GG	0.64	0.805	0.865	0.674
5NN	0.538	0.828	0.864	0.626
YAO	0.523	0.822	0.829	0.668
GPA	0.557	0.826	0.829	0.558
ER	0.414	0.864	0.736	0.548
st = Local hubs				
m/I_{max}	3	5	7	10
RNG	0.676	0.791	0.899	0.644
GG	0.563	0.818	0.84	0.66
5NN	0.487	0.83	0.836	0.602
YAO	0.495	0.823	0.801	0.622
GPA	0.555	0.844	0.825	0.562
ER	0.433	0.873	0.731	0.502
st = Degree				
m/I_{max}	3	5	7	10
RNG	0.579	0.859	0.799	0.74
GG	0.526	0.846	0.838	0.664
5NN	0.471	0.858	0.797	0.62
YAO	0.455	0.851	0.791	0.645
GPA	0.529	0.88	0.815	0.601
ER	0.425	0.847	0.742	0.558
st = Random				
m/I_{max}	3	5	7	10
RNG	0.536	0.873	0.886	0.728
GG	0.476	0.888	0.827	0.683
5NN	0.441	0.839	0.791	0.566
YAO	0.458	0.861	0.793	0.617
GPA	0.494	0.863	0.821	0.571
ER	0.42	0.839	0.742	0.484

Table C.2: Fraction of iterations that undergo an abrupt collapse for physical-logical interdependent networks built using $s = (1{:}1)$, after adding extra physical links.

C.3 Effect of adding physical links figures

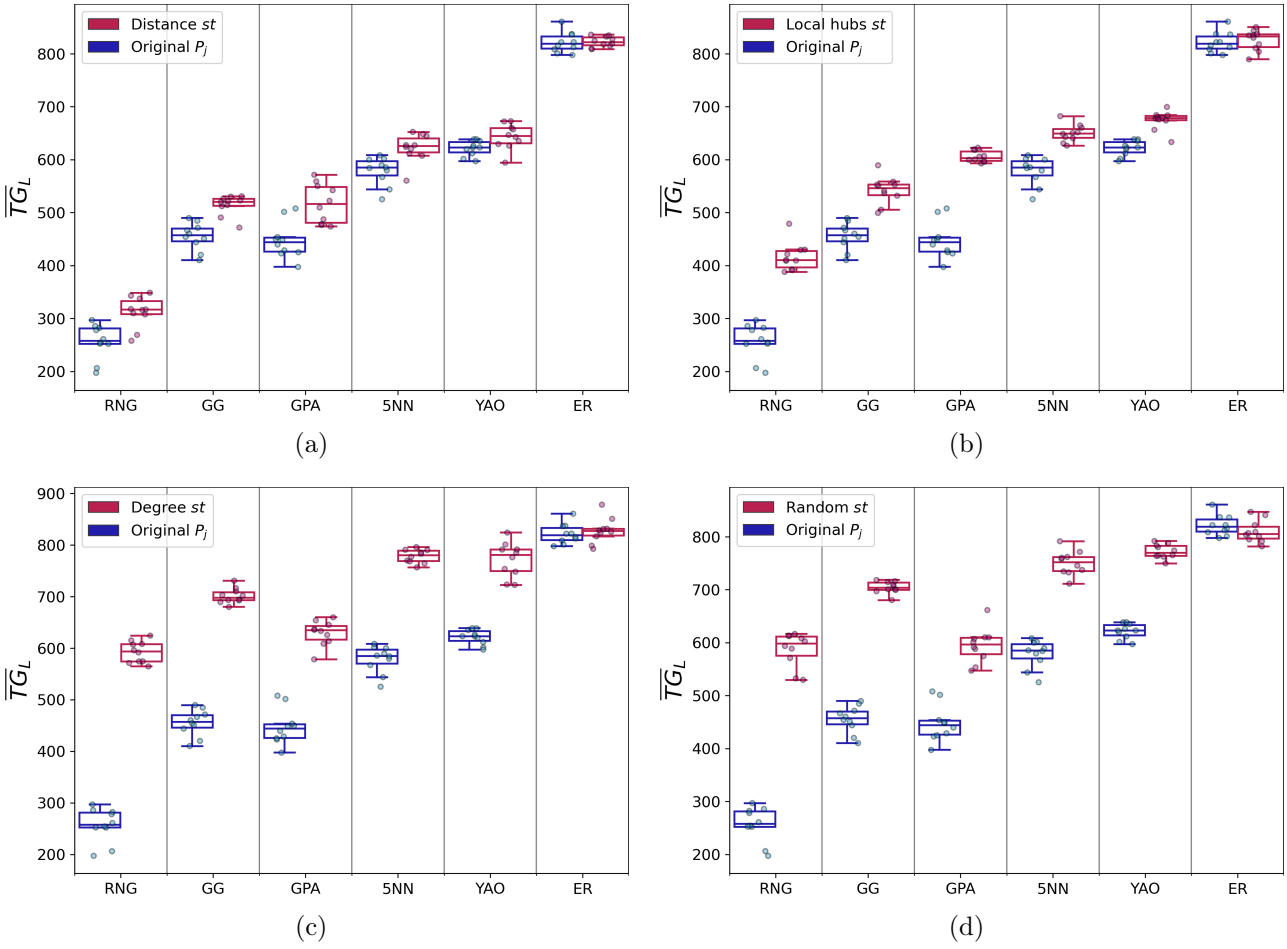


Figure C.12: $\overline{TG_L}$ comparison of systems with and without extra physical links for s =(1:25), and $I_{max} = 3$.

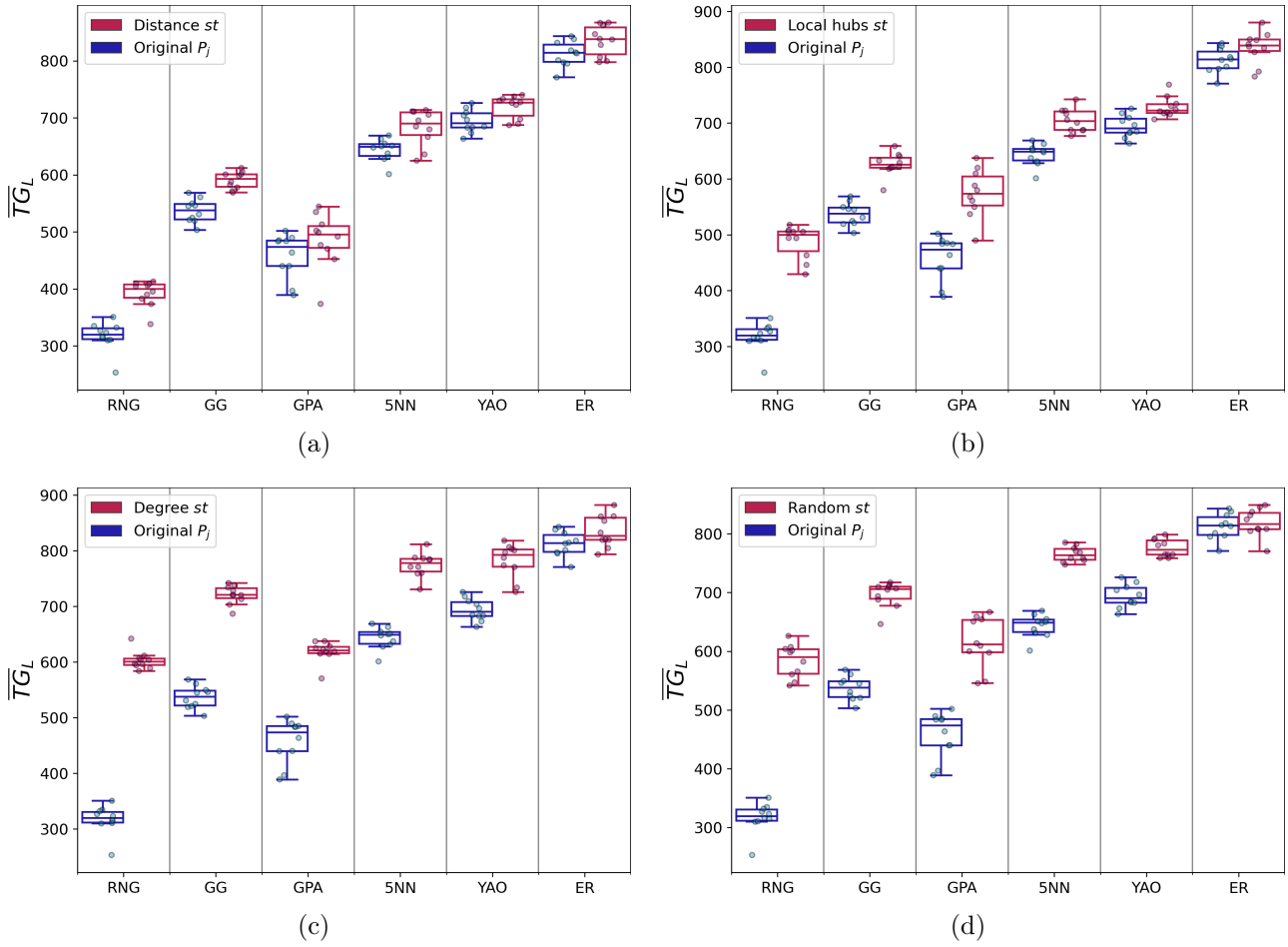


Figure C.13: $\overline{TG}_L$ comparison of systems with and without extra physical links for s =(1:1), and $I_{max} = 3$.

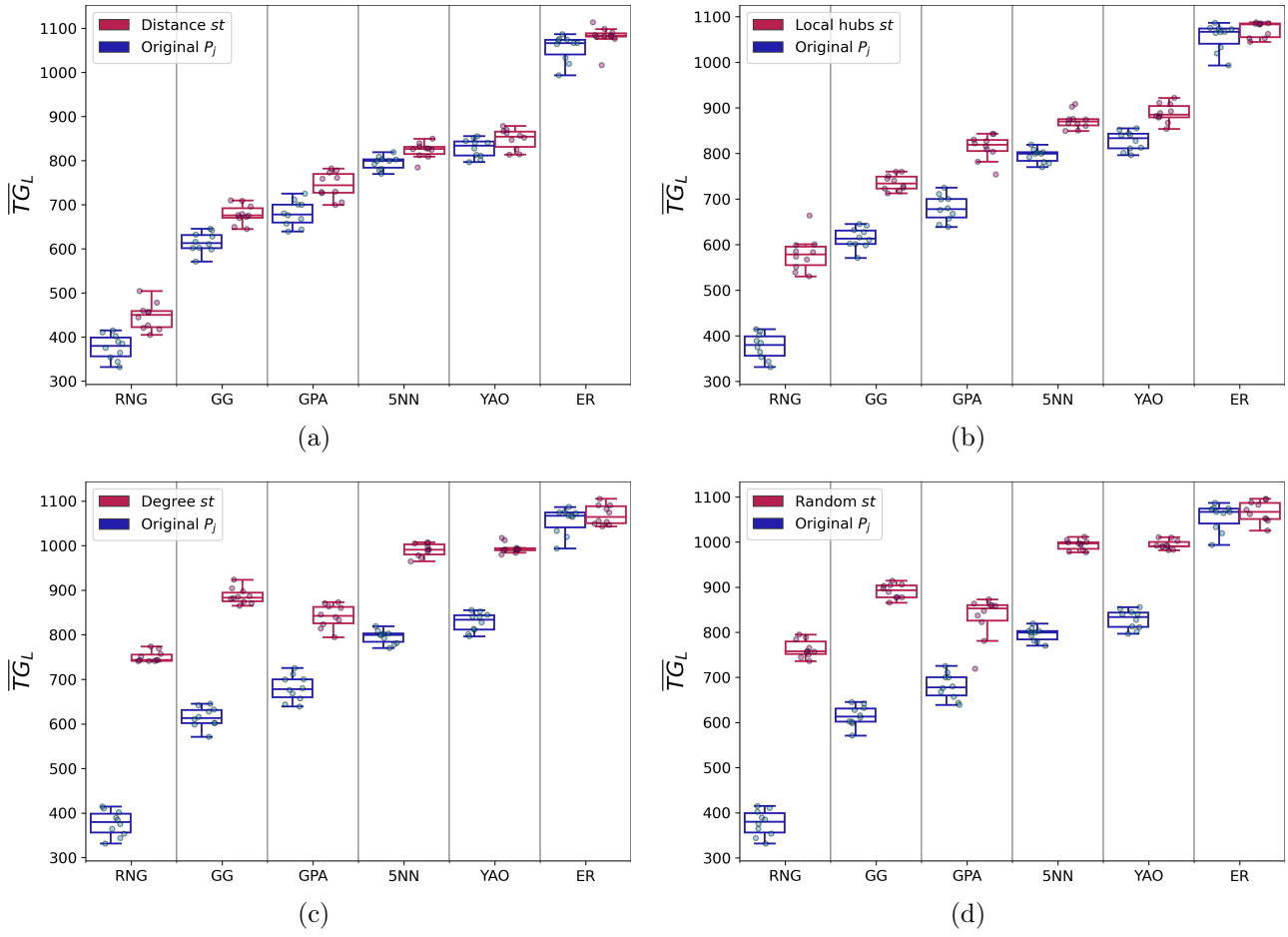


Figure C.14: $\overline{TG}_L$ comparison of systems with and without extra physical links for s =(1:25), and $I_{max} = 5$.

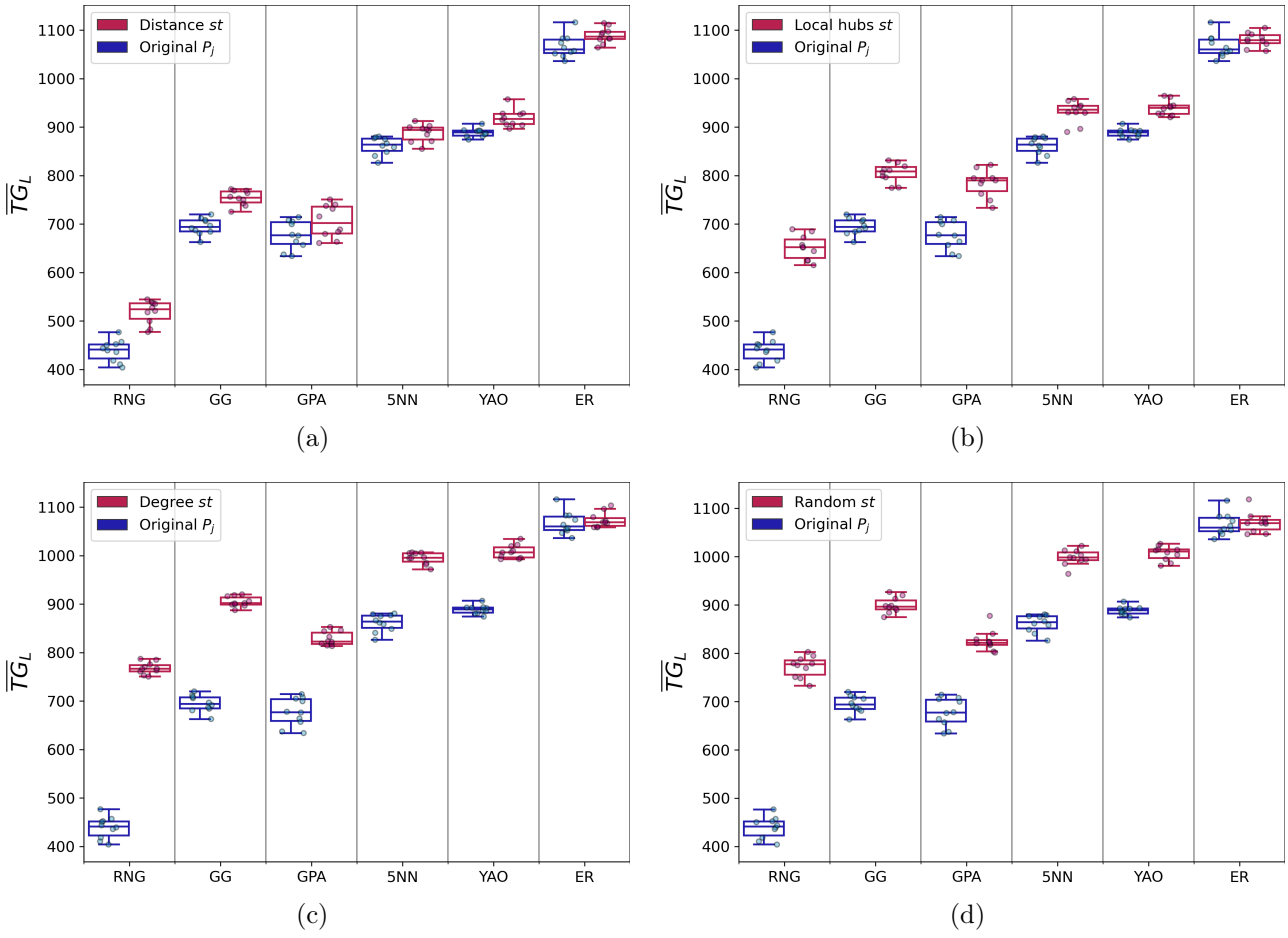


Figure C.15: $\overline{TG}_L$ comparison of systems with and without extra physical links for s =(1:1), and $I_{max} = 5$.

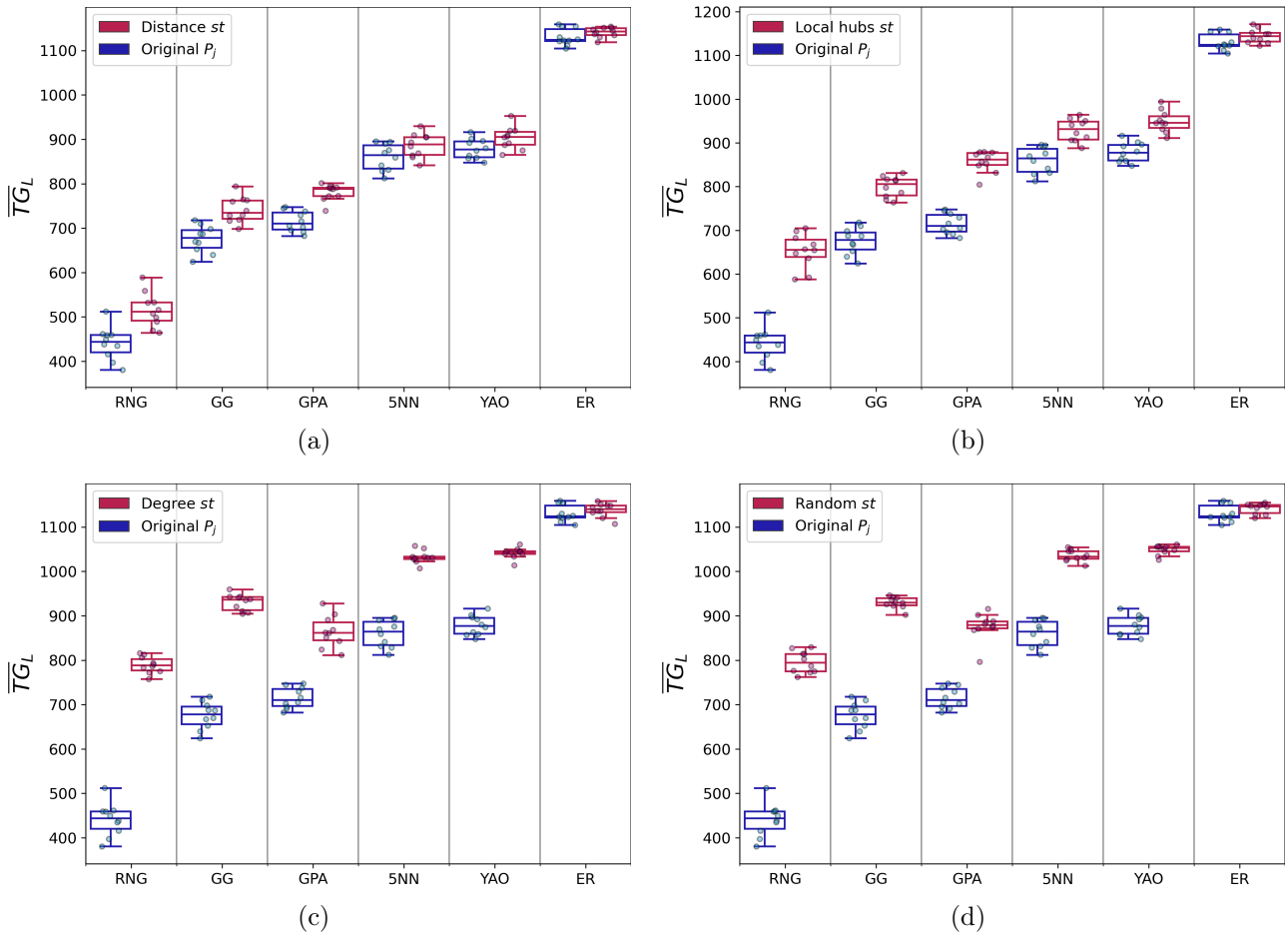


Figure C.16: $\overline{TG}_L$ comparison of systems with and without extra physical links for s =(1:25), and $I_{max} = 7$.

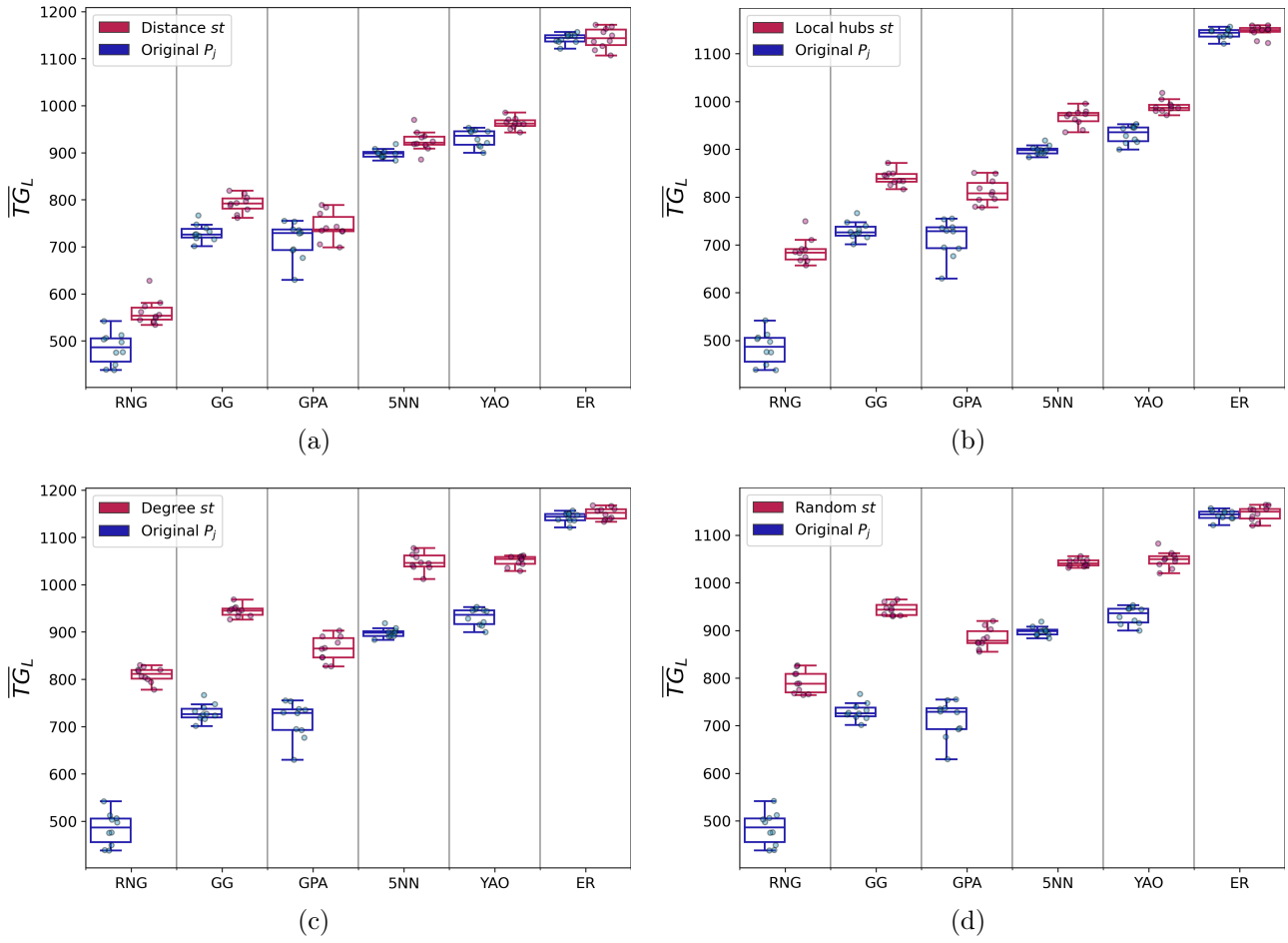


Figure C.17: $\overline{TG_L}$ comparison of systems with and without extra physical links for s =(1:1), and $I_{max} = 7$.

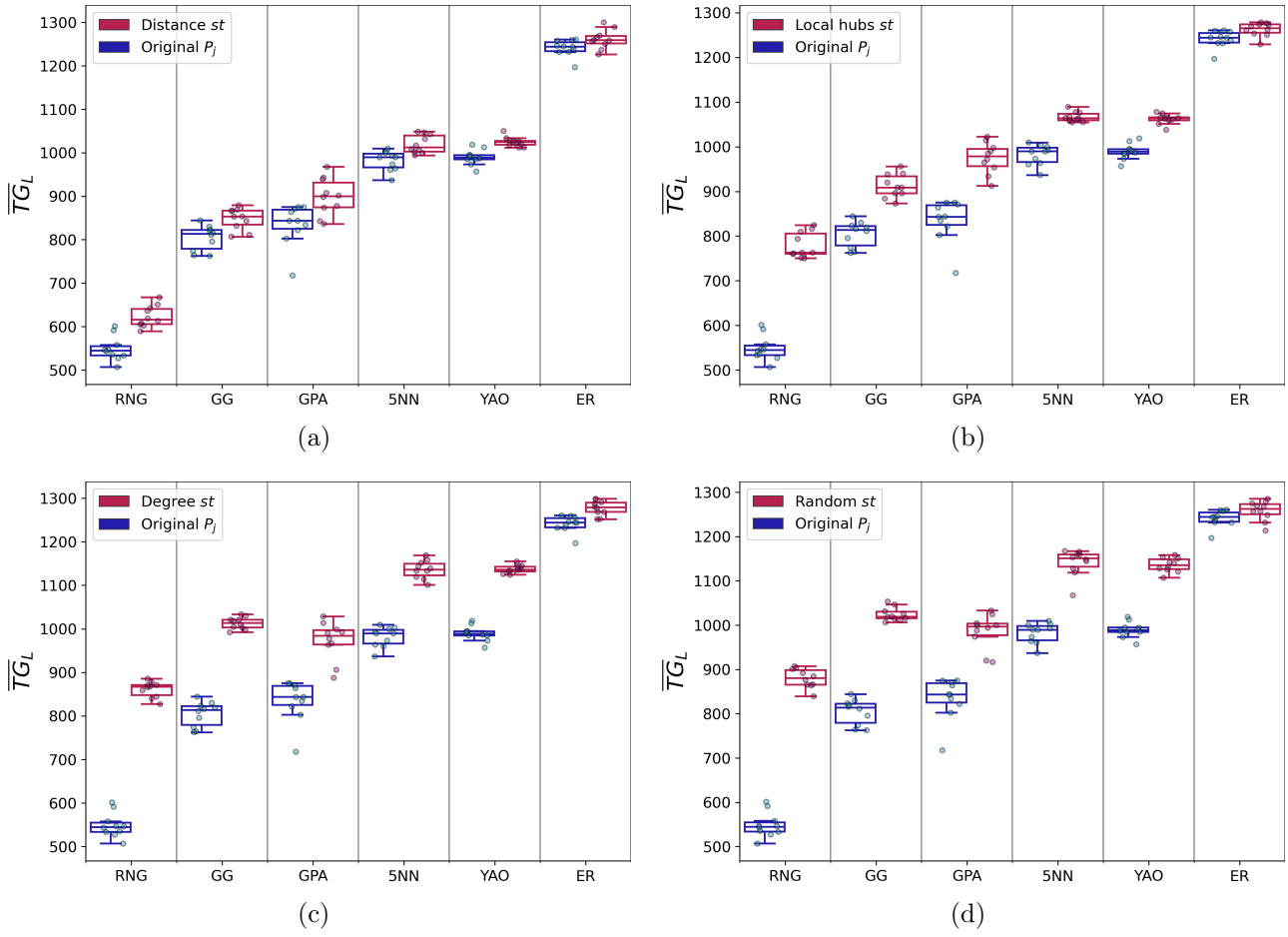


Figure C.18: $\overline{TG}_L$ comparison of systems with and without extra physical links for s =(1:25), and $I_{max} = 10$.

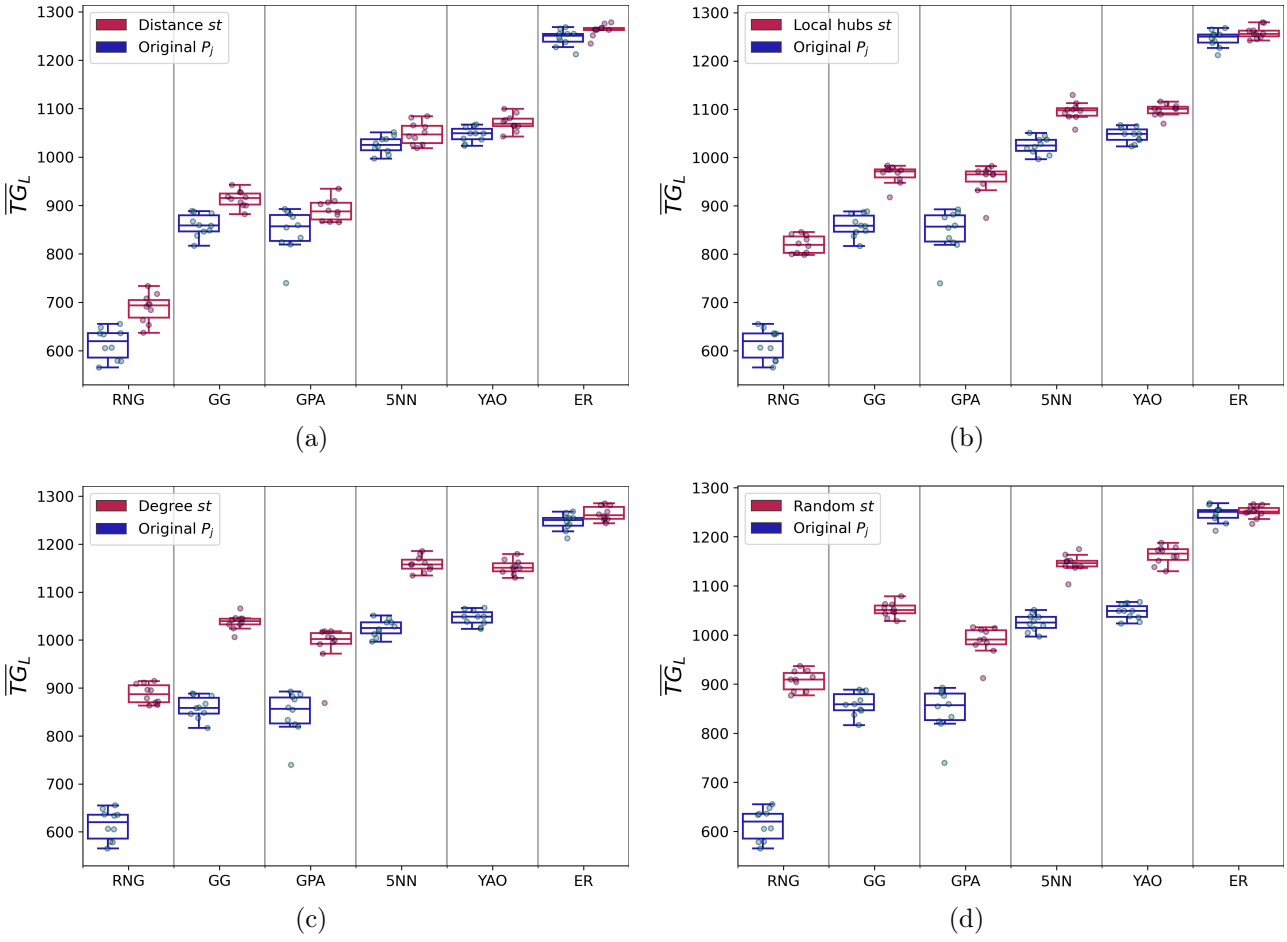
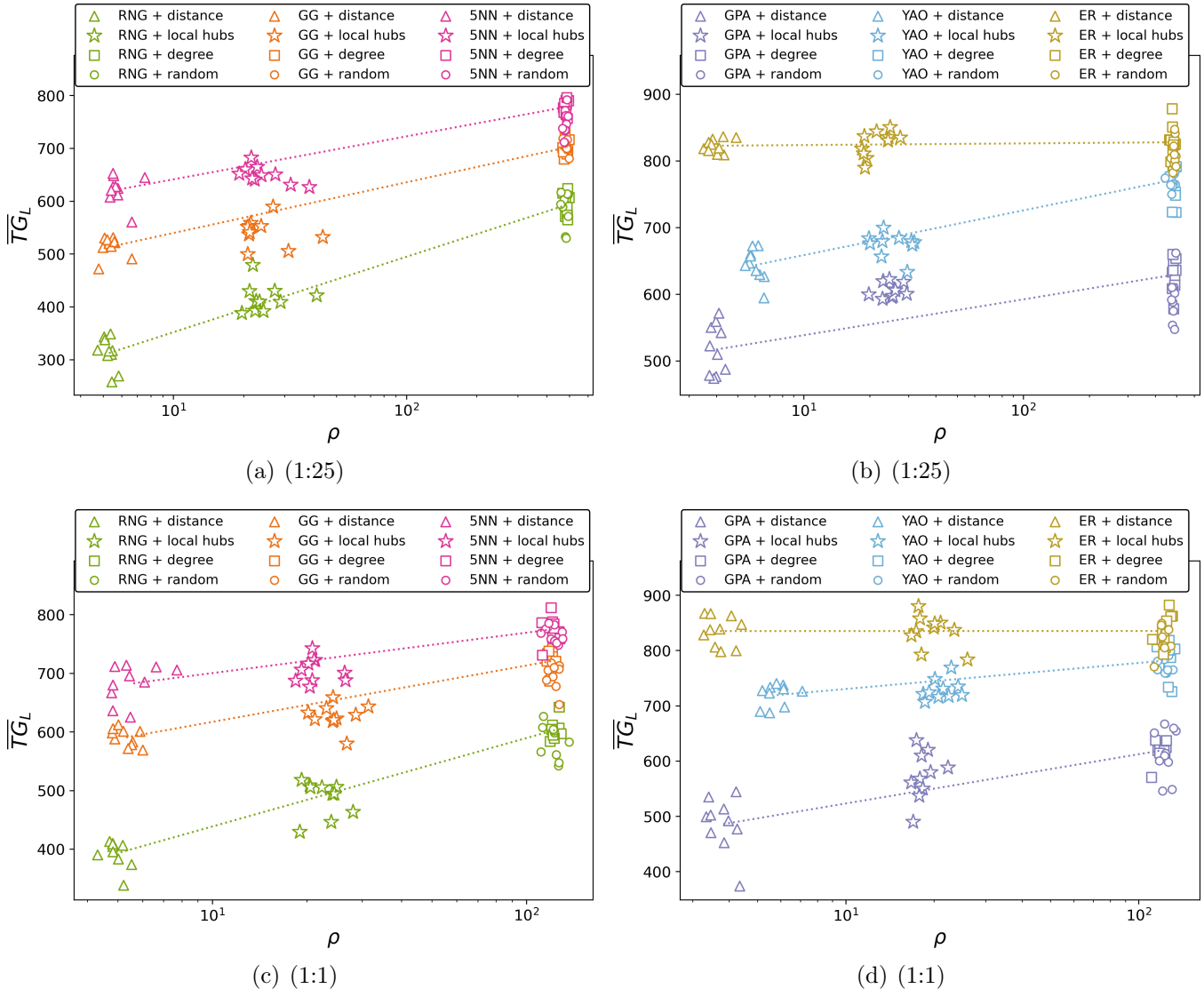


Figure C.19: $\overline{TG}_L$ comparison of systems with and without extra physical links for s =(1:1), and $I_{max} = 10$.

C.4 Relation between robustness and link length figures



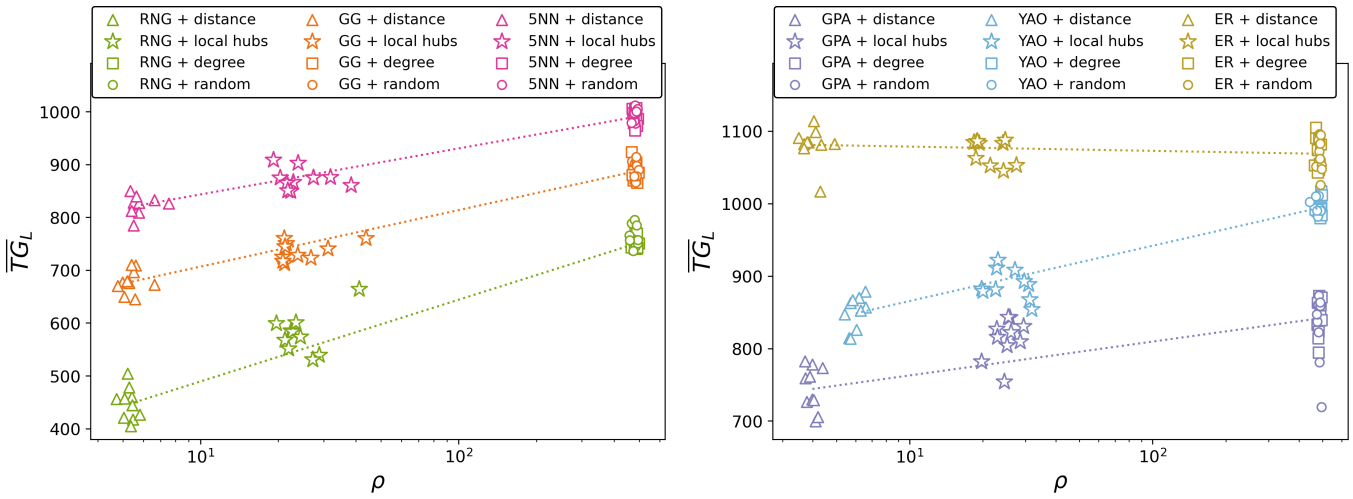
(a) (1:25)

(b) (1:25)

(c) (1:1)

(d) (1:1)

Figure C.20: Length of the longest link added by each strategy over each system tested ρ versus the $\overline{TG}_L$ for systems built using $I_{max} = 3$. ρ axis is shown using logarithmic scale.



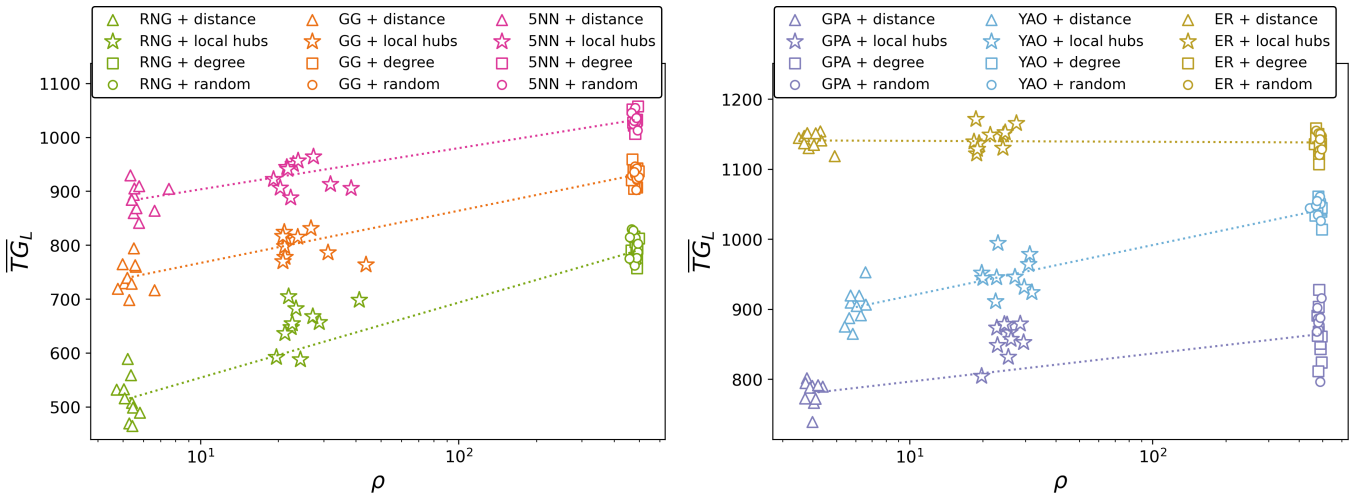
(a) (1:25)

(b) (1:25)

(c) (1:1)

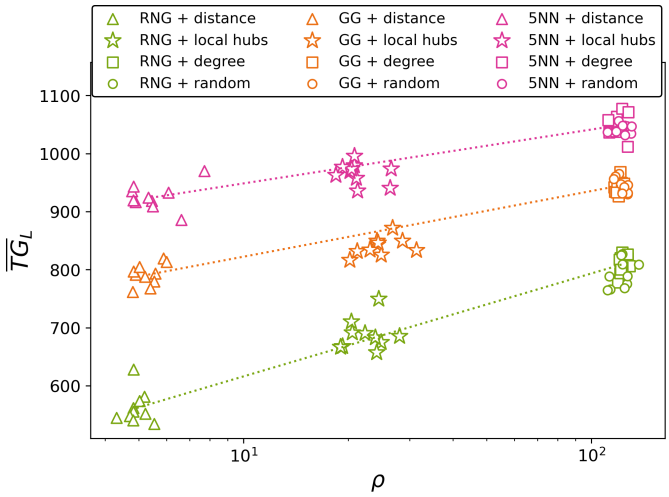
(d) (1:1)

Figure C.21: Length of the longest link added by each strategy over each system tested ρ versus the $\overline{TG}_L$ for systems built using $I_{max} = 5$. ρ axis is shown using logarithmic scale.

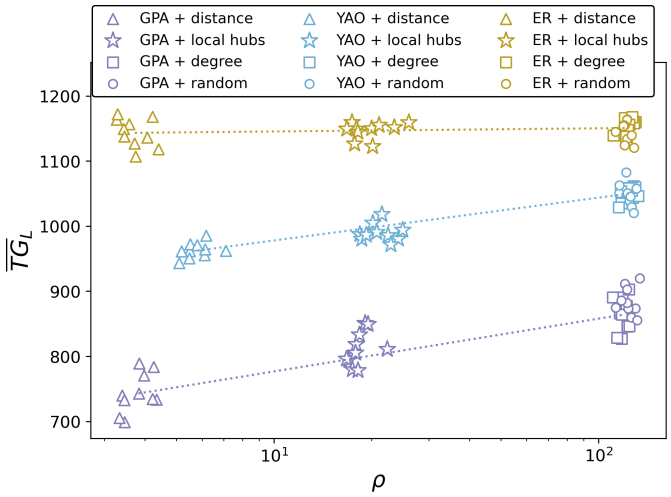


(a) (1:25)

(b) (1:25)

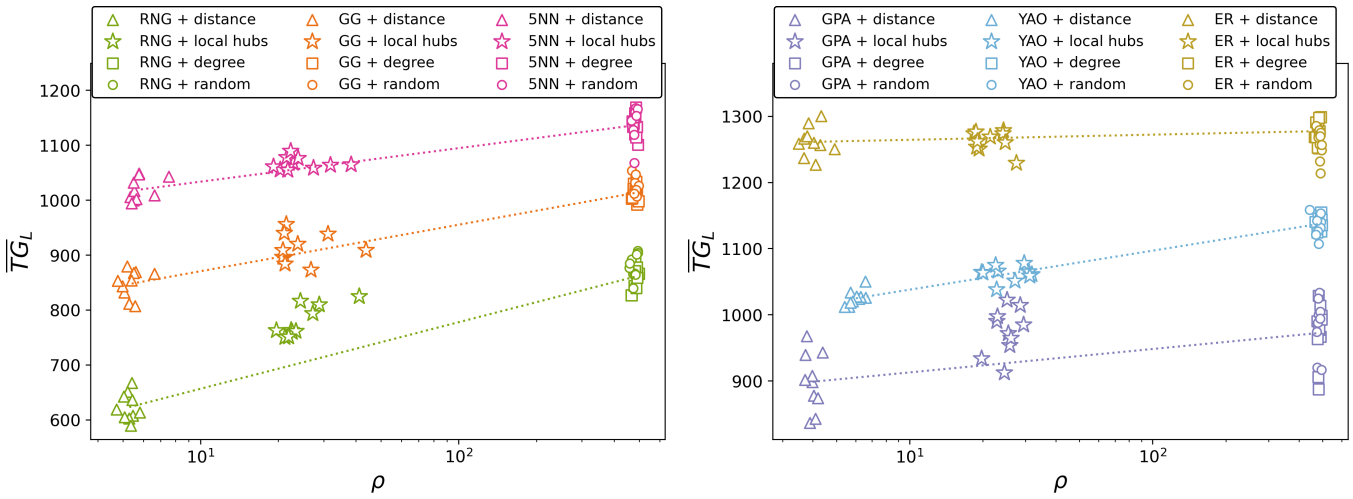


(c) (1:1)



(d) (1:1)

Figure C.22: Length of the longest link added by each strategy over each system tested ρ versus the $\overline{TG}_L$ for systems built using $I_{max} = 7$. ρ axis is shown using logarithmic scale.



(a) (1:25)

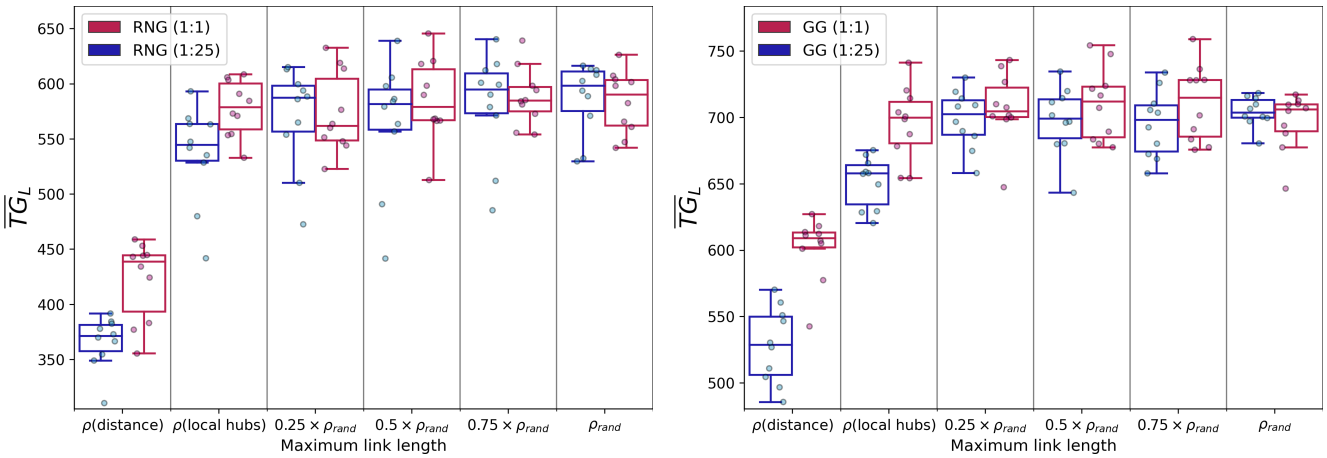
(b) (1:25)

(c) (1:1)

(d) (1:1)

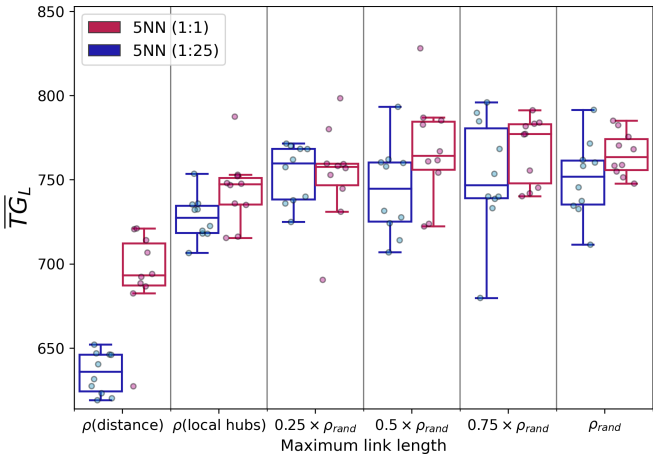
Figure C.23: Length of the longest link added by each strategy over each system tested ρ versus the $\overline{TG}_L$ for systems built using $I_{max} = 10$. ρ axis is shown using logarithmic scale.

C.5 Robustness after randomly adding physical links with maximum link length figures

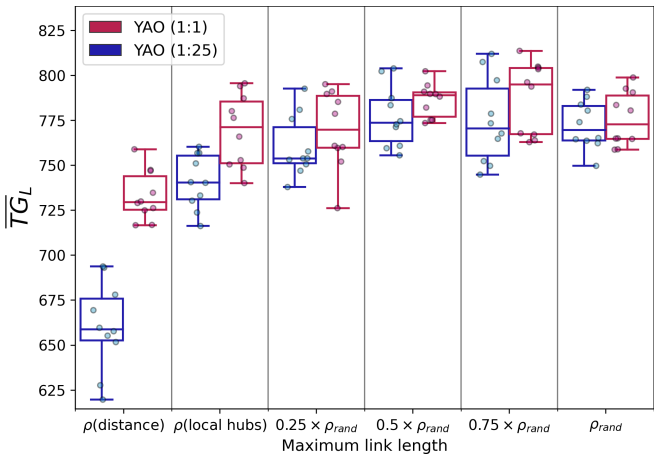


(a) RNG

(b) GG

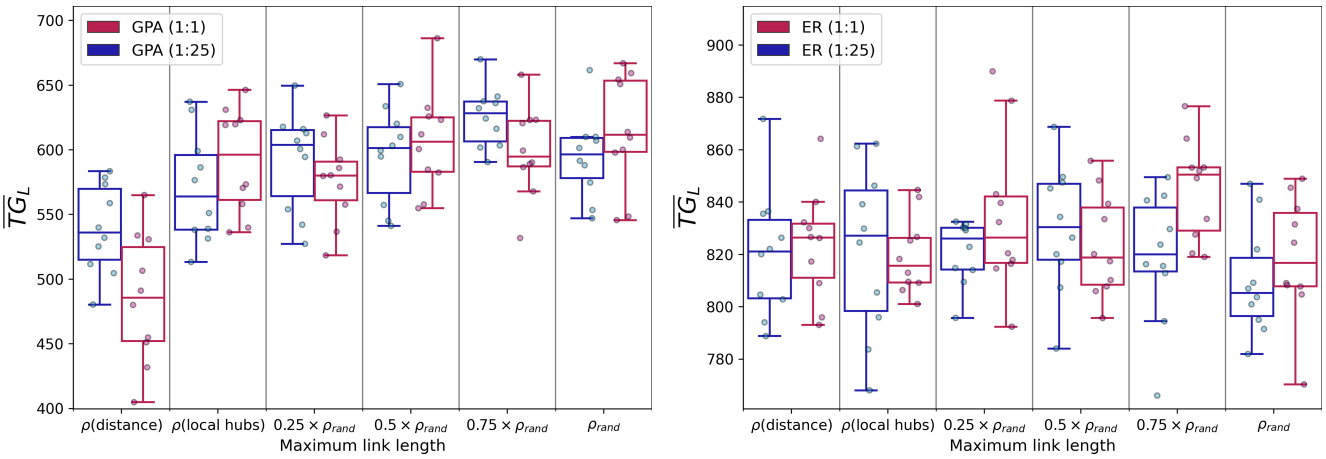


(c) 5NN



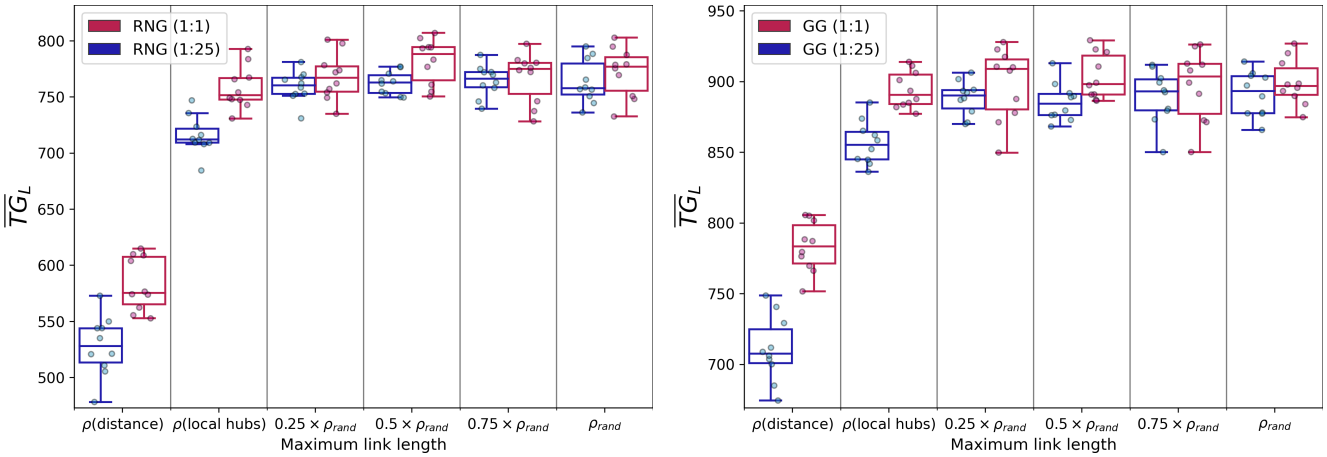
(d) YAO

Figure C.24: $\overline{TG}_L$ values after randomly adding physical links with different maximum link lengths ($I_{max} = 3$). Each point shows the $\overline{TG}_L$ of a single physical network $P_j^{st}(m, s)$.



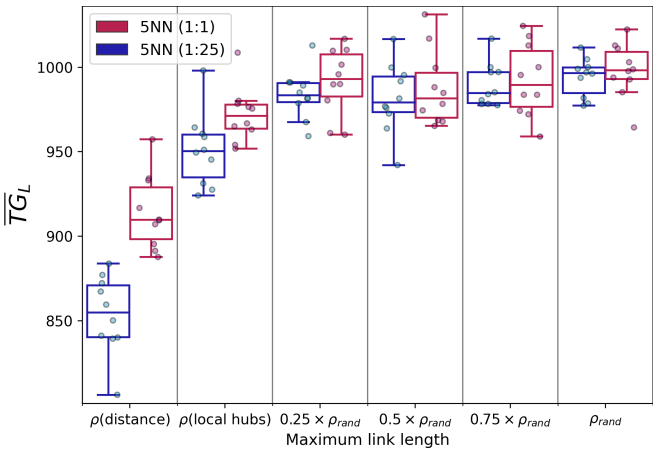
(a) GPA (b) ER

Figure C.25: $\overline{TG}_L$ values after randomly adding physical links with different maximum link length ($I_{max} = 3$). Each point shows the $\overline{TG}_L$ of a single physical network $P_j^{st}(m, s)$.

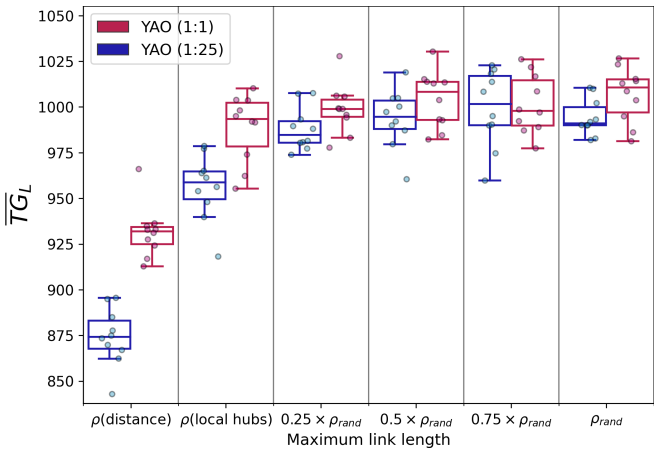


(a) RNG

(b) GG

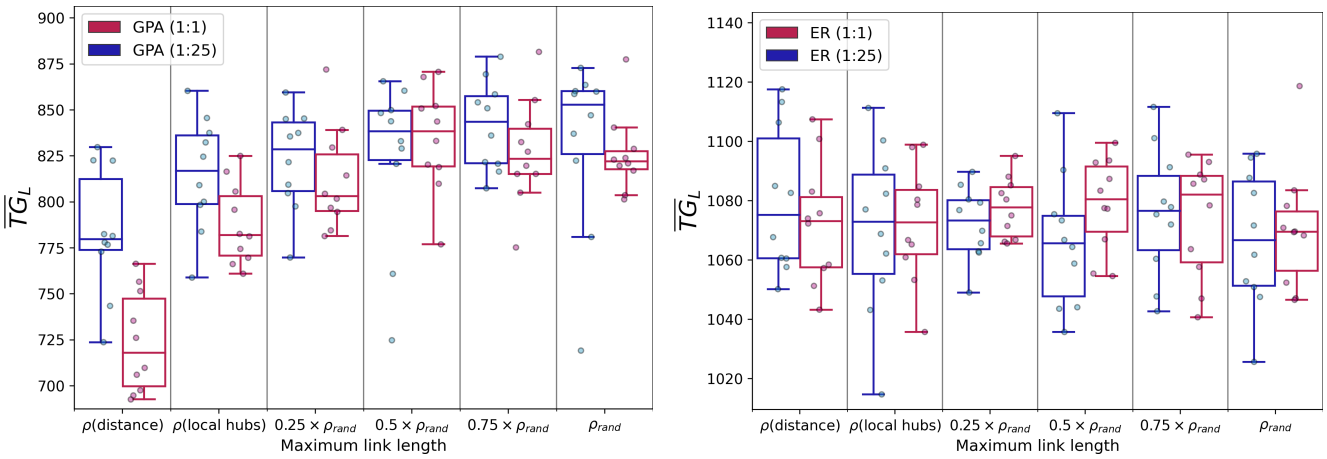


(c) 5NN



(d) YAO

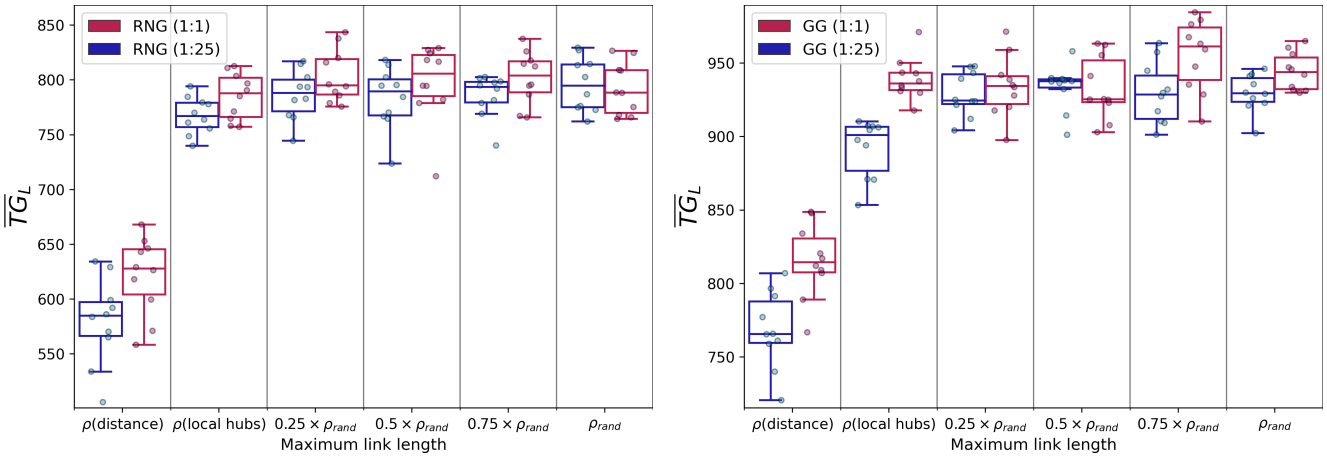
Figure C.26: $\overline{TG}_L$ values after randomly adding physical links with different maximum link lengths ($I_{max} = 5$). Each point shows the $\overline{TG}_L$ of a single physical network $P_j^{st}(m, s)$.



(a) GPA

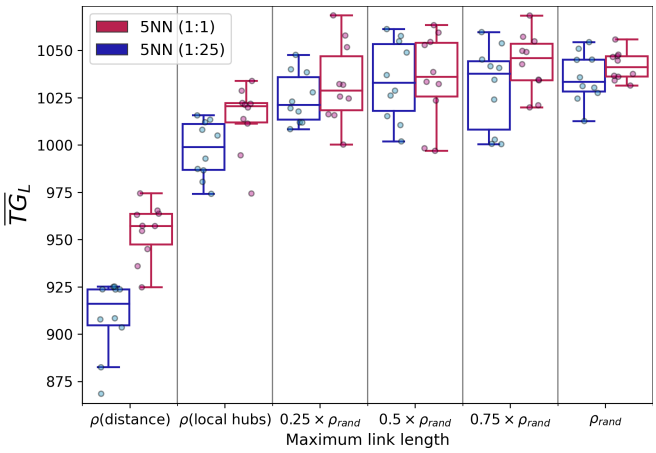
(b) ER

Figure C.27: $\overline{TG}_L$ values after randomly adding physical links with different maximum link lengths ($I_{max} = 5$). Each point shows the $\overline{TG}_L$ of a single physical network $P_j^{st}(m, s)$.

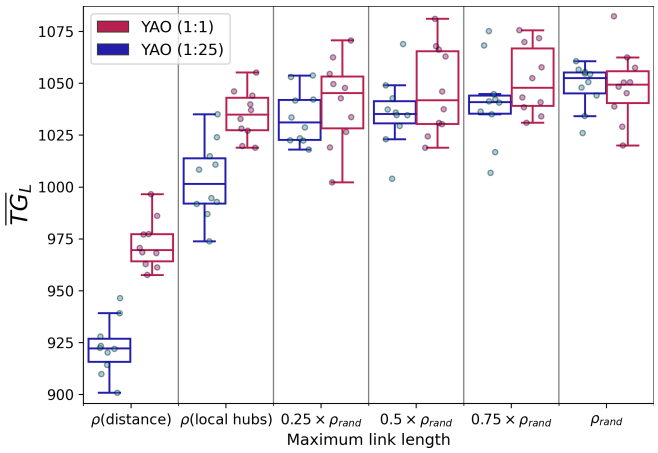


(a) RNG

(b) GG

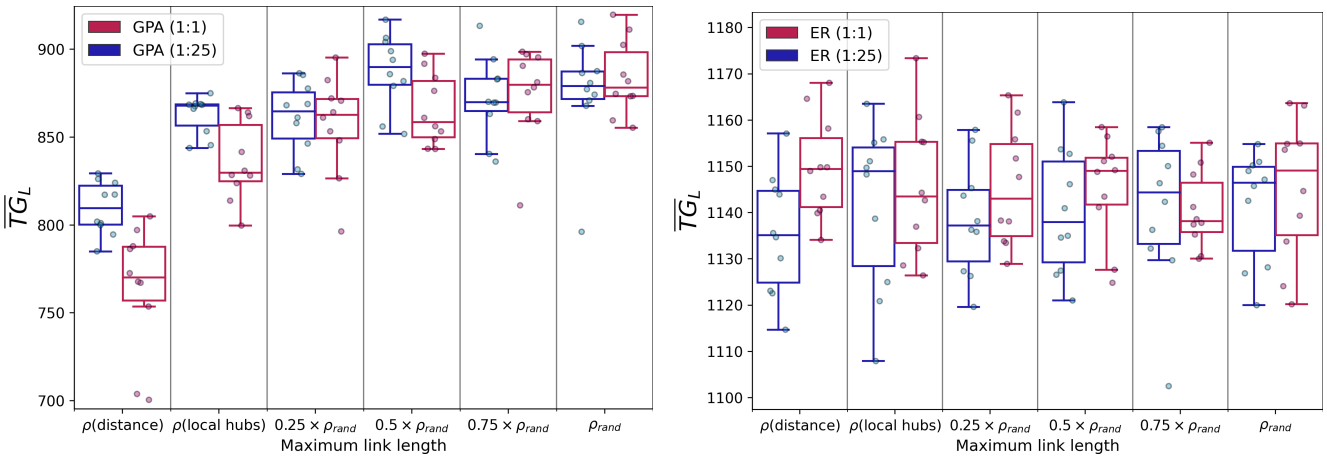


(c) 5NN



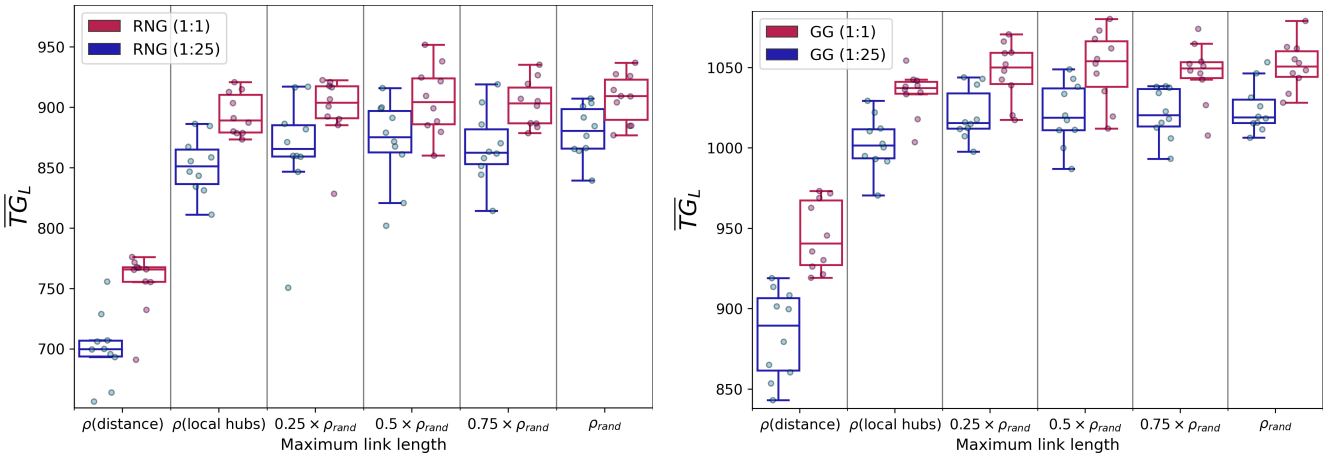
(d) YAO

Figure C.28: $\overline{TG}_L$ values after randomly adding physical links with different maximum link lengths ($I_{max} = 7$). Each point shows the $\overline{TG}_L$ of a single physical network $P_j^{st}(m, s)$.



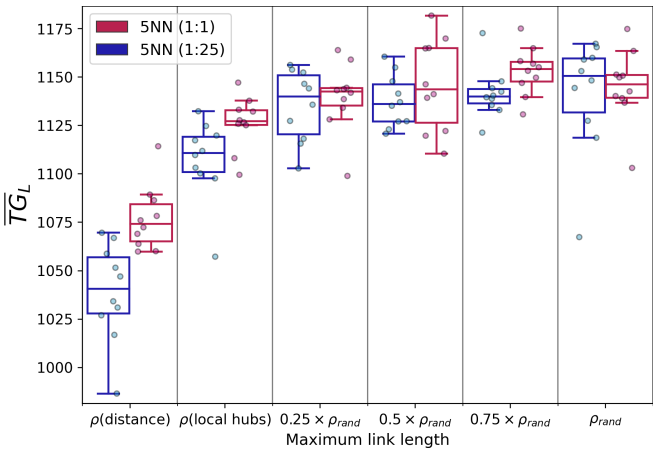
(a) GPA (b) ER

Figure C.29: $\overline{TG}_L$ values after randomly adding physical links with different maximum link lengths ($I_{max} = 7$). Each point shows the $\overline{TG}_L$ of a single physical network $P_j^{st}(m, s)$.

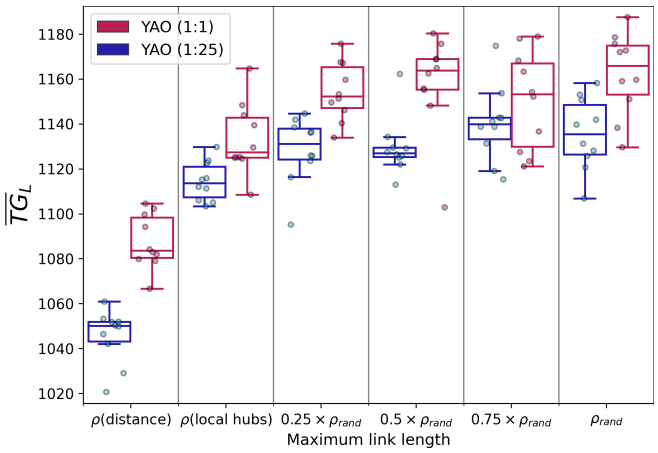


(a) RNG

(b) GG

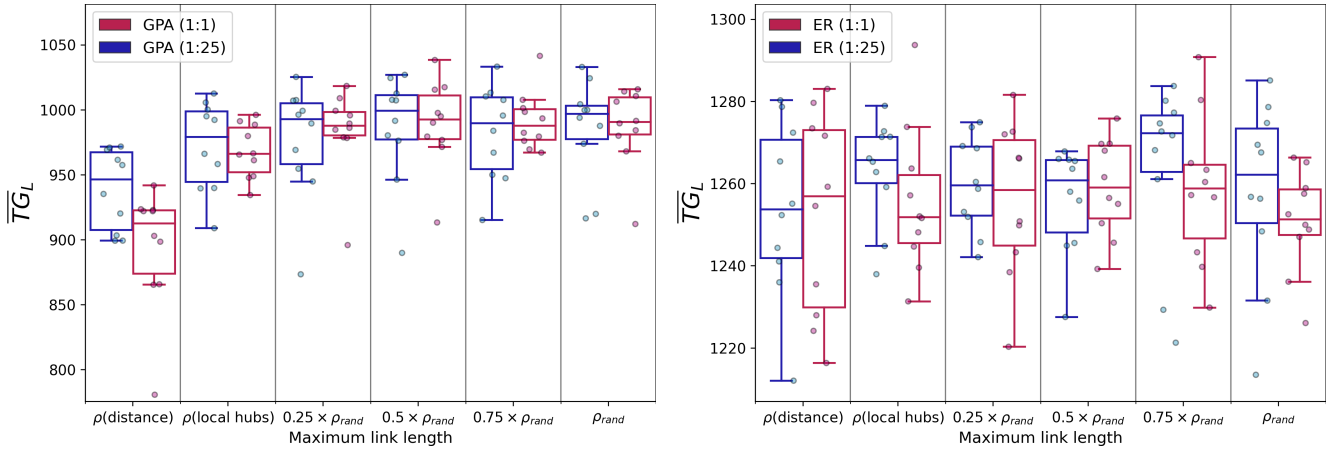


(c) 5NN



(d) YAO

Figure C.30: $\overline{TG_L}$ values after randomly adding physical links with different maximum link lengths ($I_{max} = 10$). Each point shows the $\overline{TG_L}$ of a single physical network $P_j^{st}(m, s)$.



(a) GPA (b) ER

Figure C.31: $\overline{TG}_L$ values after randomly adding physical links with different maximum link lengths ($I_{max} = 10$). Each point shows the $\overline{TG}_L$ of a single physical network $P_j^{st}(m, s)$.

C.6 Cost of adding physical links tables

$I_{max} = 3$				
(1:25)				
m/st	Distance	Local hubs	Degree	Random
RNG	42.74	31.9	3.12	3.07
GG	39.6	15.94	2.29	2.29
GPA	88.43	30.54	1.7	1.39
5NN	26.39	12.49	1.83	1.57
YAO	12.78	9.64	1.38	1.38
ER	13.43	2.94	0.15	-0.02
(1:1)				
RNG	57.09	34.94	8.51	7.91
GG	42.07	17.97	5.53	4.89
GPA	37.97	20.5	4.81	4.78
5NN	20.56	10.19	3.67	3.38
YAO	15.12	6.44	2.51	2.39
ER	16.92	3.16	0.41	-0.08

Table C.3: Cost efficiency $Cost_E^{(m,s)}$ of each link addition strategy, for systems built using $I_{max} = 3$. Cost efficiency values have been amplified by a factor of 10^3 to improve its readability.

$I_{max} = 5$				
(1:25)				
m/st	Distance	Local hubs	Degree	Random
RNG	51.16	39.91	3.44	3.57
GG	41.01	21.97	2.51	2.52
GPA	82.34	25.83	1.52	1.44
5NN	17.5	13.97	1.8	1.84
YAO	15.39	12.2	1.59	1.57
ER	24.39	2.4	0.07	0.06
(1:1)				
RNG	58.34	43.28	9.72	9.82
GG	42.02	20.93	6.14	6.07
GPA	39.48	19.02	4.56	4.56
5NN	19.19	13.87	4.05	4.15
YAO	17.4	9.32	3.39	3.43
ER	26.51	2.81	0.16	0.08

Table C.4: Cost efficiency $Cost_E^{(m,s)}$ of each link addition strategy, for systems built using $I_{max} = 5$. Cost efficiency values have been amplified by a factor of 10^3 to improve its readability.

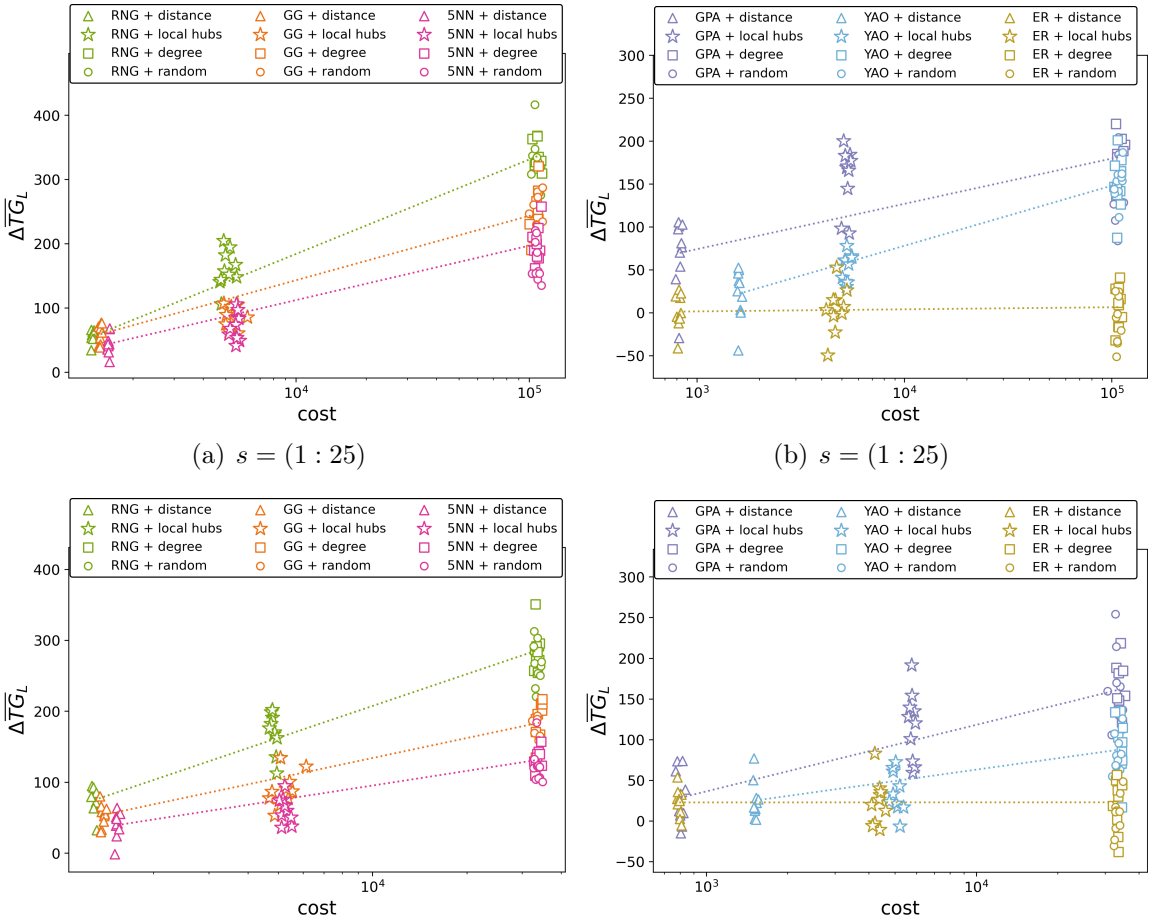
$I_{max} = 7$				
(1:25)				
m/st	Distance	Local hubs	Degree	Random
RNG	58.76	42.77	3.26	3.33
GG	41.98	22.28	2.34	2.3
GPA	74.54	26.04	1.33	1.45
5NN	20.09	13.54	1.65	1.68
YAO	15.85	13.46	1.53	1.58
ER	13.91	3.14	0.08	0.11
(1:1)				
RNG	60.32	42.22	9.74	9.19
GG	44.36	21.0	6.3	6.38
GPA	40.52	17.48	4.52	5.2
5NN	16.07	12.51	4.41	4.19
YAO	19.15	11.19	3.42	3.45
ER	11.01	2.81	0.48	0.32

Table C.5: Cost efficiency $Cost_E^{(m,s)}$ of each link addition strategy, for systems built using $I_{max} = 7$. Cost efficiency values have been amplified by a factor of 10^3 to improve its readability.

$I_{max} = 10$				
(1:25)				
m/st	Distance	Local hubs	Degree	Random
RNG	53.27	45.07	2.86	3.04
GG	35.27	21.53	2.03	2.1
GPA	66.81	24.71	1.18	1.31
5NN	22.32	14.93	1.41	1.45
YAO	19.19	12.8	1.34	1.31
ER	15.65	3.03	0.27	0.09
(1:1)				
RNG	56.77	42.56	8.16	8.73
GG	38.89	20.05	5.23	5.71
GPA	47.0	17.62	4.01	4.03
5NN	16.89	13.74	4.01	3.61
YAO	17.33	10.7	3.16	3.54
ER	22.91	3.45	0.59	0.2

Table C.6: Cost efficiency $Cost_E^{(m,s)}$ of each link addition strategy, for systems built using $I_{max} = 10$. Cost efficiency values have been amplified by a factor of 10^3 to improve its readability.

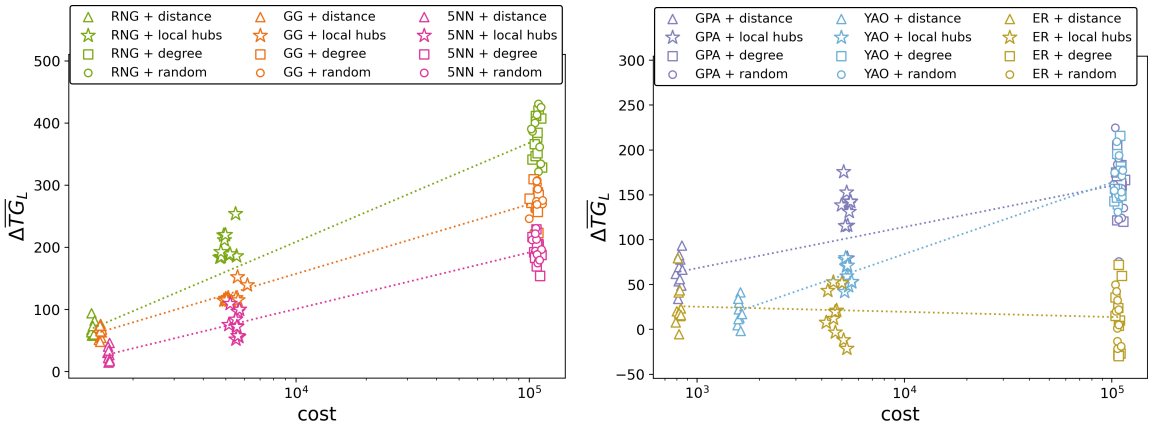
C.7 Cost of adding physical links figures



(a) $s = (1:25)$ (b) $s = (1:25)$

(c) $s = (1:1)$ (d) $s = (1:1)$

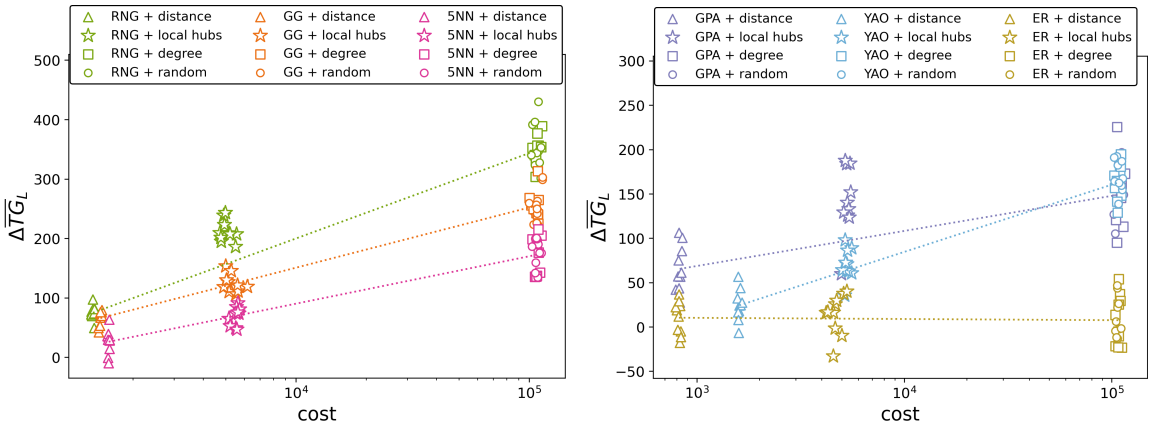
Figure C.32: Robustness gain $\Delta\overline{TG}_L$ versus the cost of adding extra physical links for systems with $I_{max} = 3$.



(a) $s = (1:25)$ (b) $s = (1:25)$

(c) $s = (1:1)$ (d) $s = (1:1)$

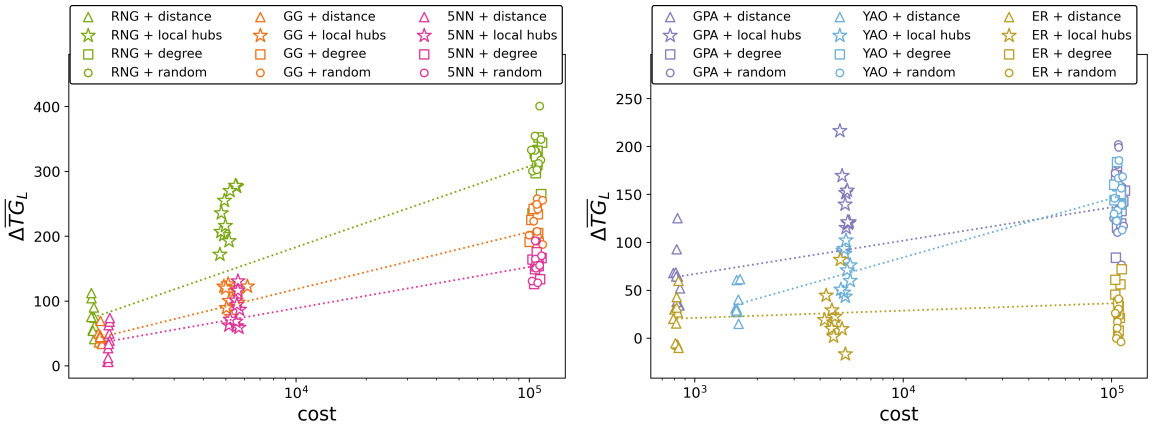
Figure C.33: Robustness gain $\Delta\overline{TG}_L$ versus the cost of adding extra physical links for systems with $I_{max} = 5$.



(a) $s = (1 : 25)$ (b) $s = (1 : 25)$

(c) $s = (1 : 1)$ (d) $s = (1 : 1)$

Figure C.34: Robustness gain $\Delta\overline{TG}_L$ versus the cost of adding extra physical links for systems with $I_{max} = 7$.



(a) $s = (1 : 25)$ (b) $s = (1 : 25)$

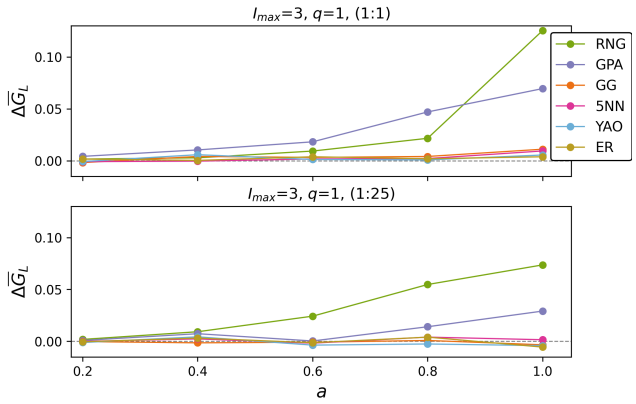
(c) $s = (1 : 1)$ (d) $s = (1 : 1)$

Figure C.35: Robustness gain $\Delta\overline{TG}_L$ versus the cost of adding extra physical links for systems with $I_{max} = 10$.

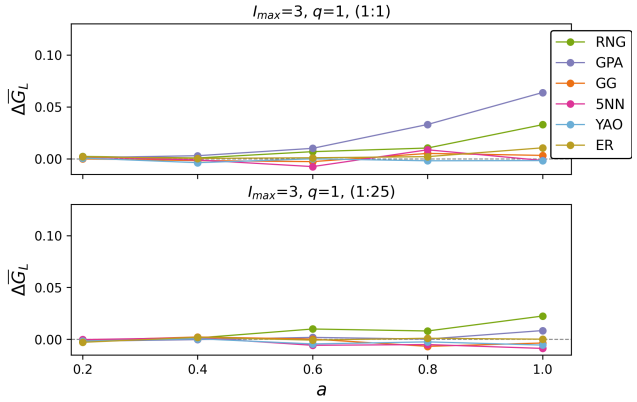
Annexed D

Chapter 6: Internet robustness against localized attacks

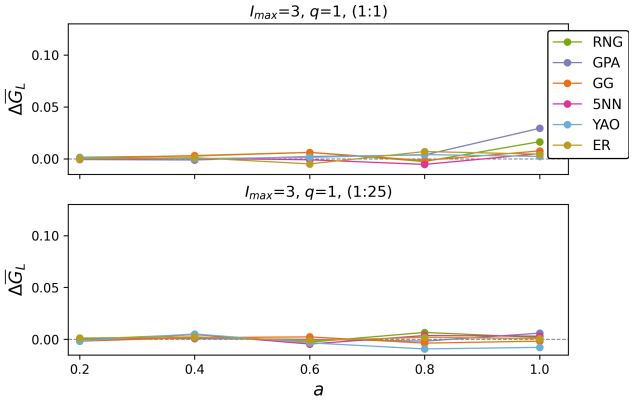
D.1 LA vs RA comparison figures



(a) No links added

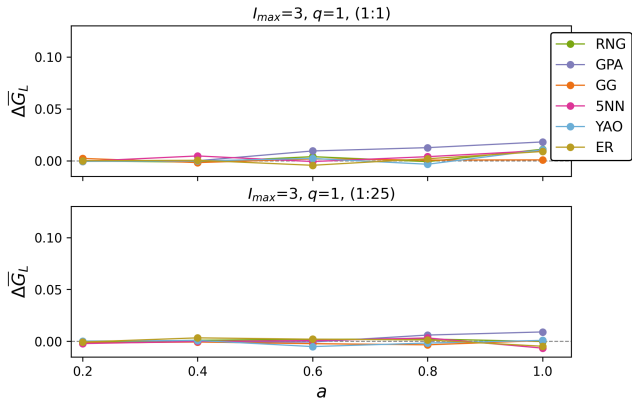


(b) Distance links added

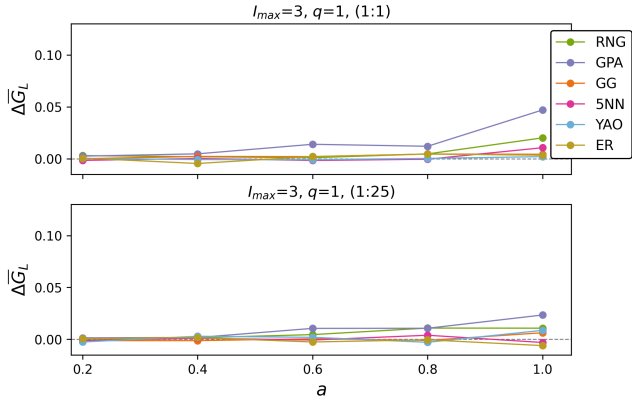


(c) Local hubs links added

Figure D.1: $\overline{G}_L$ value difference between LA and RA for $I_{max} = 3$. Here, $\Delta\overline{G}_L = \overline{G}_L(\text{LA}) - \overline{G}_L(\text{RA})$, and LA radius $r = aw_{ln}, a \in \{0.2, 0.4, 0.6, 0.8, 1\}$, with w_{ln} the width of the (1:25) space.

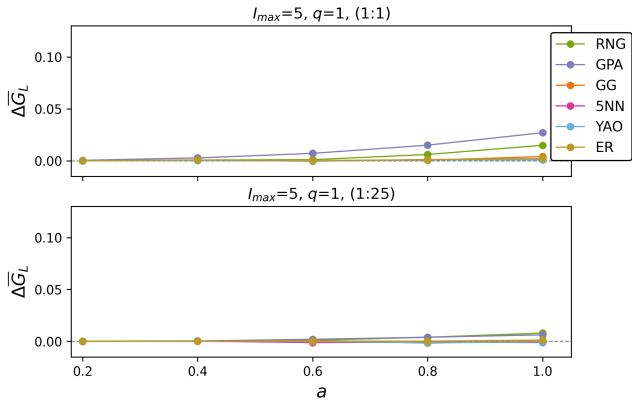


(a) Degree links added

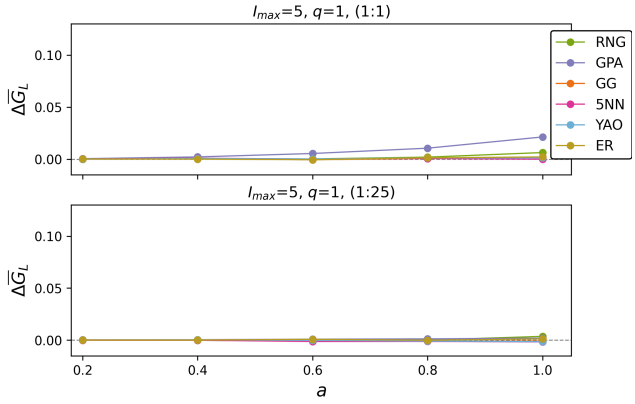


(b) Random links added

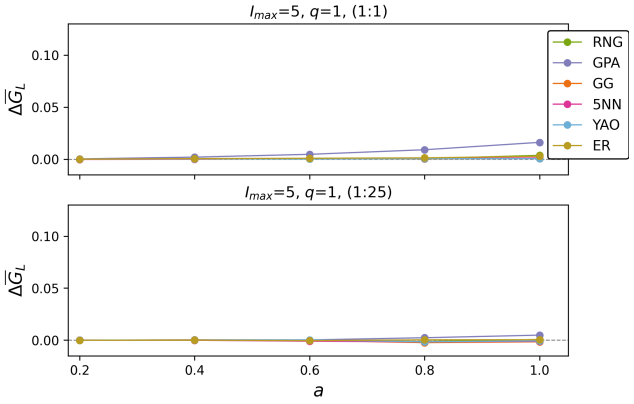
Figure D.2: $\overline{G}_L$ value difference between LA and RA for $I_{max} = 3$. Here, $\Delta\overline{G}_L = \overline{G}_L(\text{LA}) - \overline{G}_L(\text{RA})$, and LA radius $r = aw_{ln}, a \in \{0.2, 0.4, 0.6, 0.8, 1\}$, with w_{ln} the width of the (1:25) space.



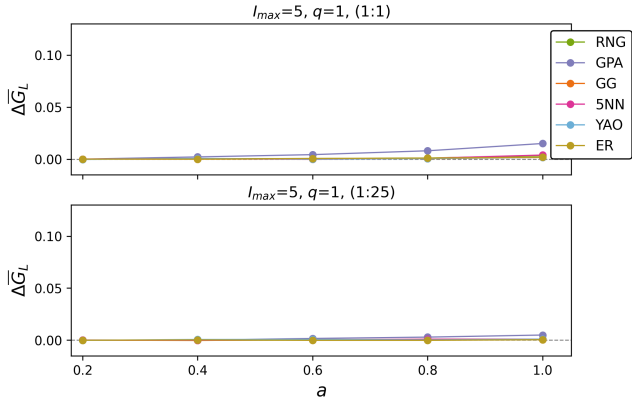
(a) No links added



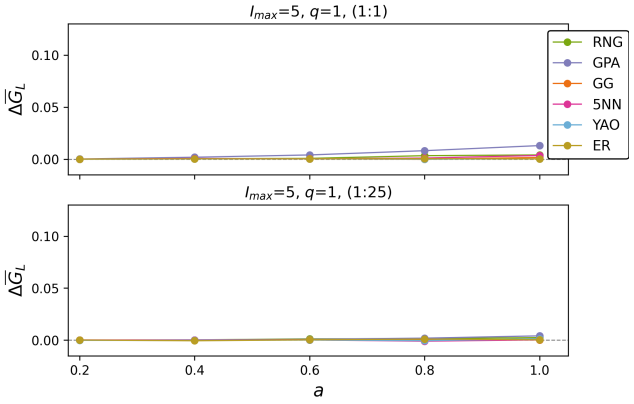
(b) Distance links added



(c) Local hubs links added

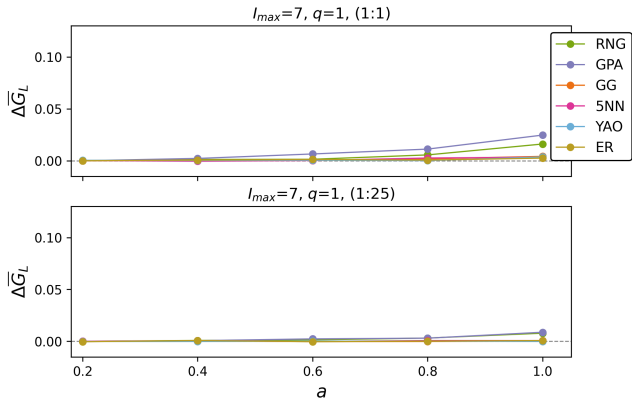


(d) Degree links added

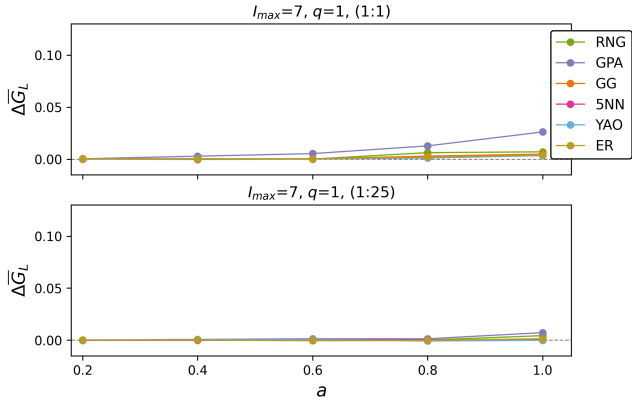


(e) Random links added

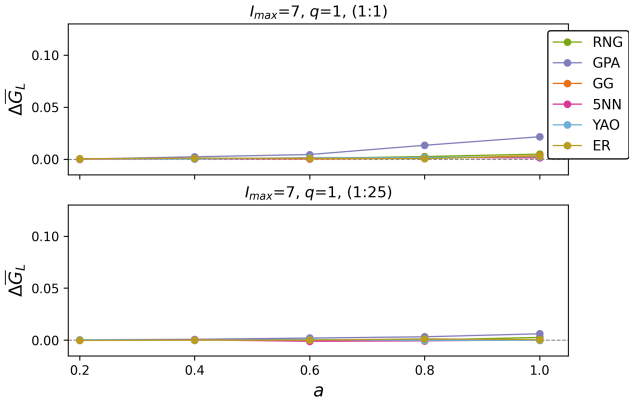
Figure D.3: $\overline{G}_L$ value difference between LA and RA for $I_{max} = 5$. Here, $\Delta\overline{G}_L = \overline{G}_L(\text{LA}) - \overline{G}_L(\text{RA})$, and LA radius $r = aw_{ln}, a \in \{0.2, 0.4, 0.6, 0.8, 1\}$, with w_{ln} the width of the (1:25) space.



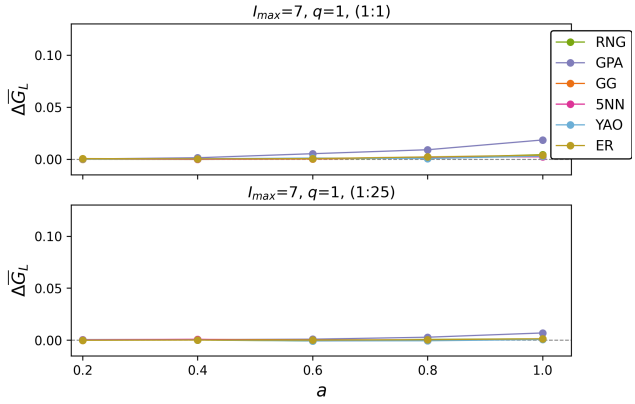
(a) No links added



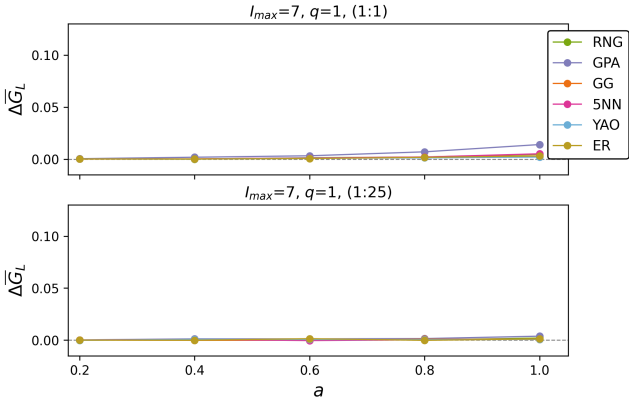
(b) Distance links added



(c) Local hubs links added

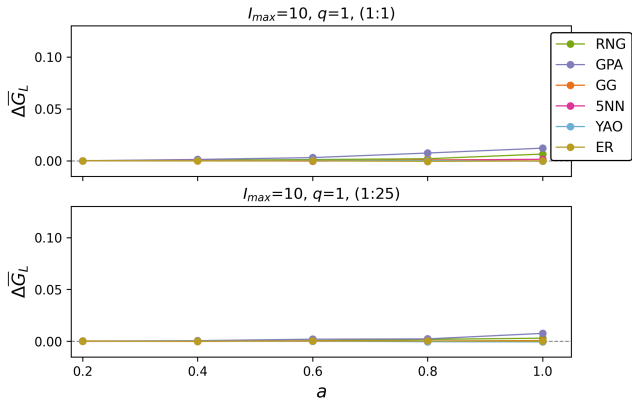


(d) Degree links added

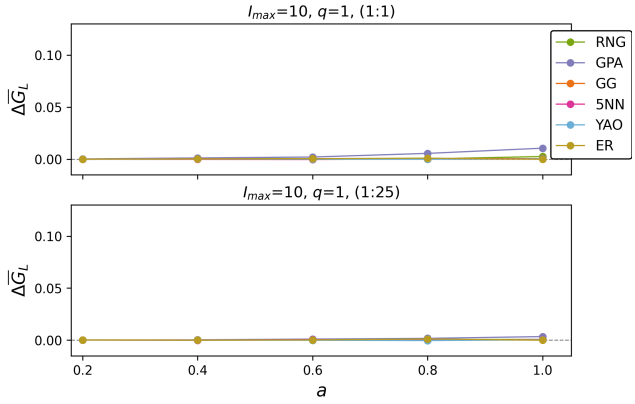


(e) Random links added

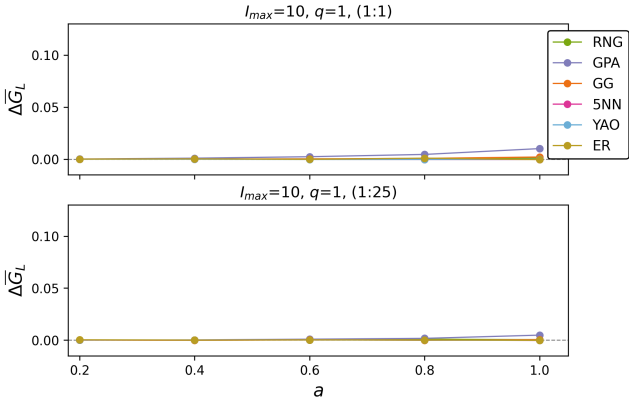
Figure D.4: $\overline{G}_L$ value difference between LA and RA for $I_{max} = 7$. Here, $\Delta\overline{G}_L = \overline{G}_L(\text{LA}) - \overline{G}_L(\text{RA})$, and LA radius $r = aw_{ln}, a \in \{0.2, 0.4, 0.6, 0.8, 1\}$, with w_{ln} the width of the (1:25) space.



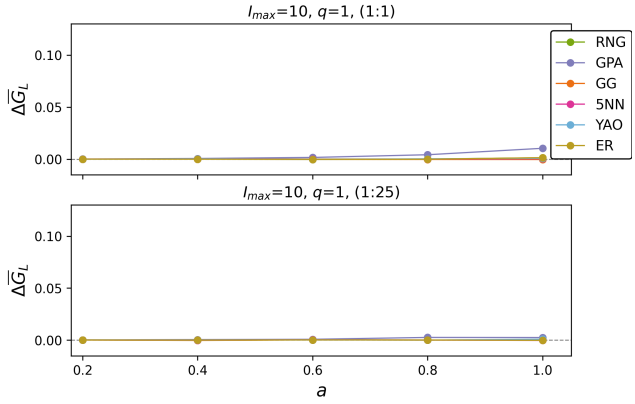
(a) No links added



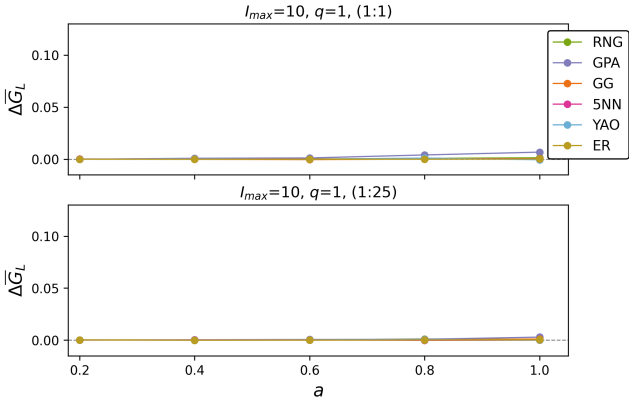
(b) Distance links added



(c) Local hubs links added



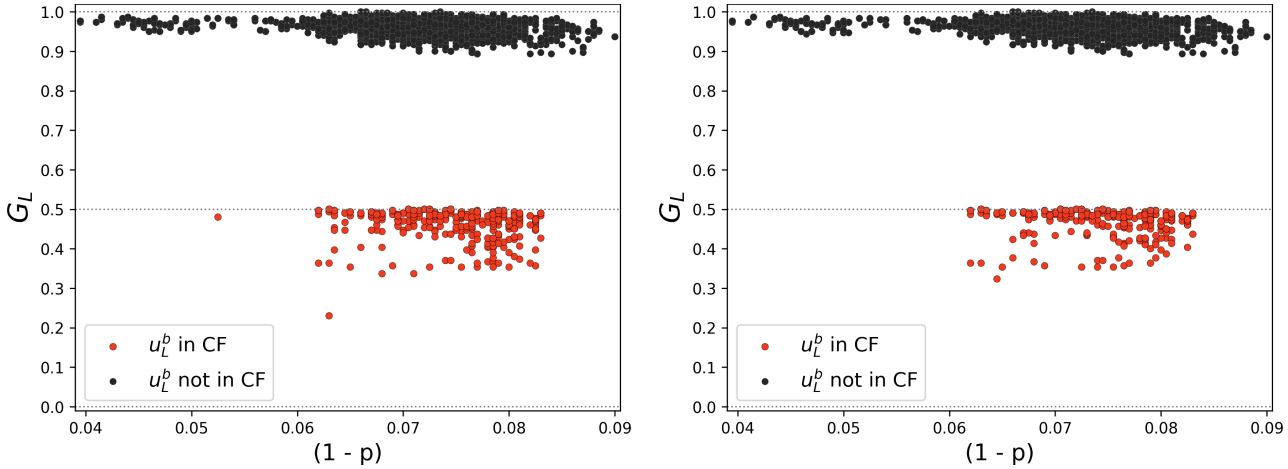
(d) Degree links added



(e) Random links added

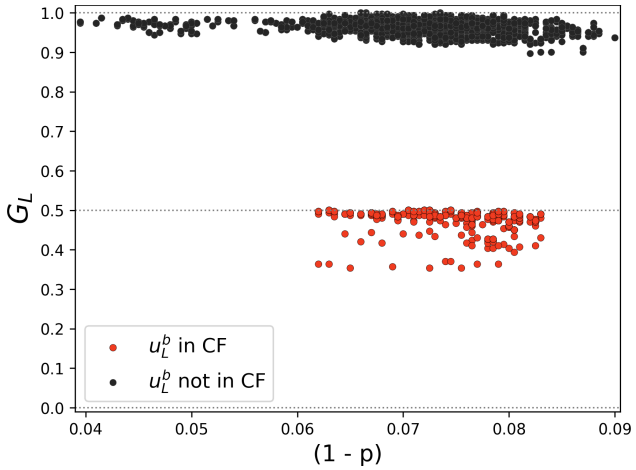
Figure D.5: $\overline{G}_L$ value difference between LA and RA for $I_{max} = 10$. Here, $\Delta\overline{G}_L = \overline{G}_L(\text{LA}) - \overline{G}_L(\text{RA})$, and LA radius $r = aw_{ln}, a \in \{0.2, 0.4, 0.6, 0.8, 1\}$, with w_{ln} the width of the (1:25) space.

D.2 High damage localized attacks figures

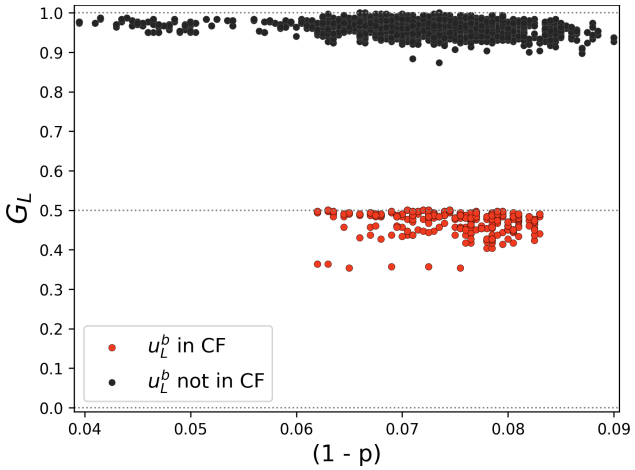


(a) Distance

(b) Local hubs

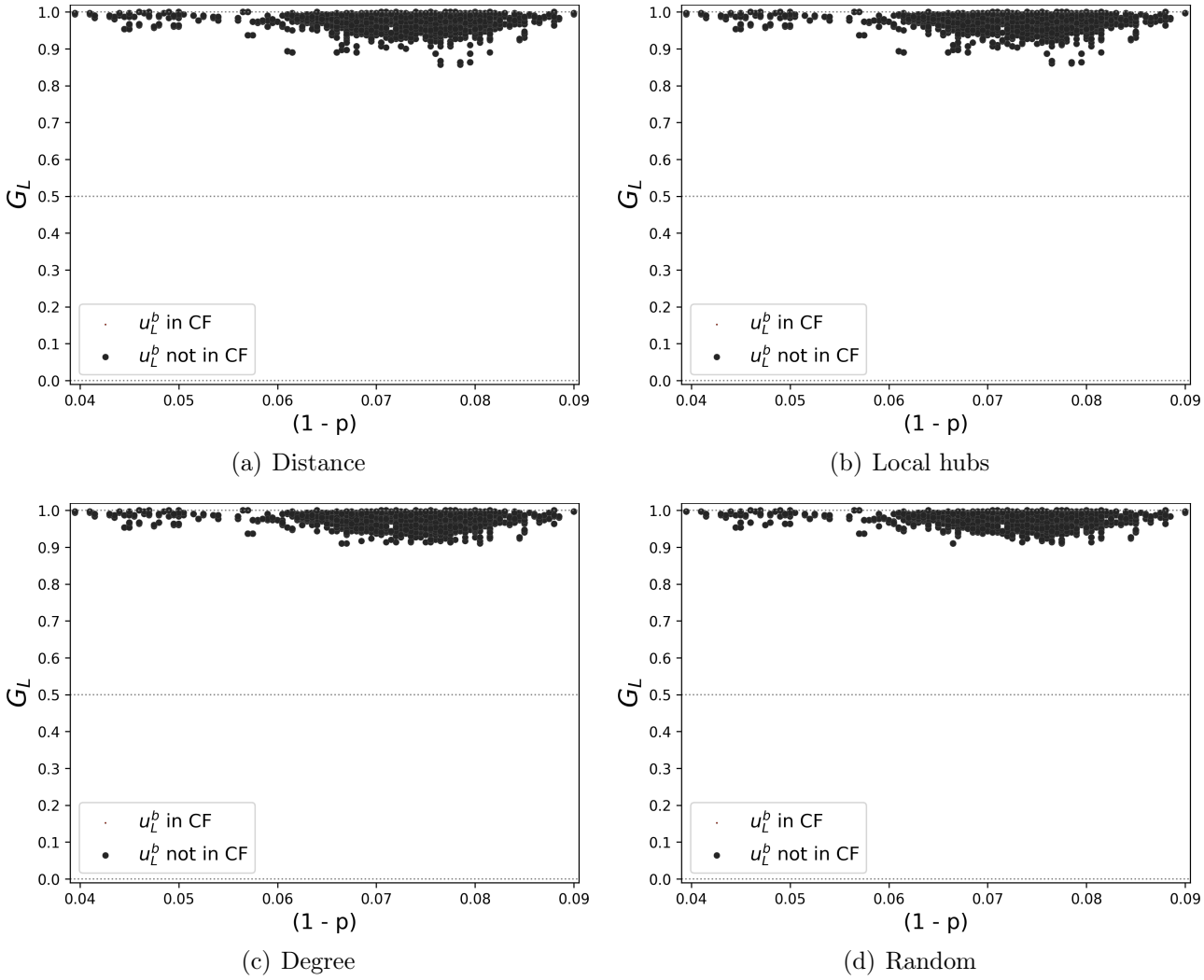


(c) Degree



(d) Random

Figure D.6: Each localized attack G_L value versus $(1-p)$ for systems built using $s = (1{:}25)$ and $I_{max} = 3$ after adding extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.



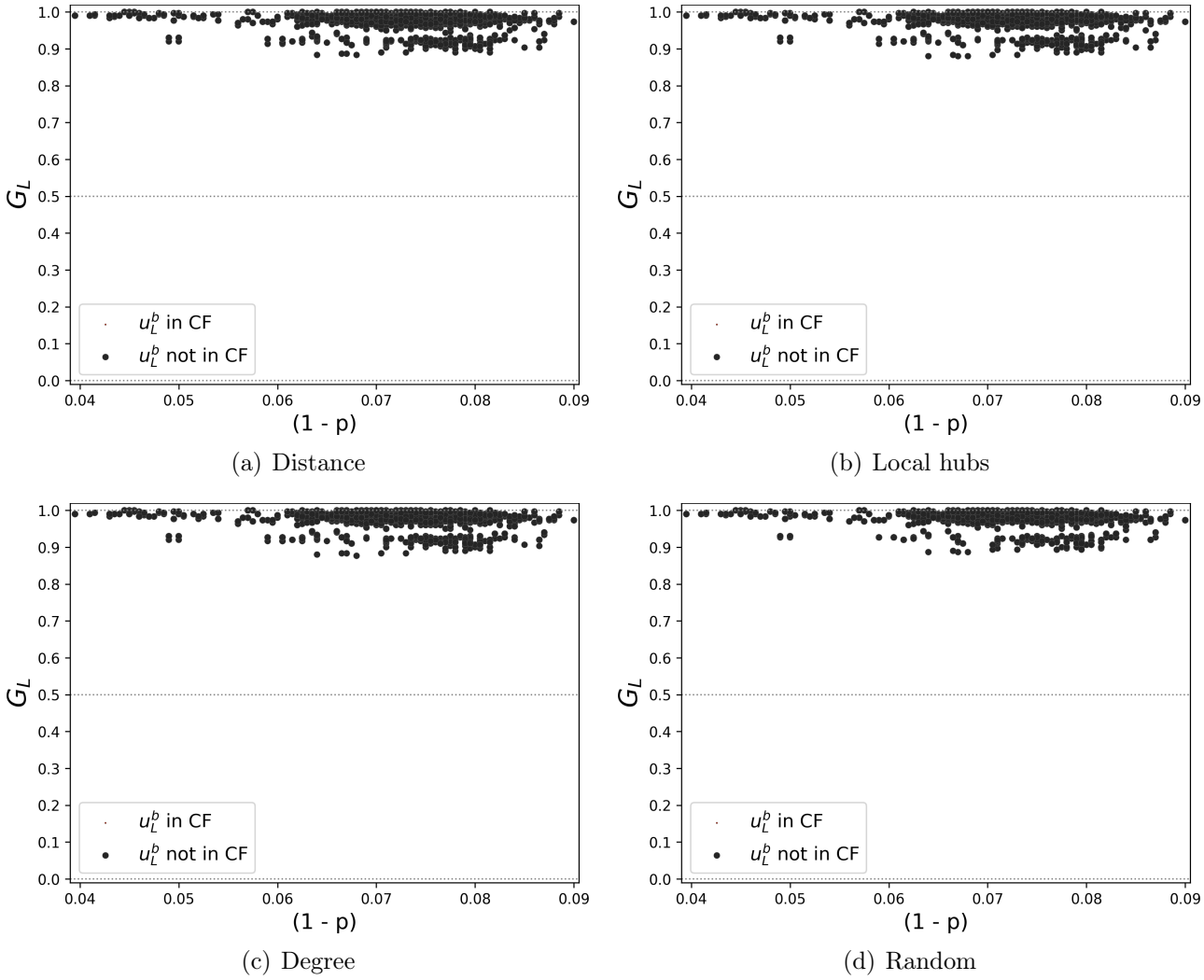
(a) Distance

(b) Local hubs

(c) Degree

(d) Random

Figure D.7: Each localized attack G_L value versus $(1-p)$ for systems built using $s = (1{:}25)$ and $I_{max} = 5$ after adding extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.



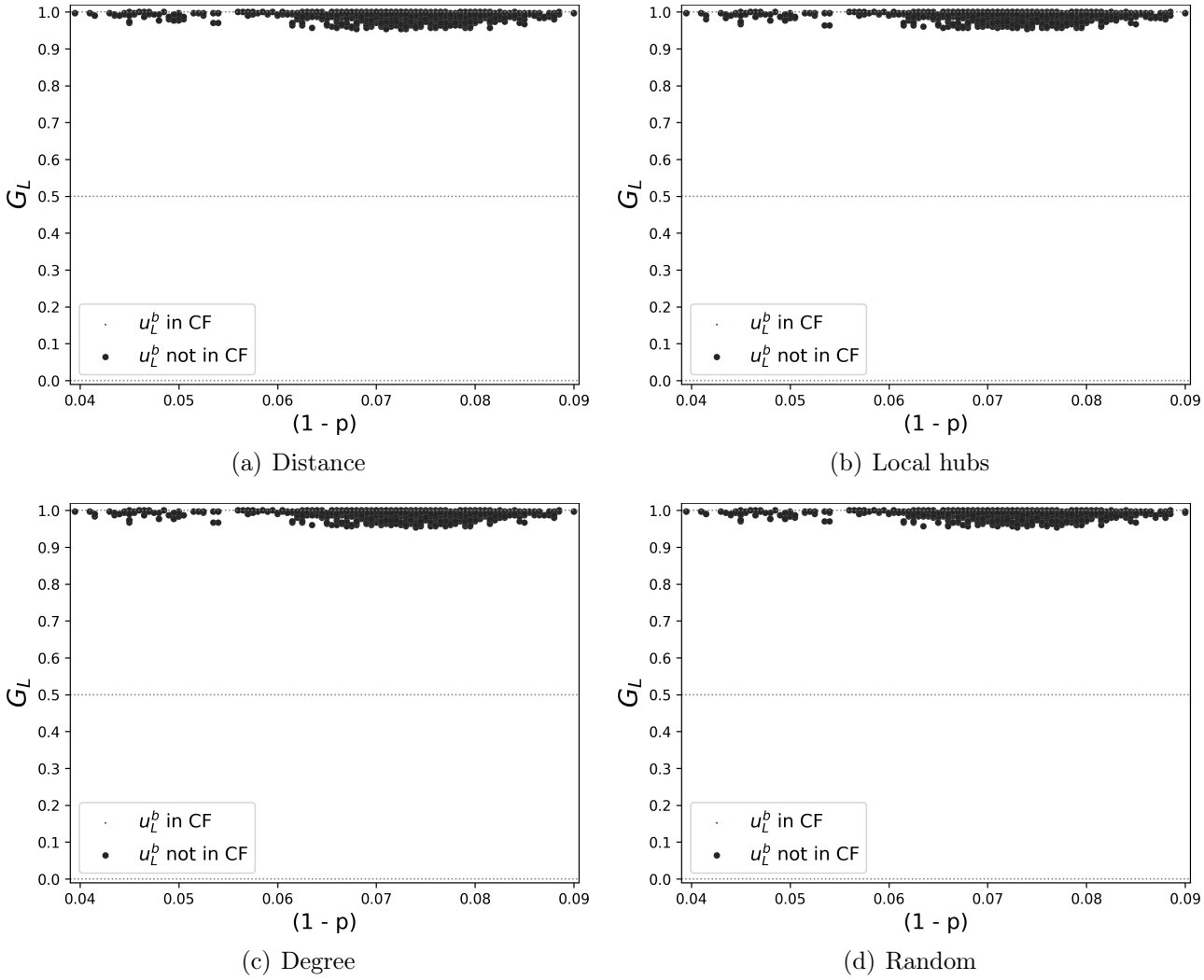
(a) Distance

(b) Local hubs

(c) Degree

(d) Random

Figure D.8: Each localized attack G_L value versus $(1-p)$ for systems built using $s = (1{:}25)$ and $I_{max} = 7$ after adding extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.



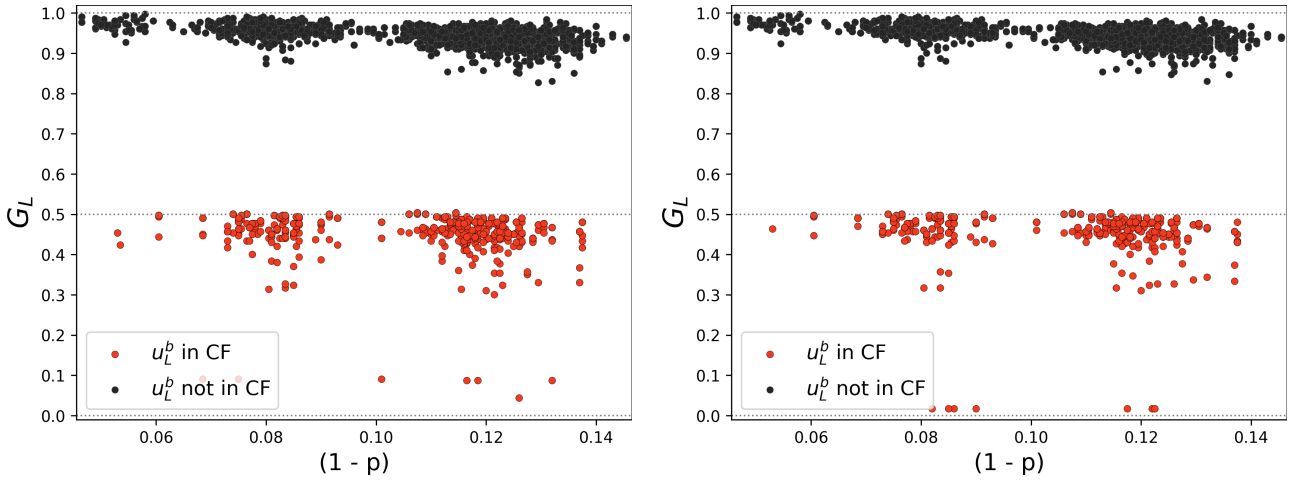
(a) Distance

(b) Local hubs

(c) Degree

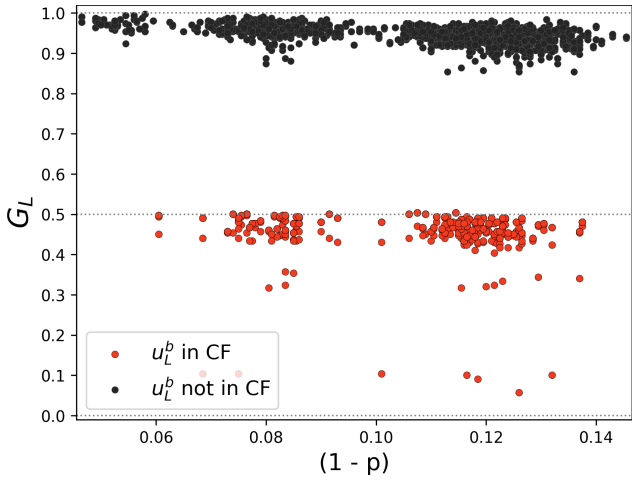
(d) Random

Figure D.9: Each localized attack G_L value versus $(1-p)$ for systems built using $s = (1{:}25)$ and $I_{max} = 10$ after adding extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

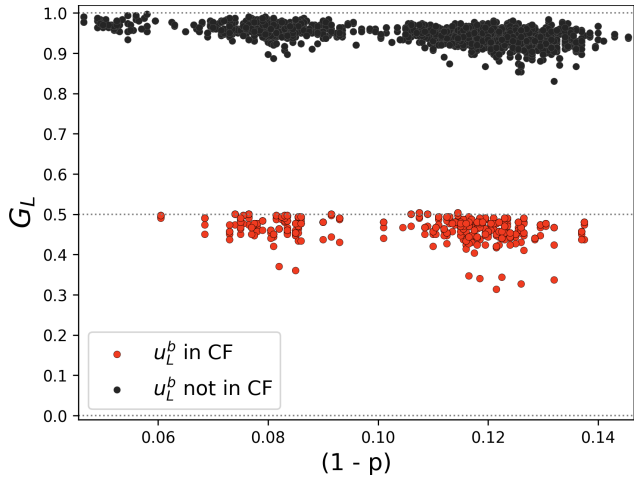


(a) Distance

(b) Local hubs

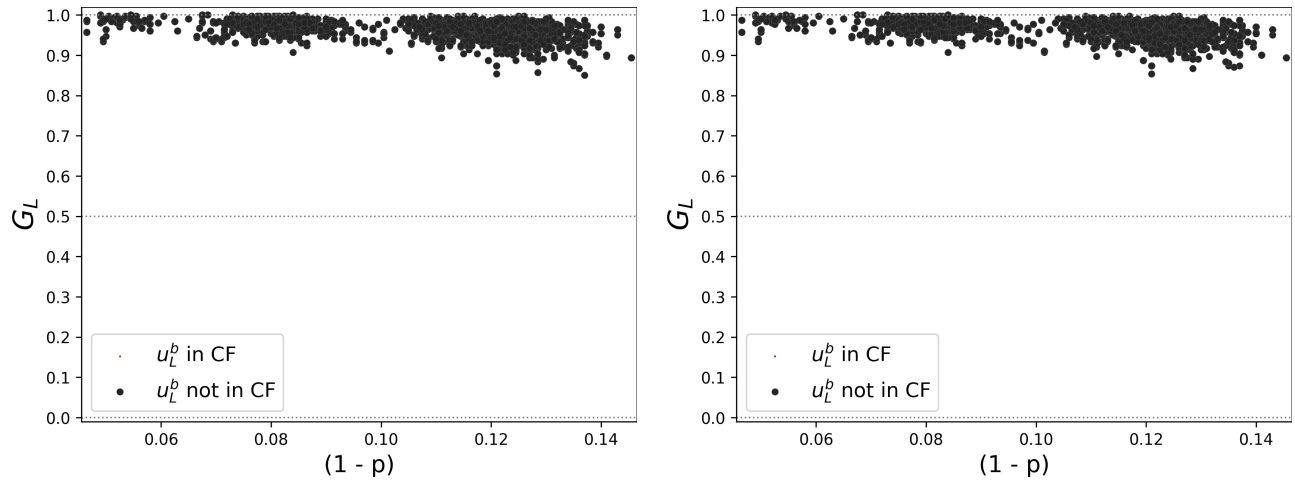


(c) Degree



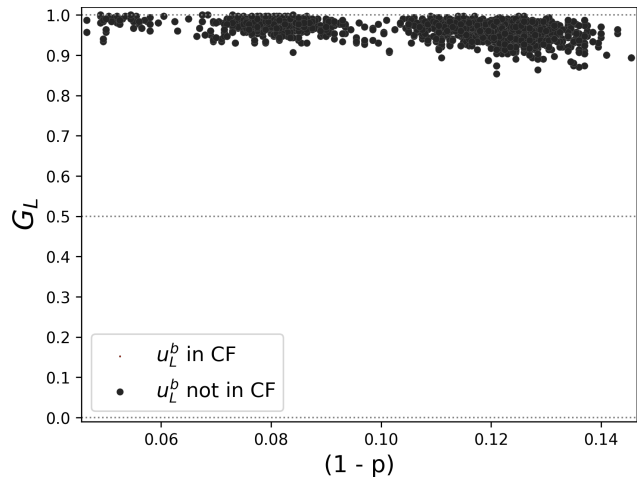
(d) Random

Figure D.10: Each localized attack G_L value versus $(1-p)$ for systems built using $s = (1{:}1)$ and $I_{max} = 3$ after adding extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

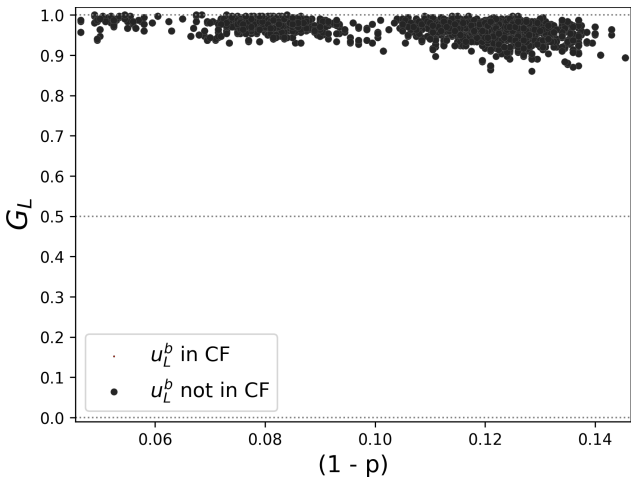


(a) Distance

(b) Local hubs

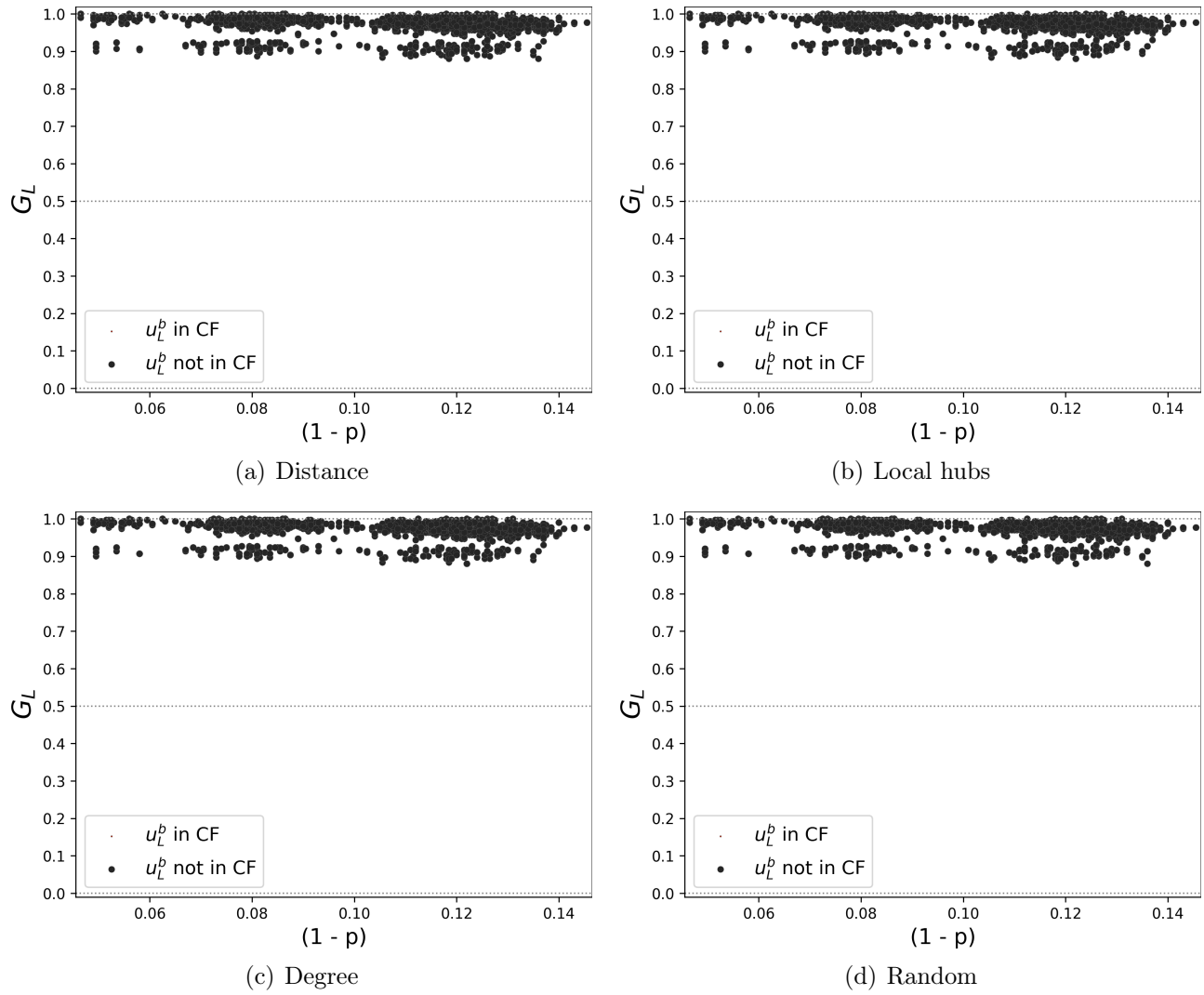


(c) Degree



(d) Random

Figure D.11: Each localized attack G_L value versus $(1-p)$ for systems built using $s = (1{:}1)$ and $I_{max} = 5$ after adding extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.



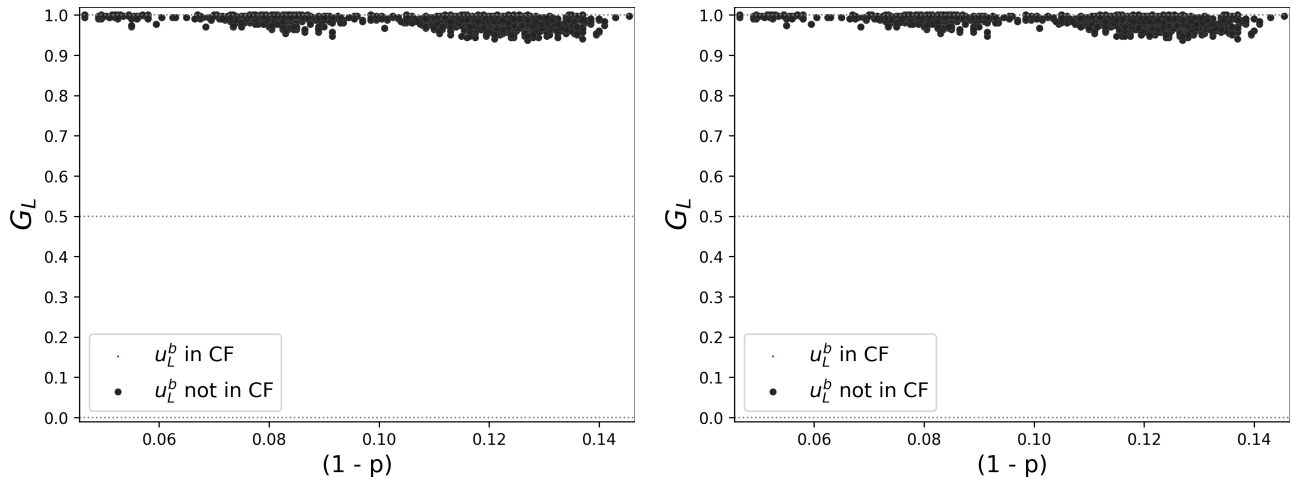
(a) Distance

(b) Local hubs

(c) Degree

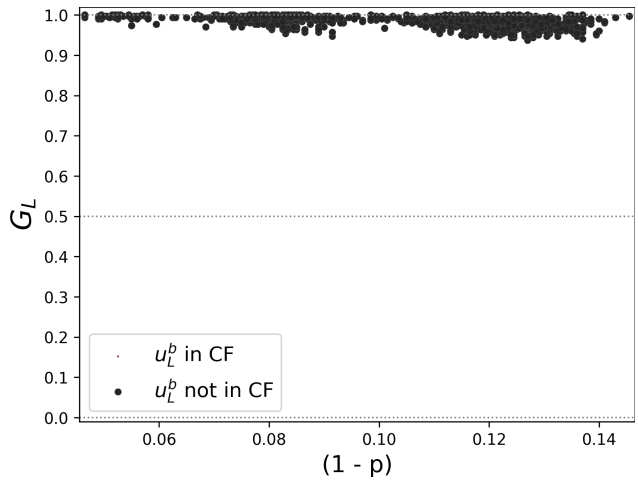
(d) Random

Figure D.12: Each localized attack G_L value versus $(1-p)$ for systems built using $s = (1{:}1)$ and $I_{max} = 7$ after adding extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

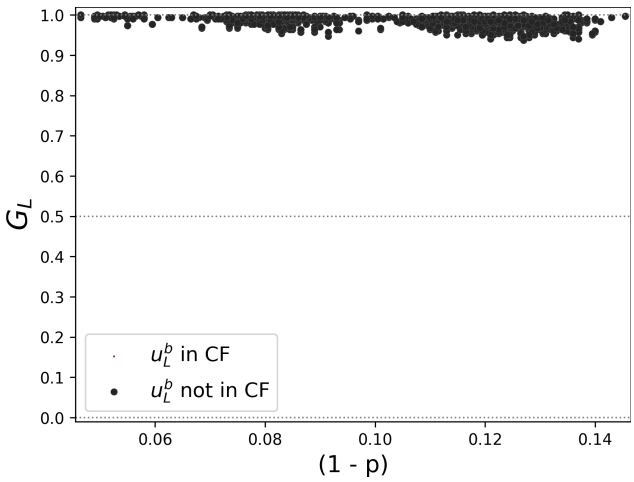


(a) Distance

(b) Local hubs



(c) Degree



(d) Random

Figure D.13: Each localized attack G_L value versus $(1-p)$ for systems built using $s = (1{:}1)$ and $I_{max} = 10$ after adding extra physical links ($r = 1 \cdot w_{ln}$). Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

D.3 Physical link addition and localized attacks tables

$I_{max} = 3$										
s	st	Number of HDLA							G_L range (HDLA)	G_L range (Non-HDLA)
		Total	RNG	GG	GPA	5NN	YAO	ER		
(1:25)	Original	480	74	73	114	73	73	73	(0.0,0.5)	(0.837,1.0)
	Distance	458	74	73	92	73	73	73	(0.23,0.5)	(0.893,1.0)
	Local hubs	447	74	73	81	73	73	73	(0.323,0.5)	(0.893,1.0)
	Degree	442	73	73	77	73	73	73	(0.353,0.5)	(0.897,1.0)
	Random	458	74	73	92	73	73	73	(0.353,0.5)	(0.873,1.0)
(1:1)	Original	619	100	99	122	100	99	99	(0.0,0.5)	(0.503,0.997)
	Distance	618	100	99	121	100	99	99	(0.043,0.5)	(0.503,0.997)
	Local hubs	607	99	99	112	99	99	99	(0.017,0.5)	(0.503,0.997)
	Degree	594	99	99	99	99	99	99	(0.057,0.5)	(0.503,0.997)
	Random	596	99	99	101	99	99	99	(0.313,0.5)	(0.503,0.997)

Table D.1: G_L ranges of HDLA, and LA minus HDLA (Non-HDLA) of systems with and without physical links added for $I_{max} = 3$, and $a = 1$.

$I_{max} = 5$										
s	st	Number of HDLA							G_L range (HDLA)	G_L range (Non-HDLA)
		Total	RNG	GG	GPA	5NN	YAO	ER		
(1:25)	Original	0	0	0	0	0	0	0	ϕ	(0.853,1.0)
	Distance	0	0	0	0	0	0	0	ϕ	(0.857,1.0)
	Local hubs	0	0	0	0	0	0	0	ϕ	(0.86,1.0)
	Degree	0	0	0	0	0	0	0	ϕ	(0.91,1.0)
	Random	0	0	0	0	0	0	0	ϕ	(0.91,1.0)
(1:1)	Original	0	0	0	0	0	0	0	ϕ	(0.85,1.0)
	Distance	0	0	0	0	0	0	0	ϕ	(0.85,1.0)
	Local hubs	0	0	0	0	0	0	0	ϕ	(0.853,1.0)
	Degree	0	0	0	0	0	0	0	ϕ	(0.853,1.0)
	Random	0	0	0	0	0	0	0	ϕ	(0.86,1.0)

Table D.2: G_L ranges of HDLA, and LA minus HDLA (Non-HDLA) of systems with and without physical links added for $I_{max} = 5$, and $a = 1$.

$I_{max} = 7$										
s	st	Number of HDLA							G_L range (HDLA)	G_L range (Non-HDLA)
		Total	RNG	GG	GPA	5NN	YAO	ER		
(1:25)	Original	0	0	0	0	0	0	0	ϕ	(0.863,1.0)
	Distance	0	0	0	0	0	0	0	ϕ	(0.883,1.0)
	Local hubs	0	0	0	0	0	0	0	ϕ	(0.88,1.0)
	Degree	0	0	0	0	0	0	0	ϕ	(0.877,1.0)
	Random	0	0	0	0	0	0	0	ϕ	(0.887,1.0)
(1:1)	Original	0	0	0	0	0	0	0	ϕ	(0.88,1.0)
	Distance	0	0	0	0	0	0	0	ϕ	(0.88,1.0)
	Local hubs	0	0	0	0	0	0	0	ϕ	(0.88,1.0)
	Degree	0	0	0	0	0	0	0	ϕ	(0.88,1.0)
	Random	0	0	0	0	0	0	0	ϕ	(0.88,1.0)

Table D.3: G_L ranges of HDLA, and LA minus HDLA (Non-HDLA) of systems with and without physical links added for $I_{max} = 7$, and $a = 1$.

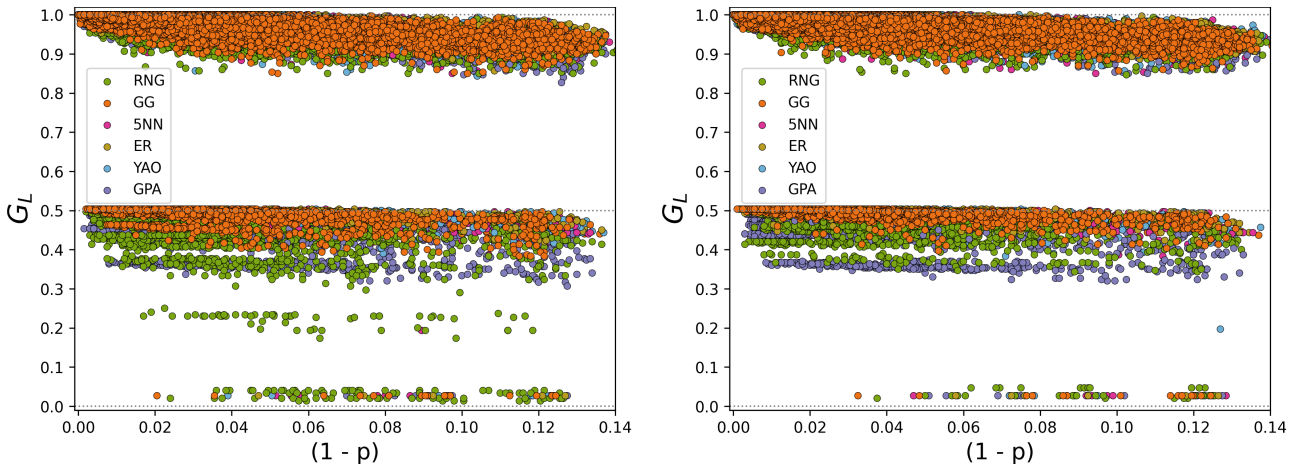
$I_{max} = 10$										
s	st	Number of HDLA							G_L range (HDLA)	G_L range (Non-HDLA)
		Total	RNG	GG	GPA	5NN	YAO	ER		
(1:25)	Original	0	0	0	0	0	0	0	ϕ	(0.953,1.0)
	Distance	0	0	0	0	0	0	0	ϕ	(0.953,1.0)
	Local hubs	0	0	0	0	0	0	0	ϕ	(0.953,1.0)
	Degree	0	0	0	0	0	0	0	ϕ	(0.953,1.0)
	Random	0	0	0	0	0	0	0	ϕ	(0.953,1.0)
(1:1)	Original	0	0	0	0	0	0	0	ϕ	(0.937,1.0)
	Distance	0	0	0	0	0	0	0	ϕ	(0.937,1.0)
	Local hubs	0	0	0	0	0	0	0	ϕ	(0.937,1.0)
	Degree	0	0	0	0	0	0	0	ϕ	(0.937,1.0)
	Random	0	0	0	0	0	0	0	ϕ	(0.937,1.0)

Table D.4: G_L ranges of HDLA, and LA minus HDLA (Non-HDLA) of systems with and without physical links added for $I_{max} = 10$, and $a = 1$.

Annexed E

Chapter 7: Localized attacks with probabilistic failure: Seismic attacks case

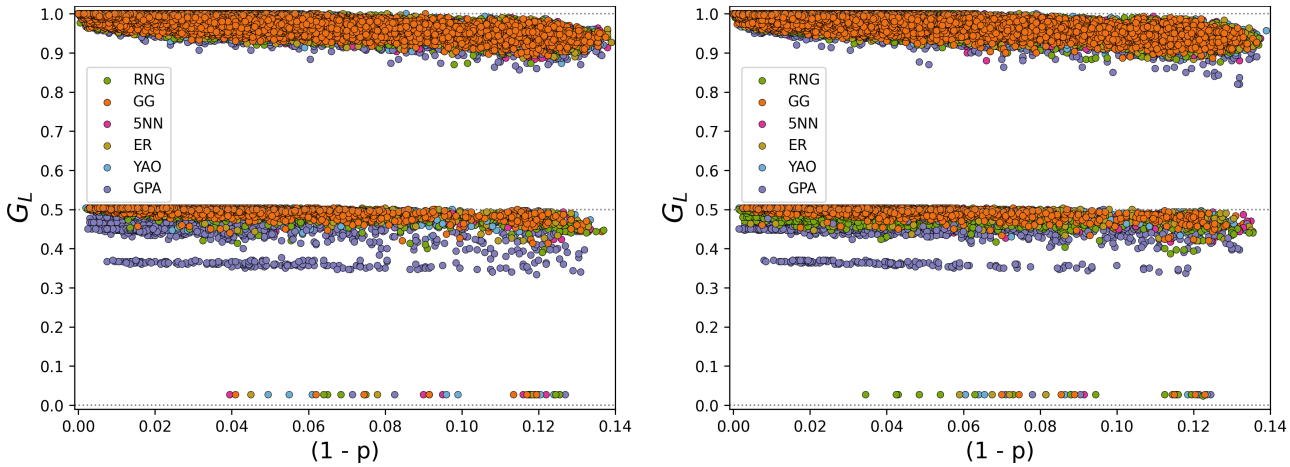
E.1 Link addition effect against seismic attacks figures



(a) Distance

(b) Local hubs

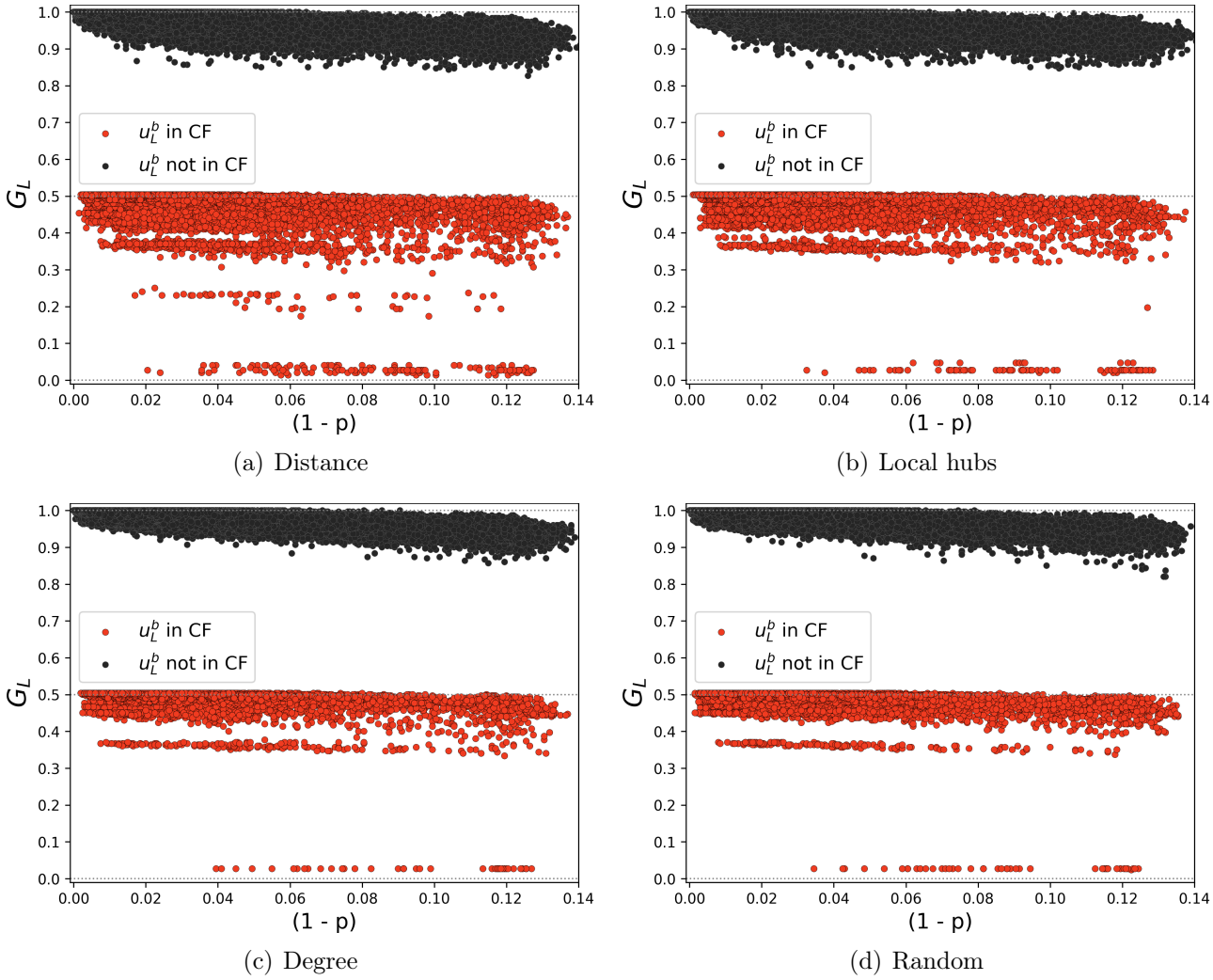
Figure E.1: G_L values obtained after each seismic attack tested for systems with extra physical links added, and $I_{max} = 3$. Each color represents a different physical model m. $st \in \{\text{Distance, Local hubs}\}$.



(a) Degree

(b) Random

Figure E.2: G_L values obtained after each seismic attack tested for systems with extra physical links added, and $I_{max} = 3$. Each color represents a different physical model m. $st \in \{\text{Degree, Random}\}$.



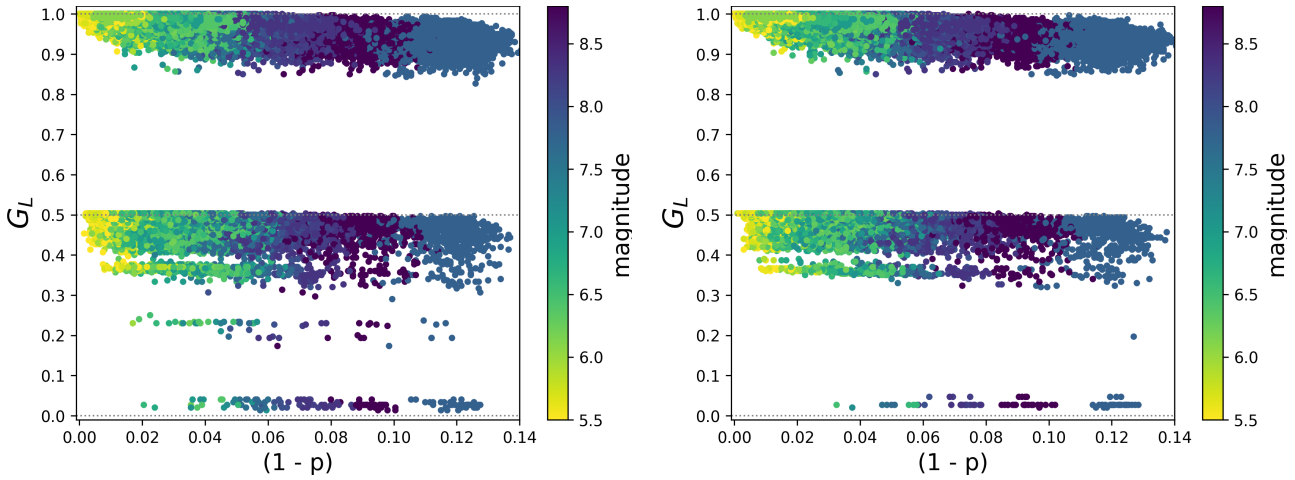
(a) Distance

(b) Local hubs

(c) Degree

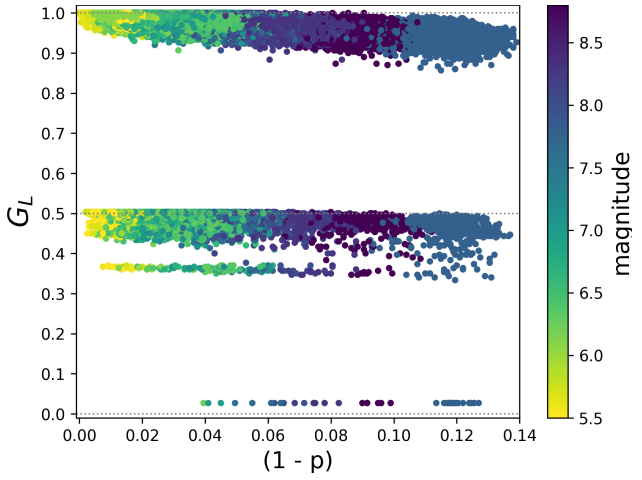
(d) Random

Figure E.3: Each seismic attack G_L value versus $(1-p)$ for systems with extra physical links added, and $I_{max} = 3$. Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

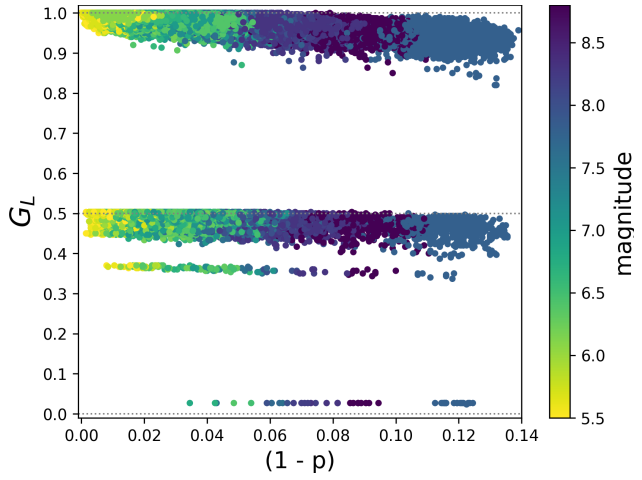


(a) Distance

(b) Local hubs

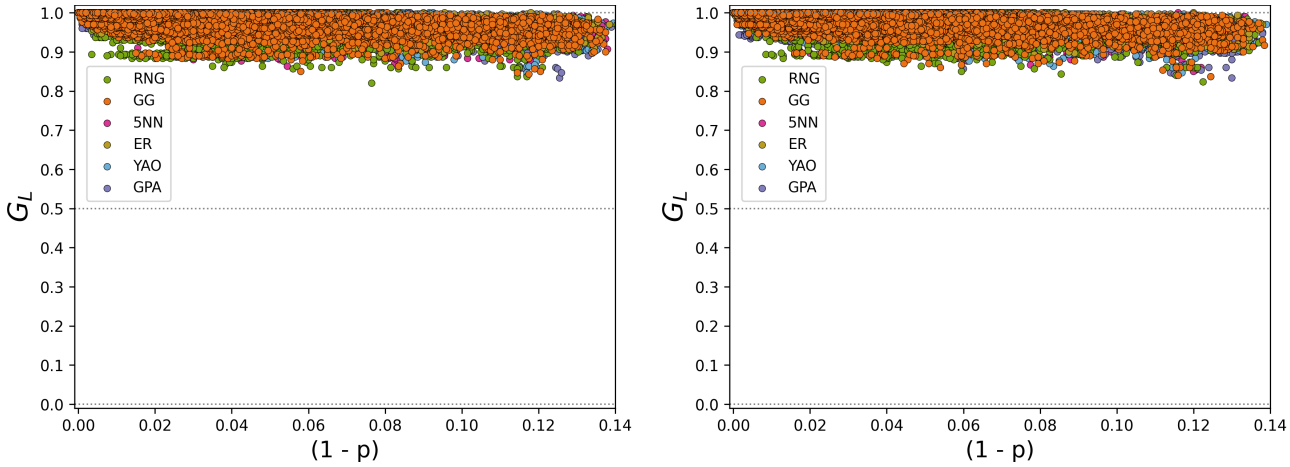


(c) Degree



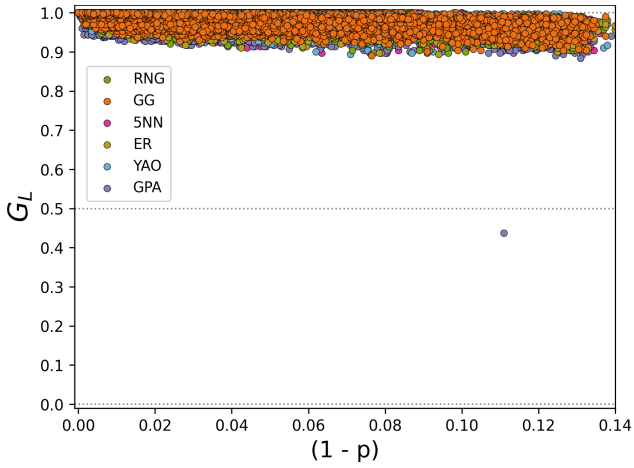
(d) Random

Figure E.4: Each seismic attack G_L value versus $(1-p)$ for systems with extra physical links added, and $I_{max} = 3$. Colors show the moment magnitude M_w associated to each seismic attack.

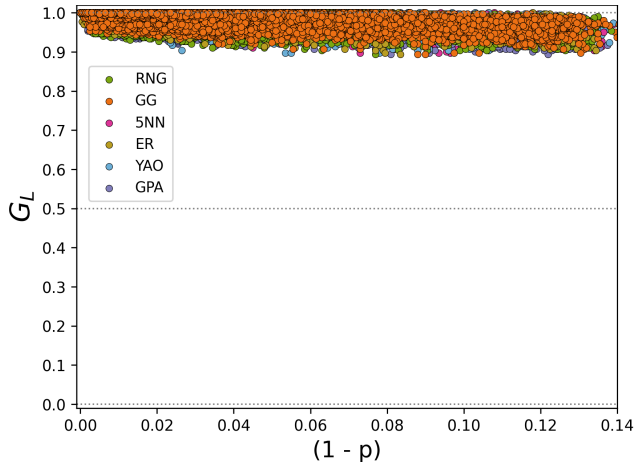


(a) Distance

(b) Local hubs

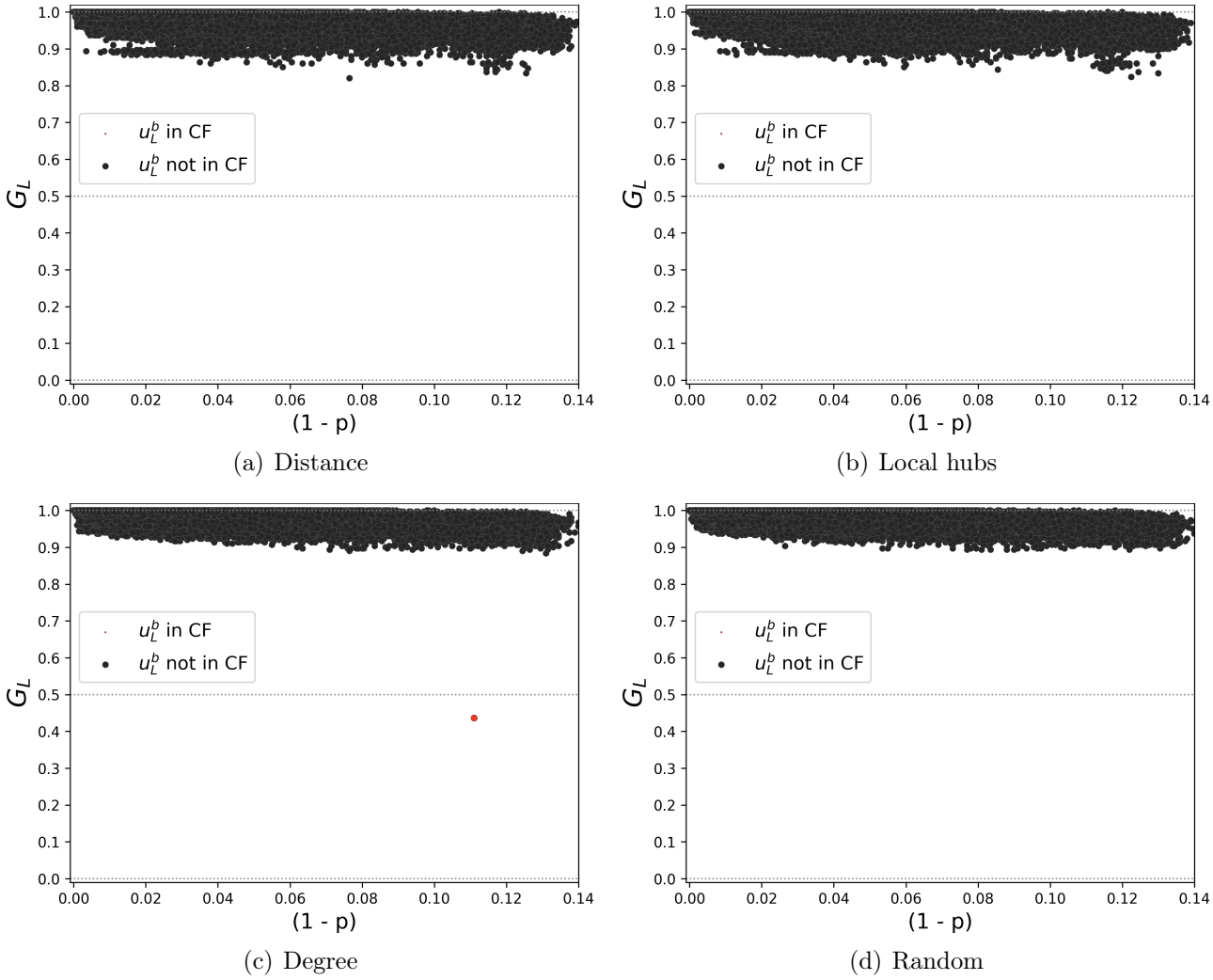


(c) Degree



(d) Random

Figure E.5: G_L values obtained after each seismic attack tested for systems with extra physical links added, and $I_{max} = 5$. Each color represents a different physical model m.



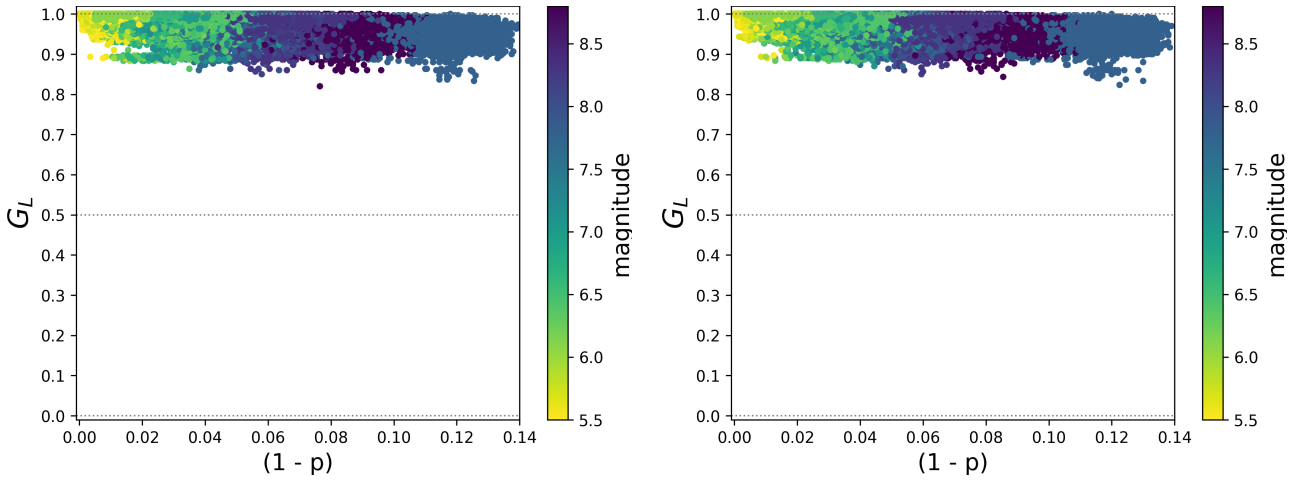
(a) Distance

(b) Local hubs

(c) Degree

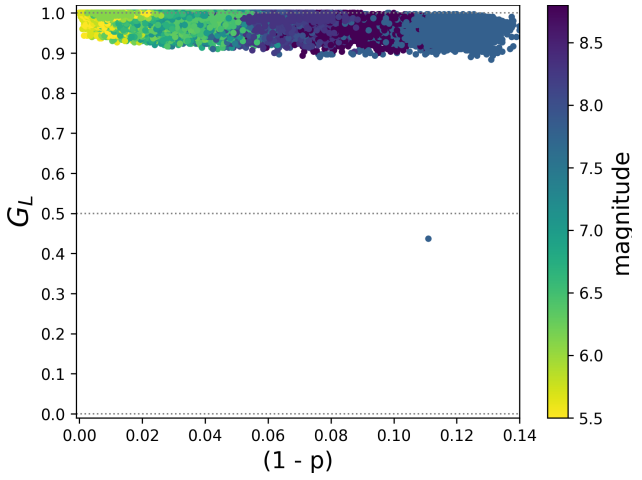
(d) Random

Figure E.6: Each seismic attack G_L value versus $(1-p)$ for systems with extra physical links added, and $I_{max} = 5$. Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

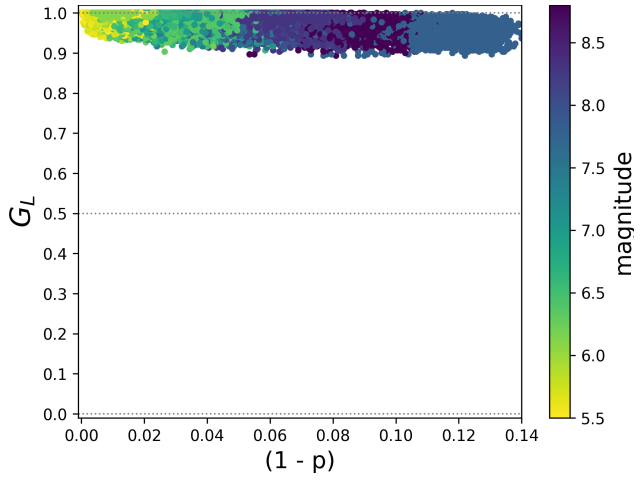


(a) Distance

(b) Local hubs

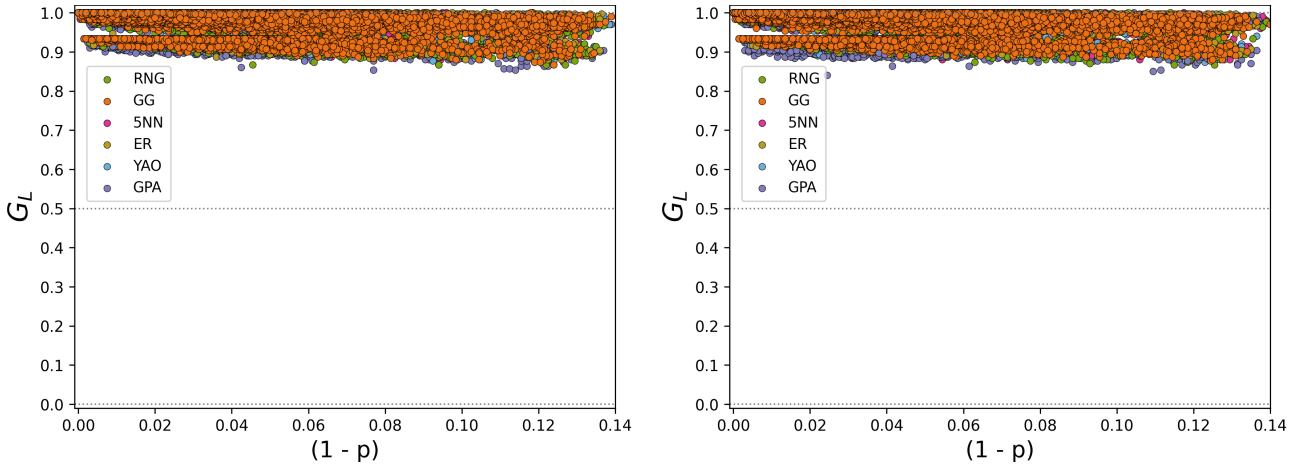


(c) Degree



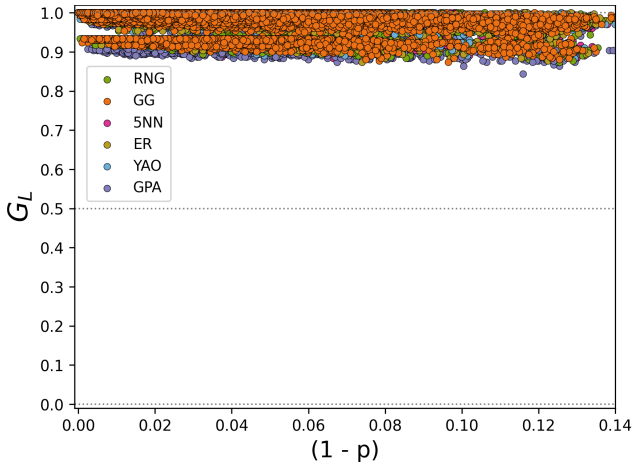
(d) Random

Figure E.7: Each seismic attack G_L value versus $(1-p)$ for systems with extra physical links added, and $I_{max} = 5$. Colors show the moment magnitude M_w associated to each seismic attack.

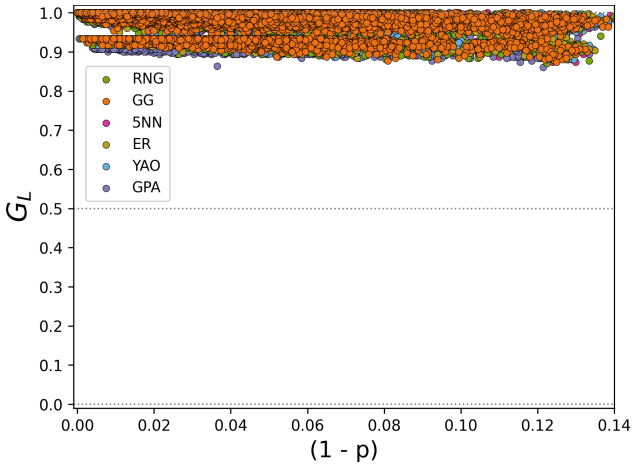


(a) Distance

(b) Local hubs

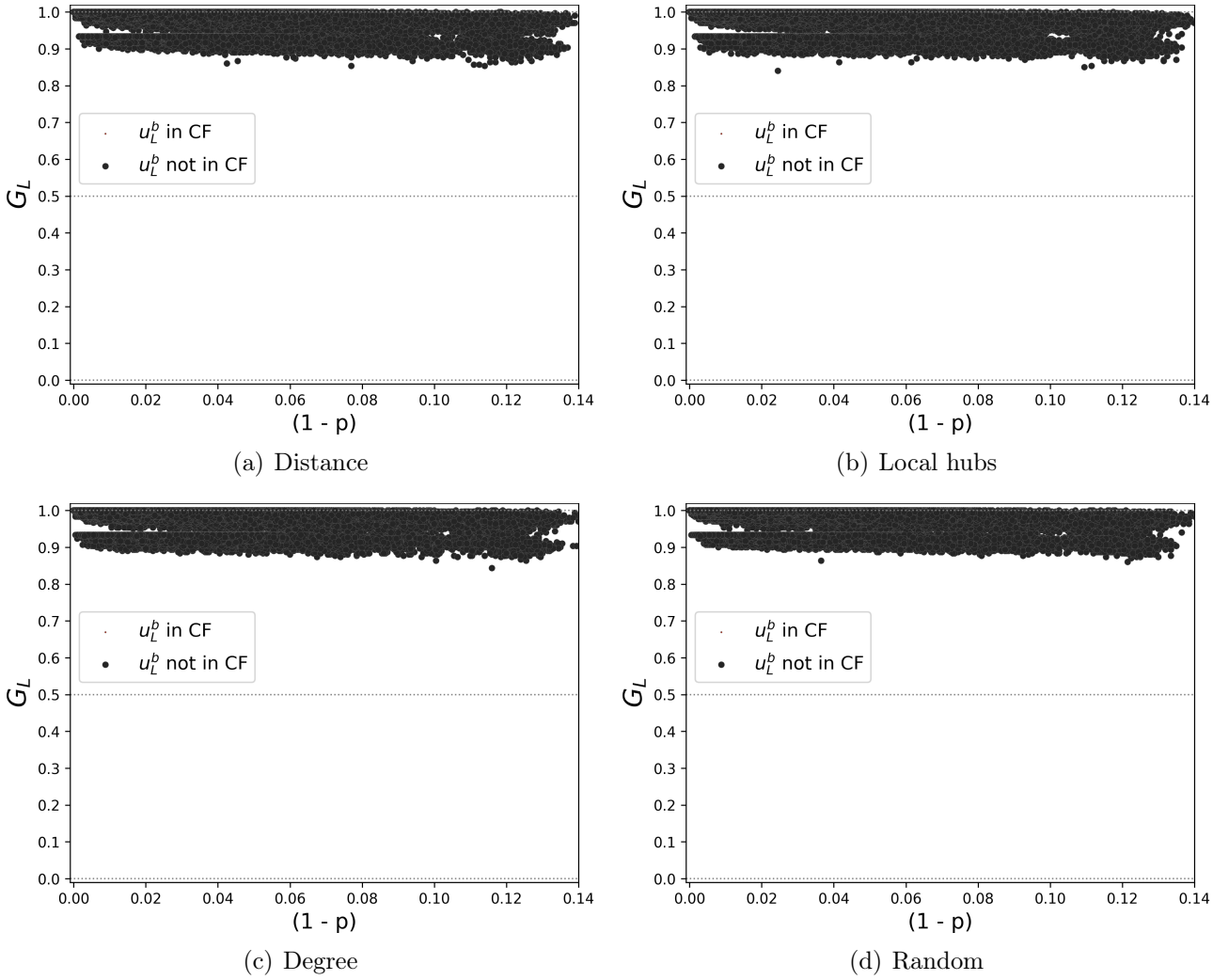


(c) Degree



(d) Random

Figure E.8: G_L values obtained after each seismic attack tested for systems with extra physical links added, and $I_{max} = 7$. Each color represents a different physical model m.



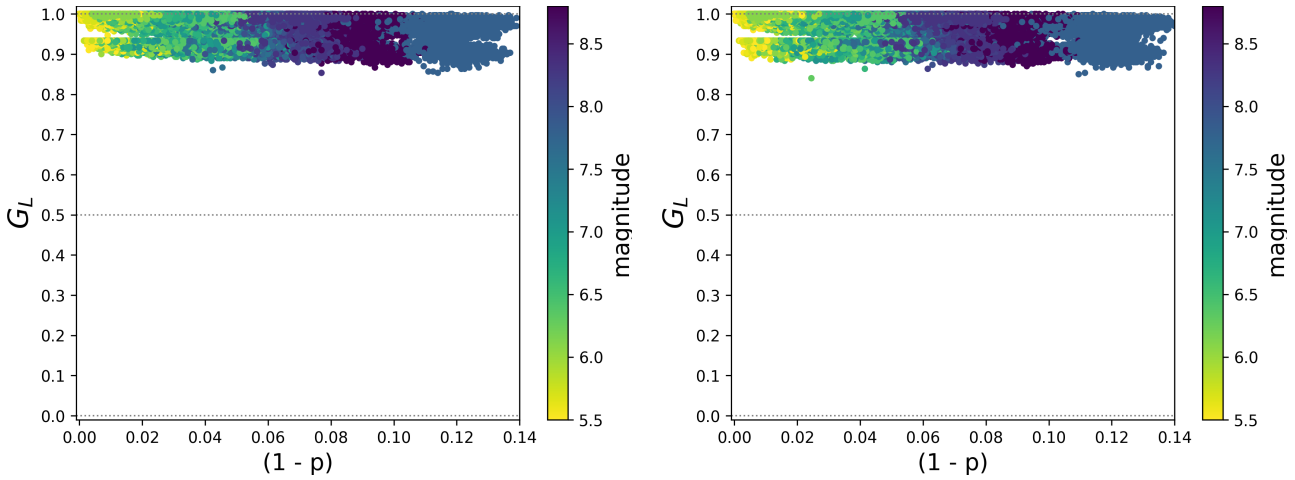
(a) Distance

(b) Local hubs

(c) Degree

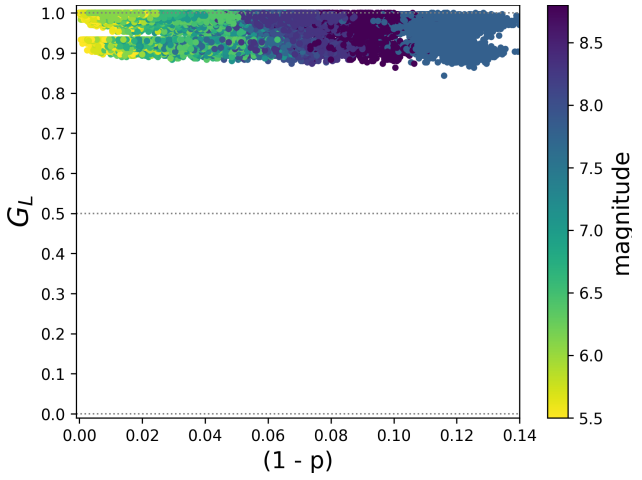
(d) Random

Figure E.9: Each seismic attack G_L value versus $(1-p)$ for systems with extra physical links added, and $I_{max} = 7$. Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

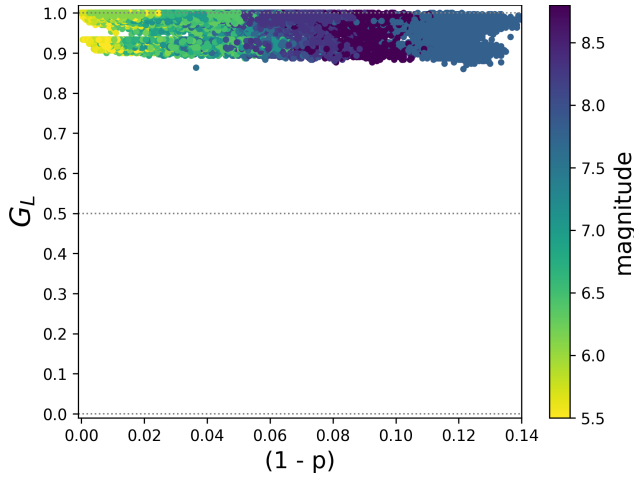


(a) Distance

(b) Local hubs

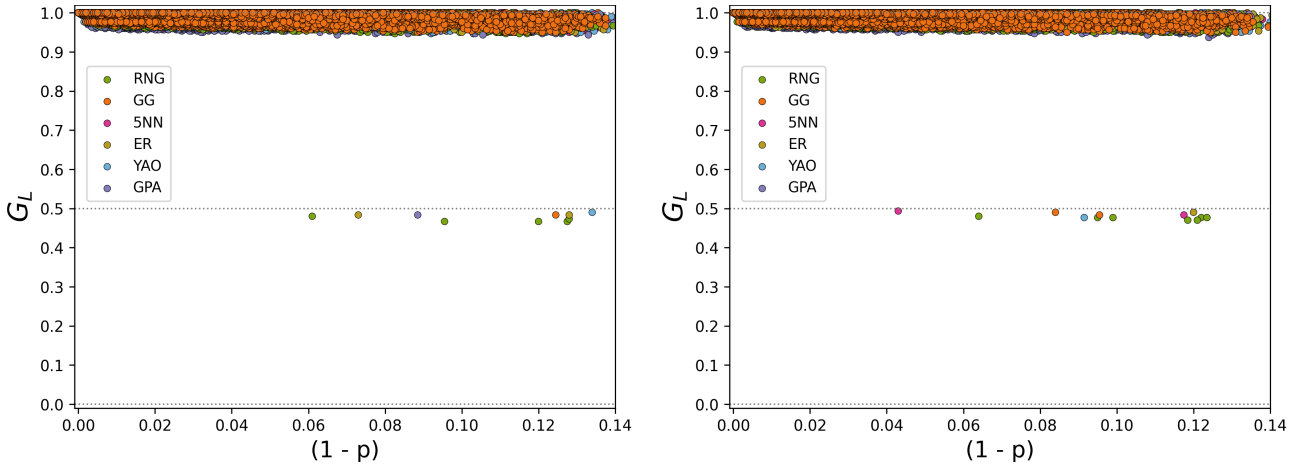


(c) Degree



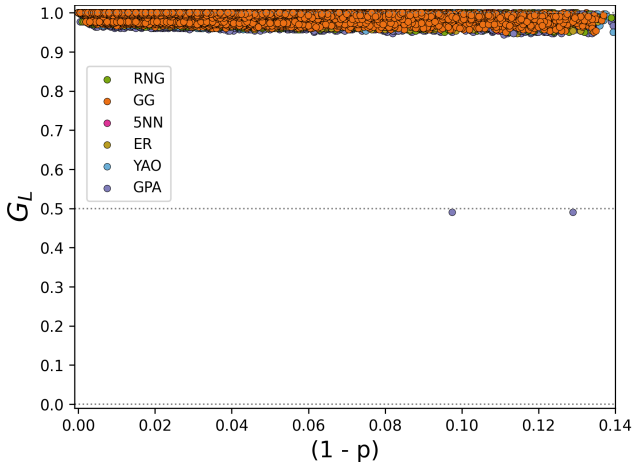
(d) Random

Figure E.10: Each seismic attack G_L value versus $(1-p)$ for systems with extra physical links added, and $I_{max} = 7$. Colors show the moment magnitude M_w associated to each seismic attack.

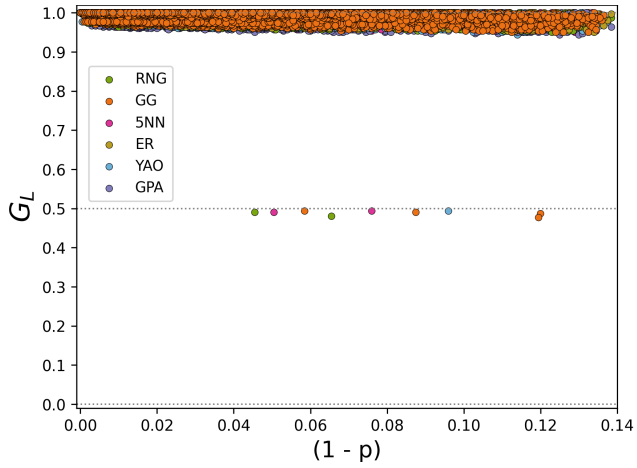


(a) Distance

(b) Local hubs

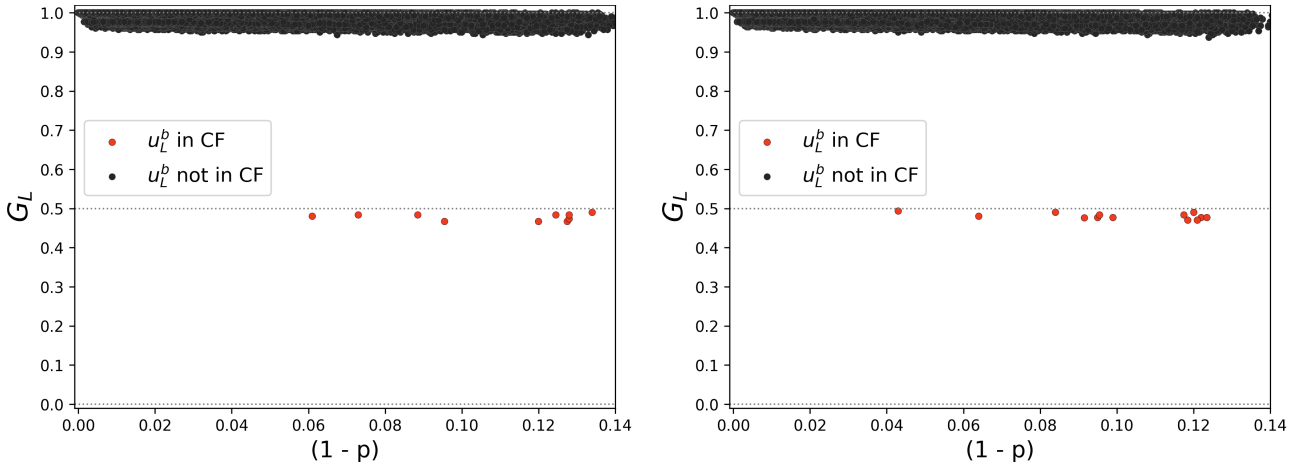


(c) Degree



(d) Random

Figure E.11: G_L values obtained after each seismic attack tested for systems with extra physical links added, and $I_{max} = 10$. Each color represents a different physical model m.



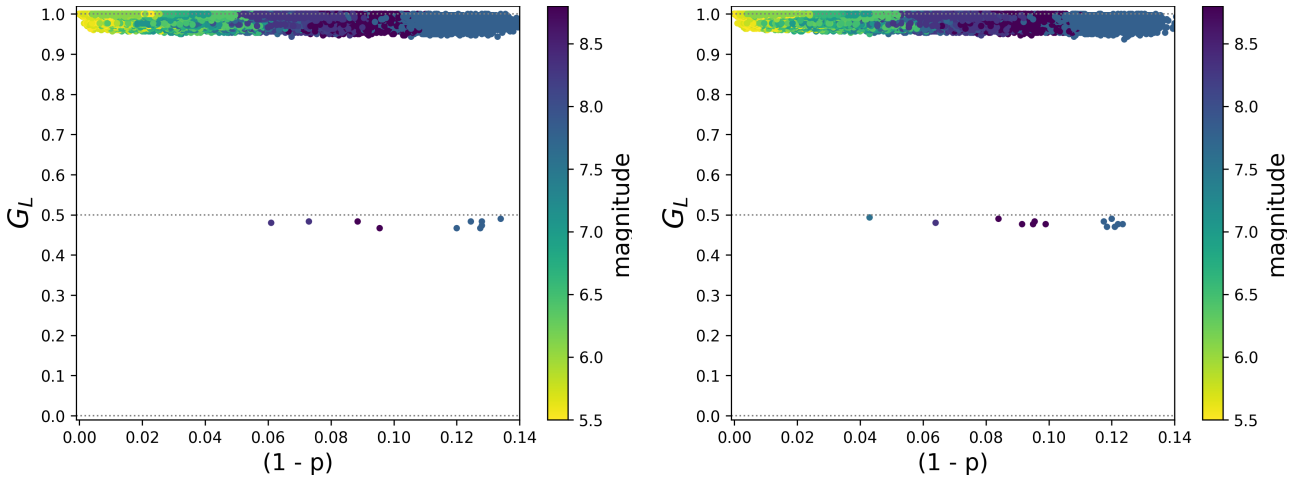
(a) Distance

(b) Local hubs

(c) Degree

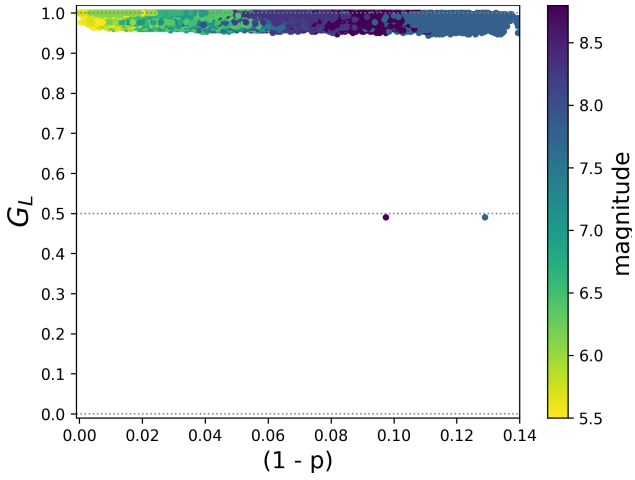
(d) Random

Figure E.12: Each seismic attack G_L value versus $(1-p)$ for systems with extra physical links added, and $I_{max} = 10$. Dots in red correspond to localized attacks x with $u_L^b \in CF(x)$, and dots in black LA with $u_L^b \notin CF(x)$.

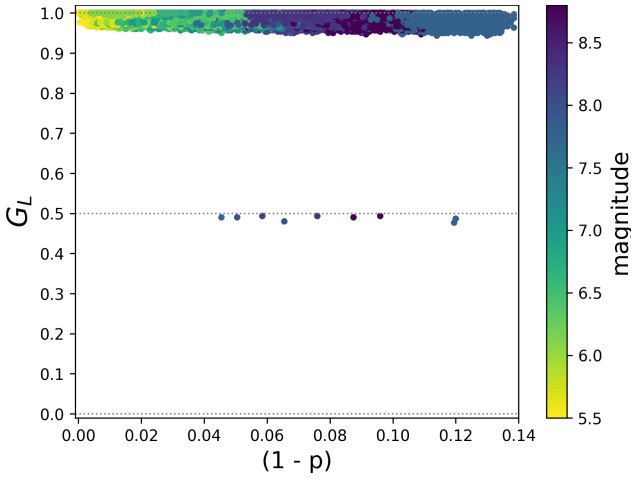


(a) Distance

(b) Local hubs



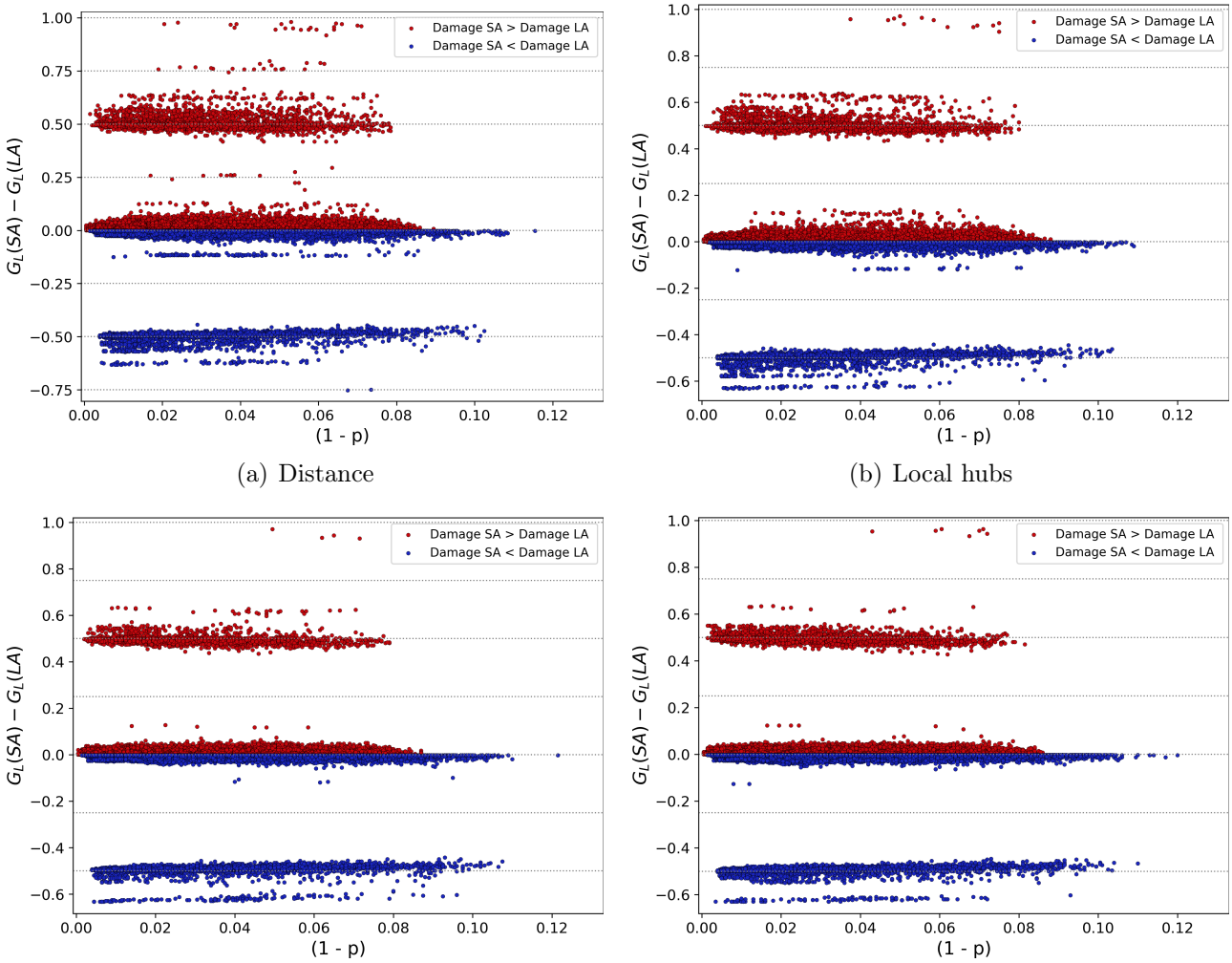
(c) Degree



(d) Random

Figure E.13: Each seismic attack G_L value versus $(1 - p)$ for systems with extra physical links added, and $I_{max} = 10$. Colors show the moment magnitude M_w associated to each seismic attack.

E.2 $G_L(LA) - G_L(SA)$ comparison figures



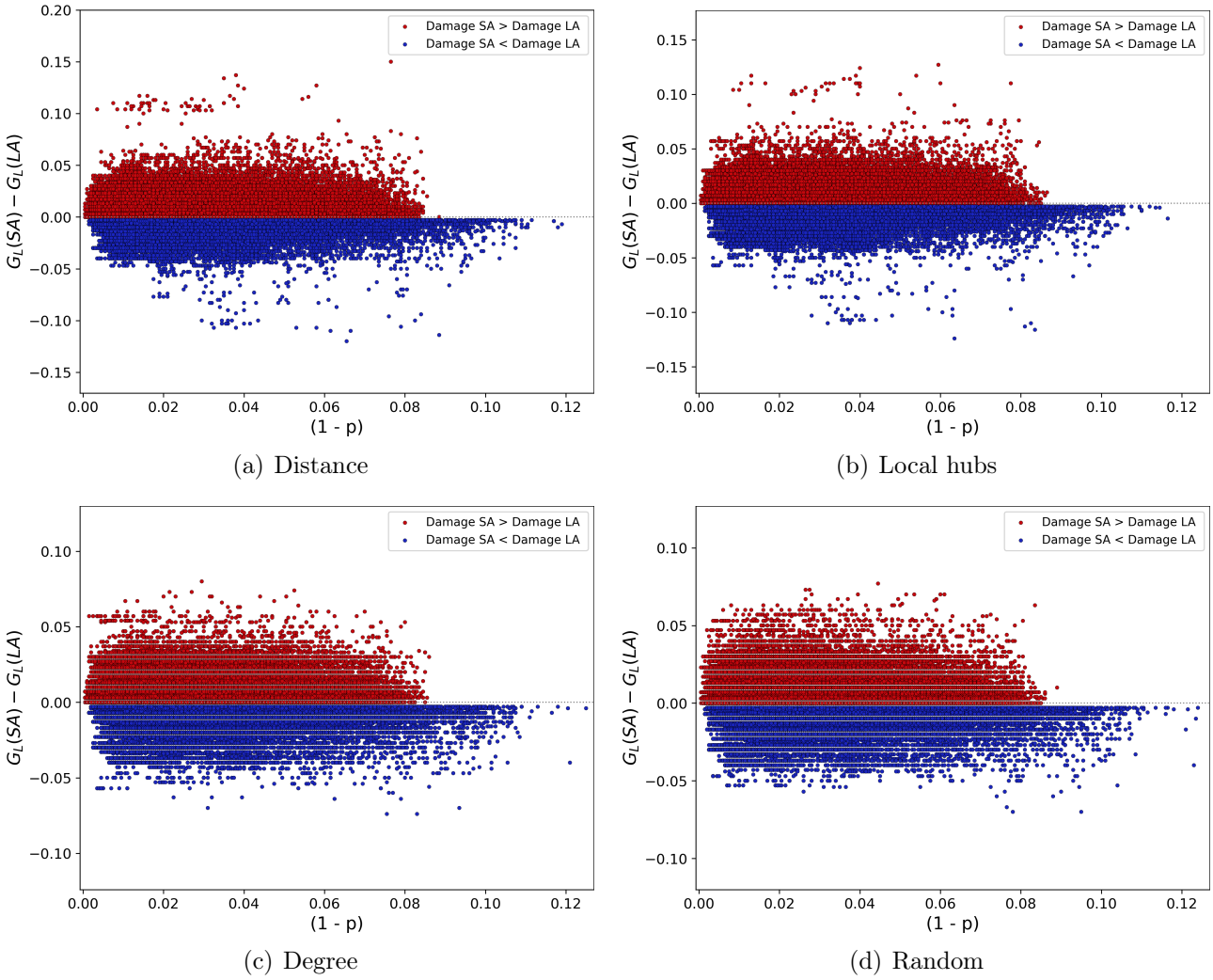
(a) Distance

(b) Local hubs

(c) Degree

(d) Random

Figure E.14: $G_L(LA) - G_L(SA)$ values obtained for each seismic attack classified within the **Damage SA** $>$ **Damage LA** category or within the **Damage SA** $<$ **Damage LA** category. Systems have extra physical links added, and were built using $I_{max} = 3$.



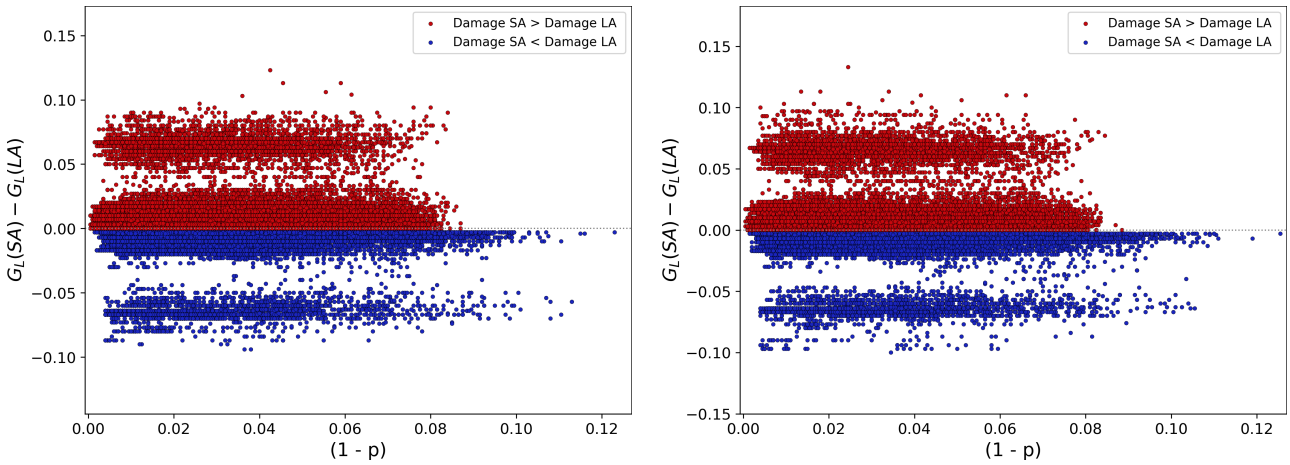
(a) Distance

(b) Local hubs

(c) Degree

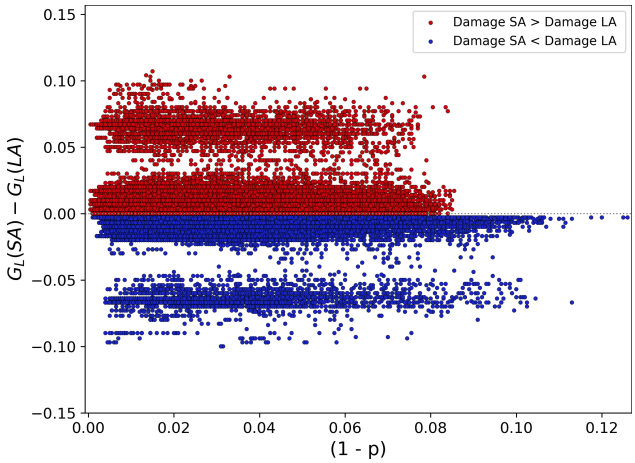
(d) Random

Figure E.15: $G_L(LA) - G_L(SA)$ values obtained for each seismic attack classified within the **Damage SA > Damage LA** category or within the **Damage SA < Damage LA** category. Systems have extra physical links added, and were built using $I_{max} = 5$.

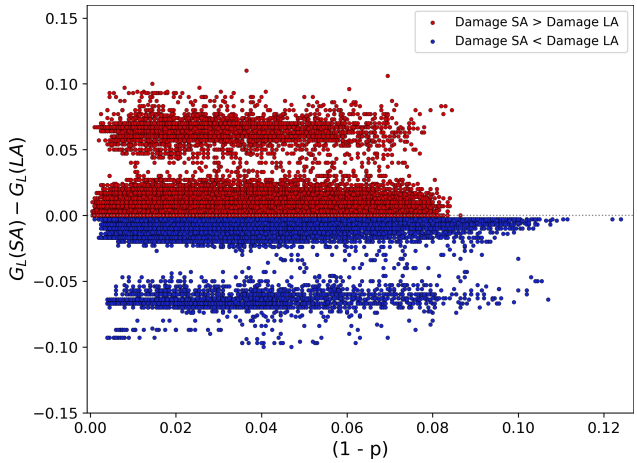


(a) Distance

(b) Local hubs

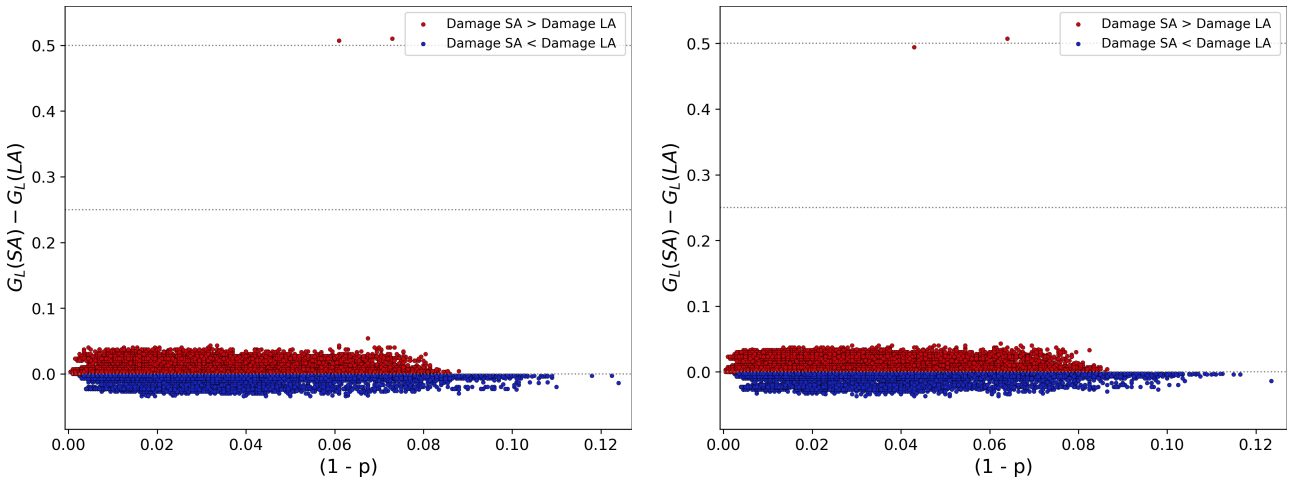


(c) Degree



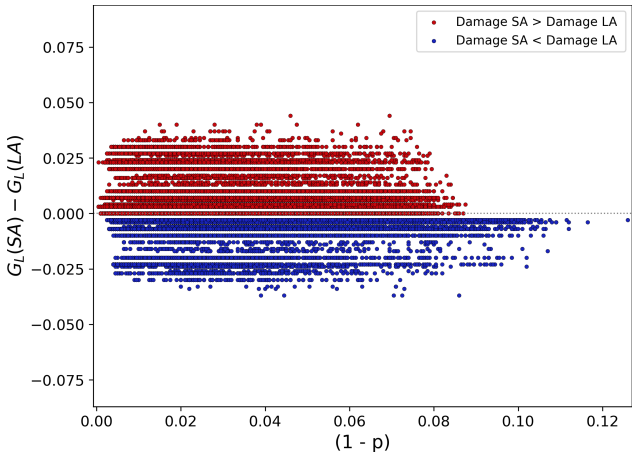
(d) Random

Figure E.16: $G_L(LA) - G_L(SA)$ values obtained for each seismic attack classified within the **Damage SA > Damage LA** category or within the **Damage SA < Damage LA** category. Systems have extra physical links added, and were built using $I_{max} = 7$.

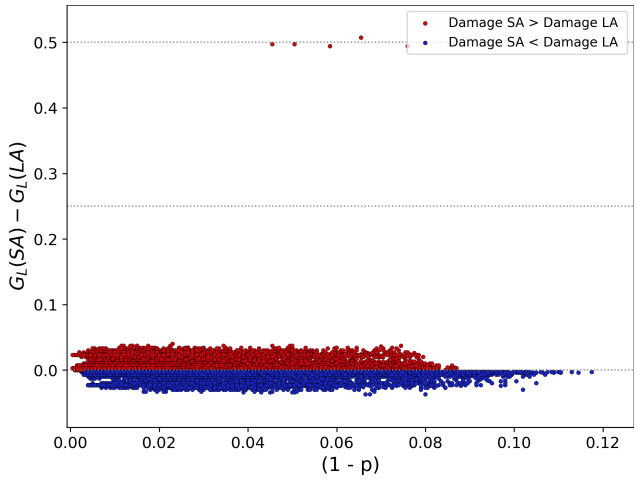


(a) Distance

(b) Local hubs



(c) Degree



(d) Random

Figure E.17: $G_L(LA) - G_L(SA)$ values obtained for each seismic attack classified within the **Damage SA** $>$ **Damage LA** category or within the **Damage SA** $<$ **Damage LA** category. Systems have extra physical links added, and were built using $I_{max} = 10$.

E.3 Link addition effect against seismic attacks summary tables

st = Original				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	3360	(5.5, 8.8)	(0.0, 0.487)	(0.82, 1.0)
GG	1963	(5.5, 8.8)	(0.027, 0.503)	(0.84, 1.0)
GPA	3889	(5.5, 8.8)	(0.01, 0.493)	(0.767, 1.0)
5NN	1659	(5.5, 8.8)	(0.027, 0.503)	(0.86, 1.0)
YAO	1607	(5.5, 8.8)	(0.027, 0.503)	(0.853, 1.0)
ER	1652	(5.5, 8.8)	(0.027, 0.503)	(0.847, 1.0)
st = Distance				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	2618	(5.5, 8.8)	(0.013, 0.497)	(0.85, 1.0)
GG	1829	(5.5, 8.8)	(0.027, 0.503)	(0.85, 1.0)
GPA	2674	(5.5, 8.8)	(0.027, 0.493)	(0.827, 1.0)
5NN	1734	(5.5, 8.8)	(0.027, 0.503)	(0.85, 1.0)
YAO	1608	(5.5, 8.8)	(0.027, 0.503)	(0.843, 1.0)
ER	1588	(5.5, 8.8)	(0.027, 0.503)	(0.857, 1.0)
st = Local hubs				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	2123	(5.5, 8.8)	(0.02, 0.503)	(0.847, 1.0)
GG	1730	(5.5, 8.8)	(0.027, 0.503)	(0.857, 1.0)
GPA	2117	(5.5, 8.8)	(0.027, 0.5)	(0.85, 1.0)
5NN	1633	(5.5, 8.8)	(0.027, 0.503)	(0.85, 1.0)
YAO	1635	(5.5, 8.8)	(0.027, 0.503)	(0.857, 1.0)
ER	1562	(5.5, 8.8)	(0.027, 0.503)	(0.873, 1.0)
st = Degree				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	1564	(5.5, 8.8)	(0.027, 0.503)	(0.87, 1.0)
GG	1609	(5.5, 8.8)	(0.027, 0.503)	(0.887, 1.0)
GPA	1669	(5.5, 8.8)	(0.027, 0.503)	(0.857, 1.0)
5NN	1570	(5.5, 8.8)	(0.027, 0.503)	(0.883, 1.0)
YAO	1540	(5.5, 8.8)	(0.027, 0.503)	(0.873, 1.0)
ER	1536	(5.5, 8.8)	(0.027, 0.503)	(0.887, 1.0)
st = Random				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	1856	(5.5, 8.8)	(0.023, 0.503)	(0.877, 1.0)
GG	1618	(5.5, 8.8)	(0.027, 0.503)	(0.887, 1.0)
GPA	2745	(5.5, 8.8)	(0.027, 0.503)	(0.82, 1.0)
5NN	1619	(5.5, 8.8)	(0.027, 0.503)	(0.88, 1.0)
YAO	1597	(5.5, 8.8)	(0.027, 0.503)	(0.883, 1.0)
ER	1557	(5.5, 8.8)	(0.027, 0.503)	(0.883, 1.0)

Table E.1: Summary of seismic attacks performed over systems with extra physical links added, and $I_{max} = 3$.

st = Original				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.823, 1.0)
GG	0	-	-	(0.827, 1.0)
GPA	0	-	-	(0.833, 1.0)
5NN	0	-	-	(0.85, 1.0)
YAO	0	-	-	(0.84, 1.0)
ER	0	-	-	(0.893, 1.0)
st = Distance				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.82, 1.0)
GG	0	-	-	(0.843, 1.0)
GPA	0	-	-	(0.833, 1.0)
5NN	0	-	-	(0.857, 1.0)
YAO	0	-	-	(0.847, 1.0)
ER	0	-	-	(0.897, 1.0)
st = Local hubs				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.823, 1.0)
GG	0	-	-	(0.837, 1.0)
GPA	0	-	-	(0.833, 1.0)
5NN	0	-	-	(0.847, 1.0)
YAO	0	-	-	(0.847, 1.0)
ER	0	-	-	(0.893, 1.0)
st = Degree				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.897, 1.0)
GG	0	-	-	(0.89, 1.0)
GPA	1	(7.8, 7.8)	(0.437, 0.437)	(0.883, 1.0)
5NN	0	-	-	(0.897, 1.0)
YAO	0	-	-	(0.893, 1.0)
ER	0	-	-	(0.893, 1.0)
st = Random				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.893, 1.0)
GG	0	-	-	(0.893, 1.0)
GPA	0	-	-	(0.893, 1.0)
5NN	0	-	-	(0.897, 1.0)
YAO	0	-	-	(0.897, 1.0)
ER	0	-	-	(0.893, 1.0)

Table E.2: Summary of seismic attacks performed over systems with extra physical links added, and $I_{max} = 5$.

st = Original				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.867, 1.0)
GG	0	-	-	(0.867, 1.0)
GPA	0	-	-	(0.833, 1.0)
5NN	0	-	-	(0.873, 1.0)
YAO	0	-	-	(0.873, 1.0)
ER	0	-	-	(0.88, 1.0)
st = Distance				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.867, 1.0)
GG	0	-	-	(0.867, 1.0)
GPA	0	-	-	(0.853, 1.0)
5NN	0	-	-	(0.87, 1.0)
YAO	0	-	-	(0.877, 1.0)
ER	0	-	-	(0.88, 1.0)
st = Local hubs				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.867, 1.0)
GG	0	-	-	(0.877, 1.0)
GPA	0	-	-	(0.84, 1.0)
5NN	0	-	-	(0.877, 1.0)
YAO	0	-	-	(0.873, 1.0)
ER	0	-	-	(0.88, 1.0)
st = Degree				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.873, 1.0)
GG	0	-	-	(0.873, 1.0)
GPA	0	-	-	(0.843, 1.0)
5NN	0	-	-	(0.877, 1.0)
YAO	0	-	-	(0.873, 1.0)
ER	0	-	-	(0.873, 1.0)
st = Random				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.87, 1.0)
GG	0	-	-	(0.873, 1.0)
GPA	0	-	-	(0.86, 1.0)
5NN	0	-	-	(0.873, 1.0)
YAO	0	-	-	(0.88, 1.0)
ER	0	-	-	(0.877, 1.0)

Table E.3: Summary of seismic attacks performed over systems with extra physical links added, and $I_{max} = 7$.

st = Original				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	6	(7.8, 8.8)	(0.46, 0.467)	(0.943, 1.0)
GG	3	(7.8, 8.3)	(0.48, 0.48)	(0.95, 1.0)
GPA	0	-	-	(0.92, 1.0)
5NN	1	(8.8, 8.8)	(0.483, 0.483)	(0.95, 1.0)
YAO	1	(7.8, 7.8)	(0.49, 0.49)	(0.95, 1.0)
ER	3	(7.8, 7.8)	(0.49, 0.49)	(0.95, 1.0)
st = Distance				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	5	(7.8, 8.8)	(0.467, 0.48)	(0.947, 1.0)
GG	1	(7.8, 7.8)	(0.483, 0.483)	(0.95, 1.0)
GPA	1	(8.8, 8.8)	(0.483, 0.483)	(0.943, 1.0)
5NN	0	-	-	(0.95, 1.0)
YAO	1	(7.8, 7.8)	(0.49, 0.49)	(0.95, 1.0)
ER	2	(7.8, 8.3)	(0.483, 0.483)	(0.95, 1.0)
st = Local hubs				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	7	(7.8, 8.8)	(0.47, 0.48)	(0.947, 1.0)
GG	2	(8.8, 8.8)	(0.483, 0.49)	(0.95, 1.0)
GPA	0	-	-	(0.937, 1.0)
5NN	2	(7.6, 7.8)	(0.483, 0.493)	(0.95, 1.0)
YAO	1	(8.8, 8.8)	(0.477, 0.477)	(0.95, 1.0)
ER	1	(7.8, 7.8)	(0.49, 0.49)	(0.95, 1.0)
st = Degree				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	0	-	-	(0.95, 1.0)
GG	0	-	-	(0.95, 1.0)
GPA	2	(7.8, 8.8)	(0.49, 0.49)	(0.943, 1.0)
5NN	0	-	-	(0.953, 1.0)
YAO	0	-	-	(0.95, 1.0)
ER	0	-	-	(0.947, 1.0)
st = Random				
m	Number of HDSA	M_w range (HDSA)	G_L range (HDSA)	G_L range (Non-HDSA)
RNG	2	(7.7, 8.0)	(0.48, 0.49)	(0.95, 1.0)
GG	4	(7.8, 8.8)	(0.477, 0.493)	(0.95, 1.0)
GPA	0	-	-	(0.943, 1.0)
5NN	2	(8.0, 8.3)	(0.49, 0.493)	(0.95, 1.0)
YAO	1	(8.8, 8.8)	(0.493, 0.493)	(0.943, 1.0)
ER	0	-	-	(0.95, 1.0)

Table E.4: Summary of seismic attacks performed over systems with extra physical links added, and $I_{max} = 10$.

E.4 Link addition effect against seismic attacks SA-LA comparison tables

st = Original							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	52.3%	37.6%	33.9%	34.2%	33.3%	32.4%	37.3%
Damage SA ∼ Damage LA	41.7%	51.4%	50.2%	52.7%	53.2%	52.7%	50.3%
Damage SA < Damage LA	6.0%	11.0%	16.0%	13.1%	13.5%	14.9%	12.4%
st = Distance							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	45.9%	35.5%	34.2%	33.2%	33.1%	32.5%	35.7%
Damage SA ∼ Damage LA	46.3%	52.2%	50.7%	53.1%	53.0%	52.7%	51.3%
Damage SA < Damage LA	7.8%	12.3%	15.1%	13.7%	13.9%	14.9%	12.9%
st = Local hubs							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	40.4%	34.7%	33.3%	32.9%	32.9%	32.2%	34.4%
Damage SA ∼ Damage LA	49.5%	52.7%	51.1%	52.8%	53.1%	53.0%	52.1%
Damage SA < Damage LA	10.1%	12.6%	15.6%	14.2%	14.0%	14.8%	13.5%
st = Degree							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	33.8%	32.8%	33.3%	32.7%	32.5%	32.4%	32.9%
Damage SA ∼ Damage LA	52.7%	52.7%	51.1%	52.7%	53.1%	52.8%	52.5%
Damage SA < Damage LA	13.5%	14.5%	15.6%	14.6%	14.4%	14.8%	14.6%
st = Random							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	36.0%	33.3%	34.0%	33.0%	32.5%	32.1%	33.5%
Damage SA ∼ Damage LA	51.6%	52.7%	50.9%	52.8%	52.8%	53.1%	52.3%
Damage SA < Damage LA	12.4%	14.0%	15.2%	14.2%	14.7%	14.8%	14.2%

Table E.5: Comparison between localized attacks and seismic attacks for systems with extra physical links added, and $I_{max} = 3$.

st = Original							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	41.5%	29.6%	29.6%	26.6%	25.9%	25.3%	29.7%
Damage SA ∼ Damage LA	52.3%	59.7%	54.8%	60.8%	61.0%	60.4%	58.2%
Damage SA < Damage LA	6.2%	10.7%	15.6%	12.7%	13.1%	14.3%	12.1%
st = Distance							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	36.1%	27.6%	29.4%	25.7%	25.6%	25.3%	28.3%
Damage SA ∼ Damage LA	56.0%	60.8%	55.6%	60.8%	60.9%	60.4%	59.1%
Damage SA < Damage LA	7.9%	11.6%	14.9%	13.4%	13.5%	14.3%	12.6%
st = Local hubs							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	31.8%	27.1%	28.9%	25.6%	25.4%	25.2%	27.3%
Damage SA ∼ Damage LA	58.5%	60.7%	56.0%	61.0%	61.1%	60.7%	59.7%
Damage SA < Damage LA	9.7%	12.2%	15.1%	13.4%	13.5%	14.1%	13.0%
st = Degree							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	26.9%	25.4%	28.6%	25.4%	25.2%	25.1%	26.1%
Damage SA ∼ Damage LA	59.9%	60.8%	56.2%	60.7%	60.8%	60.7%	59.8%
Damage SA < Damage LA	13.2%	13.8%	15.2%	14.0%	14.0%	14.2%	14.1%
st = Random							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	28.0%	25.9%	28.3%	25.6%	25.5%	25.0%	26.4%
Damage SA ∼ Damage LA	59.9%	60.6%	56.9%	60.7%	60.8%	60.8%	59.9%
Damage SA < Damage LA	12.1%	13.5%	14.9%	13.7%	13.8%	14.2%	13.7%

Table E.6: Comparison between localized attacks and seismic attacks for systems with extra physical links added, and $I_{max} = 5$.

st = Original							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	38.0%	28.2%	28.9%	26.2%	25.4%	24.8%	28.6%
Damage SA ∼ Damage LA	56.8%	63.1%	57.2%	63.5%	64.1%	63.7%	61.4%
Damage SA < Damage LA	5.3%	8.8%	13.9%	10.3%	10.6%	11.5%	10.1%
st = Distance							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	33.5%	26.7%	29.3%	25.6%	25.1%	24.8%	27.5%
Damage SA ∼ Damage LA	60.0%	63.8%	57.9%	63.7%	64.1%	64.0%	62.2%
Damage SA < Damage LA	6.5%	9.5%	12.8%	10.7%	10.8%	11.2%	10.3%
st = Local hubs							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	29.9%	26.2%	28.2%	25.2%	25.2%	24.5%	26.5%
Damage SA ∼ Damage LA	62.0%	63.9%	59.2%	63.8%	63.9%	63.9%	62.8%
Damage SA < Damage LA	8.1%	9.9%	12.6%	11.0%	10.8%	11.6%	10.7%
st = Degree							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	26.1%	25.0%	27.6%	25.0%	24.7%	24.5%	25.5%
Damage SA ∼ Damage LA	63.4%	63.8%	59.9%	63.5%	63.9%	63.9%	63.1%
Damage SA < Damage LA	10.5%	11.1%	12.5%	11.5%	11.4%	11.6%	11.4%
st = Random							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	27.0%	25.4%	27.5%	25.3%	25.1%	24.7%	25.8%
Damage SA ∼ Damage LA	63.1%	63.7%	59.9%	63.5%	63.7%	63.9%	62.9%
Damage SA < Damage LA	10.0%	10.9%	12.7%	11.2%	11.2%	11.4%	11.2%

Table E.7: Comparison between localized attacks and seismic attacks for systems with extra physical links added, and $I_{max} = 7$.

st = Original							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	30.5%	22.5%	26.0%	20.5%	19.9%	19.7%	23.2%
Damage SA ∼ Damage LA	65.5%	70.8%	63.4%	71.5%	71.9%	71.3%	69.0%
Damage SA < Damage LA	4.0%	6.8%	10.6%	7.9%	8.3%	9.1%	7.8%
st = Distance							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	26.5%	21.3%	25.7%	20.3%	19.8%	19.6%	22.2%
Damage SA ∼ Damage LA	68.5%	71.4%	64.6%	71.6%	71.6%	71.3%	69.8%
Damage SA < Damage LA	5.0%	7.4%	9.6%	8.1%	8.5%	9.0%	7.9%
st = Local hubs							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	23.8%	21.1%	24.3%	19.9%	20.0%	19.6%	21.4%
Damage SA ∼ Damage LA	69.9%	71.3%	65.6%	71.8%	71.4%	71.4%	70.2%
Damage SA < Damage LA	6.3%	7.7%	10.1%	8.3%	8.6%	9.0%	8.3%
st = Degree							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	20.6%	19.8%	23.9%	19.7%	19.8%	19.4%	20.5%
Damage SA ∼ Damage LA	71.1%	71.3%	66.3%	71.4%	71.2%	71.6%	70.5%
Damage SA < Damage LA	8.3%	8.8%	9.9%	8.9%	9.0%	8.9%	9.0%
st = Random							
	RNG	GG	GPA	5NN	YAO	ER	Total
Damage SA > Damage LA	21.5%	20.2%	23.7%	20.0%	19.4%	19.6%	20.7%
Damage SA ∼ Damage LA	70.6%	71.3%	66.4%	71.4%	71.7%	71.4%	70.5%
Damage SA < Damage LA	8.0%	8.5%	9.9%	8.6%	8.9%	9.0%	8.8%

Table E.8: Comparison between localized attacks and seismic attacks for systems with extra physical links added, and $I_{max} = 10$.